УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ ПОЛИТИЧКИХ НАУКА

Катарина С. Јонев Ћираковић

Концептуализација сајбер ратовања у доктринама и стратешким документима Руске Федерације, Сједињених Америчких Држава и Народне Републике Кине

Докторска дисертација

Београд, 2026. године

UNIVERSITY OF BELGRADE
FACULTY OF POLITICAL SCIENCE

Katarina S. Jonev Ćiraković

Conceptualisation of cyber warfare in the Doctrines and Strategic Documents of the Russian Federation, the United States of America, and the People's Republic of China

Doctoral Dissertation

Belgrade, 2026

Ментор:

Проф. др Ивана Дамњановић, Универзитет у Београду Факултет политичких наука

Чланови комисије:
Проф. др Ненад Путник
Проф. др Милан Крстић
Доц. др Дејан Јовановић

Датум одбране:

Концептуализација сајбер ратовања у доктринама и стратешким документима Руске Федерације, Сједињених Америчких Држава и Народне Републике Кине

Сажетак

Убрзани развој интернета и информационо-комуникационих технологија променио је природу савремених међународних односа. Дигитални простор више није само средство комуникације, економске размене и друштвеног повезивања, већ је постао једно од кључних поља геополитичког надметања, пројекције моћи и стратешког деловања држава. У таквом окружењу, сајбер ратовање се издваја као један од најзначајнијих феномена савремене безбедности, јер омогућава државама да делују изван традиционалних војних оквира, често прикривено, континуирано и испод прага отвореног оружаног сукоба.

Предмет овог рада јесте анализа сајбер ратовања као инструмента државне моћи у савременим међународним односима. Полазећи од улоге интернета у трансформацији политичких, безбедносних и стратешких односа међу државама, рад разматра начин на који се сајбер простор користи за остваривање националних интереса, слабљење противника, прикупљање обавештајних података, утицај на јавно мњење, угрожавање критичне инфраструктуре и обликовање глобалних односа моћи. Посебна пажња посвећена је улози држава у сајбер сукобима, проблему прикривеног деловања, тешкоћама утврђивања одговорности за сајбер нападе и чињеници да се границе између мира, кризе и сукоба у дигиталном окружењу све више замагљују. У раду се анализирају различити приступи Сједињених Америчких Држава, Руске Федерације и Народне Републике Кине сајбер простору и сајбер ратовању.

Основна теза рада јесте да сајбер ратовање представља нову димензију моћи у међународним односима и да значајно мења начин на који државе воде политичко, безбедносно и стратешко надметање. За разлику од традиционалних облика сукоба, сајбер деловање омогућава државама да остварују циљеве без директне употребе класичне војне силе, уз мањи степен видљивости, већу флексибилност и сложеније последице по стабилност међународног система. Рад указује да способност држава да развију сајбер капацитете, заштите критичну инфраструктуру, контролишу информациони простор и утичу на дигиталне токове постаје један од важних показатеља њихове моћи, отпорности и позиције у савременом светском поретку.

Кључне речи: сајбер ратовање; међународни односи; сајбер простор; интернет; државна моћ; сајбер сукоби; критична инфраструктура; информационо ратовање; атрибуција сајбер напада; сајбер суверенитет; дигитална моћ; савремени безбедносни изазови.

Научна област: Политичне науке
Ужа научна област: Политичка теорија, политичка историја и методологија политичких наука
УДК: 355.4:004.738.5(510+470+73)(043.3)

Conceptualisation of Cyber Warfare in the Doctrines and Strategic Documents of the Russian Federation, the United States of America, and the People's Republic of China

Abstract

The rapid development of the Internet and information and communication technologies has transformed the nature of contemporary international relations. Digital space is no longer merely a means of communication, economic exchange, and social connectivity; rather, it has become one of the key arenas of geopolitical competition, power projection, and strategic state action. In such an environment, cyber warfare stands out as one of the most significant phenomena of contemporary security, as it enables states to operate beyond traditional military frameworks, often covertly, continuously, and below the threshold of open armed conflict.

The subject of this dissertation is the analysis of cyber warfare as an instrument of state power in contemporary international relations. Starting from the role of the Internet in transforming political, security, and strategic relations among states, the dissertation examines the ways in which cyberspace is used to pursue national interests, weaken adversaries, collect intelligence, influence public opinion, threaten critical infrastructure, and shape global power relations. Particular attention is devoted to the role of states in cyber conflicts, the problem of covert action, the difficulties of attributing responsibility for cyber attacks, and the fact that the boundaries between peace, crisis, and conflict are becoming increasingly blurred in the digital environment. The dissertation analyses the different approaches of the United States of America, the Russian Federation, and the People's Republic of China to cyberspace and cyber warfare.

The central thesis of the dissertation is that cyber warfare represents a new dimension of power in international relations and significantly changes the way in which states conduct political, security, and strategic competition. Unlike traditional forms of conflict, cyber activity enables states to achieve their objectives without the direct use of conventional military force, with a lower degree of visibility, greater flexibility, and more complex consequences for the stability of the international system. The dissertation indicates that the ability of states to develop cyber capabilities, protect critical infrastructure, control the information space, and influence digital flows is becoming one of the important indicators of their power, resilience, and position in the contemporary world order.

Keywords: cyber warfare; international relations; cyberspace; Internet; state power; cyber conflicts; critical infrastructure; information warfare; attribution of cyber attacks; cyber sovereignty; digital power; contemporary security challenges.

Scientific field: Political Science
Specific scientific field: Political Theory, Political History, and Methodology of Political Science.
UDK number: 355.4:004.738.5(510+470+73)(043.3)

Садржај

1.Увод.....1
1.1. Формулација проблема истраживања.....1
1.2. Предмет и циљ дисертације.....6
1.2.1. Научни значај истраживања.....8
1.2.2. Друштвени значај истраживања.....9
1.2.3 Резултати претходних истраживања.....11
1.3. Теоријско одређење предмета истраживања.....16
1.3.1. Постојећа сазнања о предмету истраживања.....16
1.4. Операционо одређење предмета истраживања.....19
1.4.1. Чиниоци садржаја предмета истраживања.....19
1.4.2. Временско одређење предмета истраживања.....20
1.4.3. Просторно одређење предмета истраживања.....21
1.5. Научно-дисциплинарно одређење предмета истраживања.....22
1.6. Хипотетички оквир.....23
1.7. Методе истраживања.....25
1.8. Научна и друштвена оправданост истраживања.....27
2. Улога интернета.....29
2.1 Историја развоја интернета.....31
2.2 Појмовно одређење сајбер простора.....38
2.3. Сајбер напади као средство угрожавања безбедности држава.....45
2.4 Облици и последице сајбер напада у савременом безбедносном окружењу.....47
2.5 Интернет, рањивост држава и потреба за нормативним уређењем сајбер простора.....49
2.6 Основни принципи безбедности информационих система и технике сајбер напада.....53
2.7 Најчешћи облици илегалних активности у сајбер простору.....56
2.7.1 Сајбер тероризам.....62
2.7.2 Сајбер шпијунажа.....65
2.7.3 Сајбер саботажа.....68
3.Концепт сајбер ратовања.....70

3. 1 Дефинисање појма „сајбер ратовање“ 70
3.1.1 Кључни елементи и обележја сајбер ратовања 74
3.1.2 Облици и типологија сајбер ратовања 77
3.1.3 Средства и методе сајбер ратовања 80
3.1.4 Циљеви сајбер ратовања 83
3.1.5 Актери сајбер ратовања 85
3.2. Државе као кључни актери сукоба у сајбер простору 87
3.3 Концепт традиционалног и дигиталног суверенитета држава 91
3.4 Последице сајбер ратовања по функционисање државе и друштва 94
3.4.1 Утицај на државне институције и управљање 95
3.4.2 Утицај на критичну инфраструктуру 97
3.4.3 Економске последице сајбер ратовања 99
3.4.4 Утицај на друштво и јавно мњење 101
3.4.5 Безбедносне и војне последице 102
3.5 Стратегијско-доктринарни оквир сајбер безбедности 104
3.6 Нормативно-правни оквир сајбер безбедности 106
3.7 Организационе и институционалне структуре држава у систему сајбер безбедности 109
3.8 Важност сајбер стратегија за безбедност држава 111
4. Информациона безбедност Руске Федерације 114
4.1. Појам, стратешки оквир и руски приступ информационој безбедности 114
4.1.2 Специфичности Руске Федерације по питању информационе безбедности 116
4.2 Доктринарни развој и институционализација заштите информационе сфере 119
4.2.1 Међународна сарадња Руске Федерације у области информационе безбедности 126
4.3 Доктрина информационе безбедности Руске Федерације из 2016. године 129
4.4 Континуитет и релевантност руске политике информационе безбедности до 2026. године 134
4.5 Први међународни сајбер сукоб – напад на информационе системе у Естонији 139
4.6 Вођење сајбер рата паралелно уз конвенционални сукоб – рат у Украјини 142
5. Концепт сајбер ратовања у Сједињеним Америчким државама 151
5.1. Стратегија сајбер безбедности САД 152
5.2 Америчка концепција сајбер операција и сајбер ратовања 157
5.3 Механизми заштите сајбер простора од сајбер напада – Сајбер команда САД 162
5.4 Институционална, правна и савезничка архитектура америчког модела сајбер ратовања 167
5.5 Извођење сајбер напада САД на територијама других држава 171
5.6. Правне и политичке контроверзе америчког приступа сајбер ратовању 174
5.7. Да ли је сајбер простор једини домен где САД морају да се бране? 175

6. **Сајбер ратовање у доктрини Народне Републике Кине** 180
6.1 Савремена кинеска војна доктрина: између одбрамбеног наратива и ширења оперативних способности 183
6.2 Војне стратешке смернице као кључ за разумевање кинеске војне доктрине 184
6.3 Бела књига одбране из 2019. године и сајбер димензија кинеске војне доктрине 188
6.4 Значај заштите од сајбер напада и утицаја са интернета у НР Кини 191
6.5 Војна модернизација Кине и развој капацитета за сајбер ратовање 201
6.6 Кинеске војне јединице и извођење напада у сајбер простору 211
6.7 Улога НР Кине у обликовању глобалних трендова сајбер безбедности 215
7. Закључак 219

Литература
Биографија кандидата
Изјава о ауторству
Изјава о истоветности штампане и електронске верзије докторског рада
Изјава о коришћењу

Листа скраћеница

AI	Вештачка интелигенција
APT	Напредна упорна претња
BRI	Иницијатива „Појас и пут“
CERT	Тим за хитно реаговање на рачунарске инциденте
CII	Критична информациона инфраструктура
CISA	Агенција за сајбер безбедност и безбедност инфраструктуре САД
CNA	Напад на рачунарску мрежу
CND	Одбрана рачунарске мреже
CNE	Експлоатација рачунарске мреже
CNMF	Националне сајбер мисионе снаге САД
CPC	Комунистичка партија Кине
CSIRT	Тим за одговор на инциденте у области рачунарске безбедности
DDoS	Дистрибуирани напад ускраћивањем услуге
DHS	Министарство унутрашње безбедности САД
DISA	Агенција за одбрамбене информационе системе САД
DNI	Директор националне обавештајне службе САД
DNS	Систем доменских имена
DoD	Министарство одбране САД
DoS	Напад ускраћивањем услуге
DPI	Дубинска инспекција пакета података
EU	Европска унија
FBI	Федерални истражни биро САД
FSB	Федерална служба безбедности Руске Федерације
GGE	Група владиних експерата Уједињених нација
GRU	Главна управа Генералштаба Оружаних снага Руске Федерације
ICT/ИКТ	Информационо-комуникационе технологије
IoT	Интернет ствари
IP	Интернет протокол
IR	Међународни односи
ISR	Обавештајно деловање, надзор и извиђање
IT	Информациона технологија
MSS	Министарство државне безбедности Народне Републике Кине
NATO	Организација Северноатлантског уговора
NATO CCDCOE	НАТО Центар изврсности за кооперативну сајбер одбрану
NCSC	Национални центар за сајбер безбедност
NIST	Национални институт за стандарде и технологију САД
NSA	Агенција за националну безбедност САД
OEWG	Отворена радна група Уједињених нација
OSCE	Организација за европску безбедност и сарадњу

PLA	Народноослободилачка армија Кине
PLA SSF	Стратешке снаге подршке Народноослободилачке армије Кине
PRC	Народна Република Кина
SCO	Шангајска организација за сарадњу
TCP/IP	Основни скуп интернет протокола
UN	Уједињене нације
URL	Јединствена адреса ресурса на интернету
USA	Сједињене Америчке Државе
USCYBERCOM	Сајбер команда Сједињених Америчких Држава
VPN	Виртуелна приватна мрежа
WWW	Светска мрежа
НР Кина	Народна Република Кина
ОЕБС	Организација за европску безбедност и сарадњу
РФ	Руска Федерација
САД	Сједињене Америчке Државе
СССР	Савез Совјетских Социјалистичких Република

1.Увод

1.1. Формулација проблема истраживања

Брзи развој науке и технологије представља једно од најзначајнијих обележја савременог доба. Током двадесетог и почетком двадесет првог века технолошке иновације дубоко су измениле политичке процесе, економске односе, моделе комуникације, начин живота, индустријску производњу, научна истраживања, образовање, медицину и функционисање државних институција. Међутим, технолошки развој није утицао само на мирнодопске аспекте друштвеног напретка, већ и на трансформацију начина вођења сукоба. Историја међународних односа показује да су државе готово сваку значајну технолошку иновацију, поред цивилне примене, настојале да укључе и у системе безбедности, одбране, надзора, обавештајног рада и војног деловања. У том смислу, развој информационо-комуникационих технологија отворио је ново поље политичког и стратешког надметања међу државама.

Информациона технологија, која је средином двадесетог века била ограничена на уске научне, војне и истраживачке кругове, у двадесет првом веку постала је основни услов функционисања савременог друштва. Данас је готово немогуће замислити рад државне управе, финансијских система, образовања, здравства, транспорта, енергетике, војних структура и дипломатске комуникације без ослонца на дигиталне мреже и информационе системе. Интернет је омогућио бржу размену знања, лакшу доступност информација, убрзану комуникацију, глобалну економску повезаност и нове облике политичког и друштвеног деловања. Ипак, управо због своје распрострањености и значаја, интернет је истовремено постао простор нових безбедносних ризика, како за појединце и друштва, тако и за националне државе и међународни систем у целини.

У савременим међународним односима дигитални простор више се не може посматрати као неутрална технолошка инфраструктура. Он је постао простор у коме се обликују односи моћи, врши политички утицај, прикупљају обавештајни подаци, угрожава критична инфраструктура, спроводе информационе операције и пројектују стратешки интереси држава. Како указује Џозеф Нај, раст сајбер простора створио је нови контекст светске политике, у коме су ниска цена уласка, тешкоће утврђивања идентитета актера и асиметрије рањивости значајно измениле традиционално разумевање моћи.[1] Сајбер простор, стога, није само техничко окружење, већ и нова арена међународног надметања у којој државе, недржавни актери, приватне компаније, хакерске групе и појединци могу производити последице које превазилазе границе националних јурисдикција.

Повећана употреба и глобални домет рачунарских мрежа створили су висок степен зависности савременог друштва од информационо-комуникационих технологија. Посебно је значајна зависност држава и њихових безбедносних структура од дигиталних система, јер се одбрамбени системи, системи државне управе, комуникационе мреже, енергетска постројења, транспортни

[1] Joseph S. Nye Jr., "Cyber Power," *Belfer Center for Science and International Affairs, Harvard Kennedy School*, May 2010, 1–4.

системи, финансијске институције и други елементи критичне инфраструктуре све више ослањају на информационе технологије. Ова зависност истовремено повећава ефикасност државе, али и њену рањивост. Што је једно друштво више дигитализовано, то су потенцијалне последице сајбер напада сложеније, јер напад на дигиталну инфраструктуру може имати политичке, економске, војне и друштвене последице.

Посебну димензију овој теми даје чињеница да се савремени информациони системи све више развијају уз примену напредних алгоритама, а последњих година и уз употребу вештачке интелигенције. То додатно усложњава питање безбедности, јер државе више не штите само класичне комуникационе мреже и базе података, већ и комплексне системе који могу самостално да обрађују податке, доносе одлуке, управљају процесима и утичу на функционисање цивилних и војних структура. У таквом окружењу, сајбер безбедност постаје један од темељних услова националне безбедности, али и значајно питање међународних односа.

До последње деценије двадесетог века појам „сајбер напад" није имао значајно место у политичком и безбедносном дискурсу. Разлог за то лежи у чињеници да информационе технологије још увек нису представљале кључну инфраструктуру функционисања држава, привреде и друштва. Са убрзаним развојем рачунарских мрежа и глобалном експанзијом интернета, створени су услови за појаву нових облика угрожавања безбедности. Академска и стручна јавност користи различите термине како би описала упаде у информационе системе, укључујући појмове као што су сајбер напад, компјутерски напад, информационо ратовање, сајбер операције, интернет напад, ратовање информацијама и сајбер ратовање. Иако међу овим појмовима постоје значајне разлике, заједничко им је то што указују на могућност да злоупотреба информационо-комуникационих технологија нанесе штету државама, институцијама, економији, друштву и међународној стабилности.

Сајбер напади представљају специфичан и релативно нов облик деловања у савременим сукобима. Њихова природа разликује се од традиционалних облика ратовања, јер се одвијају у дигиталном простору, често без јасно видљивог почетка, без непосредног физичког присуства нападача и уз могућност прикривања идентитета актера. Сајбер простор, информационе технологије и рачунарске мреже све интензивније се користе у војне, обавештајне, политичке и економске сврхе. Последице таквог деловања могу бити различите: од привременог онемогућавања рада интернет страница и сервиса, преко крађе поверљивих података, до угрожавања критичне инфраструктуре и изазивања озбиљних поремећаја у функционисању државе.

Сукоби у сајбер простору јављају се у различитим облицима: као пропагандно и информационо деловање, сајбер шпијунажа, високотехнолошки криминал, злоупотреба интернета од стране терористичких организација, напади на институције, као и операције усмерене на критичне системе националне инфраструктуре. Иако се ови облици деловања понекад међусобно преклапају, њихово разликовање је важно због анализе актера, циљева, средстава и последица. Није свака злонамерна активност у сајбер простору истовремено и сајбер ратовање. Сајбер криминал, сајбер вандализам, сајбер тероризам и сајбер шпијунажа могу имати безбедносни значај, али се категорија сајбер ратовања пре свега везује за деловање држава или државно подржаних актера у контексту ширег политичког, војног или стратешког сукоба.

Управо због тога сајбер ратовање треба посматрати као проблем међународних односа, а не само као питање војне стратегије или техничке заштите информационих система. Када су актери или

мете суверене државе, сајбер деловање добија политичку и међународну димензију. Напади на државне институције, дипломатске комуникације, изборне процесе, војне системе, енергетску мрежу, транспорт или финансијски сектор могу утицати на односе међу државама, променити динамику конфликта, произвести кризу поверења и подстаћи шире геополитичко надметање. Сајбер простор тако постаје једно од поља у којем се испитују границе државног суверенитета, способности одвраћања, стратешке отпорности и политичког утицаја.

У последње две деценије забележен је значајан број сајбер инцидената који су показали да дигитални напади могу имати озбиљне политичке и безбедносне последице. Напади на Естонију 2007. године, који су укључивали масовне DDoS нападе на државне институције, медије, банке и друге сервисе, често се наводе као један од првих примера у којем је једна високо дигитализована држава била изложена координисаној кампањи у сајбер простору.[2] Сајбер напади у контексту руско-грузијског сукоба 2008. године додатно су показали да се операције у дигиталном простору могу одвијати паралелно са конвенционалним војним активностима.[3] Случај „Stuxnet“ посебно је значајан јер је показао да злонамерни софтвер може изазвати последице у физичком свету, односно утицати на индустријске и нуклеарне системе, при чему је као мета најчешће навођено иранско постројење за обогаћивање уранијума у Натанзу.[4] Ови примери указују да сајбер операције могу превазићи ниво симболичког, пропагандног или техничког инцидента и постати средство стратешког притиска.

Сајбер операције имају потенцијал да изазову друштвене, економске и политичке поремећаје. На војном плану оне могу произвести последице које се уобичајено повезују са традиционалним оружаним сукобом, посебно ако су усмерене на системе од којих зависи функционисање војних комуникација, енергетике, транспорта или командно-контролних структура. Њихова специфичност огледа се и у прекограничној природи сајбер простора. Напад може бити покренут са територије једне државе, преко сервера у другој, усмерен на мету у трећој, док прави налогодавац може остати прикривен. Ова чињеница непосредно доводи у питање традиционалне представе о територији, границама, одговорности и суверенитету у међународним односима.

Један од највећих изазова у анализи сајбер ратовања јесте проблем атрибуције. За разлику од класичних војних операција, код којих је у већини случајева могуће утврдити правац напада, средства и државу која стоји иза њих, у сајбер простору доказивање одговорности често је изузетно сложено. Технички трагови могу бити прикривени, преусмерени или намерно постављени тако да наведу на погрешан закључак. Због тога је тешко доказати да је напад на једну државу директно извршила друга држава или да је деловање хакерске групе било под контролом државних структура. Овај проблем има велики значај за међународне односе, јер без поуздане атрибуције постаје тешко формулисати политички одговор, применити мере одвраћања или изградити стабилан систем одговорности у сајбер простору.

[2] Rain Ottis, “Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective,” *NATO Cooperative Cyber Defence Centre of Excellence*, 2008; “Cyber Attacks against Estonia (2007),” *Cyber Law Toolkit*, NATO CCDCOE, 2021.

[3] “Georgia-Russia Conflict (2008),” *Cyber Law Toolkit*, NATO CCDCOE; Keir Giles, “‘Information Troops’ — A Russian Cyber Command?” *NATO Cooperative Cyber Defence Centre of Excellence*, 2011.

[4] David Albright, Paul Brannan, and Christina Walrond, “Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?” *Institute for Science and International Security*, December 22, 2010; “Natanz Enrichment Complex,” *Nuclear Threat Initiative*.

Терористичке организације, екстремистичке групе и други недржавни актери користе интернет као глобални канал комуникације, средство пропаганде, простор за регрутацију, ширење идеолошких порука и производњу страха. Иако овакве активности не представљају увек сајбер ратовање у ужем смислу, оне показују да сајбер простор омогућава актерима ограничених материјалних ресурса да остваре несразмерно велики политички и психолошки утицај. Са друге стране, крађа поверљивих индустријских, војних, научних и дипломатских информација, позната као сајбер шпијунажа, постала је једна од значајних тачака спорења у односима великих сила. Она показује да се надметање у сајбер простору не одвија само у тренуцима отворене кризе или рата, већ и у условима формалног мира.

У савременом међународном систему све већи број држава развија посебне сајбер капацитете, формира специјализоване јединице, оснива сајбер команде и усваја стратегије које сајбер простор третирају као важан домен националне безбедности. Овај процес показује да државе сајбер деловање више не посматрају само као питање техничке заштите, већ као саставни део политичког, војног и обавештајног планирања. Приватни сектор, који управља великим делом дигиталне инфраструктуре, има посебно важну улогу у овом процесу, јер државе без сарадње са технолошким компанијама, телекомуникационим операторима, финансијским институцијама и добављачима софтвера не могу изградити потпуну отпорност на сајбер претње.

Сајбер рат је у почетку најчешће био повезиван са војним операцијама које се одвијају паралелно са конвенционалним сукобом. Међутим, развој сајбер простора проширио је ово разумевање. Сајбер ратовање више није ограничено на класичне војне стратегије, већ обухвата широк спектар активности усмерених на слабљење противника, нарушавање функционисања државних система, утицај на јавно мњење, прикупљање обавештајних података, онемогућавање комуникација и угрожавање критичне инфраструктуре. Џон Аркила и Дејвид Ронфелт још су почетком деведесетих година указивали да ће информациона револуција променити природу сукоба и омогућити нове облике ратовања засноване на мрежама, информацијама и комуникационим системима.[5] Данас се та процена потврђује у све већем значају сајбер операција у савременим кризама и међудржавним односима.

Ипак, потребно је аналитички разликовати појам сајбер рата од ширег поља злонамерних активности у сајбер простору. Не може се сваки напад на интернет страницу, свака крађа података или свака дезинформациона кампања означити као сајбер ратовање. Такво некритичко ширење појма довело би до губитка његове аналитичке вредности. Сајбер ратовање треба посматрати као облик сајбер деловања који је повезан са државним интересима, стратешким циљевима, међудржавним надметањем и потенцијалом да угрози безбедност, суверенитет или функционисање државе. Управо у томе се налази његов значај за науку о међународним односима.

Сајбер простор мења и класично разумевање мира и рата. У традиционалном схватању међународних односа, рат је подразумевао релативно јасно препознатљиво стање оружаног сукоба између политичких јединица. У сајбер простору, међутим, државе могу континуирано деловати испод прага отвореног оружаног сукоба. Оне могу вршити притисак, прикупљати податке, тестирати одбрамбене системе противника, утицати на политичке процесе и нарушавати поверење у институције без формалног уласка у ратно стање. Због тога се у савременим

[5] John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (1993): 141–165; RAND Corporation reprint.

безбедносним студијама све чешће говори о „сивој зони“ између мира и рата, у којој сајбер операције имају посебно значајну улогу.

Ова дисертација полази од становишта да сајбер ратовање представља један од најзначајнијих феномена савремених међународних односа. Његов значај не произлази само из техничке способности да се нападну информациони системи, већ из чињенице да сајбер деловање омогућава државама да пројектују моћ, остварују политичке циљеве, утичу на противнике и обликују односе у међународном систему без нужне употребе класичне војне силе. Сајбер ратовање, стога, не треба посматрати као изоловану техничку појаву, већ као део ширег процеса трансформације моћи у савременој светској политици.

Циљ дисертације јесте да анализира начин на који се сајбер ратовање концептуализује у доктринама и стратешким документима Руске Федерације, Сједињених Америчких Држава и Народне Републике Кине. Ове три државе представљају изузетно значајне актере међународног система, не само због својих војних, политичких, економских и технолошких капацитета, већ и због различитих приступа разумевању сајбер простора. Сједињене Америчке Државе сајбер простор све више посматрају као оперативни домен од значаја за националну безбедност, војну предност и очување глобалног утицаја. Руска Федерација сајбер деловање најчешће повезује са ширим концептом информационог надметања, политичког утицаја и стратешког притиска. Народна Република Кина развија приступ у којем се наглашавају сајбер суверенитет, државна контрола информационог простора, технолошка самосталност и дугорочно јачање позиције у међународном поретку.

Избор ове три државе произлази из њиховог утицаја на глобалне процесе у области сајбер безбедности и сајбер ратовања. Њихови доктринарни и стратешки документи не одражавају само националне безбедносне приоритете, већ и шира схватања моћи, суверенитета, контроле, одвраћања и међународног поретка. Анализа њихових приступа омогућава да се утврди како различити политички системи и различите стратешке културе разумеју сајбер простор, које претње препознају као кључне, како дефинишу улогу државе и на који начин сајбер капацитете укључују у шире безбедносне и спољнополитичке циљеве.

Проблем истраживања посебно је значајан због чињенице да у међународној заједници још увек не постоји потпуни консензус о нормама понашања држава у сајбер простору. У оквиру Уједињених нација вођени су бројни процеси посвећени одговорном понашању држава у употреби информационо-комуникационих технологија, укључујући рад Групе владиних експерата и Отворене радне групе.[6] Ипак, разлике у интересима великих сила, различита схватања суверенитета, улоге државе, слободе информација, контроле интернета и безбедносних претњи отежавају успостављање општеприхваћених правила. Због тога сајбер простор остаје област у којој се истовремено развијају сарадња, конкуренција и стратешко неповерење.

Иако је сајбер безбедност у великој мери техничко питање, сајбер ратовање је пре свега политички и стратешки феномен. Оно укључује питања моћи, интереса, суверенитета, утицаја, одвраћања, рањивости и позиције државе у међународном систему. Због тога се анализа сајбер ратовања не може свести на опис појединачних напада или техничких метода заштите, већ мора обухватити начин на који државе разумеју сајбер простор у својим стратегијама, како дефинишу претње, како

[6] United Nations General Assembly, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN Doc. A/76/135, July 14, 2021; *Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, Draft Final Report*, July 11, 2025.

организују институционалне капацитете и како сајбер деловање уклапају у ширу визију националне безбедности и спољне политике.

Сајбер ратовање је комплексан феномен који подразумева употребу информационо-комуникационих технологија у сврху остваривања политичких, војних, обавештајних или стратешких циљева. Његова посебност огледа се у томе што се може примењивати и у миру и у кризи и у рату, док су последице таквог деловања често тешко предвидиве и не морају остати ограничене на дигитални простор. Иако је усмерено на информационе системе, његови ефекти могу погодити реално функционисање друштва: снабдевање електричном енергијом, рад болница, комуникације, финансијске трансакције, транспорт, државну управу и поверење грађана у институције.

Додатни изазов представља чињеница да до данас не постоји једна универзално прихваћена дефиниција сајбер ратовања. Различите државе, међународне организације, академски аутори и безбедносни стручњаци користе различите појмове и различите критеријуме. За неке, сајбер ратовање подразумева искључиво операције које производе физичке последице или се одвијају у оквиру оружаног сукоба. За друге, оно обухвата и шире облике стратешког деловања у сајбер простору, укључујући информационе операције, шпијунажу, саботажу и политички утицај. Ова појмовна неуједначеност један је од разлога због којих је неопходно анализирати како саме државе у својим доктринама и стратегијама концептуализују сајбер простор и сајбер ратовање.

Ова дисертација, стога, полази од потребе да се сајбер ратовање истражи као нови стратешки концепт који мења природу савремених сукоба и односа међу државама. Њен фокус није само на техничким аспектима сајбер напада, већ на политичком и међународном значају сајбер деловања. Анализом доктрина и стратешких докумената Руске Федерације, Сједињених Америчких Држава и Народне Републике Кине, дисертација настоји да покаже како велике силе разумеју сајбер простор, како га повезују са националном безбедношћу, како га укључују у стратешко надметање и на који начин сајбер ратовање постаје део шире трансформације међународних односа.

На основу тога, овај рад ће настојати да покаже да сајбер ратовање није споредна последица технолошког развоја, већ један од кључних израза савремене државне моћи. У условима у којима су политичке институције, војни системи, економија, комуникације и свакодневни живот дубоко зависни од дигиталне инфраструктуре, способност државе да делује у сајбер простору и да се одбрани од сајбер претњи постаје важан показатељ њене отпорности и позиције у међународном систему. Управо зато анализа сајбер ратовања у доктринама и стратешким документима Руске Федерације, Сједињених Америчких Држава и Народне Републике Кине омогућава дубље разумевање начина на који се моћ, безбедност и сукоб трансформишу у савременом светском поретку.

1.2. Предмет и циљ дисертације

Предмет ове дисертације јесте анализа начина на који се сајбер ратовање концептуализује у доктринама и стратешким документима Руске Федерације, Сједињених Америчких Држава и Народне Републике Кине[7]. Истраживање је усмерено на разумевање начина на који ове три велике

[7] The White House, *National Cybersecurity Strategy* (Washington, DC: The White House, March 2023); U.S. Department of Defense, *2023 Department of Defense Cyber Strategy: Summary* (Washington, DC: Department of Defense, 2023); President of the Russian Federation, *Doctrine of Information Security of the Russian Federation* (Moscow, December 5,

силе дефинишу сајбер простор, сајбер претње, сајбер нападе, улогу државе у дигиталном окружењу, одбрамбене и офанзивне сајбер капацитете, као и место сајбер ратовања у ширем оквиру националне безбедности, војне стратегије и међународног позиционирања.

У средишту истраживања налази се питање да ли се сајбер ратовање у анализираним државама посматра превасходно као техничко-безбедносни изазов, као војно-оперативни домен, као инструмент информационог и политичког утицаја, или као део шире стратегије државне моћи у међународним односима. Посебна пажња посвећује се томе на који начин различити политички системи, стратешке културе и безбедносне доктрине утичу на разумевање сајбер простора и његове употребе у савременом међудржавном надметању.

Предмет истраживања обухвата анализу званичних стратегија, доктрина, националних безбедносних докумената, војних докумената, политичких аката и релевантних институционалних приступа који се односе на сајбер безбедност, информациону безбедност, сајбер операције и сајбер ратовање. У том смислу, дисертација не третира сајбер ратовање искључиво као техничко питање заштите информационих система, већ као политички, безбедносни и стратешки феномен који има непосредан значај за савремене међународне односе.

Избор Руске Федерације, Сједињених Америчких Држава и Народне Републике Кине заснива се на њиховом значају у савременом међународном систему, развијеним војним и технолошким капацитетима, као и чињеници да ове државе у својим стратешким документима сајбер простор препознају као важно поље националне безбедности и међународног надметања. Истовремено, ове три државе развијају различите приступе сајбер простору: Сједињене Америчке Државе наглашавају оперативни, војни и стратешки значај сајбер домена[8]; Руска Федерација сајбер деловање повезује са ширим концептом информационе безбедности и информационог надметања[9]; док Народна Република Кина сајбер простор посматра кроз призму сајбер суверенитета, државне контроле, технолошке самосталности и дугорочног јачања националне моћи[10].

Основни циљ дисертације јесте да се утврди како се сајбер ратовање разуме, дефинише и стратешки позиционира у доктринама и стратешким документима Руске Федерације, Сједињених Америчких Држава и Народне Републике Кине, као и да се покаже на који начин различита схватања сајбер простора утичу на њихово деловање у савременим међународним односима.

Из овако постављеног основног циља произлази више посебних циљева. Први посебни циљ је да се објасни теоријски и појмовни оквир сајбер ратовања, са посебним освртом на разлику између сајбер напада, сајбер операција, сајбер шпијунаже, информационог ратовања и сајбер ратовања. Други посебни циљ је да се анализира како Сједињене Америчке Државе у својим стратешким и војним документима дефинишу сајбер простор као домен деловања и инструмент националне безбедности. Трећи посебни циљ је да се испита како Руска Федерација повезује сајбер деловање

2016); The State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era* (Beijing, March 2023).

[8] The White House, *National Cybersecurity Strategy* (Washington, DC: The White House, March 2023); U.S. Department of Defense, *2023 Department of Defense Cyber Strategy: Summary* (Washington, DC: Department of Defense, 2023).

[9] President of the Russian Federation, *Doctrine of Information Security of the Russian Federation* (Moscow, December 5, 2016).

[10] The State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era* (Beijing, March 2023).

са информационом безбедношћу, политичким утицајем и стратешким надметањем. Четврти посебни циљ је да се анализира кинески приступ сајбер простору, нарочито кроз концепт сајбер суверенитета, контроле дигиталног простора и технолошке самосталности. Пети посебни циљ је да се упореде приступи ове три државе и утврде њихове сличности, разлике и последице по савремене међународне односе.

1.2.1. Научни значај истраживања

Научни значај овог истраживања огледа се у систематизацији, продубљивању и критичком преиспитивању постојећих сазнања о сајбер ратовању као феномену савремених међународних односа. Иако се сајбер безбедност често анализира као техничко, институционално или безбедносно питање, ова дисертација полази од становишта да је сајбер ратовање потребно посматрати као облик испољавања државне моћи, стратешког надметања и политичког деловања у међународном систему. У том смислу, научни допринос истраживања не огледа се само у опису сајбер напада и њихових последица, већ пре свега у анализи начина на који велике силе концептуализују сајбер простор, сајбер претње и сајбер ратовање у својим доктринама и стратешким документима.

Посебан научни значај истраживања произлази из чињенице да се у раду упоредно анализирају приступи Руске Федерације, Сједињених Америчких Држава и Народне Републике Кине. Ове државе представљају значајне актере савременог међународног система, али истовремено развијају различита схватања сајбер простора, информационе безбедности, државног суверенитета, војног деловања и стратешког одвраћања. Сједињене Америчке Државе у својим стратешким документима сајбер простор повезују са националном безбедношћу, заштитом критичне инфраструктуре, одвраћањем и употребом сајбер капацитета у оквиру ширих инструмената националне моћи.[11] Руска Федерација сајбер и информациону сферу посматра кроз призму заштите националних интереса, информационог суверенитета, стабилности државе и супротстављања претњама у информационом простору.[12] Народна Република Кина развија приступ у којем су наглашени сајбер суверенитет, управљање дигиталним простором, државна контрола, технолошки развој и безбедност као елементи дугорочног јачања националне моћи.[13]

Истраживање доприноси научном фонду тиме што омогућава јасније разликовање сродних, али не и истоветних појмова као што су сајбер напад, сајбер операција, сајбер шпијунажа, информационо ратовање, сајбер тероризам, сајбер криминал и сајбер ратовање. Ова појмовна разликовања имају посебан значај јер се у академској, политичкој и безбедносној употреби наведени термини често преклапају или користе без довољне прецизности. Управо зато дисертација настоји да укаже на то да се сајбер ратовање не може свести на сваки облик злонамерне активности у дигиталном простору, већ да га треба анализирати у контексту државних интереса, стратешких циљева, међудржавног надметања и могућности да се угрозе суверенитет, стабилност и функционисање државе.

[11] The White House, *National Cybersecurity Strategy* (Washington, DC: The White House, March 2023); U.S. Department of Defense, *2023 Department of Defense Cyber Strategy: Summary* (Washington, DC: Department of Defense, 2023).
[12] President of the Russian Federation, *Doctrine of Information Security of the Russian Federation* (Moscow, December 5, 2016).
[13] The State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era* (Beijing, March 2023).

Теоријски допринос истраживања огледа се у преиспитивању начина на који се класични појмови међународних односа — моћ, суверенитет, безбедност, одвраћање, рањивост, конфликт и стратешко надметање — мењају у условима дигитализације. Сајбер простор доводи у питање традиционално разумевање територијалности, јер се сајбер операције могу покретати преко више држава, уз прикривање идентитета актера и без јасно видљивог физичког присуства нападача. На тај начин, сајбер ратовање отвара важна теоријска питања о природи савремене моћи, границама државне одговорности, односу државних и недржавних актера и промени карактера сукоба у међународном систему.

Компаративни допринос истраживања састоји се у томе што се кроз анализу три велике силе могу уочити различити модели концептуализације сајбер ратовања. Амерички приступ наглашава оперативну употребу сајбер простора, заштиту критичне инфраструктуре, интегрисано одвраћање и повезивање сајбер капацитета са другим инструментима националне моћи. Руски приступ сајбер деловање најчешће смешта у шири оквир информационе безбедности, информационог сукобљавања и заштите државе од унутрашњих и спољних претњи у информационој сфери. Кинески приступ заснива се на идеји сајбер суверенитета, државног управљања дигиталним простором и повезивања сајбер безбедности са националним развојем, политичком стабилношћу и међународним позиционирањем. Оваква упоредна анализа омогућава дубље разумевање не само појединачних државних стратегија, већ и ширих промена у структури савремених међународних односа.

У емпиријском смислу, истраживање омогућава систематизацију и анализу релевантне грађе која обухвата стратешке документе, доктрине, националне безбедносне стратегије, војне документе, институционалне приступе и примере активности државних и недржавних актера у сајбер простору. Посебан значај има анализа званичних докумената, јер они не показују само техничке и безбедносне приоритете држава, већ и начин на који државе разумеју сопствену улогу у међународном систему, своје претње, своје противнике и инструменте заштите националних интереса. На тај начин, дисертација доприноси не само разумевању сајбер ратовања, већ и ширем проучавању државног понашања у дигитализованом међународном окружењу.

Научни значај истраживања огледа се и у томе што резултати могу послужити као основа за будућа истраживања која би се бавила сајбер стратегијама других држава, положајем малих и средњих држава у сајбер простору, улогом међународних организација у изградњи норми одговорног понашања, као и утицајем вештачке интелигенције, аутоматизованих система и нових технологија на будући развој сајбер ратовања. У том смислу, дисертација има потенцијал да допринесе даљем развоју научних расправа о сајбер простору као једном од најзначајнијих поља савремене светске политике.

1.2.2. Друштвени значај истраживања

Друштвени значај овог истраживања произлази из чињенице да је савремено друштво у великој мери зависно од информационо-комуникационих технологија. Дигиталне мреже, информациони системи и интернет постали су неопходан услов функционисања државне управе, оружаних снага, финансијских институција, индустрије, енергетике, саобраћаја, здравства, просвете, истраживачке делатности, медија и свакодневног живота грађана. Управо зато сајбер напади више не представљају искључиво технички проблем, већ могу имати непосредне последице по функционисање државе, економску стабилност, јавне услуге, безбедност грађана и поверење у институције.

Посебан друштвени значај истраживања огледа се у разумевању ризика које сајбер напади могу произвести по критичну инфраструктуру. Енергетски системи, телекомуникације, транспорт, финансијски токови, здравствене установе, системи водоснабдевања, војне комуникације и државни информациони системи све више зависе од дигитално управљаних процеса. Што је већи степен дигитализације једне државе, то је већа и потреба за развијеним механизмима заштите, отпорности и брзог опоравка након сајбер инцидената. У том смислу, сајбер безбедност постаје један од предуслова нормалног функционисања друштва, а сајбер ратовање један од ризика који може имати последице далеко изван самог дигиталног простора.

Истраживање има друштвени значај и зато што указује на то да се сајбер претње не могу разумети изоловано од ширих међународних односа. Сајбер простор је постао поље на којем се преплићу сарадња, конкуренција, стратешко неповерење и геополитичко надметање. Разлике у приступима Сједињених Америчких Држава, Руске Федерације и Народне Републике Кине посебно су важне јер показују да велике силе не полазе од истих претпоставки о природи сајбер простора, улози државе, значају информационог суверенитета, слободном протоку информација и границама државног деловања у дигиталном окружењу. Због тога разумевање њихових доктрина и стратешких докумената има значај не само за академску заједницу, већ и за креаторе јавних политика, безбедносне институције, дипломатију, приватни сектор и ширу јавност.

На глобалном нивоу отвара се низ питања која се односе на међународне норме, одговорно понашање држава, изградњу поверења, спречавање ескалације и институционалну сарадњу у сајбер простору. У оквиру Уједињених нација последњих година вођени су важни процеси посвећени безбедности употребе информационо-комуникационих технологија, укључујући рад Групе владиних експерата и Отворене радне групе за безбедност у употреби ИКТ.[14] Ипак, упркос постојању одређених заједничких оквира и препорука, разлике између великих сила и даље отежавају успостављање свеобухватног, јасног и универзално прихваћеног режима понашања држава у сајбер простору.

Друштвени значај истраживања посебно је изражен у контексту Републике Србије. Иако Србија не припада кругу великих сајбер сила, она је, као и друге мале и средње државе, све више зависна од дигиталне инфраструктуре, изложена глобалним сајбер ризицима и укључена у међународне процесе који се односе на сајбер безбедност. Разумевање стратешких приступа САД, Русије и Кине може допринети промишљенијем развоју националних политика сајбер безбедности, јачању институционалне отпорности, бољој заштити критичне инфраструктуре и разумевању положаја малих и средњих држава у дигитализованом међународном окружењу.

Практична вредност истраживања огледа се у томе што резултати могу бити корисни за државне институције, органе задужене за безбедност, доносиоце одлука, академску заједницу, стручњаке за сајбер безбедност и приватни сектор. Анализа доктрина и стратешких докумената великих сила може помоћи у препознавању главних праваца развоја сајбер ратовања, али и у разумевању начина на који се међународно окружење мења под утицајем дигиталних технологија. То је посебно важно за државе које морају да граде сопствене капацитете за превенцију, заштиту, реаговање и опоравак, али и да разумеју политичке и стратешке последице сајбер претњи.

[14] United Nations General Assembly, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN Doc. A/76/135, July 14, 2021; United Nations General Assembly, *Final Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, July 1, 2025

У истраживању ће се анализирати доктрине и стратешки документи Руске Федерације, Сједињених Америчких Држава и Народне Републике Кине, као држава које имају значајан утицај на обликовање глобалних расправа о сајбер безбедности и сајбер ратовању. Наведене државе већ дуже време у својим стратегијама препознају сајбер простор као важно поље националне безбедности, војног деловања, политичког утицаја и међународног надметања. Руска Федерација и Народна Република Кина су 2015. године потписале споразум о сарадњи у области међународне информационе безбедности, који је у делу стручне јавности тумачен као важан корак ка продубљивању њиховог партнерства у сајбер простору, али га је прецизније посматрати као оквир за сарадњу у области информационе безбедности, а не као једноставан „пакт о ненападању".[15]

Са друге стране, Сједињене Америчке Државе спадају међу најзначајније и најразвијеније актере у сајбер простору, са изузетно развијеним војним, обавештајним, технолошким и институционалним капацитетима. Амерички стратешки документи наглашавају заштиту критичне инфраструктуре, одвраћање, отпорност, сарадњу са савезницима и употребу сајбер капацитета као дела ширег система националне моћи.[16] Због различитих приступа ове три државе, њихова анализа има значај за разумевање не само националних политика, већ и глобалног надметања око правила, норми и будућег уређења сајбер простора.

Разлике између САД, Русије и Кине посебно су видљиве у међународним форумима, пре свега у оквиру Уједињених нација. Док САД и њихови савезници углавном наглашавају отворен, безбедан, стабилан и интероперабилан сајбер простор, Русија и Кина у већој мери инсистирају на информационом суверенитету, улози државе и контроли информационог простора. Ове разлике не значе да је међународна сарадња немогућа, али указују да је изградња универзално прихваћених норми у сајбер простору сложен и политички осетљив процес.[17]

На основу тога, друштвени значај истраживања огледа се у бољем разумевању сајбер ратовања као феномена који може утицати на стабилност држава, безбедност грађана, функционисање критичне инфраструктуре и односе међу великим силама. Сајбер ратовање више није питање ограничено на војне или техничке кругове, већ тема од ширег друштвеног значаја, јер последице сајбер напада могу погодити институције, економију, јавне услуге, медије, приватни сектор и свакодневни живот. Због тога разумевање овог феномена представља важан предуслов за изградњу отпорнијег, безбеднијег и стратешки промишљенијег друштва.

1.2.3 Резултати претходних истраживања

Резултати претходних истраживања указују да је сајбер ратовање, иако све присутнији феномен у савременим међународним односима, и даље поље у коме постоје значајне појмовне, теоријске

[15] Government of the Russian Federation and Government of the People's Republic of China, *Agreement on Cooperation in Ensuring International Information Security*, April 30, 2015; Elaine Korzak, "Have Russia and China Signed a Cyber Nonaggression Pact?" *The Diplomat*, August 21, 2015. У делу стручне јавности овај споразум је тумачен као „сајбер пакт о ненападању", али је академски прецизније описати га као споразум о сарадњи у области међународне информационе безбедности, прим.ауг.

[16] U.S. Department of Defense, *2023 Department of Defense Cyber Strategy: Summary* (Washington, DC: Department of Defense, 2023); The White House, *National Cybersecurity Strategy* (Washington, DC: The White House, March 2023).

[17] United Nations General Assembly, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN Doc. A/76/135, July 14, 2021; United Nations General Assembly, *Final Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, July 1, 2025; Sarah McKune, "An Analysis of the International Code of Conduct for Information Security," *Citizen Lab Research Report No. 63*, University of Toronto, September 2015.

и методолошке неуједначености. Научни фонд о овој теми развијао се постепено, најпре кроз студије безбедности, војне стратегије, политичких наука и међународних односа, а затим и кроз радове који повезују техничке, институционалне, стратешке и нормативне аспекте сајбер простора. Управо због тога претходна истраживања показују да сајбер ратовање није могуће разумети искључиво као технички проблем заштите информационих система, већ као сложен политички и стратешки феномен који утиче на понашање држава, структуру моћи, суверенитет и безбедност у међународном систему.

Посматрано из историјске перспективе, сваки велики технолошки развој утицао је на промену концепата националне и међународне безбедности. Појава ваздухопловства, нуклеарног и термонуклеарног оружја, развој свемирских програма и каснија дигитална револуција показују да технологија не мења само средства ратовања, већ и начин на који државе разумеју простор, моћ, одвраћање и рањивост. У том контексту, префикс „сајбер“ постао је један од најзначајнијих појмова савремене безбедносне и академске расправе, јер означава нову област у којој се преплићу техничка инфраструктура, политички интереси, војно планирање, обавештајне активности и међудржавно надметање.

Истраживања о настанку интернета показују да су корени савременог сајбер простора повезани са хладноратовским контекстом и улагањима Сједињених Америчких Држава у научно-технолошки развој. ARPANET, као претеча интернета, развијен је крајем шездесетих година у оквиру Агенције за напредне истраживачке пројекте Министарства одбране САД, са циљем умрежавања истраживачких центара и размене дигиталних ресурса између географски удаљених рачунара.

Иако је развој интернета био повезан са војним и истраживачким потребама, истраживачи који су учествовали у његовом стварању истицали су и његов потенцијал за сарадњу, размену знања и повезивање научних заједница. Leiner, Cerf, Clark, Kahn, Kleinrock и други аутори у класичном прегледу историје интернета наглашавају да интернет није само технолошка инфраструктура, већ и резултат заједнице истраживача, институција и корисника који су развијали и унапређивали мрежу.[18] Исти простор је временом омогућио глобалну комуникацију, трговину, образовање и научну сарадњу постао и простор нових безбедносних ризика, укључујући шпијунажу, саботажу, дезинформационе активности, криминал и могућност међудржавног сукобљавања у дигиталној сфери.

Један део претходних истраживања полази од става да сајбер напади представљају стварну и растућу претњу националној и међународној безбедности. Аутори који припадају овом приступу указују да све већа зависност држава од дигиталних система ствара нове облике рањивости, нарочито у секторима критичне инфраструктуре као што су енергетика, транспорт, финансије, телекомуникације, здравство, војне комуникације и државна управа. Џозеф Нај истиче да сајбер простор мења расподелу моћи јер омогућава деловање широког спектра актера, смањује трошкове уласка у простор надметања и отежава класичне механизме одвраћања и контроле.[19] У том смислу, сајбер простор се не може посматрати само као технолошка инфраструктура, већ као ново поље светске политике.

[18] Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff, “A Brief History of the Internet,” *Internet Society*, 1997.
[19] Joseph S. Nye Jr., “Cyber Power,” *Belfer Center for Science and International Affairs, Harvard Kennedy School*, May 2010.

Значајан део литературе посвећен је питању да ли сајбер напади могу произвести последице упоредиве са традиционалним оружаним сукобом. Џејмс Ендру Луис, у раној анализи ризика од сајбер тероризма, сајбер рата и других сајбер претњи, указује да је потребно разликовати сценарије високог ризика од претераних процена, али истовремено наглашава да напади на критичну инфраструктуру могу имати озбиљне последице по националну безбедност.[20] Kenneth Geers, у делу *Strategic Cyber Security*, полази од становишта да се рачунарска безбедност развила из техничке дисциплине у стратешки концепт, јер зависност држава од интернета и дигиталних система отвара питања националне и међународне безбедности.[21]

Посебно место у претходним истраживањима заузима проблем атрибуције, односно питање утврђивања одговорности за сајбер напад. За разлику од класичних војних операција, у сајбер простору нападач може прикрити трагове, користити инфраструктуру трећих држава, злоупотребити заражене уређаје и створити лажне техничке индикаторе који упућују на погрешног актера. Због тога велики број аутора указује да је утврђивање са сигурношћу да иза одређеног напада стоји конкретна држава изузетно тешко, посебно када се сајбер операције спроводе преко посредника, хакерских група или мрежа компромитованих рачунара. Овај проблем има посебан значај за међународне односе, јер без поуздане атрибуције државе тешко могу формулисати политички, дипломатски или безбедносни одговор.

У литератури се често истиче да карактер мреже омогућава висок степен прикривања. Напади се могу спроводити преко ботнет мрежа, односно мрежа заражених уређаја који се контролишу без знања њихових власника. Таква инфраструктура може бити распоређена у више држава, чиме се додатно отежава утврђивање правог извора напада. Управо због тога сајбер простор омогућава државама и недржавним актерима да делују уз релативно висок степен порицања одговорности. Та могућност „порецивости“ представља једну од кључних разлика између сајбер операција и традиционалних облика употребе силе.

У делу литературе сајбер ратовање се дефинише превасходно кроз улогу државе. Richard A. Clarke и Robert K. Knake дефинишу сајбер рат као активности једне државе усмерене на продор у рачунаре или мреже друге државе ради изазивања штете или поремећаја.[22] Овакво разумевање наглашава државни карактер сајбер ратовања и разликује га од сајбер криминала, хактивизма или појединачних техничких инцидената. У том смислу, сајбер ратовање се не може свести на сваки облик злонамерног деловања у дигиталном простору, већ се мора повезати са политичком намером, стратешким циљем и међудржавним контекстом.

Ипак, већина аутора упозорава да су многе дефиниције сајбер ратовања прешироке. Не могу се сви сукоби између држава у сајбер простору сматрати војним акцијама, нити сваки сајбер напад представља почетак оружаног сукоба. Сајбер напади које спроводе државе разликују се по намери, интензитету, средствима, трајању и последицама. P. W. Singer и Allan Friedman указују да је појам сајбер рата често оптерећен медијским и политичким преувеличавањем, због чега је

[20] James A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats* (Washington, DC: Center for Strategic and International Studies, December 2002).
[21] Kenneth Geers, *Strategic Cyber Security* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publications, 2011).
[22] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco/HarperCollins, 2010). Clarke и Knake дефинишу сајбер рат као акције државе усмерене на продор у рачунаре или мреже друге државе ради изазивања штете или поремећаја.

неопходно разликовати технички инцидент, шпијунажу, саботажу, криминал и акт који би могао имати карактер употребе силе.[23]

Ово питање има посебан значај у контексту међународних односа. Члан 41 Повеље Уједињених нација предвиђа могућност прекида економских односа, саобраћајних, поштанских, телеграфских, радио и других средстава комуникације као мере које не подразумевају употребу оружане силе.[24] Ово показује да прекид комуникација, иако може бити озбиљна мера притиска, није нужно истоветан оружаном нападу. Пренето на сајбер простор, то значи да је неопходно пажљиво проценити када сајбер операција представља политички притисак, када економску или обавештајну активност, а када може достићи праг употребе силе или оружаног напада.

Управо зато значајан део претходних истраживања настоји да утврди критеријуме за разликовање сајбер напада од сајбер ратовања. Као могући критеријуми најчешће се наводе: идентитет актера, политичка намера, веза са државним интересом, обим последица, утицај на критичну инфраструктуру, степен физичке штете и повезаност са ширим оружаним или политичким сукобом. Један део аутора сматра да се само оне сајбер операције чији су ефекти еквивалентни или приближни кинетичком насиљу могу посматрати као акти сајбер рата. Други аутори, међутим, сматрају да је овакво схватање преуско, јер занемарује политичке, психолошке, економске и стратешке последице које сајбер операције могу произвести и без непосредне физичке штете.

Истраживања такође показују да развој сајбер простора мења однос између мира, кризе и рата. Сајбер операције могу се спроводити у миру, у условима политичке кризе, паралелно са конвенционалним сукобом или као део ширих хибридних стратегија. Пример руско-грузијског рата 2008. године, у контексту сукоба око Јужне Осетије, често се наводи као један од првих случајева у којем су сајбер напади пратили конвенционалне војне операције.[25] Слично томе, рат у Украјини од 2022. године показао је да се деструктивни малвер, DDoS напади, операције утицаја и напади на дигиталну инфраструктуру могу одвијати упоредо са класичним војним операцијама.[26]

Истовремено, треба нагласити да претходна истраживања не показују јединствен став о домету сајбер ратовања. Једна група аутора сматра да сајбер операције могу постати централни елемент будућих сукоба, јер државама омогућавају да делују брзо, прикривено и уз релативно мале трошкове. Друга група аутора упозорава да су тврдње о „сајбер рату“ често претеране. Thomas Rid у раду *Cyber War Will Not Take Place* тврди да сајбер напади, иако могу бити озбиљни, најчешће не испуњавају класичне критеријуме рата као насилног, инструменталног и политичког акта.[27] Erik Gartzke у раду *The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth*

[23] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014).
[24] United Nations, *Charter of the United Nations*, art. 41. Члан 41 Повеље УН наводи прекид економских односа, саобраћајних, поштанских, телеграфских, радио и других средстава комуникације као мере које не укључују употребу оружане силе.
[25] Cyber Law Toolkit, “Georgia-Russia Conflict (2008),” NATO Cooperative Cyber Defence Centre of Excellence; Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, “Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War,” *Security Dialogue* 43, no. 1 (2012): 3–24.
[26] Microsoft Security Response Center, “Cyber Threat Activity in Ukraine: Analysis and Resources,” February 28, 2022; Canadian Centre for Cyber Security, *Cyber Threat Activity Associated with the Russian Invasion of Ukraine*, 2022.
[27] Thomas Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies* 35, no. 1 (2012): 5–32.

такође истиче да сајбер сукоби вероватније допуњују постојеће облике политичког и војног надметања него што их у потпуности замењују.[28]

Ови критички приступи имају велики значај јер спречавају некритичко ширење појма сајбер ратовања. Они указују да сајбер простор не укида традиционалну војну силу, територију, економске ресурсе и политичку вољу, већ их надопуњује и трансформише. У том смислу, сајбер ратовање не треба посматрати као потпуну замену за конвенционално ратовање, већ као нову димензију сукоба која се може комбиновати са дипломатским притисцима, обавештајним активностима, економским мерама, информационим операцијама и класичном употребом силе.

Са друге стране, чињеница да сајбер ратовање не замењује традиционалне облике сукоба не значи да је његов значај споредан. Напротив, претходна истраживања показују да државе све више развијају институционалне, војне и технолошке капацитете за деловање у сајбер простору. Сједињене Америчке Државе, Руска Федерација и Народна Република Кина у различитим облицима развијају специјализоване структуре, доктрине, стратегије и капацитете који се односе на сајбер безбедност, информациону безбедност, сајбер операције и војну употребу дигиталног простора. Ово потврђује да државе сајбер простор све више посматрају као значајно поље националне безбедности и стратешког надметања.

Претходна истраживања посебно су значајна за ову дисертацију јер показују да постоји потреба за упоредном анализом начина на који велике силе концептуализују сајбер ратовање. Досадашња литература често се бави или техничким аспектима сајбер напада, или појединачним случајевима, или општим питањем међународне регулације. Мањи број радова систематски упоређује доктринарне и стратешке документе великих сила са становишта међународних односа. Управо у том простору ова дисертација настоји да понуди допринос кроз анализу САД, Русије и Кине као три различита модела разумевања сајбер простора, државне моћи и стратешког деловања.

У том смислу, истраживачки фокус ове дисертације усмерен је на анализу природе, циљева, методологије, динамике и последица политика и активности држава у области сајбер ратовања и сајбер безбедности. Посебна пажња биће посвећена питању како се у стратешким документима ове три државе дефинишу сајбер претње, како се описује улога државе, како се сајбер простор повезује са националном безбедношћу и како се сајбер капацитети укључују у шире политичке, војне и спољнополитичке циљеве.

На основу досадашњих истраживања може се закључити да сајбер ратовање остаје спорно, али изузетно значајно поље савремене науке о међународним односима. Спорно је зато што не постоји јединствена дефиниција, зато што су границе између криминала, шпијунаже, саботаже и ратовања нејасне, и зато што је тешко утврдити одговорност актера. Значајно је зато што државе све више зависе од дигиталне инфраструктуре, зато што сајбер операције могу произвести политичке и економске последице, и зато што велике силе сајбер простор све јасније укључују у своје стратегије моћи, безбедности и међународног позиционирања.

Ова дисертација не полази од претпоставке да ће конвенционално ратовање нестати или да ће сајбер рат у потпуности заменити класичне облике оружаног сукоба. Напротив, полази се од становишта да ће се традиционални и сајбер облици деловања све чешће преплитати. Управо зато

[28] Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (Fall 2013): 41–73.

је неопходно разумети како велике силе дефинишу сајбер простор, како у њему виде сопствене интересе, како процењују претње и како обликују доктринарне и стратешке одговоре. Сајбер ратовање се, стога, у овом истраживању посматра као нова димензија међународног надметања, а не као изоловани технички феномен.

1.3. Теоријско одређење предмета истраживања

1.3.1. Постојећа сазнања о предмету истраживања

Постојећа сазнања о сајбер безбедности и сајбер ратовању обележена су појмовном неуједначеношћу, различитим теоријским приступима и недовољно стабилизованим критеријумима за разликовање сајбер напада, сајбер операција, сајбер шпијунаже, информационог ратовања и сајбер ратовања. Управо због тога ова област захтева пажљиво теоријско и појмовно одређење, јер се у академској, политичкој, војној и медијској употреби наведени појмови често користе као синоними, иако не означавају исте појаве. Сајбер ратовање, као предмет овог истраживања, неће бити посматрано као сваки облик злонамерне активности у дигиталном простору, већ као сложен феномен који је повезан са државним интересима, стратешком намером, међудржавним надметањем и последицама које могу угрозити функционисање државе, критичну инфраструктуру, политичку стабилност или безбедност грађана.

У домаћој научној заједници тема сајбер ратовања јесте присутна, али још увек није развијена у мери која би одговарала њеном значају за савремене међународне односе, посебно када је реч о упоредној анализи доктрина и стратешких докумената великих сила. На међународном нивоу научни фонд је знатно развијенији, али је и даље обележен расправама о томе шта се може сматрати сајбер ратом, када сајбер напад достиже праг оружаног сукоба, како се утврђује одговорност државе и на који начин се сајбер операције уклапају у постојеће теорије моћи, безбедности и конфликта.[29]

Проблем појмовног одређења посебно је изражен зато што сајбер сукоби не подразумевају нужно употребу физичке силе, нити се морају одвијати на јасно одређеном географском простору. За разлику од традиционалних облика оружаног сукоба, сајбер операције могу бити покренуте са једне територије, технички изведене преко инфраструктуре више држава, усмерене ка мети у трећој држави, док стварни налогодавац може остати прикривен. Ова карактеристика сајбер простора доводи у питање класичне представе о територији, границама, одговорности и суверенитету у међународним односима.

Сајбер ратовање има неконвенционалну и асиметричну природу. Државе које немају снажне конвенционалне војне капацитете могу у сајбер простору препознати могућност да делују против технолошки развијенијих противника, јер офанзивне сајбер операције могу бити релативно јефтиније од развоја класичних војних капацитета, док потенцијалне последице могу бити несразмерно велике. Истовремено, високо дигитализоване државе постају посебно рањиве, јер

[29] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014); Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–32.

њихова војна, економска, енергетска, финансијска и административна инфраструктура у великој мери зависи од дигиталних система.[30]

Иако Сједињене Америчке Државе, Руска Федерација и Народна Република Кина различито концептуализују сајбер простор, заједничко им је то што га препознају као област од стратешког значаја за националну безбедност, заштиту државних интереса и међународно позиционирање.

Русија и Кина су, заједно са другим државама, годинама настојале да у оквиру Уједињених нација промовишу концепт међународног уређења информационог простора. Кина, Руска Федерација, Таџикистан и Узбекистан су 2011. године поднеле Генералној скупштини УН предлог „Међународног кодекса понашања за информациону безбедност", док је 2015. поднета ажурирана верзија тог документа од стране држава чланица Шангајске организације за сарадњу.[31] Ови предлози показују да се сајбер простор не посматра само као техничко питање, већ као област у којој се укрштају различита схватања суверенитета, безбедности, слободе информација, државне контроле и међународног поретка.

Посебно место у досадашњим расправама заузима Талински приручник о међународном праву применљивом на сајбер ратовање, као и његова проширена верзија Tallinn Manual 2.0. Приручник је припремила међународна група експерата на позив NATO Cooperative Cyber Defence Centre of Excellence, а не сам Центар као институција у ужем смислу. Прва верзија бавила се применом међународног права на сајбер операције у контексту употребе силе и оружаног сукоба, док је Tallinn Manual 2.0 проширио анализу и на сајбер инциденте испод прага употребе силе или оружаног сукоба.[32] Иако овај приручник нема обавезујућу правну снагу, његов значај је у томе што је отворио важну расправу о томе како постојећа правила, норме и концепти могу бити примењени на сајбер простор. За потребе овог истраживања, Талински приручник неће бити третиран као централни оквир рада, јер дисертација није примарно правна, већ политиколошка и сагледава аспект међународних односа. Његов значај је пре свега у томе што показује да сајбер операције могу достићи степен озбиљности који отвара питања одговорности држава, употребе силе, оружаног сукоба и заштите критичних система. Ипак, главни фокус овог рада остаје на начину на који државе у својим доктринама и стратегијама концептуализују сајбер ратовање као инструмент моћи и стратешког деловања.

Kenneth Geers указује да је сајбер безбедност прерасла оквир техничке заштите и постала питање стратешког значаја, јер државе дигитални простор све више посматрају као област одбране, надметања и пројекције моћи.[33] Слично томе, Martin Libicki анализира могућности и ограничења сајбер одвраћања, указујући да сајбер простор не функционише на исти начин као традиционални домени војне моћи и да је погрешно сајбер ратовање једноставно посматрати као кинетички рат

[30] Joseph S. Nye Jr., "Cyber Power," *Belfer Center for Science and International Affairs, Harvard Kennedy School,* May 2010; Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009).
[31] United Nations General Assembly, "Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General," UN Doc. A/66/359, September 14, 2011; United Nations General Assembly, "Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General," UN Doc. A/69/723, January 13, 2015.
[32] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017); NATO Cooperative Cyber Defence Centre of Excellence, "The Tallinn Manual."
[33] Kenneth Geers, *Strategic Cyber Security* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publications, 2011).

другим средствима.[34] Ови приступи су важни јер показују да сајбер ратовање захтева сопствени аналитички оквир, али да се истовремено не може потпуно одвојити од ширих питања стратегије, одвраћања и међународне безбедности.

Dorothy Denning је међу ауторима који су рано указивали на то да се интернет може користити као средство политичког утицаја, активизма, хактивизма, терористичке пропаганде и угрожавања безбедности.[35] Њен рад је важан јер показује да сајбер простор није само поље државног деловања, већ и простор активности недржавних актера. Ипак, за ову дисертацију од посебног значаја су случајеви у којима сајбер активности добијају државну, стратешку и међународнополитичку димензију.

Richard A. Clarke и Robert K. Knake дефинишу сајбер рат кроз деловање једне државе усмерено на продор у рачунаре или мреже друге државе ради изазивања штете или поремећаја.[36] Овакво разумевање наглашава улогу државе као кључног актера и омогућава разликовање сајбер ратовања од сајбер криминала, појединачног хакерског деловања или хактивизма. Ипак, ова дефиниција мора бити примењена опрезно, јер не представља сваки продор у систем друге државе акт сајбер рата. Сајбер шпијунажа, на пример, може бити противправна или политички неприхватљива, али се не може аутоматски изједначити са оружаним нападом или ратним дејством.

P. W. Singer и Allan Friedman указују да је појам сајбер рата често оптерећен политичким и медијским преувеличавањем, због чега је неопходно разликовати техничке инциденте, шпијунажу, саботажу, криминал, информационе операције и сајбер операције које могу имати стратешки или војни значај.[37] Ово је посебно важно за међународне односе, јер некритичко ширење појма сајбер ратовања може довести до аналитичке непрецизности и погрешног разумевања понашања држава у сајбер простору.

У том контексту значајан је и члан 41 Повеље Уједињених нација, који предвиђа могућност прекида економских односа, саобраћајних, поштанских, телеграфских, радио и других средстава комуникације као мере које не подразумевају употребу оружане силе.[38] Ова чињеница показује да прекид комуникација, иако може бити озбиљна мера притиска, није нужно истоветан оружаном нападу. Пренето на сајбер простор, то значи да је потребно пажљиво проценити када сајбер операција представља политички притисак, када шпијунажу или саботажу, а када може достићи праг употребе силе или сајбер ратовања.

Значајан део савремене литературе упозорава и на опасност од преувеличавања претње сајбер рата. Thomas Rid у познатом раду *Cyber War Will Not Take Place* тврди да сајбер напади, иако могу бити озбиљни, најчешће не испуњавају класичне критеријуме рата као насилног, инструменталног и политичког акта.[39] Erik Gartzke такође указује да сајбер рат вероватније

[34] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009).
[35] Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND Corporation, 2001); Dorothy E. Denning, "Cyberwarriors: Activists and Terrorists Turn to Cyberspace," *Harvard International Review* 23, no. 2 (2001): 70–75.
[36] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco/HarperCollins, 2010).
[37] Singer and Friedman, *Cybersecurity and Cyberwar*.
[38] United Nations, *Charter of the United Nations*, art. 41.
[39] Rid, "Cyber War Will Not Take Place," 5–32.

допуњује постојеће облике политичког и војног надметања него што их у потпуности замењује.[40] Ови критички приступи су важни јер спречавају поједностављено разумевање сајбер простора као потпуне замене за традиционално ратовање.

Ова дисертација не полази од претпоставке да ће сајбер рат укинути конвенционално ратовање, нити да ће сваки напад на дигиталну инфраструктуру представљати акт сајбер рата. Напротив, полази се од става да ће се конвенционални и сајбер облици деловања све чешће преплитати. Сајбер ратовање се у овом истраживању одређује као облик сајбер деловања који је повезан са државним интересима, стратешком намером, међудржавним надметањем и последицама које могу угрозити функционисање државе, критичну инфраструктуру, политичку стабилност или безбедност грађана. Такво одређење омогућава да се сајбер ратовање разликује од ширег скупа злонамерних активности у дигиталном простору, али и да се препозна његов значај за савремене међународне односе.

1.4. Операционо одређење предмета истраживања

1.4.1. Чиниоци садржаја предмета истраживања

Операционо одређење предмета истраживања обухвата анализу кључних чинилаца сајбер ратовања попут актера, циљева, средстава, метода, домета, последица и начина на који се ови елементи појављују у доктринама и стратешким документима Сједињених Америчких Држава, Руске Федерације и Народне Републике Кине.

Предмет истраживања није свака активност у сајбер простору, већ су предмет оне активности које имају стратешки значај за државу, њену националну безбедност, међународно позиционирање и односе међу великим силама и могу бити искоришћене у сукобу.

Први чинилац предмета истраживања јесу актери. У фокусу су пре свега државе, јер се дисертација бави доктринама и стратешким документима три велике силе. Ипак, анализа ће узети у обзир и улогу недржавних актера, хакерских група, приватног сектора, технолошких компанија и међународних организација, јер је сајбер простор специфичан управо по томе што државе у њему не делују саме. Недржавни актери могу бити самостални, али могу деловати и као посредници, партнери или инструменти државног утицаја, што додатно усложњава питање одговорности и атрибуције.

Други чинилац односи се на циљеве сајбер деловања. Они могу бити различити: заштита националне безбедности, прикупљање обавештајних података, слабљење противника, тестирање одбрамбених система, нарушавање поверења у институције, угрожавање критичне инфраструктуре, утицај на јавно мњење или остваривање политичког притиска. Управо различитост циљева показује зашто није могуће све сајбер активности подвести под један појам. Сајбер шпијунажа, сајбер саботажа, информационо деловање и сајбер напад могу бити међусобно повезани, али немају увек исти интензитет, последице и стратешки значај.

Трећи чинилац односи се на средства и методе. Сајбер операције могу укључивати напад на доступност система, компромитовање поверљивости података, нарушавање интегритета информација, злоупотребу софтверских рањивости, дезинформационе активности, упаде у

[40] Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (Fall 2013): 41–73

мреже, манипулацију подацима и напад на системе критичне инфраструктуре. За потребе ове дисертације, технички аспекти неће бити анализирани као оперативна упутства или технички приручник, већ као елементи који омогућавају разумевање стратешких последица сајбер деловања.

Четврти чинилац односи се на последице. Последице сајбер операција могу бити техничке, политичке, економске, војне, психолошке и друштвене. Неке операције могу изазвати само привремени прекид рада система, док друге могу угрозити функционисање државних институција, поверење грађана, економску стабилност, војну комуникацију или критичну инфраструктуру. Управо последице представљају један од најважнијих критеријума за разликовање обичних сајбер инцидената од операција које могу имати карактер сајбер ратовања.

Пети чинилац односи се на стратешки контекст. Сајбер операције се не могу анализирати изоловано од политичких односа међу државама. Иста техничка активност може имати различито значење у зависности од тога да ли се одвија у миру, током политичке кризе, у условима хибридног сукоба или паралелно са конвенционалним оружаним операцијама. Због тога ће ова дисертација сајбер ратовање анализирати као део ширег стратешког надметања, а не као изолован технички феномен.

1.4.2. Временско одређење предмета истраживања

У ширем временском оквиру, истраживање обухвата период од шездесетих година XX века, када се развијају идеје о рачунарском умрежавању и ARPANET као претеча интернета, до савременог периода. DARPA наводи да је ARPANET као четворочворна мрежа активиран 1969. године, док је каснији развој TCP/IP протокола омогућио формирање техничке основе савременог интернета.[41] Овај шири оквир важан је зато што показује да се сајбер простор није појавио изоловано, већ као резултат дуготрајног развоја војних, научних, истраживачких и технолошких процеса.

У ужем временском оквиру, истраживање обухвата период од 1999. до 2026. године. Година 1999. узима се као симболички значајна јер је током НАТО интервенције против Савезне Републике Југославије интернет био коришћен као простор информационог деловања, пропаганде, хакерских активности и напада на интернет странице. У делу литературе и медијских анализа овај сукоб је означаван као један од раних примера „интернет рата“, јер су се поред конвенционалних војних операција одвијале и активности у дигиталном простору.[42]

Ипак, посебан значај у развоју савременог разумевања сајбер ратовања има период након 2007. године. Сајбер напади на Естонију 2007. године често се наводе као један од првих великих примера у којима је високо дигитализована држава била изложена координисаним нападима на државне институције, медије, банке и друге сервисе.[43] Руско-грузијски сукоб 2008. године, у контексту Јужне Осетије, показао је да се сајбер напади могу одвијати паралелно са

[41] Defense Advanced Research Projects Agency, “ARPANET,” DARPA; Barry M. Leiner et al., “A Brief History of the Internet,” *Internet Society*, 1997.
[42] “Serbs Launch Cyberattack on NATO,” *Nextgov*, April 4, 1999; “Inside the First ‘Internet War,’” *Wired*, January 1999.
[43] Rain Ottis, “Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective,” NATO Cooperative Cyber Defence Centre of Excellence, 2008.

конвенционалним војним операцијама.[44] Рат у Украјини од 2022. године додатно је потврдио да сајбер операције, деструктивни малвер, DDoS напади, операције утицаја и напади на дигиталну инфраструктуру могу бити саставни део савременог оружаног сукоба.[45]

Избор 2026. године као краја временског оквира условљен је потребом да се истраживање обухвати до тренутка израде дисертације и да укључи најновије стратешке документе и међународне процесе релевантне за анализу. То је посебно важно јер су у периоду после 2022. године усвојени или ажурирани важни документи који утичу на разумевање сајбер простора, укључујући америчку *National Cybersecurity Strategy* из 2023. године, *2023 Department of Defense Cyber Strategy Summary*, кинески документ *China's Law-Based Cyberspace Governance in the New Era* из 2023. године, као и наставак процеса Уједињених нација у оквиру Отворене радне групе за безбедност у употреби информационо-комуникационих технологија.[46]

Овако постављен временски оквир омогућава да се анализира развој сајбер ратовања од раних облика употребе интернета у политичким и војним сукобима, преко великих сајбер инцидената који су променили безбедносне стратегије држава, до савремених доктрина и стратешких докумената САД, Руске Федерације и НР Кине.

1.4.3. Просторно одређење предмета истраживања

Сајбер простор има глобални домет и не може се просторно ограничити на начин на који се ограничавају класични територијални простори. Сајбер операције могу бити покренуте са различитих локација, преко инфраструктуре више држава и против мета које се налазе у различитим политичким, економским и безбедносним системима. Због тога сајбер простор истовремено превазилази класичне границе и дубоко утиче на питања државног суверенитета, контроле, безбедности и међународне одговорности.

Ипак, за потребе овог истраживања, просторно одређење предмета односи се пре свега на анализу доктрина и стратешких докумената Сједињених Америчких Држава, Руске Федерације и Народне Републике Кине. Ове три државе изабране су зато што представљају значајне актере савременог међународног система. Њихови приступи сајбер простору имају утицај на глобалне расправе о сајбер безбедности, сајбер ратовању, информационом суверенитету, технолошком развоју и међународним нормама.

Просторно одређење, дакле, није ограничено на физичку територију ових држава, већ на њихове стратешке, институционалне и доктринарне приступе сајбер простору. На тај начин, истраживање обухвата и шири међународни контекст у коме ове државе делују, укључујући Уједињене нације,

[44] Cyber Law Toolkit, "Georgia-Russia Conflict (2008)," NATO Cooperative Cyber Defence Centre of Excellence; Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," *Security Dialogue* 43, no. 1 (2012): 3–24.
[45] Microsoft Security Response Center, "Cyber Threat Activity in Ukraine: Analysis and Resources," February 28, 2022; Canadian Centre for Cyber Security, *Cyber Threat Activity Associated with the Russian Invasion of Ukraine*, 2022.
[46] The White House, *National Cybersecurity Strategy* (Washington, DC: The White House, March 2023); U.S. Department of Defense, *2023 Department of Defense Cyber Strategy: Summary*; The State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era*; United Nations General Assembly, *Final Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, July 2025.

НАТО, Шангајску организацију за сарадњу, билатералне односе, савезничке структуре и глобалне расправе о одговорном понашању држава у сајбер простору.

1.5. Научно-дисциплинарно одређење предмета истраживања

У научно-дисциплинарном смислу, предмет истраживања припада пре свега области политичких наука, међународних односа, студија безбедности и стратешких студија. Сајбер ратовање се у овом раду не посматра искључиво као техничко питање, нити као ужи проблем примене права на сајбер сукобе, већ као политички и стратешки феномен који утиче на понашање држава, односе моћи, безбедносне дилеме и структуру савременог међународног система.

Истраживање ће користити мултидисциплинарни приступ, али ће његово тежиште остати у пољу међународних односа. Сазнања из правних наука, информатике, социологије, економије и студија технологије користиће се као помоћни аналитички оквири, у оној мери у којој доприносе разумевању сајбер ратовања као инструмента државне моћи и стратешког надметања. Овакво научно-дисциплинарно одређење омогућава да се избегне свођење сајбер ратовања на техничку заштиту информационих система или на уско правно питање, и да се оно анализира као део шире трансформације савремених међународних односа.

Основни теоријски оквир овог истраживања представља неореализам, јер омогућава анализу држава као кључних актера, њихове тежње ка безбедности, развоја офанзивних и дефанзивних капацитета и понашања у условима анархичне структуре међународног система. У неореалистичком схватању међународни систем је анархичан, што значи да не постоји наддржавни ауторитет који може у потпуности гарантовати безбедност држава.[47] У таквом систему државе настоје да повећају сопствену безбедност и моћ, али тиме могу изазвати несигурност код других држава, што се у сајбер простору испољава кроз развој офанзивних и дефанзивних капацитета, стратегије одвраћања, прикривено деловање и стратешко неповерење.

Неореализам је посебно користан за разумевање зашто велике силе развијају сајбер капацитете чак и у условима формалног мира. Сајбер простор омогућава државама да прикупљају информације, тестирају рањивости противника, развијају капацитете одвраћања и пројектују моћ без непосредне употребе класичне војне силе. У литератури се често указује на перцепцију офанзивне предности у сајбер простору, јер релативно јефтини офанзивни алати могу произвести несразмерно велике последице, док је одбрана сложена због потребе да се заштити велики број међусобно повезаних система.[48]

Ипак, због специфичности сајбер простора, неореализам не може бити једини аналитички оквир. Либерализам је значајан јер указује на улогу међународне сарадње, институција, режима, приватног сектора и недржавних актера у управљању сајбер претњама. У области сајбер безбедности државе не могу деловати потпуно самостално, јер велики део дигиталне инфраструктуре припада приватном сектору, а сајбер претње често прелазе националне границе. Због тога су међународна сарадња, размена информација, изградња поверења и развој заједничких норми важни елементи разумевања сајбер простора.

---

[47] Kenneth N. Waltz, *Theory of International Politics* (Reading, MA: Addison-Wesley, 1979); John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: W. W. Norton, 2001).

[48] Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30, no. 2 (1978): 167–214; Libicki, *Cyberdeterrence and Cyberwar*.

Конструктивизам је користан зато што омогућава анализу начина на који државе различито тумаче сајбер простор, сајбер претње, информациони суверенитет, слободу интернета и одговорно понашање у дигиталном окружењу. САД, Русија и Кина не разликују се само по технолошким и војним капацитетима, већ и по нормама, политичким представама, стратешким културама и начинима на које дефинишу безбедност у сајбер простору. Управо зато је за ово истраживање важно анализирати не само материјалне капацитете држава, већ и њихове доктринарне формулације, стратешке наративе и политичке концепте.

На основу тога, предмет истраживања биће разматран пре свега у оквиру савремених теорија међународних односа, са неореализмом као основним оквиром, али уз ограничену употребу увида либерализма и конструктивизма. Такав приступ омогућава да се сајбер ратовање анализира као облик државног деловања у анархичном међународном систему, али и као феномен у којем важну улогу имају норме, институције, недржавни актери, технолошке компаније и различита схватања суверенитета.

У закључном смислу, сајбер ратовање се у овој дисертацији операционо одређује као стратешко деловање у сајбер простору које је повезано са државним интересима, безбедносним циљевима и међународним надметањем. Оно не подразумева нужно непосредну физичку штету, али мора имати потенцијал да произведе последице по функционисање државе, критичну инфраструктуру, политичку стабилност, војне капацитете или безбедност грађана. На тај начин, сајбер ратовање се разликује од ширих облика сајбер криминала, хактивизма и појединачних инцидената, али се истовремено препознаје као једна од важних димензија савремених међународних односа.

1.6. Хипотетички оквир

Општа хипотеза дисертације гласи:

„Сајбер ратовање представља специфичан облик стратешког деловања држава у савременим међународним односима, који се од традиционалне примене силе разликује по средствима, методама, простору извођења, актерима, проблему атрибуције и врсти последица које може произвести. У условима растућих геополитичких тензија и борбе за очување и пројекцију моћи, може се очекивати да ће велике силе наставити да развијају сајбер капацитете и да ће сајбер простор све изразитије укључивати у своје доктрине, стратешке документе и безбедносне политике“.

Посебне хипотезе:

1. Развој сајбер простора и информационо-комуникационих технологија повећава зависност савремених држава од дигиталне инфраструктуре, чиме се истовремено увећавају њихове могућности за развој, комуникацију и управљање, али и њихова рањивост на сајбер претње.
2. Сајбер ратовање представља специфичан облик међународног сукобљавања који се може одвијати и у миру и у кризи и у рату, при чему се од традиционалних облика ратовања разликује по средствима, методама, простору деловања, актерима и тешкоћама утврђивања одговорности.
3. Сајбер ратовање не може се изједначити са сваком злонамерном активношћу у дигиталном простору, већ се као посебан облик стратешког деловања препознаје онда када је повезано са државним интересима, политичком намером, међудржавним

надметањем и последицама по функционисање државе, критичну инфраструктуру, војне капацитете или безбедност грађана.
4. У сајбер простору, поред држава, значајну улогу имају и недржавни актери, укључујући хакерске групе, приватне компаније и технолошке организације, што додатно усложњава питање атрибуције и отежава доказивање директне одговорности суверених држава за сајбер нападе.
5. Сајбер безбедност и сајбер ратовање све више утичу на међудржавне односе, јер сајбер простор постаје важно поље геополитичког надметања, стратешког одвраћања, пројекције моћи и обликовања савременог међународног поретка.
6. Доктрине и стратешки документи Сједињених Америчких Држава, Руске Федерације и Народне Републике Кине показују да ове државе сајбер простор препознају као област од посебног значаја за националну безбедност, војно планирање, заштиту критичне инфраструктуре и међународно позиционирање.
7. Различита схватања сајбер простора у САД, Руској Федерацији и Народној Републици Кини одражавају њихове различите стратешке културе, политичке системе и концепте моћи: САД наглашавају одвраћање, отпорност и оперативно деловање; Русија информациону безбедност и стратешко надметање; а Кина сајбер суверенитет, државну контролу и технолошку самосталност.

Индикатори:

Индикатори за анализу доктрина и стратешких докумената

1. Начин дефинисања сајбер простора, сајбер безбедности, сајбер претњи, сајбер операција и сајбер ратовања у званичним документима.
2. Учесталост и контекст употребе појмова као што су: национална безбедност, критична инфраструктура, одвраћање, информациона безбедност, сајбер суверенитет, офанзивни капацитети, дефанзивни капацитети и међународна сарадња.
3. Постојање и развој институционалних и војних структура задужених за сајбер безбедност, сајбер операције и информационо деловање.
4. Начин на који државе повезују сајбер простор са заштитом националних интереса, војним планирањем и спољнополитичким циљевима.
5. Однос држава према међународним нормама, УН процесима, мултилатералним иницијативама и питању одговорног понашања држава у сајбер простору.
6. Начин на који се у документима представљају претње које долазе од других држава, недржавних актера, хакерских група, терористичких организација и приватног сектора.
7. Постојање доктринарних или стратешких формулација које указују на употребу сајбер капацитета као инструмента одвраћања, притиска, заштите, пројекције моћи или међународног позиционирања.

Индикатори политичког и стратешког утицаја

1. Учешће анализираних држава у међународним форумима и процесима који се односе на сајбер безбедност.
2. Предлагање међународних иницијатива, кодекса понашања, стратегија и норми у области сајбер простора.

3. Степен утицаја анализираних држава на обликовање глобалних расправа о сајбер безбедности, сајбер суверенитету, слободном протоку информација и одговорном понашању држава.
4. Обим сарадње са савезницима, партнерским државама, међународним организацијама и приватним сектором.
5. Видљивост сајбер простора у националним стратегијама безбедности, војним стратегијама, доктринама и званичним политичким документима.

Индикатори институционалног и војног развоја

1. Постојање специјализованих институција, агенција, команди или војних структура задужених за сајбер безбедност и сајбер операције.
2. Начин организације сајбер капацитета у оквиру државног, војног и обавештајног система.
3. Степен повезивања сајбер капацитета са класичним војним, обавештајним и дипломатским инструментима државне моћи.
4. Присуство сајбер операција у војним стратегијама, одбрамбеним документима и концептима националне безбедности.

Релевантност истраживања

Релевантност истраживања заснива се на чињеници да сајбер ратовање представља један од најзначајнијих изазова савремених међународних односа, јер повезује питања државне моћи, националне безбедности, критичне инфраструктуре, технолошке зависности, међународног надметања и стабилности светског поретка.

Истраживање доприноси употпуњавању научног фонда у области међународних односа, студија безбедности, стратешких студија и савремених теоријских приступа анализи државне моћи у условима дигитализованог међународног система. Посебна релевантност истраживања огледа се у упоредној анализи Сједињених Америчких Држава, Руске Федерације и Народне Републике Кине, јер ове државе на различите начине концептуализују сајбер простор и својим доктринама, стратегијама и међународним деловањем утичу на обликовање глобалних расправа о сајбер безбедности, сајбер суверенитету, информационој безбедности и правилима понашања држава у дигиталном простору.

1.7. Методе истраживања

Имајући у виду предмет, циљеве и хипотезе дисертације, истраживање ће бити засновано на квалитативном методолошком приступу. Овакав приступ је најпримеренији јер се предмет истраживања не односи на једноставно мерење појава, већ на разумевање начина на који се сајбер ратовање концептуализује у доктринама и стратешким документима Сједињених Америчких Држава, Руске Федерације и Народне Републике Кине.

Сајбер ратовање је сложен политички, безбедносни и стратешки феномен, чије се значење не може у потпуности објаснити само бројчаним показатељима, већ захтева анализу садржаја, контекста, намера, стратешких формулација и начина на који државе дефинишу своје интересе, претње и капацитете у сајбер простору.

Коришћење искључиво квантитативног приступа не би било адекватно за проверу постављених хипотеза, јер број сајбер напада, учесталост инцидената или финансијска улагања у сајбер капацитете не могу сама по себи објаснити доктринарно и стратешко разумевање сајбер ратовања. Поред тога, у овој области постоје значајне потешкоће у погледу утврђивања извора напада, степена претње, намере актера, интензитета последица и улоге државе у конкретним сајбер активностима. Управо због проблема атрибуције, различитих нивоа тајности и неуједначености доступних података, квалитативни приступ омогућава дубље и прецизније разумевање истраживаног феномена.

У циљу провере постављених хипотеза, истраживање ће користити компаративни приступ. Упоредна анализа биће усмерена на три државе које имају посебан значај за разумевање савременог сајбер ратовања: Сједињене Америчке Државе, Руску Федерацију и Народну Републику Кину.

Компаративни приступ омогућава да се утврде сличности и разлике у начину на који ове државе дефинишу сајбер простор, сајбер претње, сајбер безбедност, информациону безбедност, војну употребу сајбер капацитета и место сајбер ратовања у ширем оквиру националне безбедности и међународног позиционирања.

Посебно значајна метода у овом истраживању биће анализа садржаја. Она ће бити примењена на званичне доктринарне, стратешке, безбедносне и политичке документе анализираних држава. Анализом садржаја утврђиваће се који се појмови најчешће користе, на који начин се дефинишу сајбер претње, како се описује улога државе у сајбер простору, да ли се наглашавају офанзивни или дефанзивни капацитети, како се сајбер простор повезује са критичном инфраструктуром, националном безбедношћу, војним планирањем, технолошком самосталношћу, информационим суверенитетом и међународном сарадњом.

У истраживању ће бити примењен и метод студије случаја. Сједињене Америчке Државе, Руска Федерација и Народна Република Кина посматраће се као три посебна случаја, али и као три различита модела концептуализације сајбер ратовања. Студија случаја омогућава детаљније разумевање унутрашњег контекста сваке државе, њене стратешке културе, институционалног оквира, безбедносних приоритета и начина на који у својим документима повезује сајбер простор са државном моћи, безбедношћу и међународним односима.

Поред наведеног, у раду ће бити коришћене и аналитичко-синтетичка метода, дескриптивна метода и историјска метода. Аналитичко-синтетичка метода биће коришћена ради разлагања сложеног феномена сајбер ратовања на његове основне елементе — актере, циљеве, средства, методе, последице и стратешки контекст — а затим ради њиховог поновног повезивања у јединствену целину. Дескриптивна метода биће примењена приликом приказа основних карактеристика доктрина, стратегија и институционалних приступа анализираних држава. Историјска метода биће коришћена у делу који се односи на развој интернета, настанак сајбер простора, еволуцију сајбер претњи и постепено укључивање сајбер ратовања у безбедносне и војне стратегије држава.

Начини прикупљања података биће прилагођени предмету истраживања и карактеру доступних извора. Основу истраживачке грађе чиниће писани извори, пре свега званични документи држава и међународних организација, као и релевантна научна и стручна литература. Пошто се истраживање бави доктринама и стратешким документима, посебан значај имаће анализа

формалних државних аката, стратегија националне безбедности, војних доктрина, сајбер стратегија, докумената о информационој безбедности, резолуција и извештаја међународних организација.

Као примарни извори у истраживању биће коришћени званични документи и акти Сједињених Америчких Држава, Руске Федерације и Народне Републике Кине, укључујући стратегије националне безбедности, сајбер стратегије, војне доктрине, доктрине информационе безбедности, политичке одлуке, институционалне документе и релевантне изјаве државних органа. Поред тога, као примарни извори биће коришћени документи међународних организација, нарочито Уједињених нација и НАТО-а, у мери у којој су релевантни за разумевање међународних норми, сарадње и расправа о одговорном понашању држава у сајбер простору.

Као секундарни извори биће коришћена научна и стручна литература из области међународних односа, студија безбедности, стратешких студија, сајбер безбедности, сајбер ратовања, политикологије и, у ограниченој мери, међународног права. Секундарни извори обухватиће монографије, научне чланке, истраживачке извештаје, анализе релевантних института, радове аутора који се баве сајбер ратовањем, сајбер одвраћањем, информационим ратовањем, државном моћи и безбедношћу у дигиталном простору.

Методолошки приступ биће усмерен на утврђивање везе између званичних докумената, стратешких циљева и ширег понашања држава у сајбер простору. То значи да ће се у раду настојати да се покаже не само шта државе формално наводе у својим документима, већ и како се кроз те документе одражавају њихови безбедносни приоритети, схватање претњи, однос према међународном поретку, концепт суверенитета и начин употребе сајбер простора као инструмента државне моћи.

На овај начин, примена квалитативног, компаративног и аналитичког приступа омогућиће да се сајбер ратовање истражи као сложен феномен савремених међународних односа. Изабране методе омогућавају проверу постављених хипотеза, утврђивање сличности и разлика између САД, Руске Федерације и Народне Републике Кине, као и разумевање начина на који сајбер простор постаје једно од кључних поља савременог стратешког надметања.

1.8. Научна и друштвена оправданост истраживања

Научна оправданост овог истраживања заснива се на чињеници да сајбер ратовање представља релативно нов, сложен и још увек недовољно теоријски стабилизован феномен у савременим међународним односима. Иако постоји значајан број радова који се баве сајбер безбедношћу, сајбер нападима, информационим ратовањем и техничким аспектима заштите информационих система, и даље постоји потреба за систематичним истраживањем начина на који се сајбер ратовање концептуализује у доктринама и стратешким документима великих сила. Посебан значај има упоредна анализа Сједињених Америчких Држава, Руске Федерације и Народне Републике Кине, јер ове државе развијају различите приступе сајбер простору, сајбер безбедности, информационој безбедности, државном суверенитету и употреби сајбер капацитета као инструмента националне моћи.

Научни допринос истраживања огледа се у обједињавању, систематизацији и критичкој анализи постојећих сазнања из области међународних односа, студија безбедности, стратешких студија, сајбер безбедности и сајбер ратовања. Истраживање настоји да допринесе јаснијем појмовном

разграничењу сајбер напада, сајбер операција, сајбер шпијунаже, информационог ратовања и сајбер ратовања, као и да укаже на специфичности сајбер ратовања у односу на традиционалне облике употребе силе. Овакво разграничење има посебну научну вредност, јер омогућава прецизније разумевање феномена који се у политичком, медијском и стручном дискурсу често користи недовољно јасно и недовољно доследно.

Научна оправданост истраживања произлази и из потребе да се сајбер ратовање анализира као део шире трансформације моћи, безбедности и сукоба у међународном систему. Развој сајбер простора отворио је нова питања о природи државне моћи, проблему атрибуције, стратешком одвраћању, заштити критичне инфраструктуре, улози недржавних актера и границама између мира, кризе и рата. Због тога је неопходно истражити не само техничке могућности сајбер напада, већ и политичке, војне, безбедносне и стратешке последице које сајбер операције могу произвести у односима међу државама.

Друштвена оправданост истраживања заснива се на чињеници да сајбер напади могу угрозити не само државне институције и војне системе, већ и свакодневно функционисање друштва. Савремене државе све више зависе од дигиталне инфраструктуре, информационих система и мрежа које омогућавају рад енергетике, саобраћаја, телекомуникација, финансијског сектора, здравства, образовања, јавне управе и безбедносних структура. У таквим околностима, напад из сајбер простора може имати последице које превазилазе технички ниво и непосредно утичу на економску стабилност, јавне услуге, безбедност грађана, поверење у институције и способност државе да нормално функционише.

Посебна друштвена оправданост истраживања огледа се у потреби бољег разумевања ризика који настају услед све чешћег коришћења сајбер простора као средства политичког притиска, стратешког надметања и пројекције моћи. Сајбер ратовање више није питање ограничено на војне и техничке кругове, већ постаје тема од ширег друштвеног значаја, јер последице сајбер напада могу погодити институције, привреду, медије, критичну инфраструктуру, приватни сектор и грађане. Због тога разумевање доктрина и стратешких докумената великих сила може допринети бољем разумевању савремених безбедносних ризика и правовременијем развоју одговарајућих политика заштите.

Резултати овог истраживања могу имати практичну вредност за креаторе јавних политика, државне институције, безбедносни сектор, академску заједницу и стручњаке који се баве сајбер безбедношћу. Истраживање може послужити као основ за боље разумевање начина на који велике силе дефинишу сајбер претње, развијају сајбер капацитете и укључују сајбер простор у своје војне, политичке и стратешке планове. Таква сазнања могу бити корисна и за Републику Србију, посебно у погледу развоја националних политика сајбер безбедности, јачања институционалне отпорности, заштите критичне инфраструктуре и разумевања положаја малих и средњих држава у дигитализованом међународном окружењу.

На основу наведеног, научна и друштвена оправданост овог истраживања произлазе из потребе да се сајбер ратовање проучи као један од кључних феномена савремене безбедности и међународних односа. Његово разумевање омогућава не само теоријско продубљивање постојећих научних сазнања, већ и практично сагледавање ризика, изазова и могућих праваца деловања држава у сајбер простору.

2. Улога интернета

У савременој литератури, интернет се дефинише као „глобални информационо-комуникациони систем који обухвата велики број међусобно повезаних мрежа које омогућавају размену података на светском нивоу“[49]. Његово функционисање заснива се на стандардизованим комуникационим протоколима који обезбеђују међусобну повезаност различитих уређаја и мрежа, чиме се омогућава континуирани ток информација.

Последње три деценије, интернет више не представља само и искључиво техничку инфраструктуру, већ је постао комплексно окружење у савременим међународним односима у којем се одвијају политичке, економске и безбедносне интеракције. Државе га све чешће посматрају као стратешки ресурс, чија заштита и контрола добијају централно место у оквиру националних безбедносних политика.[50] Интернет се све више препознаје као простор у којем се реализују различити облици сајбер операција, укључујући и активности које имају карактер сајбер ратовања.

Савремени интернет користи више милијарди људи широм света, што га чини једном од најраспрострањенијих комуникационих платформи у историји.[51] Ова масовна употреба глобалне комуникационе мреже омогућила је незабележен степен повезаности између појединаца, институција и држава, док је истовремено створила и нове облике рањивости. Управо ова зависност од дигиталне инфраструктуре чини интернет критичним ресурсом чије нарушавање рада или угрожавање рада може да има значајне последице по функционисање друштва. Поред тога, интернет омогућава брзо ширење информација, али и дезинформација, које се све чешће користе као инструмент политичког утицаја у међудржавним односима.[52] У том смислу, интернет превазилази своју првобитну комуникациону улогу и постаје средство пројекције моћи у савременом свету.

Посебно је битно истаћи да зависност савремених друштава од интернета и ИКТ система доводи до појаве нових облика асиметричних претњи, у којима актери са ограниченим ресурсима могу изазвати значајне последице по далеко развијеније системе.[53] Ова чињеница додатно компликује традиционалне концепте безбедности и захтева адаптацију постојећих стратегија.

У својој техничкој основи, интернет представља скуп рачунара и комуникационих линија који омогућавају размену података између различитих уређаја.[54] Међутим, савремено разумевање интернета обухвата далеко шири спектар различтих елемената и актера који циркулишу унутар тог простора.[55] Управо ова сложеност омогућава државама да интернет користе као средство за остваривање различитих стратешких циљева, укључујући, између осталих, и надзор грађана, утицај и заштиту сопствених интереса.

---

[49] Manuel Castells, *The Rise of the Network Society* (Oxford: Wiley-Blackwell, 2010), 70–72.
[50] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND, 2009), 5–7.
[51] International Telecommunication Union (ITU), *Measuring Digital Development* (Geneva: ITU, 2022), 12–14.
[52] Joseph S. Nye Jr., *The Future of Power* (New York: PublicAffairs, 2011), 113–115.
[53] Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013), 18–20.
[54] Сам термин „интернет“ потиче од израза „internetwork“, који означава повезивање више мрежа у јединствен систем.
[55] Janet Abbate, *Inventing the Internet* (Cambridge, MA: MIT Press, 1999), 3–5.

Интернет је данас интегрални део свакодневног живота, али његова улога све више превазилази цивилну сферу и све више улази у домен безбедности и одбране стављајући државе пред различите изазове. Државе интензивно развијају капацитете за деловање у сајбер простору, што укључује како одбрамбене, тако и офанзивне способности.[56] Ова трансформација указује да интернет више не може бити посматран као неутрална платформа, већ као динамично окружење у којем се преплићу интереси различитих актера. У том контексту, питања дигиталног суверенитета, контроле података и заштите инфраструктуре постају кључна питања националних држава, савремених међународних односа, као и међународних организација.

Развој технологија као што су вештачка интелигенција, машинско учење и анализа великих података додатно проширује могућности деловања у сајбер простору, али истовремено повећава и сложеност безбедносних изазова.[57] Ове технологије омогућавају аутоматизацију сајбер операција, што може довести до бржег и интензивнијег извођења војних напада, али и до ефикасније одбране.[58]

Историјски посматрано, развој комуникационих технологија, попут телеграфа, телефона и радија, значајно је утицао на друштвене промене, али је интернет довео до квалитативно нове фазе у развоју комуникације. Он омогућава не само размену информација, већ и интеракцију у реалном времену на глобалном нивоу. Ова карактеристика чини интернет изузетно погодним за извођење, односно реализацију различитих облика сајбер операција.[59] Државама се пружа могућност да могу истовремено да делују на више нивоа – техничком, информативном и психолошком – што значајно проширује спектар могућих стратегија деловања.

Интернет се често описује као један од најуспешнијих резултата дугорочног улагања у развој информационе инфраструктуре.[60] Овај успех указује на значај систематског приступа технолошком развоју, али и на улогу државних инвестиција у формирању глобалних комуникационих система. Данас, међутим, интернет више није само технолошко достигнуће, већ и простор стратешког надметања између држава. Улагања у дигиталне капацитете постају важан фактор међународног позиционирања, што додатно потврђује његов значај у савременим конфликтима о којима ће бити речи у наставку рада.

Да би се у потпуности разумела улога интернета у савременом свету, неопходно је пружити анализу историјског развоја и трансформацију из техничке иновације у стратешки ресурс. Посебно је важно сагледати како су државе препознале његов потенцијал у области безбедности као и употребе током конфликта као и у мирнодопско време. У том смислу, интернет се може посматрати као један од кључних елемената савременог сајбер простора, који све више добија карактер новог домена ратовања[61].

[56] David T. Kuehl, "From Cyberspace to Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: NDU Press, 2009), 28–30.
[57] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 75–77.
[58] Ibid., 80–82.
[59] John Arquilla and David Ronfeldt, *Networks and Netwars* (Santa Monica: RAND, 2001), 6–8.
[60] Barry M. Leiner et al., "A Brief History of the Internet," *ACM SIGCOMM Computer Communication Review* 39, no. 5 (2009): 22–24.
[61] David T. Kuehl, "From Cyberspace to Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: NDU Press, 2009), 28–30.

2.1 Историја развоја интернета

У последњих неколико деценија, технологија је доживела убрзан и континуиран развој, који је у значајној мери обликовао савремено друштво. Период од шездесетих година XX века до данас обележен је интензивним технолошким иновацијама и процесима дигитализације који су трансформисали начин комуникације, рада и функционисања друштва и држава.

Нове идеје и техничка достигнућа подстицали су развој различитих апликација, док је истовремено расла и потражња корисника за бржим и ефикаснијим облицима комуникације. Технолошке могућности и захтеви друштва довели су до иновација, нових апликација али и нових навика без којих је свакодневни живот постао готово незамислив – е-пошта, приступ информацијама, дељење датотека, друштвене мреже, блогови, е-здравство, онлајн учење и студирање, итд.[62] Ове промене нису имале само социјалну димензију, већ су постепено добијале и безбедносни значај, јер су дигиталне технологије постајале кључна инфраструктура савремених држава. У том контексту, интернет се све више препознаје као критична инфраструктура чија стабилност директно утиче на функционисање државних система од којих зависи функционисање друштва. Поред тога, развој дигиталних платформи омогућио је нове облике утицаја, укључујући информационе операције које имају за циљ обликовање јавног мњења у међудржавним односима. Оваква трансформација указује да интернет више није само технички систем, већ и простор политичког деловања[63].

Разноврсне и сложене друштвене и технолошке трансформације имају своје корене у начину на који је интернет развијен уз помоћ грантова за истраживање од стране Агенције за напредне истраживачке пројекте Министарства одбране САД.[64] Ово указује да интернет од самог тренутка свог настанка није био искључиво цивилни пројекат, већ је имао изражену безбедносну и стратешку димензију.

Већ у првим годинама развоја, државе су препознале потенцијал нових комуникационих технологија као средства за остваривање предности у геополитичком контексту. Истовремено, рани развој интернета поставио је темеље за касније облике дигиталног надметања између држава. Ова веза између технологије и државне моћи постаје све израженија у савременом добу, где дигитална инфраструктура представља један од кључних елемената националне безбедности. У том смислу, интернет се може посматрати као ресурс чија контрола има директне геополитичке импликације.[65]

Као што је већ истакнуто у претходним редовима, историја интернета почиње у Сједињеним Америчким Државама током раних 1960-их година, у специфичном геополитичком контексту хладног рата. Тај период карактерише биполарни светски поредак у коме су Сједињене Америчке Државе и Совјетски Савез са савезницима настојали да прошире свој утицај на глобалном нивоу. Поред војног надметања и дипломатских активности, значајна средства улагана су у научна истраживања и технолошки развој. Ова улагања нису била случајна, већ су представљала део стратегије за стицање дугорочне предности у различитим доменима, укључујући и комуникационе технологије. Надметање две суперсиле довело је и до изузетних научних

[62] Manuel Castells, *The Rise of the Network Society*, 2nd ed. (Oxford: Wiley-Blackwell, 2010), xviii–xix, 17–18.
[63] Joseph S. Nye Jr., *The Future of Power* (New York: PublicAffairs, 2011), 113–115.
[64] Andrew L. Russell, "Ideological and Policy Origins of the Internet, 1957–1969" (paper presented at the 29th Telecommunications Policy Research Conference, Alexandria, VA, October 28, 2001), 1–5.
[65] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), 5–7.

достигнућа и развоја у свим областима. Трка се није одвијала само у стицању политичке моћи и војном наоружању.[66] Управо овај контекст омогућио је настанак технологија које ће касније постати основа интернета. Поред тога, конкуренција између две силе довела је до убрзаног развоја рачунарских система, који су били неопходни за обраду и размену информација. Такође, овај период карактерише и институционализација научних истраживања, што је додатно допринело развоју нових технологија.

Посебан подстицај развоју научно-технолошког сектора у Сједињеним Америчким Државама представљао је догађај из 1957. године, када је Совјетски Савез лансирао сателит „Спутњик“. Тај догађај имао је снажан политички и психолошки ефекат, јер је указао на могућност технолошке надмоћи супротстављене стране. Као одговор на овај изазов, Сједињене Америчке Државе су интензивирале улагања у научна истраживања и развој нових технологија. Овај процес довео је до оснивања институција и програма који су имали за циљ унапређење технолошких капацитета, укључујући и развој рачунарских мрежа. Последично, створени су предуслови за настанак интернета као иновативног комуникационог система са стратешким значајем. Овај догађај се често тумачи као прекретница која је убрзала технолошку трку и довела до стварања инфраструктуре која ће касније постати основа дигиталног доба.[67]

Сам интернет је настао у оквиру пројекта АРПАНЕТ, који је развијен под окриљем Министарства одбране Сједињених Америчких Држава. Основна идеја била је да се развије комуникациона мрежа отпорна на евентуалне нападе, посебно у условима нуклеарног сукоба.[68] Предвиђено је да то буде децентрализована мрежа рачунара која би могла да функционише у условима делимичног уништења.[69] Управо овај концепт представља један од кључних принципа савремених мрежа, а то је да се обезбеди отпорност система и континуитет комуникације. Истовремено, принцип децентрализације постао је основа за развој модерних сајбер одбрамбених механизама које користе војне структуре држава. У савременом контексту, исти принцип омогућава државама да одрже функционалност критичних система чак и у условима сајбер напада. Ово додатно наглашава значај раних концептуалних решења у обликовању данашњих безбедносних стратегија.[70]

Кључна практична фаза у развоју АРПАНЕТ-а отпочела је током 1969. године, када су успостављене прве везе између почетних чворова мреже. У септембру 1969. године први чвор је инсталиран на UCLA колеџу, док је Stanford Research Institute постао други чвор мреже. Убрзо је остварена и прва host-to-host комуникација.[71] Овај тренутак представља једну од пресудних тачака у историји интернета, јер је показао да се удаљени рачунарски системи могу ефикасно повезати у функционалну мрежу.[72] Резултат овог развоја био је настанак мреже која показује висок степен техничке отпорности и флексибилности иако је у својој раној фази била ограничена

[66] Andrew L. Russell, “Ideological and Policy Origins of the Internet, 1957–1969,” 2–5.
[67] Ибид. 4–5.
[68] Barry M. Leiner et al., “A Brief History of the Internet,” *ACM SIGCOMM Computer Communication Review* 39, no. 5 (2009): 22–24.
[69] Paul Baran, *On Distributed Communications Networks* (Santa Monica: RAND Corporation, 1962), 1–5.
[70] David T. Kuehl, “From Cyberspace to Cyberpower: Defining the Problem,” in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: NDU Press, 2009), 28–30.
[71] Internet Society, *A Brief History of the Internet* (Reston, VA: Internet Society, 2012), 3.
[72] Barry M. Leiner et al., “A Brief History of the Internet,” *ACM SIGCOMM Computer Communication Review* 39, no. 5 (2009): 24

по обиму. Управо та флексибилност касније је постала један од темељних принципа савремених комуникационих система и има директну примену у концептима сајбер одбране.

Иако су први експерименти били ограничени на научне и војне кругове, њихов значај је временом постајао све већи. Године 1965. када се догодио први мрежни експеримент, и када су први пут коришћени пакети за комуникацију између рачунара, научници нису замишљали вишеструку употребу ове технологије у друштву каква је данас.[73] Током 1960-их и 1970-их година, мрежа је постепено расла и развијала се у систем који користи комутацију пакета као основни принцип преноса података. Развој ове технологије касније је омогућио експанзију интернета у глобалну инфраструктуру. Поред тога, пакетски пренос података представља основу за функционисање савремених дигиталних система који су истовремено и средство комуникације и потенцијално средство сајбер операција. У савременим условима, ова технологија омогућава и прикривање извора напада, што додатно компликује одбрану у сајбер простору.[74]

Постепено формирање великог броја међусобно повезаних мрежа временом се интегрисало у јединствени систем познат као интернет.[75] Рана примена ових технологија у академским и војним круговима створила је основу за каснију комерцијализацију интернета. Фаза развоја размене електронске поште показује да су комуникационе потребе биле кључни покретач технолошких иновација. Све већа појава размене е-поште означила је прелазак интернета из уско стручног у шири комуникациони контекст, што је додатно убрзало његов развој[76]. Истовремено, већ у овом периоду постају видљиве прве назнаке зависности друштва од дигиталних система[77].

У литератури се датум 1. јануар 1983. године најчешће означава као кључна прекретница у развоју интернета. Тог дана је извршен прелазак на протоколски оквир TCP/IP, који је омогућио уједначену комуникацију између различитих мрежа[78]. Пре тога су различите рачунарске мреже функционисале као релативно изоловани системи. Увођењем протокола TCP/IP (Transmission Control Protocol/Internet Protocol) створени су услови за повезивање хетерогених система у јединствену функционалну мрежу.[79] Протокол је омогућио различитим типовима рачунара да ефикасно размењују податке, чиме је постављен темељ савременог интернета. У техничком смислу, TCP/IP представља један од најзначајнијих стандарда у историји информационих технологија због своје флексибилности и скалабилности. Увођење овог протокола означава и почетак трансформације интернета у глобалну инфраструктуру од стратешког значаја.

Интернет је у почетним фазама развоја био под снажним утицајем и финансијском подршком владе Сједињених Америчких Држава. Ипак, сам дизајн није био заснован на централизацији. Архитектура интернета је омогућавала дистрибуирано функционисање без јединственог центра контроле.[80] Интернет је и данас децентрализована, отворена и неутрална мрежа самих мрежа. Таква структура је омогућила бржи развој интернета, његово ширење и способност прилагођавања различитим наменама и корисничким потребама. Истовремено, одсуство

[73] Barry M. Leiner et al., "A Brief History of the Internet," 23.
[74] Leonard Kleinrock, "An Early History of the Internet," *IEEE Communications Magazine* 48, no. 8 (2010): 26–30.
[75] Barry M. Leiner et al., "A Brief History of the Internet," *ACM SIGCOMM Computer Communication Review* 39, no. 5 (2009): 22–24.
[76] Ибид. 24–26.
[77] Ибид, 24-26
[78] Barry M. Leiner et al., "A Brief History of the Internet," *ACM SIGCOMM Computer Communication Review* 39, no. 5 (2009): 26.
[79] Ибид, 26
[80] Manuel Castells, *The Rise of the Network Society*, 2nd ed. (Oxford: Wiley-Blackwell, 2010), 70–72.

јединствене контролне тачке створило је и трајне изазове у погледу управљања, надзора и безбедности. Отуда се парадокс интернета огледа у томе што је његова отвореност и децентрализованост истовремено извор његове снаге али и извор његове рањивости. Управо због тога интернет у савременом свету добија све израженију улогу у међудржавним односима. Државе настоје да пронађу механизме заштите сопствених интереса у окружењу које по својој природи превазилази националне границе, што је данас изузетно изазовно.[81] Овај парадокс између отворености и (мањка) контроле постаје једно од централних питања савременог сајбер простора.

Отворена архитектура интернета омогућила је слободан приступ протоколима и инфраструктури са различитих географских локација, као и повезивање различитих уређаја, мрежа и техничких система. Овакав приступ подстакао је развој великог броја услуга и апликација које су значајно проширile функционалност интернета. Међу најзначајнијим иновацијама издвајају се електронска пошта, World Wide Web, а касније и друштвене мреже. Те технологије нису само унапредиле комуникацију, већ су створиле и нове облике друштвене, економске и политичке интеракције. Интернет је у само неколико деценија постао не само платформа за размену информација, већ и инструмент утицаја, мобилизације и обликовања јавног мњења. Таква трансформација отворила је простор и за нове облике деловања држава у дигиталном окружењу, укључујући информационе операције и различите облике пројекције моћи.[82]

Током 1990-их година интернет се из Сједињених Америчких Држава проширио на глобални ниво изузетно брзим темпом. Ова експанзија била је праћена технолошким иновацијама које су омогућиле да интернет постане доступан далеко ширем кругу корисника него у претходним фазама. Године 1989. Тим Бернерс-Ли предложио је концепт World Wide Web-а, који је убрзо развијен и постао један од кључних покретача даљег ширења интернета.[83] Развој WWW-а омогућио је једноставнији приступ информацијама, већу видљивост садржаја и значајно повећао број корисника који користе интернет. Ова иновација представља један од пресудних тренутака у историји развоја интернета, јер је омогућила његову масовну употребу и створила услове за нове облике дигиталне комуникације и интеракције. World Wide Web се почетком 1990-их година развио у најзначајнији сервис на интернету, омогућавајући приступ великој количини информација на релативно једноставан и приступачан начин. Основна идеја овог система била је да омогући повезивање и приступ информацијама из различитих извора у што ефикаснијем и ширем облику.[84] Појава WWW-а допринела је комерцијализацији интернета и његовој интеграцији у различите сфере друштва. Овај процес је, с једне стране, довео до раста економског значаја дигиталних технологија, а с друге стране отворио нове безбедносне ризике и нове могућности за злоупотребу. У том смислу, интернет више није био само средство комуникације, већ и простор потенцијалних конфликата, политичког надметања и стратешког деловања.[85]

Пројекат АРПАНЕТ је званично окончан 1990. године чиме је интернет постао јавно доступан широј, глобалној популацији. Овај тренутак означио је прелазак интернета из експерименталне у

[81] Joseph S. Nye Jr., *The Future of Power* (New York: PublicAffairs, 2011), 113–115.
[82] Ибид. 113–115.
[83] Barry M. Leiner et al., "A Brief History of the Internet," *ACM SIGCOMM Computer Communication Review* 39, no. 5 (2009): 29–30
[84] Ибид., 29–30
[85] Barry M. Leiner et al., "A Brief History of the Internet," *ACM SIGCOMM Computer Communication Review* 39, no. 5 (2009): 29–30.

оперативну фазу. Истовремено, омогућена је његова даља комерцијализација и интеграција у све сфере друштва. Данас су ИКТ системи и интернет један од кључних ресурса савременог света.

Интернет саобраћај се одвија путем оптичких влакана, кабловских система, радио таласа и других комуникационих технологија које заједно чине физичку и бежичну основу савремене глобалне мреже.[86] Међутим, у савременом контексту, интернет представља не само комуникациони систем, већ и кључни домен у којем се одвијају различити облици међудржавних активности, укључујући и сајбер конфликте.[87]

По завршетку хладног рата, фокус се са традиционалних војних капацитета постепено проширује на информациону надмоћ.[88] Упоредо са ширењем интернета ван војно-истраживачких оквира и његовим постепеним уласком у цивилну, економску и друштвену употребу, почињу да се јављају и разматрања о могућностима вођења потенцијалних конфликата у сајбер простору. Крајем 1980-их и почетком 1990-их година, у периоду када је интернет престао да буде претежно истраживачка и стручна инфраструктура и прерастао у ширу комуникациону мрежу, државе су почеле да увиђају да систем који је првобитно развијан ради отпорније и ефикасније размене података истовремено може постати и извор нових рањивости. Са порастом веће умрежености и примерне дигиталних мрежа од стране државних институција, привреде и комуникационих система, појављују се и идеје да ће се потенцијални конфликти такође пренети у ново поље. Фактички, будући сукоби неће бити нужно ограничени на физичко бојиште, већ ће се све више преносити и у сферу информација, мрежне инфраструктуре и управљања подацима. У том контексту, фокус безбедносних и војних разматрања постепено се са традиционалне кинетичке надмоћи шири ка информационој надмоћи, контроли комуникационих токова и заштити мрежно повезаних система.[89]

Након што је интернет почетком постао јавно доступан и почео да се шири изван затворених научних и војних кругова, државе су почеле да препознају његов војно-стратешки потенцијал. У тој почетној фази, овај процес још увек није био доследно именован и категорисан као „сајбер ратовање“, већ се најчешће развијао кроз концепте информационог ратовања, борбу за предност у домену информација, надзора, комуникација[90]. Додатни подстицај овим разматрањима дала је убрзана дигитализација критичних инфраструктура, укључујући енергетске системе, телекомуникације и финансијске мреже, које су постале потенцијалне мете напада.[91] Истовремено, појава првих значајних сајбер инцидената указала је на реалну могућност злоупотребе дигиталних система у сврху дестабилизације држава.[92]

[86] International Telecommunication Union, *Measuring Digital Development: Facts and Figures 2023* (Geneva: ITU, 2023), 24–25.
[87] David T. Kuehl, “From Cyberspace to Cyberpower: Defining the Problem,” in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: NDU Press, 2009), 28–30
[88] Joseph S. Nye Jr., *The Future of Power* (New York: PublicAffairs, 2011), 113–115.
[89] Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff, “A Brief History of the Internet,” *ACM SIGCOMM Computer Communication Review* 39, no. 5 (2009): 24–29.
[90] Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Pub 3-13 (Washington, DC: Joint Chiefs of Staff, October 9, 1998), I-1–I-3.
[91] President’s Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America’s Infrastructures* (Washington, DC: Government Printing Office, 1997), 17–18.
[92] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), 121–123.

Све већи развој глобалних мрежа омогућио је нове облике деловања који су превазилазили класичне географске границе сукоба попут могућности за прикупљање обавештајних података, ширење психолошког утицаја и извођење потенцијалних сајбер напада. У овом периоду почиње и озбиљније институционално препознавање потребе да се заштита информационих система третира као део националне безбедности, а не само као технички проблем администрације и одржавања мрежа.[93]

Крајем 1990-их година почиње јасније да се профилише појам „критичне информационе инфраструктуре", који обухвата системе од виталног значаја за функционисање државе, као што су енергетски системи, телекомуникације, финансијски сектор и здравствени системи.[94] Зависност савремених држава од ових система условила је да њихова заштита постане приоритет националне безбедности држава, чиме сајбер простор добија нову, стратешку димензију.[95]

Сједињене Америчке Државе биле су међу првим државама које су систематски развијале концепте употребе дигиталних и информационих система у војне сврхе. У оквиру америчких стратешких разматрања појављује се појам информационог ратовања, који не обухвата само техничку заштиту сопствених система, већ и могућност ометања, деградације или неутралисања противничких информационих ресурса. На тај начин, информације и мреже постају не само средство подршке војним операцијама, већ и самосталан простор надметања. Уместо да буду схваћене искључиво као логистички или комуникациони ресурс, мреже све више добијају карактер борбеног множиоца моћи. Овај помак имао је дубоке последице по војне доктрине, јер је наметнуо потребу за интеграцијом обавештајних, комуникационих, психолошких и техничких капацитета у јединствен оперативни оквир.[96]

Један од најважнијих раних примера те промене у доктрини вођења сукоба јесте операција „Пустињска олуја" 1991. године. Иако интернет у том периоду још није био масовно употребљаван као што је данас, Заливски рат је показао колики значај у модерним војним операцијама могу да имају напредне електронске технологије, интероперабилност снага и брз проток и размена информација. У том смислу, „Пустињска олуја" није била пример сајбер рата у пуном значењу тог појма, али јесте представљала пресудан моменат у коме је постало јасно да се војна супериорност све више везује за брзину обраде, дистрибуције и употребе информација. Операција је показала да се технолошка предност више не исцрпљује у ватреној моћи, већ све изразитије почива и на способности да се информација претвори у оперативну предност.[97]

Истовремено, како је интернет улазио у ширу цивилну употребу, постајало је све јасније да дигитална повезаност не производи само нове могућности сарадње, већ и нове облике политичког и безбедносног деловања. Посебно значајан пример из касних 1990-их представља конфликт на простору бивше Југославије, а нарочито НАТО интервенција 1999. године, која се у литератури често описује као један од првих сукоба у којем је интернет имао видљиву политичку и оперативну улогу. У овом случају дигитални простор није био само позадина сукоба, већ арена у

[93] Ибид.121–122.
[94] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, DC: Government Printing Office, 1997), 17–18.
[95] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (London: Routledge, 2008), 45–47
[96] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), iii–iv, 122–123
[97] Richard W. Stewart, *War in the Persian Gulf: Operations Desert Shield and Desert Storm, August 1990–March 1991* (Washington, DC: Center of Military History, United States Army, 2010), v–vi.

којој су се истовремено водиле борбе за легитимитет, перцепцију и политички утицај. Значај овог примера лежи управо у томе што показује да сајбер простор може бити средство асиметричног деловања, доступно и државама и недржавним актерима, при чему ниједна страна не мора поседовати класичну војну надмоћ да би произвела политички ефекат.[98]

Још један важан сигнал о војној и безбедносној важности сајбер простора појавио се унутар самог америчког безбедносног апарата кроз случај „Solar Sunrise“ 1998. године. Упади у системе Министарства одбране Сједињених Америчких Држава указали су на чињеницу да чак и најразвијенији војни системи могу бити изложени озбиљним сајбер претњама. Значај овог случаја није само у техничком аспекту напада, већ и у политичко-безбедносној поруци коју је произвео а то је да државе постају свесне да дигиталне мреже нису више само подршка војним структурама, већ и критична тачка њихове рањивости. Уједно, овај случај је јасно показао колико је проблематично питање атрибуције, јер је у сајбер простору често тешко поуздано утврдити ко стоји иза конкретне операције, са којом намером и у чије име. Управо ова комбинација мрежне рањивости, техничке сложености и политичке неодређености учинила је сајбер простор посебно осетљивим доменом безбедносне политике.[99]

Почетком новог века, државе постепено прелазе са ад хок реаговања на систематску институционализацију својих активности у сајбер простору. Дигитализација критичних инфраструктура — нарочито енергетских, телекомуникационих, финансијских и транспортних система — наметнула је потребу да се заштита мрежа и информационих ресурса интегрише у шири оквир националне безбедности. Уместо да се сајбер претње посматрају као изоловани технички инциденти, оне почињу да се третирају као потенцијални инструменти дестабилизације државе, нарушавања јавног поретка и слабљења политичке моћи. Тако се постепено развија и доктринарно разликовање између оперативног сајбер деловања, које подржава класичне војне операције, и стратешког сајбер деловања, које може бити усмерено на ширу политичку, економску и друштвену дестабилизацију противника.[100]

Сајбер простор у XXI веку добија још јаснији институционални статус у војним доктринама, не само држава већ и међународних организација. У савременој НАТО доктрини, сајбер операције се више не третирају као споредна техничка активност, већ као саставни део планирања, извођења и процене савезничких заједничких операција. Allied Joint Publication AJP-3.20 изричито дефинише сајбер операције као део НАТО оперативне архитектуре и истовремено препознаје и офанзивне сајбер операције као дејства у или кроз сајбер простор којима се пројектује моћ ради постизања војних циљева[101]. Овакво нормативно и доктринарно формулисање представља снажан показатељ да је сајбер простор прешао пут од техничке инфраструктуре до признатог домена савременог војног деловања. У тој трансформацији промене природе рата границе између мира и

[98] Dorothy E. Denning, “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy,” *NAPSNet Special Reports*, December 23, 2000.
[99] Federal Bureau of Investigation, memorandum to Director, FBI, “Solar Sunrise; CITAC Matters; OO: HQ,” February 20, 1998, National Security Archive.
[100] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), 69, 122, 146–147, 178–179.
[101] NATO Standardization Office, *Allied Joint Doctrine for Cyberspace Operations (AJP-3.20), Edition A, Version 1* (Brussels: NATO Standardization Office, 2020), xiii, Lex-3.

конфликта постају мање јасне, јер државе могу да остварују стратешке ефекте кроз сајбер средства и онда када не постоји формално проглашено ратно стање.[102]

Сајбер простор треба разумети као средину у којој се преплићу између осталог и шпијунажа, саботажа, информациони утицај, правна нејасноћа и демонстрација технолошке моћи, што државе ставља пред безбедносне изазове.

Развој интернета омогућио је настанак нових облика хибридног деловања чиме омогућавају државама да настоје да постигну политичке и стратегијске циљеве без директне употребе конвенционалне силе. Сајбер простор је отворио простор и за асиметричне актере, који, и без великих класичних ресурса, могу производити озбиљне безбедносне последице. Зато је разумевање историјског процеса у коме је интернет прешао пут од истраживачке мреже до средства државног надметања неопходно за разумевање савремених сајбер конфликата као и доктринарне институционализације сајбер операција у оквиру савремених војних савеза и националних стратегија.[103]

У теоријском и стратешком смислу почиње да се прави разлика између појмова „информационо ратовање“ и „сајбер ратовање“, при чему први обухвата шири спектар активности, укључујући психолошке операције и медијски утицај, док се други конкретније односи на техничке нападе и одбрану у оквиру рачунарских мрежа.[104] Ова терминолошка диференцијација допринела је прецизнијем дефинисању улоге сајбер простора у савременим конфликтима.

Искуства из 1990-их година директно су утицала на обликовање савремених сајбер стратегија показавши да дигитални простор може да буде и средство и мета у конфликтима. То је довело до интеграције сајбер капацитета у шире војне доктрине.[105] Истовремено, уочен је и проблем недовољно развијених правних оквира, као и тешкоћа у приписивању одговорности за сајбер нападе, посебно у случајевима када су у њима учествовали недржавни актери.[106]

2.2 Појмовно одређење сајбер простора

У савременој арени међународних односа, сајбер простор се профилисао као један од кључних домена у којем се преплићу безбедносни, политички и економски интереси држава. Сајбер безбедност, као његов неодвојиви сегмент, више не представља искључиво техничко питање, већ суштински елемент глобалне стабилности и националне безбедности. Развој информационо-комуникационих технологија довео је до дубоких трансформација савременог друштва, при чему су дигитални системи постали основ функционисања институција, тржишта и свакодневног живота појединаца.[107] Ова зависност од дигиталне инфраструктуре истовремено повећава

[102] NATO Standardization Office, *Allied Joint Doctrine for Cyberspace Operations (AJP-3.20), Edition A, Version 1* (Brussels: NATO Standardization Office, 2020), xiii, Lex-3.
[103] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), 178–179.
[104] Martin C. Libicki, *What Is Information Warfare?* (Washington, DC: National Defense University Press, 1995), 7–10.
[105] David T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: NDU Press, 2009), 32–34.
[106] Michael N. Schmitt, gen. ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 3–7, 9–11.
[107] Manuel Castells, *The Rise of the Network Society*, 2nd ed. (Oxford: Wiley-Blackwell, 2010), xviii–xix; 45.

ефикасност, али и рањивост савремених држава, што сајбер простор чини критичним безбедносним окружењем.[108]

Савремене државе све више напуштају искључиво традиционално схватање безбедности засновано на војној сили и територијалном интегритету, и у своје стратегије укључују дигиталну димензију као кључни елемент националне заштите.[109] Сајбер простор се у том контексту позиционира као инфраструктурна основа савременог друштва, али и као потенцијално бојиште у којем се одвијају различити облици конфликта. Посебно је значајно то што савремени конфликти све више попримају асиметричан карактер, где актери са ограниченим ресурсима могу изазвати значајне последице по технолошки развијене системе.[110] Овај феномен додатно усложњава постојеће безбедносне концепте и захтева нове приступе у области одбране и заштите.

Полазећи од теоријске перспективе Копенхашке школе, процес секјуритизације сајбер простора може се разумети као дискурзивни процес у којем политички актери одређене појаве дефинишу као егзистенцијалне претње, чиме оправдавају примену изузетних мера.[111]У том смислу, сајбер претње се све чешће представљају као ризици који захтевају хитну реакцију државе и мобилизацију ресурса. Ипак, из реалистичке перспективе, неопходно је нагласити да сајбер простор није само конструкција дискурса, већ и конкретно оперативно окружење у којем се реализују војне активности.[112] Ова двојна природа сајбер простора – као друштвене конструкције и материјалне инфраструктуре – чини га изузетно сложеним предметом анализе.

У том контексту, секјуритизација сајбер простора подразумева не само препознавање претњи, већ и институционалну трансформацију безбедносних система, укључујући развој нових организационих структура и оперативних капацитета.[113] Ове промене доводе до постепеног брисања граница између цивилног и војног сектора, јер се критична инфраструктура све више налази у домену приватних компанија.[114] Последично, државе су приморане да развијају нове моделе сарадње са приватним сектором, како би обезбедиле адекватан ниво заштите.[115]

Прогресивна милитаризација сајбер простора значајно утиче на природу савремених конфликата. За разлику од традиционалних облика ратовања, сајбер операције омогућавају деловање испод прага оружаног сукоба, што отежава њихово правно квалификовање и политичку интерпретацију.[116] Сајбер напади све чешће погађају критичну инфраструктуру, укључујући енергетске системе, телекомуникације и финансијске мреже, што може довести до озбиљних

[108] David T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 27–30.
[109] Joseph S. Nye Jr., *The Future of Power* (New York: PublicAffairs, 2011), 115–117.
[110] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), 95; 147–148.
[111] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (London: Routledge, 2008), 1–2; 11–12.
[112] David T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 28–30.
[113] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (London: Routledge, 2008), 52–54.
[114] James Andrew Lewis, *Cybersecurity and Critical Infrastructure Protection* (Washington, DC: Center for Strategic and International Studies, 2014), 14–16.
[115] Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World* (Santa Barbara, CA: Praeger, 2013), 102–104.
[116] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), 37–39.

поремећаја у функционисању државе.[117] Овакав развој указује на висок степен међузависности савремених система, где поремећај једног сегмента може изазвати ланчане ефекте у другим секторима.[118]

Посебан изазов у сајбер простору представља питање атрибуције, односно утврђивања одговорности за извршене нападе. Због специфичности дигиталног окружења, напади се често изводе путем посредничких система, што отежава идентификацију починиоца.[119] Овај проблем има значајне импликације на примену међународног права, јер је утврђивање одговорности кључно за легитимност евентуалног одговора.[120] Управо на ове изазове указује и *Tallinn Manual 2.0*, који анализира примену постојећих норми међународног права у сајбер простору и истиче њихова ограничења.[121]

У савременим стратешким документима, сајбер простор се све чешће дефинише као посебан домен ратовања. НАТО је, на пример, формално признао сајбер простор као оперативни домен, наглашавајући његов значај за колективну безбедност.[122] Овај приступ подразумева интеграцију сајбер капацитета у шире војне структуре и стратегије, чиме се додатно потврђује његов значај у савременим конфликтима.[123]

У оквиру овог комплексног окружења, информационо ратовање постаје важна компонента стратегија тзв. „паметне моћи“. Оно обухвата активности усмерене на контролу информација, утицај на јавно мњење и манипулацију дигиталним садржајима.[124] Са техничког становишта, сајбер операције могу остварити ефекте који су упоредиви са традиционалним војним дејствима, посебно када су усмерене на системе од стратешког значаја.[125]

Иако се понекад праве паралеле са нуклеарним оружјем, оваква поређења треба посматрати пре свега као аналитичке метафоре које указују на перцепцију сајбер претњи као високоризичних.[126] Ова перцепција има значајан утицај на процес секјуритизације и обликовање јавних политика у области безбедности.[127]

---

[117] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 67–69.
[118] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 70–72.
[119] Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013), 41–43.
[120] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), 39–41.
[121] Michael N. Schmitt, gen. ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 3–7.
[122] NATO Standardization Office, *Allied Joint Doctrine for Cyberspace Operations (AJP-3.20), Edition A, Version 1* (Brussels: NATO Standardization Office, 2020), xiii–xiv.
[123] NATO Standardization Office, *Allied Joint Doctrine for Cyberspace Operations (AJP-3.20), Edition A, Version 1* (Brussels: NATO Standardization Office, 2020), 1–3.
[124] John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica: RAND, 2001), 12–15.
[125] NATO Standardization Office, *Allied Joint Doctrine for Cyberspace Operations (AJP-3.20), Edition A, Version 1* (Brussels: NATO Standardization Office, 2020), 5–7.
[126] Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013), 89–91
[127] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (London: Routledge, 2008), 1–2, 11–12.

Појам сајбер простора има своје теоријске корене у радовима Норберта Винера, који је у оквиру кибернетике указао на значај комуникације и контроле као универзалних принципа.[128] Његове идеје поставиле су основу за разумевање повезаности техничких и друштвених система, што је касније омогућило развој концепта сајбер простора. Са појавом интернета, ове теоријске поставке добијају своју практичну примену, што доводи до формирања глобалног дигиталног окружења.[129]

Савремене дефиниције сајбер простора наглашавају његову мултидимензионалну природу, која обухвата технолошке, друштвене и политичке аспекте.[130] Управо ова комплексност чини сајбер простор једним од најзначајнијих домена савременог света, у којем се одвијају кључни процеси који обликују будућност међународних односа.

Иако је термин „сајбер простор“ своје порекло имао у научној фантастици и књижевности, веома брзо је преузет у академске, безбедносне и војне дискурсе. Разлог томе лежи у чињеници да је експанзија информационо-комуникационих технологија суштински изменила начин функционисања савремених друштава и држава. Сајбер простор се постепено трансформисао из апстрактног концепта у конкретан оперативни домен у којем се одвијају економске активности, политичке интеракције и безбедносни процеси.[131] Управо због те трансформације, јавила се потреба за његовим прецизним дефинисањем, посебно у контексту националне и међународне безбедности.

Једну од најутицајнијих дефиниција понудило је Министарство одбране Сједињених Америчких Држава, које сајбер простор одређује као глобално подручје унутар информационог окружења, састављено од међусобно повезаних информационих инфраструктура.[132] Ова инфраструктура обухвата интернет, телекомуникационе системе, рачунарске мреже, али и уграђене системе и контролере који управљају различитим техничким процесима. Овакво одређење указује на сложеност сајбер простора, који није ограничен само на виртуелну комуникацију, већ обухвата и физичке компоненте дигиталних система. Истовремено, оно наглашава његову међузависну природу, у којој поремећај једног сегмента може имати шире последице.

Са теоријског становишта, сајбер простор се може дефинисати као глобална мрежа дигиталних информационих система у којој се подаци креирају, обрађују и размењују у реалном времену.[133] Он представља виртуелну димензију насталу умрежавањем рачунара и других дигиталних уређаја, омогућавајући комуникацију, економске активности и друштвене интеракције без обзира на географске границе. За разлику од традиционалних простора, сајбер простор није физички ограничен, већ је динамичан и подложан сталним променама. Његово функционисање заснива се на комбинацији формалних правила и неформалних норми, што му даје висок степен

[128] Norbert Wiener, *Cybernetics: Or Control and Communication in the Animal and the Machine* (Cambridge, MA: MIT Press, 1948), 19–21
[129] Manuel Castells, *The Rise of the Network Society*, 2nd ed. (Oxford: Wiley-Blackwell, 2010), 45–47.
[130] David T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 27–30
[131] Ибид. 27–28.
[132] Joint Chiefs of Staff, *Joint Publication 3-12: Cyberspace Operations* (Washington, DC: Joint Chiefs of Staff, 2018), GL-4
[133] David T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 28–30.

флексибилности. Међутим, управо та флексибилност отвара простор за различите облике злоупотреба, укључујући сајбер криминал и сајбер нападе.[134]

Значајно је нагласити да сајбер простор није изоловано окружење, већ да је у тесној интеракцији са физичким светом, што значи да догађаји у дигиталном домену могу имати директне последице по реалне системе и инфраструктуру. Ова повезаност доводи до тога да се граница између виртуелног и физичког све више брише, што представља један од кључних изазова савременог безбедносног окружења.

Сајбер простор представља простор великих могућности, али и нову арену сукоба. Он омогућава технолошки напредак, глобалну повезаност и економски развој, али истовремено излаже државе и појединце бројним ризицима, укључујући сајбер шпијунажу, дезинформације и различите облике дигиталног криминала.[135] Недостатак јасно дефинисаног система глобалног управљања, као и његова прекогранична природа, отежавају примену закона и усаглашавање међународних норми.[136] Ово доводи до правних празнина и нејасноћа у погледу надлежности, што додатно компликује реаговање на сајбер претње.

У том контексту, све је израженија потреба за развојем међународних норми и правила која би регулисала понашање актера у сајбер простору.[137] Иницијативе попут извештаја Уједињених нација о понашању држава у сајбер простору указују на покушаје да се успостави минимални консензус о основним принципима, укључујући суверенитет, немешање и одговорност држава.[138]

Сличан приступ дефинисању сајбер простора може се уочити и у националним стратегијама, као што је стратегија сајбер безбедности Уједињеног Краљевства из 2011. године, где се он описује као интерактиван домен састављен од дигиталних мрежа које омогућавају складиштење, обраду и размену информација.[139] Ова дефиниција наглашава његову улогу у функционисању економије и јавних услуга, што указује на његов системски значај.

С друге стране, термин „сајбер простор“ популаризовао је књижевник Вилијам Гибсон, који га је описао као нефизички простор створен деловањем рачунарских система.[140] Иако је ова дефиниција настала у уметничком контексту, она је имала значајан утицај на касније теоријске и научне интерпретације.

---

[134] David T. Kuehl, “From Cyberspace to Cyberpower: Defining the Problem,” in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 27–30.

[135] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 67–69.

[136] UK Cabinet Office, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (London: Cabinet Office, 2011), 8–9.

[137] United Nations Institute for Disarmament Research, *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century* (Geneva: UNIDIR, 2015), 14–15.

[138] United Nations Institute for Disarmament Research, *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century* (Geneva: UNIDIR, 2015), 14–15.

[139] UK Cabinet Office, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (London: Cabinet Office, 2011), 11.

[140] David T. Kuehl, “From Cyberspace to Cyberpower: Defining the Problem,” in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 27–28.

Европска комисија приступа дефинисању сајбер простора на општији начин, наглашавајући његову виртуелну природу и улогу у циркулацији електронских података.[141] Са друге стране, Међународна организација за стандардизацију (ISO) даје свеобухватније одређење, наглашавајући интеракцију људи, софтвера и услуга у оквиру овог окружења.[142]

Савремени приступи све више истичу да сајбер простор треба посматрати као социо-технички систем, који обједињује технолошке компоненте и људске активности.[143] Ова перспектива омогућава боље разумевање сложених односа који се у њему одвијају, укључујући политичке, економске и безбедносне процесе.[144]

Сајбер простор се може разумети као мултидимензионално окружење које обухвата техничку инфраструктуру, информационе токове и друштвене интеракције. Управо ова комплексност чини га једним од кључних домена савременог света, у којем се све интензивније одвијају процеси који обликују међународне односе и безбедносну динамику.

Једна од основних карактеристика сајбер простора јесте његова динамичка природа, односно стална променљивост и временска зависност. Он обухвата огроман број међусобно повезаних система, уређаја и корисника који непрекидно размењују информације и међусобно делују. Управо ова константна интеракција чини сајбер простор изузетно сложеним и тешко предвидивим окружењем, у којем и мање промене могу произвести значајне последице. За разлику од традиционалних система, који функционишу у релативно стабилним условима, сајбер простор је подложан брзим трансформацијама, што захтева континуирано прилагођавање актера који у њему делују.[145]

Посебно важан аспект сајбер простора представља људски фактор, који има двоструку улогу – као корисник, али и као креатор овог окружења. Људске одлуке, понашање и ниво техничке писмености директно утичу на функционисање и безбедност дигиталних система.[146] Сајбер простор је, у суштини, вештачки конструисан домен који постоји захваљујући људској активности и интеракцији. Без активног учешћа људи, он не би имао ни функционалну ни друштвену вредност. У том смислу, може се закључити да је сајбер простор не само технолошки, већ и социо-технички систем, у којем су људски и технички елементи нераздвојно повезани.[147]

Поред тога, људски фактор представља и једну од најслабијих карика у систему сајбер безбедности, јер су многи сајбер напади засновани управо на манипулацији људским понашањем,

[141] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (Brussels: European Commission, 2013), 3–5.
[142] European Union Agency for Network and Information Security (ENISA), *Definition of Cybersecurity: Gaps and Overlaps in Standardisation*, version 1.0 (Heraklion: ENISA, 2015), 16.
[143] Manuel Castells, *The Rise of the Network Society*, 2nd ed. (Oxford: Wiley-Blackwell, 2010), 45–47.
[144] Joseph S. Nye Jr., *The Future of Power* (New York: PublicAffairs, 2011), 120–122.
[145] David T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 27–30.
[146] David T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 30–32.
[147] Manuel Castells, *The Rise of the Network Society*, 2nd ed. (Oxford: Wiley-Blackwell, 2010), 45–47.

као што су фишинг или социјални инжењеринг. Ово указује на то да техничка заштита сама по себи није довољна, већ да је неопходно развијати и свест и образовање корисника.

Одржавање и даљи развој сајбер инфраструктуре представљају кључни предуслов за функционисање овог домена. С обзиром на огроман број чворова, мрежа и система који га чине, управљање сајбер простором представља изузетно сложен задатак. Управо ова сложеност довела је до тога да се сајбер простор често описује као један од најкомплекснијих система савременог света[148]. Истовремено, његов даљи развој не зависи искључиво од технолошког напретка, већ и од нивоа одговорности свих актера који у њему учествују. Начини на које појединци, организације и државе користе сајбер простор директно утичу на његов будући развој и безбедност.

Савремене анализе указују да управљање сајбер простором подразумева мултиактерски приступ, у којем учествују државе, међународне организације и приватни сектор.[149] Овај модел управљања одражава сложену природу сајбер простора, али истовремено поставља и бројне изазове у погледу координације и усаглашавања интереса.[150] Сајбер простор данас има кључну улогу у функционисању савременог друштва, како у економском, тако и у безбедносном смислу. Његова важност огледа се у чињеници да представља основу за функционисање финансијских система, комуникација и других кључних друштвених процеса. Истовремено, он постаје све значајнији фактор у међународним односима, јер омогућава нове облике деловања и утицаја.

Развој науке и технологије током двадесетог века довео је до дубоких промена у свим сферама друштва, укључујући политику, економију и начин живота. Ове промене одразиле су се и на природу сукоба, који све више укључују и дигиталну димензију. Технологија више није искључиво средство напретка, већ и потенцијални извор ризика и нестабилности. Савремени облици ратовања све више се ослањају на сајбер капацитете, који омогућавају деловање без директне употребе физичке силе.[151] Стога се сајбер простор се све чешће посматра као пети домен ратовања, уз копно, море, ваздух и свемир, што је препознато и у савременим војним стратегијама.[152] Овај приступ указује на све већу интеграцију сајбер операција у традиционалне војне доктрине.[153]

Опасност од злоупотребе технологије представља један од највећих изазова савременог доба. Брз развој научних и технолошких достигнућа довео је до ситуације у којој потенцијал за деструктивну употребу технологије расте паралелно са њеним развојем. У том смислу, сајбер простор представља и ризик и прилику – он може бити средство конфликта, али и платформа за сарадњу и развој.

---

[148] David T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 27–30.

[149] NATO Standardization Office, *Allied Joint Doctrine for Cyberspace Operations (AJP-3.20), Edition A, Version 1* (Brussels: NATO Standardization Office, 2020), xiii–xiv.

[150] Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World* (Santa Barbara, CA: Praeger, 2013), 102–104.

[151] Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013), 18–20.

[152] NATO Standardization Office, *Allied Joint Doctrine for Cyberspace Operations (AJP-3.20), Edition A, Version 1* (Brussels: NATO Standardization Office, 2020), xiii–xiv.

[153] NATO Standardization Office, *Allied Joint Doctrine for Cyberspace Operations (AJP-3.20), Edition A, Version 1* (Brussels: NATO Standardization Office, 2020), xiii–xiv. 1- 3

Иницијативе на међународном нивоу све више наглашавају потребу за развојем заједничких правила понашања у сајбер простору, како би се смањили ризици од конфликта и обезбедила стабилност. Управо баланс између безбедности и отворености представља један од кључних изазова будућег развоја сајбер простора.

Сходно наведеном, сајбер простор се може посматрати као један од најзначајнијих феномена савременог доба, који истовремено обликује друштвене процесе, економске токове и безбедносну динамику. Његов значај ће у будућности наставити да расте, што захтева континуирано унапређење знања, политика и механизама управљања овим комплексним доменом.

2.3. Сајбер напади као средство угрожавања безбедности држава

До последње деценије двадесетог века, појам „сајбер напад“ није имао значајно место у политичком и безбедносном дискурсу. Разлог за то лежи у чињеници да информационе технологије још увек нису представљале кључну инфраструктуру функционисања држава, привреде и друштва. Са убрзаним развојем рачунарских мрежа и глобалном експанзијом интернета, створени су услови за појаву нових облика угрожавања безбедности.[154] Академска и стручна јавност користи различите термине како би описала упаде у информационе системе, укључујући појмове као што су сајбер напад, компјутерски напад, информационо ратовање и сајбер ратовање. Иако не постоји потпуно уједначена терминологија, суштина ових појава остаје иста – реч је о намерним активностима усмереним на нарушавање, ометање или уништавање информационих система и података.[155]

Развој информационих технологија, поред бројних предности, отворио је простор за нове облике угрожавања државног суверенитета. Савремене државе суочавају се са чињеницом да се претње више не испољавају искључиво у физичком простору, већ све више у дигиталном окружењу.[156] Сајбер напади су постали константа у међународним односима и савременим конфликтима, при чему се разликују по интензитету, обиму и последицама.[157] Док неки напади имају ограничене ефекте, други могу довести до системских поремећаја и дугорочних последица по функционисање државе.

Мотиви извршилаца сајбер напада су разноврсни и често међусобно испреплетени. Државе користе сајбер операције као средство остваривања стратешких циљева, често путем војних и обавештајних структура.[158] Истовремено, у циљу прикривања одговорности, оне могу деловати преко посредничких актера, као што су хакерске групе. Недржавни актери, укључујући криминалне организације и терористичке групе, такође активно користе сајбер простор ради

[154] Дејан Вулетић, „Сајбер безбедност,“ у *Интегрална безбедност Републике Србије*, ур. Б. Форца (Београд: Универзитет „Унион – Никола Тесла“, Факултет за пословне студије и право и Факултет за стратешки и оперативни менаџмент, 2017), 169–170.
[155] Ненад Путник, *Сајбер рат и сајбер мир* (Београд: Академска мисао и Иновациони центар Факултета безбедности Универзитета у Београду, 2022), 59–72.
[156] Дејан Вулетић, „Претње у сајбер простору и њихов утицај на савремену безбедност,“ у *Зборник радова са VI међународног научног скупа „Савремени изазови и пријетње безбједности“* (Бања Лука: Факултет безбједносних наука, 2026), 142–144.
[157] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 67–100; Вулетић, „Претње у сајбер простору,“ 142–145.
[158] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 19–27.

остваривања својих циљева, било да је реч о финансијској добити или ширењу страха и пропаганде.[159]

Сајбер напади представљају глобалну и наднационалну претњу која не познаје географске границе. Мете могу да буду државне институције, привредни субјекти, али и системи критичне инфраструктуре од значаја за функционисање друштва.[160] Напади усмерени на енергетске, финансијске и комуникационе системе могу имати далекосежне последице, укључујући дестабилизацију читавих држава. Овакав развој указује на висок степен зависности савремених друштава од дигиталних технологија.

Сајбер напади представљају специфичан облик савремених конфликата, који се значајно разликује од традиционалних облика ратовања. Они се често одвијају прикривено, без јасно утврђеног извршиоца, што отежава њихову правну квалификацију и политички одговор.[161] Ова карактеристика директно је повезана са једним од кључних проблема у области сајбер безбедности а то је проблем атрибуције.[162]

Проблем атрибуције представља један од највећих изазова у области сајбер безбедности, јер техничке могућности омогућавају прикривање идентитета нападача и коришћење посредничких система.[163] Атрибуција подразумева процес идентификације извршиоца напада, али и утврђивање његове повезаности са државним или недржавним актерима. У пракси, нападачи користе сложене технике прикривања, укључујући прокси сервере, ботнет мреже и лажне дигиталне трагове, чиме се значајно отежава утврђивање порекла напада.[164]

Поред техничких, атрибуција има и изражену политичку димензију. Државе често оклевају да јавно оптуже друге актере без чврстих и недвосмислених доказа, јер такве оптужбе могу имати озбиљне дипломатске последице.[165] Ово доводи до ситуације у којој чак и када постоје индиције о пореклу напада, изостаје формална реакција. Један од раних примера који илуструје овај проблем јесу сајбер напади на Естонију 2007. године, када је било тешко недвосмислено доказати државну умешаност упркос постојећим техничким индицијама.[166]

Државе негирају учешће у сајбер нападима чак и у случајевима када постоје индиректни докази.[167] Ова пракса додатно усложњава примену међународног права и смањује ефикасност механизама одвраћања. Управо због тога, проблем атрибуције остаје једно од централних питања у анализи сајбер напада и развоју безбедносних политика.[168]

---

[159] Вулетић, „Сајбер безбедност," 169–170; Singer and Friedman, *Cybersecurity and Cyberwar*, 88–118.
[160] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: National Institute of Standards and Technology, 2018), 1–3.
[161] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 79–100.
[162] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, nos. 1–2 (2015): 4–7.
[163] Rid and Buchanan, "Attributing Cyber Attacks," 4–10; Libicki, *Cyberdeterrence and Cyberwar*, 41–49.
[164] Вулетић, „Сајбер безбедност," 177–178.
[165] Rid and Buchanan, "Attributing Cyber Attacks," 24–31.
[166] NATO Strategic Communications Centre of Excellence, *2007 Cyber Attacks on Estonia* (Riga: NATO Strategic Communications Centre of Excellence, 2019), 10–11.
[167] NATO Strategic Communications Centre of Excellence, *2007 Cyber Attacks on Estonia*, 10–11, 18; J. K. Canfil, "The Illogic of Plausible Deniability: Why Proxy Conflict in Cyberspace May No Longer Pay," *Journal of Cybersecurity* 8, no. 1 (2022): 1–4.
[168] Schmitt, *Tallinn Manual 2.0*, 79–100; Rid and Buchanan, "Attributing Cyber Attacks," 31–37.

Сајбер простор и информационе технологије све више се интегришу у војне структуре и стратегије, што доводи до трансформације савремених конфликата.[169] Сајбер операције постају неизоставан елемент међудржавних сукоба, који обухватају различите облике деловања, од сајбер шпијунаже и саботаже до информационих операција. Терористичке организације користе интернет за регрутовање и координацију активности, док високотехнолошки криминал постаје све значајнији фактор угрожавања безбедности.

Посебно опасан облик сајбер напада представљају напади на критичну инфраструктуру, који могу имати директне последице по функционисање државе и друштва. У том контексту, сајбер напади се све више посматрају као средство пројекције моћи, које омогућава државама да остваре своје циљеве без директне употребе војне силе.[170]

Као илустрација сложености савремених сајбер напада, често се наводи случај „SolarWinds“ из 2020. године, који је представљао један од најсофистицираних напада на институције Сједињених Америчких Држава. Нападачи су компромитовали софтверску компанију и путем ажурирања њеног система омогућили приступ великом броју државних агенција и приватних компанија.[171] Иако су истраге указивале на умешаност страних актера, процес атрибуције био је сложен и дуготрајан, што додатно потврђује изазове са којима се савремене државе суочавају у сајбер простору. Сложеност, динамика и потенцијалне последице сајбер претњи захтевају развој свеобухватних стратегија заштите и међународне сарадње, како би се обезбедила стабилност и безбедност у дигиталном окружењу.

2.4 Облици и последице сајбер напада у савременом безбедносном окружењу

Сајбер напади представљају намерне и плански осмишљене активности усмерене на нарушавање поверљивости, интегритета или доступности дигиталних система, мрежа и података.[172] У стручној литератури ова три елемента позната су као основни принципи информационе безбедности, који представљају темељ заштите савремених информационих система.[173] Сајбер напади се реализују применом различитих техника и алата, укључујући злонамерни софтвер, фишинг кампање, рансомвер нападе, нападе ускраћивањем услуге (DoS/DDoS), као и неовлашћене упаде у рачунарске системе. Развој ових метода прати и континуирана еволуција нападача, који своје технике прилагођавају све сложенијим безбедносним механизмима.[174]

Сајбер нападе могу изводити различити актери, од појединаца до организованих криминалних група, хактивиста и актера повезаних са државама.[175] Посебну забринутост изазива чињеница да

[169] Путник, *Сајбер рат и сајбер мир*, 42–57; Joseph S. Nye Jr., *Cyber Power* (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010), 3–5.
[170] Nye, *Cyber Power*, 3–4; National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, 1–3.
[171] U.S. Government Accountability Office, *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents*, GAO-22-104746 (Washington, DC: U.S. Government Accountability Office, 2022), 2, 42–43; SolarWinds, "An Investigative Update of the Cyberattack," May 7, 2021; Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, and National Security Agency, "Russian Foreign Intelligence Service Exploiting Five Publicly Known Vulnerabilities to Compromise U.S. and Allied Networks," April 15, 2021.
[172] Michael Nieles, Kelley Dempsey, and Victoria Yan Pillitteri, *An Introduction to Information Security*, NIST Special Publication 800-12 Revision 1 (Gaithersburg, MD: National Institute of Standards and Technology, 2017), 2–3.
[173] Ибид.
[174] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2024* (Athens: European Union Agency for Cybersecurity, 2024), 4, 7, 45–46, 56–63, 78–79.
[175] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2024*, 4, 20–33.

се границе између криминалних, политички мотивисаних и војних активности све више бришу, што додатно усложњава њихову класификацију и одговор на њих. У пракси, исти напад може имати више мотива – економски, политички или стратешки – што указује на комплексност савременог сајбер окружења.

Савремени сајбер напади све чешће имају карактер „вишеслојних операција“, у којима се комбинују техничке технике са психолошким и информационим утицајем, што значајно повећава њихову ефикасност.[176] Овакав приступ омогућава нападачима да истовремено угрозе техничке системе и поверење јавности, што може имати дугорочне друштвене последице.[177]

Последице сајбер напада могу бити вишеструке и обухватају прекид рада кључних служби, крађу осетљивих података, финансијске губитке, као и саботажу критичне инфраструктуре.[178] Управо због тога, сајбер напади се све више препознају као једна од најзначајнијих претњи савременог дигиталног доба. Учесталост и растућа софистицираност ових напада представљају озбиљан изазов за глобалну безбедност и економску стабилност.[179] Савремена друштва у великој мери зависе од информационо-комуникационих технологија, што повећава њихову изложеност ризицима.

Потенцијални утицај сајбер напада на критичну инфраструктуру, као што су енергетски системи, финансијске институције и комуникационе мреже, је све израженији.[180] Напади на ове системе могу довести до поремећаја у функционисању државе, али и до ширих економских и друштвених последица. У том контексту, сајбер напади се све више посматрају као средство угрожавања националне безбедности.

Додатни изазов представља чињеница да сајбер напади могу имати индиректне последице, које се испољавају кроз губитак поверења у институције и дигиталне системе.[181] Овај аспект сајбер безбедности често је занемарен, иако има значајан утицај на стабилност друштва.[182]

Анонимност сајбер простора значајно отежава идентификацију починилаца и утврђивање одговорности, што представља један од кључних проблема у области сајбер безбедности.[183] Недовољно развијени механизми атрибуције често успоравају или онемогућавају адекватан институционални одговор. Због тога се све више указује на потребу напуштања искључиво

[176] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2024*, 91–95; Дејан Вулетић, „Претње у сајбер простору и њихов утицај на савремену безбедност,“ у *Зборник радова са VI међународног научног скупа „Савремени изазови и пријетње безбједности“* (Бања Лука: Факултет безбједносних наука, 2026), 146.
[177] Ryan Shandler and Miguel Alberto Gomez, “The Hidden Threat of Cyber-Attacks—Undermining Public Confidence in Government,” *Journal of Information Technology & Politics* 20, no. 4 (2023): 359–361.
[178] Вулетић, „Претње у сајбер простору,“ 146–147; European Union Agency for Cybersecurity, *ENISA Threat Landscape 2024*, 4–7.
[179] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2024*, 4–7; Вулетић, „Претње у сајбер простору,“ 146–148.
[180] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, NIST CSWP 29 (Gaithersburg, MD: National Institute of Standards and Technology, 2024), 1, 18–24; Вулетић, „Претње у сајбер простору,“ 144–147.
[181] Shandler and Gomez, “The Hidden Threat of Cyber-Attacks,” 359–361, 369–370
[182] Ибид, 369-370
[183] Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” *Journal of Strategic Studies* 38, nos. 1–2 (2015): 4–10, 24–31; Вулетић, „Претње у сајбер простору,“ 147–148.

реактивних приступа и преласка на проактивне стратегије, које подразумевају превенцију, рано откривање претњи и међународну сарадњу.[184]

Граница између различитих врста нелегалних активности у сајбер простору често је веома нејасна. Сајбер шпијунажа, криминал и ратовање могу се међусобно преплитати, што отежава њихову правну квалификацију и адекватан одговор држава.[185] Ова комплексност указује на потребу развоја нових правних и институционалних оквира који би могли да одговоре на изазове савременог сајбер окружења.

Сајбер простор је постао нераскидиви део глобалне и националне економије, при чему савремено пословање у великој мери зависи од дигиталних технологија.[186] Ова зависност истовремено повећава рањивост економских система, јер поремећаји у функционисању сајбер простора могу довести до значајних финансијских губитака и економске нестабилности.

Информациона безбедност представља један од кључних елемената националне безбедности у савременом свету. Она подразумева заштиту информација и информационих система од неовлашћеног приступа, злоупотребе и уништења.[187] Основни циљ информационе безбедности јесте очување поверљивости, интегритета и доступности података, што представља темељ функционисања савремених безбедносних система.

У савременом окружењу, угрожавање информационе безбедности потиче од различитих фактора, укључујући злоупотребу технологија, развој злонамерног софтвера и растући обим сајбер криминала.[188] Сајбер шпијунажа представља сталну претњу државама и компанијама, док злоупотреба личних података угрожава приватност и безбедност појединаца. Ови изазови указују на потребу континуираног унапређења механизама заштите и развоја свеобухватних стратегија сајбер безбедности.

2.5 Интернет, рањивост држава и потреба за нормативним уређењем сајбер простора

Интернет је током последњих деценија прерастао у глобални феномен који је, у различитим облицима и са различитим нивоом приступа, постао доступан готово свим савременим друштвима. Његова отвореност, децентрализованост и технолошка флексибилност истовремено представљају и његову највећу предност и један од најозбиљнијих извора безбедносног ризика.[189] Из перспективе државне безбедности, ова двострука природа интернета значи да готово сваки корисник, институција или систем може постати потенцијална мета злоупотребе. Поједине

[184] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, 3–5, 19–24; Alex Nelson, Sanjay Rekhi, Murugiah Souppaya, and Karen Scarfone, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*, NIST Special Publication 800-61 Revision 3 (Gaithersburg, MD: National Institute of Standards and Technology, 2025), 1–6.
[185] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 67–118; Ненад Путник, *Сајбер рат и сајбер мир* (Београд: Академска мисао и Иновациони центар Факултета безбедности Универзитета у Београду, 2022), 59–72.
[186] Nieles, Dempsey, and Pillitteri, *An Introduction to Information Security*, 1–4; Дејан Вулетић, „Сајбер безбедност," у *Интегрална безбедност Републике Србије*, ур. Б. Форца (Београд: Универзитет „Унион – Никола Тесла", Факултет за пословне студије и право и Факултет за стратешки и оперативни менаџмент, 2017), 169–170.
[187] Nieles, Dempsey, and Pillitteri, *An Introduction to Information Security*, 2–3.
[188] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2024*, 4, 45–63, 78–79; Вулетић, „Сајбер безбедност," 172–178.
[189] Joseph S. Nye Jr., *Cyber Power* (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010), 2–4.

државе су ову чињеницу препознале релативно рано, због чега су информациону безбедност почеле да третирају као област упоредиву по значају са војном, економском и политичком безбедношћу.[190] Као последица таквог приступа, постепено су усвајани закони, стратегије и институционални механизми чији је циљ био јачање отпорности државе у сајбер простору. Развијани су и људски, технички и организациони капацитети неопходни за превенцију, откривање и одговор на сајбер претње.[191] Све то указује да информациона безбедност више не представља споредно техничко питање, већ један од темељних стубова функционисања савремене државе.

Као глобална комуникациона и информациона инфраструктура, интернет истовремено ствара нове могућности и производи све сложеније ризике по безбедност државе. Што је већи степен умрежености и зависности од информационо-комуникационих технологија, то се више умножавају и рањивости савремених државних система. Кључни сегменти јавне управе, безбедносног сектора, финансијског система, привреде и јавних услуга данас су повезани у јединствене дигиталне токове, при чему њихова функционална међузависност повећава и њихову укупну осетљивост.[192] Та међузависност доноси већу ефикасност, брже доношење одлука и бољу координацију, али истовремено ствара могућност да поремећај у једном делу система произведе последице у читавом институционалном ланцу. Посебно су осетљиви они делови инфраструктуре који се ослањају на сложене, централизоване и аутоматизоване дигиталне системе. На тај начин, дигитална трансформација не мења само начин функционисања државе, већ и саму природу безбедносне парадигме у којој она делује.[193]

Ова појава посебно долази до изражаја у области виталних и критичних инфраструктура, које су у све већој мери компјутеризоване, аутоматизоване и ослоњене на мреже за пренос и обраду података. Озбиљно ометање или компромитовање рачунарских система и мрежа у овим секторима не представља искључиво технички проблем, већ безбедносни изазов са снажним политичким, економским и друштвеним импликацијама.[194] Напади усмерени на критичну информациону инфраструктуру могу довести до прекида рада система, измене њихових функција, губитка контроле над појединим процесима и ширих поремећаја у друштву. Последице таквих напада могу обухватити материјалну штету, велике финансијске губитке, поремећаје у снабдевању, угрожавање јавне безбедности и дуготрајну дестабилизацију институционалног поретка.[195] Потенцијалне мете таквих напада нису само владине и војне мреже, већ и телекомуникациони системи, навигациони системи у саобраћају, системи за водоснабдевање, енергетске мреже, банкарски системи и друге функције од виталног значаја за друштво. Управо

[190] Дејан Вулетић, „Сајбер безбедност," у *Интегрална безбедност Републике Србије*, ур. Б. Форца (Београд: Универзитет „Унион – Никола Тесла", Факултет за пословне студије и право и Факултет за стратешки и оперативни менаџмент, 2017), 169–170.
[191] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, NIST CSWP 29 (Gaithersburg, MD: National Institute of Standards and Technology, 2024), 2–5.
[192] Michael Nieles, Kelley Dempsey, and Victoria Yan Pillitteri, *An Introduction to Information Security*, NIST Special Publication 800-12 Revision 1 (Gaithersburg, MD: National Institute of Standards and Technology, 2017), 8–9.
[193] Дејан Вулетић, „Претње у сајбер простору и њихов утицај на савремену безбедност," у *Зборник радова са VI међународног научног скупа „Савремени изазови и пријетње безбједности"* (Бања Лука: Факултет безбједносних наука, 2026), 142–145.
[194] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: National Institute of Standards and Technology, 2018), 1–3.
[195] Вулетић, „Претње у сајбер простору," 146–148; National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, 1–3.

због тога, питање заштите критичне инфраструктуре заузима централно место у националним стратегијама сајбер безбедности.

Приликом анализе утицаја сајбер простора на безбедност државе и друштва, неопходно је јасно разликовати појмове као што су сајбер криминал, сајбер шпијунажа, сајбер тероризам и сајбер ратовање. Иако се све ове појаве могу испољити кроз сличне техничке облике деловања, њихова правна природа, политичка тежина и безбедносне последице нису истоветне.[196] Границе између њих у пракси су често флуидне, а понекад и намерно замагљене, што отежава квалификацију конкретног догађаја и избор одговарајућег механизма реаговања. За њихово прецизније одређење од пресудне су важности намера извршиоца, карактер мете, начин извршења и обим последица које је напад произвео. Управо комбинација мотива, средстава и ефеката представља основу за њихово правно, политичко и стратешко тумачење. Оваква анализа је посебно важна у случајевима када државе настоје да утврде да ли је реч о криминалном делу, обавештајној активности, терористичком акту или облику непријатељског дејства које може имати и елементе сајбер ратовања.[197]

Сајбер напади представљају специфичан и релативно нов облик вођења сукоба, чија примена у међународним односима бележи сталан раст. Њихова природа се битно разликује од традиционалних облика ратовања, како по средствима, тако и по домену у којем се одвијају. Сајбер простор, информационе технологије и рачунарски капацитети све интензивније се користе у војне и безбедносне сврхе, укључујући и међудржавне конфликте.[198] Ови сукоби могу попримити различите облике — од дезинформационих и пропагандних кампања, преко дефејсинга веб-сајтова и крађе поверљивих података, до сајбер шпијунаже и директног дејства на информационе системе од војног значаја. У екстремним случајевима, овакве активности могу створити услове за озбиљне поремећаје у функционисању инфраструктуре и државних механизама, што сајбер тероризму и сајбер саботажи даје посебно опасну димензију. На тај начин, сајбер простор постаје не само средство утицаја, већ и оперативно окружење у којем се испољава савремена моћ држава и других актера.

Сајбер простор је данас неодвојив од функционисања глобалне и националне економије. Државе се у све већој мери ослањају на информационо-комуникационе технологије, што истовремено повећава њихову изложеност сајбер претњама. Та зависност не погађа искључиво државне институције, већ и привреду, финансијска тржишта, логистику и свакодневно функционисање друштва.[199] Док су у ранијим фазама дигиталног развоја нападе углавном изводили појединци или мање неформалне групе, савремени сајбер простор карактерише деловање знатно сложенијих и боље организованих актера. Развој дигиталних алата, комерцијализација злонамерних услуга и појава „cybercrime-as-a-service“ модела додатно су повећали обим и опасност ових претњи.[200] Сајбер нападе као средство деловања користе не само криминалне мреже, већ и безбедносни

[196] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 67–118; Ненад Путник, *Сајбер рат и сајбер мир* (Београд: Академска мисао и Иновациони центар Факултета безбедности Универзитета у Београду, 2022), 59–72.
[197] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 79–100; Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” *Journal of Strategic Studies* 38, nos. 1–2 (2015): 4–10, 24–31.
[198] NATO, *Warsaw Summit Communiqué*, July 9, 2016, para. 70; Путник, *Сајбер рат и сајбер мир*, 42–57.
[199] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 1–5, 19–27.
[200] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2024* (Athens: European Union Agency for Cybersecurity, 2024), 20–33, 45–46.

апарати и оружане снаге бројних држава, што овом проблему даје изразито геополитичку димензију.

Савремене војске и безбедносне институције улажу значајна финансијска средства у научноистраживачки и технолошки развој у области сајбер способности. Истовремено, организовани криминал и екстремистичке групе све интензивније користе предности интернета за остваривање сопствених циљева, укључујући прикривање идентитета, координацију активности и приступ осетљивим системима.[201] Ова паралелна еволуција државних и недржавних капацитета изазива посебну забринутост, јер се последице злоупотребе сајбер простора могу испољити брзо, тешко предвидиво и у широком распону интензитета. Због тога је основано очекивати да ће учесталост и интензитет сајбер претњи у будућности наставити да расту. Ако се сајбер простор посматра као ново глобално економско и безбедносно поље деловања, онда је неопходно јасније одредити шта представља прихватљиво понашање, а шта недозвољено дејство.[202] Посебан проблем представља чињеница да слабости и рањивости једне државе, због међународне природе интернета, могу произвести последице и по друге актере широм света. Недостатак ефикасних националних регулаторних оквира у појединим државама додатно доприноси стварању такозваних „виртуелних уточишта“ за незаконите активности.

У области сајбер безбедности и даље постоји изражен недостатак општеприхваћених појмова, стандарда и концепата, како на националном, тако и на међународном нивоу. Ова нормативна и концептуална неуједначеност може имати озбиљне последице, посебно ако се има у виду да су поједине велике силе у својим стратешким и војним документима предвиделе могућност одговора на одређене сајбер нападе и средствима која превазилазе искључиво дигитални домен.[203] Кључну улогу у доношењу таквих одлука имаће обим, карактер и последице напада. Иако је велики број држава усвојио стратегије, законе и програме у вези са сајбер простором, то још увек није довољно за ефикасно управљање овим доменом на глобалном нивоу. На међународном плану већ дуго постоје иницијативе за формулисање заједничких правила под окриљем Уједињених нација и других форума, како би се државама понудиле опште смернице за понашање у сајбер простору.[204] Као и копно, море, ваздух и свемир, и сајбер простор захтева координацију, сарадњу и применљиве правне механизме.

Неопходност међународне сарадње и партнерства између држава, као и између јавног и приватног сектора, у области сајбер безбедности данас је неспорна. Та сарадња подразумева политичку вољу, институционалну координацију, размену информација и дугорочну економску посвећеност свих релевантних актера. Заједнички и међународно прихваћен нормативни оквир могао би

[201] Вулетић, „Сајбер безбедност,“ 172–178; European Union Agency for Cybersecurity, *ENISA Threat Landscape 2024*, 20–33.
[202] Council of Europe, *Convention on Cybercrime*, ETS No. 185 (Budapest, November 23, 2001), preamble, arts. 2–11, 23–35.
[203] The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, 2011), 14; The White House, *National Cybersecurity Strategy* (Washington, DC: The White House, 2023), 14; NATO, *Warsaw Summit Communiqué*, para. 70; Schmitt, *Tallinn Manual 2.0*, 328–356.
[204] United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, July 22, 2015, paras. 24–28, 55–58; United Nations General Assembly, *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report*, A/75/816, March 18, 2021, paras. 7, 34, 80.

значајно да допринесе смањењу рањивости, претњи и ризика на прихватљив ниво.[205] Истовремено, ефикасна сарадња не зависи само од формалних споразума, већ и од изградње поверења, развоја капацитета и усклађивања процедура реаговања на инциденте. Управо због тога, сајбер безбедност све више постаје питање заједничке одговорности, а не искључиво унутрашње надлежности појединачних држава.

Паралелно са развојем глобалне рачунарске мреже, еволуирале су и претње које у њој настају и делују. Оно што су некада били релативно једноставни дигитални поремећаји, временом је прерасло у сложене безбедносне изазове са којима се суочавају државе, институције и друштва широм света. Црви, вируси и други облици злонамерног кода током времена су прешли пут од техничких аномалија до средстава која могу угрозити националну безбедност и стабилност читавих система.[206] За разлику од традиционалних облика демонстрације војне моћи, сајбер простор не омогућава визуелну пројекцију силе на начин на који то чине војне параде, вежбе или приказивање конвенционалног наоружања. Дигитална моћ није лако уочљива, није опипљива и не може се једноставно представити јавности као физички симбол одвраћања. Ипак, одсуство видљивог спектакла ни на који начин не умањује њен разорни потенцијал. Напротив, управо невидљивост, тешка детектабилност и могућност прикривеног дејства чине сајбер оружје изузетно опасним средством савремених конфликата. Постоји широк спектар програма, алата и техника које нападачи могу развити или прилагодити ради извршења различитих облика штетних активности, што додатно повећава сложеност одбране у овом домену.[207]

2.6 Основни принципи безбедности информационих система и технике сајбер напада

Безбедност информационих система традиционално се заснива на три кључна принципа: поверљивости, интегритету и доступности, који заједно чине основу савремених концепата информационе безбедности.[208] Поверљивост подразумева да осетљивим подацима могу приступити искључиво овлашћени корисници, чиме се спречава неовлашћено откривање информација.[209] Интегритет се односи на заштиту података и система од неовлашћених измена, обезбеђујући да су информације тачне, поуздане и непромењене осим у случајевима када је измена извршена на легитиман начин.[210] Доступност, као трећи стуб, подразумева да су системи и подаци доступни овлашћеним корисницима у тренутку када су им потребни.[211]

Ова три принципа чине основу свих безбедносних политика и механизама заштите, али истовремено представљају и главне мете сајбер напада. Савремени напади су често усмерени на нарушавање једног или више ових елемената, што може довести до озбиљних последица по

[205] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, arts. 7, 11–14, 21, 23; National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, 2–5.
[206] Вулетић, „Сајбер безбедност," 172–178; European Union Agency for Cybersecurity, *ENISA Threat Landscape 2024*, 45–63, 78–79.
[207] Singer and Friedman, *Cybersecurity and Cyberwar*, 67–118; Libicki, *Cyberdeterrence and Cyberwar*, 41–49; Путник, *Сајбер рат и сајбер мир*, 42–57.
[208] Michael Nieles, Kelley Dempsey, and Victoria Yan Pillitteri, *An Introduction to Information Security*, NIST Special Publication 800-12 Revision 1 (Gaithersburg, MD: National Institute of Standards and Technology, 2017), 2–3.
[209] Nieles, Dempsey, and Pillitteri, *An Introduction to Information Security*, 2–3.
[210] Ибид, 2-3
[211] Ибид, 2-3

функционисање информационих система.[212] Да би до напада дошло, неопходно је постојање одређене рањивости у систему, било да је реч о техничком пропусту, лошој конфигурацији или људској грешци.[213]

У том контексту, посебан значај имају алати или технике којима се искоришћавају постојеће слабости у систему ради стицања неовлашћеног приступа, ескалације привилегија или онемогућавања рада система.[214] Након откривања рањивости, произвођачи софтвера настоје да развију и примене безбедносне закрпе, али у периоду између откривања и исправке постоји простор за злоупотребу. У случајевима када нападач искористи рањивост пре него што она буде јавно позната или исправљена, говори се о „zero-day“ нападима, који представљају један од најопаснијих облика сајбер претњи.[215]

Сајбер напади се реализују кроз широк спектар техника, од којих су неке усмерене на ометање рада система, а друге на неовлашћени приступ или крађу података. Једна од најраспрострањенијих техника јесте напад ускраћивањем услуге (Denial of Service – DoS), чији је циљ нарушавање доступности система.[216] Ови напади се заснивају на преоптерећењу ресурса система, чиме се онемогућава приступ легитимним корисницима. Када се овакви напади изводе истовремено са више уређаја, говори се о дистрибуираним нападима (DDoS), који представљају знатно већи изазов за одбрану.[217]

За извођење DDoS напада често се користе ботнет мреже, односно групе компромитованих уређаја који делују под контролом нападача.[218] Ове мреже могу обухватати хиљаде или чак милионе уређаја, укључујући рачунаре, сервере и IoT уређаје, што нападачима омогућава да генеришу огроман обим саобраћаја и изазову озбиљне поремећаје у раду система.[219] Посебно опасан облик представљају перзистентни DoS напади (PDoS), који могу довести до трајног оштећења хардвера и захтевају физичку замену компоненти.

Међу техникама усмереним на компромитовање приступа систему издвајају се brute-force напади, који се заснивају на систематском испробавању великог броја комбинација лозинки и

[212] Richard Kissel, ed., *Glossary of Key Information Security Terms*, NIST Interagency Report 7298 Revision 2 (Gaithersburg, MD: National Institute of Standards and Technology, 2013), s.v. “confidentiality,” “integrity,” and “availability”; Nieles, Dempsey, and Pillitteri, *An Introduction to Information Security*, 2–6.
[213] National Institute of Standards and Technology, Computer Security Resource Center Glossary, s.v. “vulnerability,” accessed May 13, 2026; Karen Scarfone, Murugiah Souppaya, Amanda Cody, and Angela Orebaugh, *Technical Guide to Information Security Testing and Assessment*, NIST Special Publication 800-115 (Gaithersburg, MD: National Institute of Standards and Technology, 2008), 2-2.
[214] National Institute of Standards and Technology, Computer Security Resource Center Glossary, s.v. “exploit,” May 13, 2026.
[215] National Institute of Standards and Technology, Computer Security Resource Center Glossary, s.v. “zero day attack,” accessed May 13, 2026; European Union Agency for Cybersecurity, *ENISA Threat Landscape 2024* (Athens: European Union Agency for Cybersecurity, 2024), 78–79.
[216] National Institute of Standards and Technology, Computer Security Resource Center Glossary, s.v. “denial of service,” 2026; Cybersecurity and Infrastructure Security Agency, “Understanding Denial-of-Service Attacks,” February 1, 2021.
[217] Cybersecurity and Infrastructure Security Agency, *Understanding and Responding to Distributed Denial-of-Service Attacks* (Washington, DC: Cybersecurity and Infrastructure Security Agency, March 21, 2024),
[218] National Institute of Standards and Technology, Computer Security Resource Center Glossary, s.v. “botnet,” accessed May 13, 2026; Cybersecurity and Infrastructure Security Agency, *Understanding and Responding to Distributed Denial-of-Service Attacks*, 1–2.
[219] Stanislav Abaimov, “Understanding and Classifying Permanent Denial-of-Service Attacks,” *Journal of Cybersecurity and Privacy* 4, no. 2 (2024): 324–339.

корисничких имена.[220] Иако технички једноставни, ови напади могу бити веома ефикасни уколико системи не поседују адекватне механизме заштите. Слично томе, spoofing напади подразумевају лажно представљање нападача ради стицања поверења жртве или прикривања идентитета.

Фишинг напади представљају комбинацију техничких метода и социјалног инжењеринга, при чему нападач настоји да превари корисника и наведе га да открије осетљиве податке.[221] Ови напади се често реализују путем лажних веб-страница које имитирају легитимне сервисе. Поред тога, напади као што су buffer overflow, code injection и SQL injection користе пропусте у програмском коду како би омогућили извршавање злонамерних инструкција у систему.

За припрему и извођење напада користе се различити алати, укључујући програме за пресретање мрежног саобраћаја (sniffer), алате за разбијање лозинки (password crackers) и скенере рањивости.[222] Ови алати омогућавају нападачима да идентификују слабости у систему и искористе их за даље деловање.

Посебну улогу у сајбер нападима има злонамерни софтвер (malware), који представља један од најчешћих инструмената компромитовања система. Малвер обухвата различите типове софтвера, укључујући вирусе, тројанце, црве, backdoor програме и rootkit-ове.[223] Вируси се везују за друге програме и шире се њиховим извршавањем, док црви имају способност самосталног ширења преко мреже. Тројански програми се представљају као легитимни софтвер, али у позадини извршавају злонамерне активности. Backdoor механизми омогућавају нападачима трајан приступ систему, док rootkit-ови омогућавају прикривање присуства нападача унутар система.

Савремени малвер све чешће користи напредне технике прикривања, као што су енкрипција и полиморфизам, што значајно отежава његову детекцију и анализу.[224] Овакав развој указује на континуирану еволуцију сајбер претњи и потребу за унапређењем одбрамбених механизама.[225]

Највећи степен деструктивности у сајбер простору постиже се комбиновањем више различитих техника и алата, што омогућава нападачима да истовремено делују на више нивоа система. Ова комплексност значајно отежава детекцију, анализу и одбрану од напада, јер захтева интегрисан

[220] Scarfone et al., *Technical Guide to Information Security Testing and Assessment*, 5-1–5-3; National Institute of Standards and Technology, *Digital Identity Guidelines: Authentication and Lifecycle Management*, NIST Special Publication 800-63B (Gaithersburg, MD: National Institute of Standards and Technology, 2017), sec. 5.2.2.
[221] Cybersecurity and Infrastructure Security Agency, "Avoiding Social Engineering and Phishing Attacks," February 1, 2021; European Union Agency for Cybersecurity, *ENISA Threat Landscape 2024*, 56–63.
[222] OWASP Foundation, "Buffer Overflow Attack," accessed May 13, 2026; OWASP Foundation, "A03:2021 – Injection," 2026.
[223] Scarfone et al., *Technical Guide to Information Security Testing and Assessment*, 2-2, 5-1; Karen Scarfone, Wayne Jansen, and Miles Tracy, *Guide to General Server Security*, NIST Special Publication 800-123 (Gaithersburg, MD: National Institute of Standards and Technology, 2008), 6-8–6-9.
[224] Murugiah Souppaya and Karen Scarfone, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, NIST Special Publication 800-83 Revision 1 (Gaithersburg, MD: National Institute of Standards and Technology, 2013), 4-1–4-4.
[225] Souppaya and Scarfone, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, 4-4–4-6; European Union Agency for Cybersecurity, *ENISA Threat Landscape 2024*, 45–63, 78–79.

приступ који укључује техничке, организационе и стратешке мере.[226] Управо због тога, сајбер напади представљају један од најизазовнијих безбедносних феномена савременог доба.

2.7 Најчешћи облици илегалних активности у сајбер простору

Као што је истакнуто у претходним редовима, сајбер простор не може више да се посматра као искључиво технолошка инфраструктура, односно као скуп рачунара, мрежа, сервера, софтвера и комуникационих канала, Сајбер простор је последњих деценија еволуирао у посебан друштвени, економски, правни и безбедносни амбијент. Његова специфичност огледа се у томе што омогућава истовремено комуникацију, размену података, политичко деловање, економске трансакције, приступ јавним услугама и складиштење огромне количине личних, пословних и државних информација.

Уз све предности које је сајбер простор створио, нажалост, због своје специфичности, постао је и простор нелегитимних друштвених активности. У преамбули Конвенције о високотехнолошком криминалу Савет Европе је указао на „дубоке промене“ које су настале дигитализацијом, конвергенцијом и глобализацијом рачунарских мрежа, као и на ризик да се рачунарске мреже и електронске информације користе у све већој мери за извршење кривичних дела.[227]

У сајбер простору се класични облици криминалитета не губе, већ добијају нове техничке облике, већи број потенцијалних жртава, већу брзину извршења и израженији прекогранични карактер. Превара, уцена, изнуда, крађа идентитета, неовлашћено присвајање туђе имовине, повреда приватности, незаконито објављивање садржаја или повреда права интелектуалне својине нису настали са интернетом, али су у дигиталном окружењу добили нове механизме извршења.[228] Уместо физичког контакта са жртвом, извршилац може да делује путем електронске поште, злонамерног софтвера, лажне интернет странице, компромитованог налога, друштвене мреже или апликације за комуникацију. Ово је посебан простор у коме се мењају начин извршења, начин прикривања, начин доказивања и обим последица кривичних дела.

Поред трансформације традиционалних кривичних дела, у сајбер простору настају и облици противправног деловања који не би могли да постоје без самих информационо-комуникационих технологија. То су, на пример, неовлашћени приступ заштићеном рачунарском систему, уношење и ширење рачунарских вируса, рачунарска саботажа, ометање рада информационог система, неовлашћено пресретање рачунарских података, злоупотреба лозинки и приступних кодова, као и прављење, набављање или давање средстава намењених за извршење кривичних дела против безбедности рачунарских података.[229] Рачунарски систем у овим случајевима није само средство којим се врши неко противправно дело, већ сам постаје непосредни објекат напада. То значи да је за постојање ових дела неопходно управо дигитално окружење, јер без рачунара, мрежа, података и информационих система не би било ни саме радње извршења.

---

[226] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2024*, 4–7, 45–63; Nieles, Dempsey, and Pillitteri, *An Introduction to Information Security*, 8–10.

[227] Council of Europe, *Convention on Cybercrime*, ETS No. 185, Budapest, November 23, 2001,

[228] European Parliamentary Research Service, *Understanding Cybercrime* (Brussels: European Parliament, 2024), 1.

[229] Бранко Стаменковић, Саша Живановић, Бојана Пауновић и Ивана Стевановић, *Водич за судије и тужиоце на тему високотехнолошког криминала и заштите малолетних лица у Републици Србији* (Сарајево/Београд: Save the Children / Правосудна академија, 2017), 66.

У најширем смислу, нелегалне активности у сајбер простору могу да се поделе на две основне групе. Прву групу чине дела која се у страној литератури често означавају као cyber-dependent crimes, односно дела која могу да буду извршена само употребом рачунара, рачунарских мрежа или других облика ИКТ. У ову групу спадају упади у системе, злонамерни софтвер, рансомвер, DDoS напади, ометање рада система и уништавање или измена података.[230] Другу групу чине cyber-enabled crimes, односно традиционална кривична дела чије је извршење омогућено, олакшано или проширено употребом интернета и дигиталних технологија. Ту спадају различите врсте превара, фишинг, уцене, злоупотреба платних картица, прогањање, угрожавање сигурности, повреда приватности, неовлашћено објављивање снимака, као и други облици криминалитета код којих дигитална технологија није нужно предмет напада, али је кључно средство извршења.[231]

Када је рачунарски систем непосредни објекат напада, правна заштита је усмерена на поверљивост, интегритет и доступност података и система. Када се, међутим, дигиталне технологије користе као средство за извршење већ познатих кривичних дела, тежиште анализе помера се на последице по имовину, приватност, слободу, достојанство, безбедност или друга заштићена добра. То објашњава зашто се у литератури наглашава да сајбер криминал не треба да се своди само на „нападе на рачунаре“, јер се таквим приступом занемарује чињеница да дигиталне технологије данас посредују у великом броју кривичних дела која су по својој суштини имовинска, лична, привредна, безбедносна или политички мотивисана.[232]

У домаћој литератури и пракси сличан приступ изражен је кроз појам високотехнолошког криминала. Он обухвата не само кривична дела против безбедности рачунарских података, већ и друга кривична дела код којих се, због начина извршења или употребљених средстава, рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци јављају као битан елемент дела. Ова област се не исцрпљује само кривичним делима против безбедности рачунарских података, већ може да обухвати и „кривична дела против интелектуалне својине, имовине, привреде, правног саобраћаја, слобода и права човека и грађанина, полне слободе, јавног реда и мира, као и уставног уређења и безбедности Републике Србије, уколико су испуњени услови предвиђени законом.“ [233] Правни оквир Републике Србије прихвата управо овакав шири приступ. Према Закону о организацији и надлежности државних органа за борбу против високотехнолошког криминала, високотехнолошки криминал представља вршење кривичних дела код којих се као објекат или средство извршења јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику.[234] Под производима у електронском облику посебно се подразумевају рачунарски програми и ауторска дела која могу да се употребе у електронском облику.[235] Оваква дефиниција показује да домаћи законодавац није желео да високотехнолошки криминал сведе само на незаконит упад у систем или оштећење рачунарских података, већ га је поставио као посебну категорију кривичних дела код којих дигитална инфраструктура има суштинску улогу.

---

[230] European Parliamentary Research Service, *Understanding Cybercrime*, 1.
[231] United Nations Office on Drugs and Crime, “Cybercrime in Brief,” *Cybercrime Module 1: Introduction to Cybercrime*.
[232] Љуба Слијепчевић, „Високотехнолошки криминал у домаћим и међународним прописима, с посебним освртом на одредбе Кривичног законика које су ступиле на снагу од 1. јуна 2017. и Конвенцију Савета Европе о високотехнолошком криминалу,“ *Адвокатска канцеларија*, април 2018, 1–2.
[233] Стаменковић, Живановић, Пауновић и Стевановић, *Водич за судије и тужиоце*, 65–66.
[234] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, „Службени гласник РС,“ бр. 61/2005, 104/2009, 10/2023, 10/2023 — др. закон и 9/2026, чл. 2.
[235] Посебно тужилаштво за борбу против високотехнолошког криминала, „Почетна страна,“ приступљено 18. маја 2026.

Такав приступ има и значајне процесне и институционалне последице. Сајбер простор ствара посебне изазове за откривање, доказивање и кривично гоњење, јер су електронски докази често нестабилни, лако променљиви, распоређени на више локација и зависни од инфраструктуре приватних компанија или страних држава. Зато се борба против високотехнолошког криминала не може заснивати само на општим правилима класичног кривичног поступка, већ захтева специјализоване органе, техничко знање, дигиталну форензику и брзу међународну сарадњу.[236]

Међународни оквир за разумевање ових појава најчешће се везује за Конвенцију Савета Европе о високотехнолошком криминалу, познату као Будимпештанска конвенција. Конвенција је први свеобухватни међународни уговор који је настојао да уједначи национална законодавства у области сајбер криминала и да створи основу за ефикаснију међународну сарадњу.

Конвенција систематизује више група кривичних дела попут следећих: дела против поверљивости, интегритета и доступности рачунарских података и система, компјутерски повезана кривична дела, кривична дела у вези са садржајем и кривична дела повезана са повредом ауторских и сродних права.[237] У том смислу, Будимпештанска конвенција не третира сајбер криминал само као техничко питање, већ као правни и безбедносни проблем који захтева хармонизацију материјалног кривичног права, процесних овлашћења и међународне сарадње.

Значај Конвенције није само у набрајању кривичних дела, већ и у томе што полази од чињенице да су електронски докази од значаја не само за сајбер криминал у ужем смислу, већ и за велики број других кривичних дела. Управо зато је други додатни протокол уз Будимпештанску конвенцију усмерен на појачану сарадњу и откривање електронских доказа, уз истовремено наглашавање заштите људских права, владавине права и заштите података.[238]

Неовлашћени приступ рачунарским системима, мрежама и подацима представља један од основних и најраније препознатих облика нелегалног деловања у сајбер простору. Иако се ова појава у јавности најчешће поједностављено назива „хаковањем“, у правном и безбедносном смислу она обухвата много шири спектар радњи. У неовлашћени приступ спадају, између осталог, приступ систему без дозволе, заобилажење заштитних механизама, прибављање туђих приступних података, упад у корисничке налоге, злоупотребу дигиталног идентитета и приступ пословним, личним или државним базама података.[239] Будимпештанска конвенција неовлашћени приступ рачунарском систему препознаје као једно од основних кривичних дела против интегритета, поверљивости, и доступности рачунарских података и система.[240]

Једна од највећих опасности неовлашћеног приступа је у томе што ова активност често представља почетну тачку за друге облике сајбер криминала, попут крађе података, финансијске преваре, уцене, изнуде, сајбер шпијунаже или саботаже. Нападач не мора одмах да изазове

[236] Вања Корач, Драган Прља и Андреј Дилигенски, *Дигитална форензика* (Београд: Центар за нове технологије Виминацијум, Археолошки институт и Институт за упоредно право, 2016), 85–90.
[237] Council of Europe, *Convention on Cybercrime*, чланови 2–10.
[238] Закон о потврђивању Другог додатног протокола уз Конвенцију о високотехнолошком криминалу о појачаној сарадњи и откривању електронских доказа, „Службени гласник РС — Међународни уговори,“ бр. 7/2022, чл. 1; Министарство спољних послова Републике Србије, „Србија прва држава која је ратификовала Други додатни протокол уз Конвенцију о високотехнолошком криминалу,“ 9. фебруар 2023.
[239] Љуба Слијепчевић, „Високотехнолошки криминал у домаћим и међународним прописима, с посебним освртом на одредбе Кривичног законика које су ступиле на снагу од 1. јуна 2017. и Конвенцију Савета Европе о високотехнолошком криминалу,“ *Адвокатска канцеларија*, април 2018, 1–2
[240] Council of Europe, *Convention on Cybercrime*, ETS No. 185, Budapest, November 23, 2001, art. 2.

видљиву штету, довољно је да успостави приступ систему, прикупи информације, испита слабости и припреми касније деловање.[241] Та прикривена и одложена природа чини овај облик противправног деловања једним од кључних проблема савремене сајбер безбедности јер је за доказивање неопходно очувати електронске трагове и реконструисати ток напада.[242]

Са неовлашћеним приступом непосредно је повезано и незаконито пресретање комуникација, као и повреда поверљивости података. У дигиталном окружењу комуникација се одвија путем електронске поште, апликација за размену порука, друштвених мрежа, пословних платформи, банкарских апликација и облачних сервиса. Пресретање комуникације може да доведе до откривања пословних тајни, компромитовања личних података, нарушавања приватности или припреме за извршење других кривичних дела.[243] Будимпештанска конвенција препознаје незаконито пресретање преноса рачунарских података техничким средствима као кривично дело, чиме се наглашава значај заштите поверљивости комуникационог процеса.[244] Једном компромитовани подаци могу да се копирају, продају, комбинују са другим базама и користе дуго након првобитне злоупотребе, што овом облику криминалитета даје продужене и тешко контролисане последице.

Поред напада на поверљивост, значајан део нелегалних активности у сајбер простору усмерен је на нарушавање интегритета и доступности података и система. То подразумева, између осталог, незаконито оштећење, измену, брисање, прикривање или онемогућавање коришћења рачунарских података.[245] У савременим друштвима подаци нису само технички записи, већ су основ за рад јавне управе, финансија, здравства, енергетике, саобраћаја, образовања и привреде. Њихово уништавање, мењање или онемогућавање може да има велике последице. Ова нелегална дела посебно су опасна када су усмерена на системе који подржавају јавне услуге или критичну инфраструктуру, јер могу да угрозе рад институција, безбедност грађана и континуитет рада основних функција друштва.[246] Ови облици деловања могу да се повежу са основним принципима информационе безбедности, а то су поверљивост, интегритет и доступнст. Неовлашћено пресретање комуникација угрожава поверљивост, измена или брисање података угрожава интегритет, док онемогућавање рада система угрожава доступност.[247] Стога штета од сајбер криминала не може да се мери само висином материјалног губитка, већ и последицама које настају када системи престану да функционишу, када институције изгубе контролу над подацима или када грађани не могу да приступе услугама од којих зависе, чиме губе поверење у систем и саму државу.

Један од најраспрострањенијих инструмената сајбер криминала је и злонамерни софтвер, односно његово ширење. Злонамеран софтвер може да буде усмерен на оштећење система, крађу података, прикривено праћење активности корисника, преузимање контроле над уређајем или омогућавање

[241] Council of Europe, *Explanatory Report to the Convention on Cybercrime*, ETS No. 185, Budapest, November 23, 2001, paras. 44–50
[242] Вања Корач, Драган Прља и Андреј Дилигенски, *Дигитална форензика* (Београд: Центар за нове технологије Виминацијум, Археолошки институт и Институт за упоредно право, 2016), 85–90.
[243] United Nations Office on Drugs and Crime, "Offences against the Confidentiality, Integrity and Availability of Computer Data and Systems," in *Cybercrime Module 2*.
[244] Council of Europe, *Convention on Cybercrime*, art. 3.
[245] Ибид.
[246] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2025* (Athens: ENISA, 2025), 9–12.
[247] Корач, Прља и Дилигенски, *Дигитална форензика*, 31–35.

даљег приступа мрежи.[248] У савременој пракси посебно се издваја рансомвер, као облик злонамерног софтвера који се најчешће користи за дигиталну изнуду. Његова суштина није само у техничкој блокади података, већ у економском и психолошком притиску на жртву да плати откупнину коју траже сајбер криминалци како би повратила приступ систему или спречила јавно објављивање украдених података. Europol је у процени организованог интернет криминала за 2024. годину рансомвер, онлајн преваре и сексуално искоришћавање деце на интернету издвојио као једне од најозбиљнијих манифестација сајбер криминала у Европској унији.[249] Рансомвер није изолован технички напад, већ део ширег криминалног екосистема у коме се преплићу крађа података, уцена, прање новца, злоупотреба криптовалута и организована дигитална изнуда. ENISA у својим извештајима такође указује да злонамерни софтвер, искоришћавање рањивости фишинг и напади на доступност система остају значајни елементи савремених сајбер претњи.[250] Последице рансомвера посебно су оптерећујуће за јавни сектор, здравствене установе, школе, локалне самоуправе, мала и средња предузећа и организације које немају довољно развијене механизме заштите. Оне се не своде само на финансијски губитак, већ укључују прекид рада, нарушавање приватности корисника, губитак поверења, трошкове обнове система и дугорочну репутациону штету.

Један од изузетно присутних облика сајбер криминала и нелегалног деловања на интернету представљају сајбер преваре. За разлику од напада који су усмерени превасходно на системе, сајбер преваре су неретко усмерене на човека као најслабију тачку безбедносног ланца. Оне укључују лажно представљање, манипулацију поверењем, преваре у електронској трговини, злоупотребу електронске комуникације, лажне пословне понуде, злоупотребу платних картица, крађу приступних података и компромитацију налога.[251] Будимпештанска конвенција препознаје компјутерску превару као изазивање имовинске штете путем уноса, измене, брисања или прикривања рачунарских података, односно ометања рада система, када се то чини ради стицања противправне економске користи.[252]

Фишинг представља један од примера сајбер превара. Његова улога је да наведе кориснике да открију лозинке, приступне кодове, податке о платним картицама или друге осетљиве информације. Europol указује да се тржиште фишинг услуга, малвера и других криминалних дигиталних сервиса све више развија по моделу легалне индустрије, при чему се криминалне услуге рекламирају, изнајмљују и/или продају другим извршиоцима.[253]

Са развојем сајбер криминала све је израженија и незаконита трговина подацима, приступима, алатима и криминалним дигиталним услугама. Савремени сајбер криминал све мање зависи од појединачних извршилаца, а све више од нелегалног тржишта на коме се продају украдени подаци, компромитовани налози, приступи системима, малвер, фишинг услуге и техничка подршка за извођење напада. Овај модел, познат као „crime-as-a-service“, омогућава да у сајбер криминалу учествују и лица која немају висок ниво техничког знања, али имају приступ већ

[248] Бранко Стаменковић, Саша Живановић, Бојана Пауновић и Ивана Стевановић, *Водич за судије и тужиоце на тему високотехнолошког криминала и заштите малолетних лица у Републици Србији* (Сарајево/Београд: Save the Children / Правосудна академија, 2017), 65–66.
[249] Europol, *Internet Organised Crime Threat Assessment 2024* (The Hague: Europol, 2024), 8–11
[250] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2025*, 9–14
[251] Marija Pavlović, *Borba protiv visokotehnološkog kriminala u Srbiji: dostignuća i izazovi* (Beograd: prEUgovor, 2022), 3–5.
[252] Council of Europe, *Convention on Cybercrime*, art. 8.
[253] Europol, *Internet Organised Crime Threat Assessment 2024*, 11–13.

припремљеној криминалној инфраструктури.[254] Посебан проблем представља чињеница да украдени подаци могу да се препродају више пута и да се користе у различитим контекстима као што су финансијске преваре, уцене, крађу идентитета, фишинг или нападе на друге организације.

Крађа идентитета и злоупотреба личних података представљају посебно осетљив облик сајбер криминала, јер погађају и имовинску и личну сферу жртве. У дигиталном окружењу идентитет није везан само за име и презиме, већ и за налоге, лозинке, бројеве телефона, биометријске и финансијске податке, електронску пошту, фотографије. Када се ови елементи комбинују, могу да се користе за отварање лажних налога, уцене, финансијске преваре, нарушавање угледа, или даље нападе на познанике и пословне контакте жртве.[255] Због тога злоупотреба личних података у сајбер простору има снажан криминолошки значај, јер једна жртва може да постане средство за извршење нових кривичних дела.

Посебан облик нелегалних активности односи се на повреду приватности и незаконито објављивање садржаја. Незаконито прикупљање, обрада, продаја, објављивање или коришћење личних података може да доведе до финансијске штете, нарушавања угледа, дискриминације, психолошког притиска, уцене или дуготрајног осећаја несигурности. Ова област се не исцрпљује само кривичним делима против безбедности рачунарских података, већ може да обухватити и дела против слобода и права човека и грађанина, имовине, интелектуалне својине, полне слободе, јавног реда и мира или безбедности, ако су извршена употребом рачунара, мрежа или рачунарских података.[256] Нарочито тешке последице настају када се објављују приватне фотографије, снимци, преписке или осетљиви подаци деце, младих, јавних личности или лица у зависном положају. У тим случајевима сајбер простор постаје средство секундарне виктимизације, јер се штетан садржај брзо шири, чува, копира и поново појављује чак и након уклањања са платформе на коју је првобитно постављен.

Једна од најосетљивијих области нелегалних активности у сајбер простору односи се на незаконите садржаје и дигитално посредовану злоупотребу деце. Ова дела захтевају посебну пажњу јер интернет омогућава брз контакт са потенцијалним жртвама, прикривање идентитета извршилаца, ширење незаконитих материјала и прекогранично деловање криминалних мрежа.[257] Дигитална технологија у овом контексту појачава рањивост деце и младих, који често не разумеју у потпуности домет дигиталне комуникације, трајност садржаја, ризик од лажног идентитета и последице дељења приватних информација[258]. Због тога се ова област не може третирати само као кривичноправни проблем, већ и као питање превенције, дигиталне писмености, школске подршке, родитељске едукације и међусекторске сарадње.[259]

Сајбер простор је изменио и начин на који се врше повреде права интелектуалне својине. Дигитални садржаји могу лако да се деле, копирају, мењају и дистрибуирају без дозволе носилаца права. Интелектуална својина се односи на софтвер, музику, филмове, књиге, фотографије, базе података, образовне материјале, научне радове и друга ауторска дела. Дигиталне повреде

[254] Europol, *Cyber-Attacks: The Apex of Crime-as-a-Service* (The Hague: Europol, 2023), 5–8.
[255] Стаменковић, Живановић, Пауновић и Стевановић, *Водич за судије и тужиоце*, 67–70.
[256] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, „Службени гласник РС,“ бр. 61/2005, 104/2009, 10/2023, 10/2023 — др. закон и 9/2026, чл. 2–3.
[257] Стаменковић, Живановић, Пауновић и Стевановић, *Водич за судије и тужиоце*, 103–118.
[258] Катарина Јонев ,,Безбедност деце на интернету – водич за родитеље“, Београд 2019
[259] United Nations Office on Drugs and Crime, “Cybercrime in Brief,” in *Cybercrime Module 1: Introduction to Cybercrime*.

интелектуалне својине често имају масован карактер, јер једна незаконита копија може да постане основ за хиљаде даљих копирања. Будимпештанска конвенција укључује и кривична дела у вези са повредом ауторских и сродних права када се она врше путем рачунарских система.[260] Овај облик криминалитета има и економску и културну димензију, јер наноси штету носиоцима права, али истовремено утиче и на културу поштовања туђег рада у дигиталном окружењу.

Интернет и друштвене мреже могу да буду злоупотребљени и за ширење говора мржње, расистичких и ксенофобичних садржаја, позива на насиље, претњи, екстремистичке пропаганде и радикализације. Овај облик деловања налази се на граници између кривичног права, заштите људских права, слободе изражавања и безбедносне политике. Зато је важно правити разлику између увредљивог, штетног, друштвено неприхватљивог и кривично релевантног говора. Не може сваки неприхватљив говор бити предмет кривичноправне реакције, али садржаји који директно подстичу мржњу, дискриминацију, претње или насиље захтевају посебну пажњу. Додатни протокол уз Конвенцију о високотехнолошком криминалу, који се односи на дела расистичке и ксенофобичне природе извршена преко рачунарских система, показује да међународно право препознаје опасност злоупотребе дигиталних екосистема за ширење садржаја који угрожавају достојанство, равноправност и демократску стабилност.[261]

Битно је истаћи да је за све облике сајбер криминала заједничко то што дигитално окружење омогућава већу брзину, анонимност, прекограничност и тежу доказивост, због чега борба против ових облика криминалитета захтева истовремено правни, технички, институционални и превентивни приступ и, у најчешћем броју случајева, међународну сарадњу.[262]

2.7.1 Сајбер тероризам

Посебно сложен облик нелегалног деловања у сајбер простору представља сајбер тероризам, као појава која се налази на пресеку тероризма, информационе безбедности, кривичног права и националне безбедности.

За разлику од класичних облика сајбер криминала, код којих је доминантан мотив стицање противправне финансијске користи, сајбер тероризам подразумева политички, идеолошки, верски или други екстремистички мотивисано деловање усмерено на застрашивање становништва, притисак на државне органе или дестабилизацију важних друштвених система.[263] Сајбер тероризам није појам који треба да се користити олако, нити га треба изједначавати са сваким незаконитим нападом на рачунарски систем, обарањем интернет странице, ширењем пропаганде или злоупотребом друштвених мрежа.

Посебно је битно да се направи јасна разлика између сајбер тероризма као нелегалног акта у сајбер простору и употребе интернета у терористичке сврхе. Сајбер тероризам представља претњу за државу и њену безбедност, али истовремено истиче није свака активност терориста на интернету

[260] Council of Europe, *Convention on Cybercrime*, art. 10.
[261] Council of Europe, *Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems*, Strasbourg, January 28, 2003.
[262] Слијепчевић, „Високотехнолошки криминал у домаћим и међународним прописима," 1–3; Pavlović, Borba protiv visokotehnološkog kriminala u Srbiji, 8–10.
[263] Dorothy E. Denning, "Statement of Dorothy E. Denning," testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, May 23, 2000.

исто што и сајбер терористички напад.[264] Терористичке организације могу да користе интернет за комуникацију, пропаганду, регрутовање, ширење идеологије, прикупљање средстава или психолошко деловање, али такве активности саме по себи не морају да представљају сајбер тероризам у ужем смислу.[265] Сајбер тероризам постоји онда када је сам напад усмерен на рачунаре, мреже, информационе системе или критичну инфраструктуру, и када његове последице могу произвести страх, озбиљну штету, друштвену дестабилизацију или угрожавање живота и безбедности људи[266].

Једну од најчешће навођених дефиниција дала је Дороти Денинг, која сајбер тероризам описује као спој тероризма и сајбер простора. Према њеном схватању, реч је о противправним нападима или претњама нападима на рачунаре, мреже и информације, када се они врше са намером да се застраши или принуди влада или становништво ради остваривања политичких или друштвених циљева.[267] Ова дефиниција је значајна јер уводи два важна критеријума: прво, напад мора да буде усмерен на дигиталну инфраструктуру или податке и друго, последице напада морају бити довољно озбиљне да изазову страх, принуду или озбиљан поремећај. Због тога обичан вандализам на интернету, привремено обарање мање значајне странице или ширење пропагандног садржаја не би требало аутоматски квалификовати као акт сајбер тероризма.

Управо у том разграничењу лежи један од највећих теоријских проблема. Појам сајбер тероризма често је у јавности коришћен сензационалистички, посебно након терористичких напада 11. септембра 2001. године, када је страх од нових облика терористичког деловања значајно порастао.[268] Међутим, научни приступ захтева да се разликују три сродне, али не истоветне појаве: прво, сајбер криминал који може да има финансијске, имовинске или друге противправне мотиве; друго, употреба интернета у терористичке сврхе, као што су пропаганда, комуникација и регрутовање; и треће, сајбер тероризам у ужем смислу, који подразумева напад на информационе системе са терористичком намером и потенцијално тешким последицама.[269] Ова разлика је од посебног значаја у кривичноправном и безбедносном смислу. Ако се свака злоупотреба интернета од стране екстремистичких група означи као сајбер тероризам, онда се појам превише шири и губи аналитичку прецизност. Са друге стране, ако се сајбер тероризам посматра сувише уско, постоји опасност да се занемари реална могућност да терористичке групе у будућности стекну или ангажују техничке капацитете за напад на виталне информационе системе. Због тога је најпримереније прихватити став да сајбер тероризам представља ужу категорију од шире употребе интернета у терористичке сврхе, али да обе појаве имају значај за националну и међународну безбедност.[270]

Савремене државе се све више ослањају на рачунарске системе у функционисању критичне инфраструктуре, као што су енергетски системи, финансијске трансакције, транспортни саобраћај, комуникације, војни и одбрамбени системи.[271] Потенцијални напад терористичких група на ове системе могао би да произведе последице које превазилазе уобичајени сајбер

[264] Катарина Јонев, „Сајбер тероризам и употреба сајбер простора у терористичке сврхе,“ *Безбедност* 58, бр. 2 (2016): 206–207
[265] Јонев, „Сајбер тероризам и употреба сајбер простора у терористичке сврхе,“ 207–208.
[266] Ибид.
[267] Denning, “Statement of Dorothy E. Denning.”
[268] Maura Conway, “Cyberterrorism: Hype and Reality,” 2007, 1–3.
[269] Јонев, „Сајбер тероризам и употреба сајбер простора у терористичке сврхе,“ 208–210
[270] Gabriel Weimann, *Cyberterrorism: How Real Is the Threat?*, Special Report 119 (Washington, DC: United States Institute of Peace, 2004), 1–4
[271] Јонев, „Сајбер тероризам и употреба сајбер простора у терористичке сврхе,“ 206–207.

инцидент. Уколико би напад довео до прекида снабдевања, поремећаја јавних услуга, угрожавања безбедности грађана или ширења страха, такав акт би се могао да се посматра као сајбер тероризам у ужем смислу.[272]

Ипак, значајан део литературе упозорава да опасност од сајбер тероризма не треба преувеличавати. Габријел Вајман указује да је претња сајбер тероризма изазвала велику пажњу јавности, политичара и стручњака, али да је потребно разликовати стварне капацитете терористичких организација од претпостављених или медијски појачаних сценарија.[273] Ово не значи да опасност не постоји, већ да је треба анализирати трезвено, без сензационализма. Сајбер тероризам је могућ, али његово извршење захтева специфична знања, ресурсе, приступ системима и способност да се дигитални напад претвори у стварну друштвену, економску или безбедносну последицу.

Много чешћи и практично потврђени облик деловања јесте употреба интернета у терористичке сврхе. Канцеларија Уједињених нација за дрогу и криминал указује да интернет може да буде коришћен за ширење пропаганде, радикализацију, регрутовање, финансирање, обуку, планирање и комуникацију.[274] У овом случају интернет није нужно предмет напада, већ средство деловања терориста. Терористичке групе користе предности дигиталног окружења као што су брзина комуникације, релативна анонимност, могућност ширења порука великом броју људи, ниске трошкове и лакоћу повезивања са потенцијалним симпатизерима. Ово показује да сајбер простор може да се користити као инфраструктура терористичког деловања чак и онда када не постоји директан напад на рачунарски систем.

Са становишта кривичног права, ова разлика има практичан значај. Употреба интернета за терористичке сврхе може да буде повезана са кривичним делима јавног подстицања на тероризам, вербовања, финансирања тероризма, припремања терористичких аката или удруживања ради терористичког деловања. Сајбер тероризам у ужем смислу, међутим, подразумева и елементе напада на информационе системе, што га приближава кривичним делима против безбедности рачунарских података, као што су неовлашћени приступ, рачунарска саботажа, ометање рада система, оштећење података или уношење злонамерног софтвера.[275] Због тога је у анализи неопходно посматрати и мотив извршиоца и објекат напада и последице које напад производи.

Три елемента могу се издвојити као кључна за квалификацију сајбер тероризма. Први је мотив, који мора бити политички, идеолошки, верски или екстремистички, јер без таквог мотива радња може представљати сајбер криминал, али не нужно и тероризам. Други је средство извршења, односно употреба рачунара, рачунарских мрежа, информационих система или података као непосредног простора напада. Трећи је последица или циљ напада, који мора бити усмерен на изазивање страха, принуде, озбиљног поремећаја или угрожавања виталних функција друштва.[276] Ова три елемента омогућавају да се сајбер тероризам разграничи од сајбер вандализма, хактивизма, обичног сајбер криминала или пропагандне активности екстремистичких група.

[272] Јонев, „Сајбер тероризам и употреба сајбер простора у терористичке сврхе,“ 209–210.
[273] Јонев, „Сајбер тероризам и употреба сајбер простора у терористичке сврхе,“ 209–210.
[274] United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes* (Vienna: United Nations, 2012), 3–11.
[275] Council of Europe, *Convention on Cybercrime*, ETS No. 185, Budapest, November 23, 2001, arts. 2–10.
[276] Јонев, „Сајбер тероризам и употреба сајбер простора у терористичке сврхе,“ 210.

Посебну пажњу треба посветити односу сајбер тероризма и критичне инфраструктуре. Као што је истакнуто претходним редовима, савремене државе функционишу кроз високо умрежене системе, па прекид рада једног сегмента може да утиче на друге секторе. Напад на информационе системе енергетике, саобраћаја, финансија, здравства, телекомуникација или јавне управе може да има последице које превазилазе техничку штету.[277] Уколико је такав напад извршен са терористичком намером и има за циљ изазивање страха или принуде, онда може да се говорити о сајбер тероризму. Међутим, ако је напад мотивисан искључиво финансијском изнудом, индустријском шпијунажом или криминалном добити, онда је прецизније говорити о сајбер криминалу, чак и када су последице веома озбиљне.

За ову тему овог истраживања, од значаја је истаћи разлику сајбер тероризма и сајбер ратовања. Сајбер тероризам се везује за недржавне или субдржавне актере који користе дигитална средства ради терористичких циљева. Сајбер ратовање, са друге стране, припада домену међудржавних односа, оружаних сукоба, војних операција и стратегијског надметања држава. Иако у пракси може доћи до преклапања метода, посебно када се користе слични технички алати, правна и политичка природа ових појава није иста. Зато сајбер тероризам треба обрадити у оквиру нелегалних активности у сајбер простору, док сајбер ратовање оправдано остаје засебна и централна тема дисертације.

Сајбер тероризам треба разумети као потенцијално високоризичан, али појмовно осетљив феномен. Његова опасност проистиче из све веће зависности друштва од дигиталних система, али његово дефинисање мора да буде прецизно. Највећи број активности терористичких организација на интернету данас се односи на комуникацију, пропаганду, радикализацију, регрутовање и организационо повезивање, док је сајбер терористички напад у ужем смислу знатно специфичнија категорија. Неопходно је истовремено развити капацитете за спречавање злоупотребе интернета у терористичке сврхе и задржати јасне критеријуме за квалификацију сајбер тероризма, како би се избегло неосновано ширење појма и омогућила ефикасна правна и безбедносна реакција.

2.7.2 Сајбер шпијунажа

Сајбер шпијунажа представља облик деловања усмерен на прикривено прибављање поверљивих, осетљивих или стратешки важних информација посредством дигиталних средстава. Њени циљеви могу да буду државне институције, дипломатска представништва, војни системи, обавештајне и безбедносне службе, истраживачки центри, универзитети, технолошке компаније, привредни субјекти, медији, невладине организације, политичке странке или појединци који располажу вредним информацијама.

За разлику од класичне шпијунаже, која је подразумевала физичко присуство агента, дипломатско покриће, људске изворе или непосредан приступ документима, сајбер шпијунажа омогућава да се приступ циљу оствари на даљину, преко рачунарских мрежа, компромитованих налога, злонамерног софтвера, лажних комуникационих канала или злоупотребе безбедносних пропста.[278]

[277] Denning, "Statement of Dorothy E. Denning"; Јонев, „Сајбер тероризам и употреба сајбер простора у терористичке сврхе," 209–212.
[278] Richard J. Buchan, "The International Legal Regulation of Cyber Espionage," in *Cyber Espionage and International Law* (2016), 1–5.

У савременим међународним односима сајбер шпијунажа је постала један од најчешћих облика деловања држава у сајбер простору. Државе једна другу континуирано надзиру, прикупљају податке, испитују слабости система, прате дипломатску, војну, економску и технолошку комуникацију и настоје да стекну информациону предност у односу на конкуренте. У литератури се све чешће истиче да се велики део савременог сајбер надметања не одвија у облику отвореног рата, већ у „сивој зони“ обавештајног и информационог супарништва држава.[279]

Сајбер шпијунажа је посебно привлачна државама зато што омогућава прибављање великих количина података уз релативно низак ризик у поређењу са класичним обавештајним операцијама. Уместо слања агената на територију друге државе, држава може да преко сајбер актера, посредника, група повезаних са обавештајним структурама или формално независних хакерских група покуша да дође до поверљивих информација. Такав приступ омогућава и одређени степен порицања одговорности, јер је у сајбер простору атрибуција сложена, а технички трагови често непотпуни, намерно прикривени или усмерени тако да наведу истражитеље на погрешан закључак. Зато сајбер шпијунажа често функционише као средство државне политике које остаје испод прага оружаног сукоба, али ипак има значајне последице по националну безбедност, економску конкурентност и дипломатске односе.[280]

У међународноправном смислу, сајбер шпијунажа је сложена јер класично међународно право не садржи јасну и општу забрану шпијунаже у миру. У том смислу, ни сама чињеница да једна држава прикупља информације о другој држави не значи нужно да је дошло до повреде међународног права.[281] Међутим, конкретне методе које се користе у сајбер шпијунажи могу да буду правно проблематичне ако укључују неовлашћени приступ системима, повреду суверенитета, мешање у унутрашње послове друге државе, крађу података, повреду дипломатске комуникације, злоупотребу личних података или нарушавање заштићене инфраструктуре. Сајбер шпијунажа се често налази у правној „сивој зони“ јер може да буде инструмент државне обавештајне политике, али истовремено може да повреди унутрашње кривично право, прописе о тајности података, заштити пословне тајне, заштити личних података и безбедности информационих система.[282]

Посебно су значајне такозване напредне упорне претње, познате као APT актери. Према NIST-овом речнику, реч је о актерима који располажу високим нивоом стручности и значајним ресурсима, користе више вектора деловања и настоје да успоставе и одрже присуство у информационој инфраструктури циљане организације ради континуираног извлачења информација или позиционирања за будуће деловање.[283] У контексту сајбер шпијунаже, ова упорност је кључна јер није увек циљ тренутно оштећење система или јавни ефекат, већ дуготрајан, прикривен и тешко уочљив приступ информацијама.

[279] Miloš Vukelić, „Sukobi u sajber prostoru ‘ispod praga rata’: sajber oružje u obaveštajnom nadmetanju država,“ *Međunarodni odnosi* (2023): 51–52.
[280] Vukelić, „Sukobi u sajber prostoru ‘ispod praga rata,’“ 52–55; NATO Cooperative Cyber Defence Centre of Excellence, “Peacetime Cyber Espionage,” *International Cyber Law*, 2025
[281] NATO Cooperative Cyber Defence Centre of Excellence, “Peacetime Cyber Espionage,” *International Cyber Law*, 2025; Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).
[282] Buchan, “The International Legal Regulation of Cyber Espionage,” 6–12
[283] National Institute of Standards and Technology, “Advanced Persistent Threat,” *Computer Security Resource Center Glossary*, accessed May 18, 2026

Савремени извештаји о претњама показују да државно подржани актери у сајбер простору најчешће не делују само ради саботаже, већ пре свега ради прикупљања обавештајних података. Microsoft Digital Defense Report 2025 наводи да су активности државних актера у тој години биле превасходно усмерене на шпијунажу против традиционалних обавештајних мета, као што су информационе технологије, истраживачке и академске институције, владе, тинк-тенкови и невладине организације.[284] Ово је значајно јер показује да државе у сајбер простору не траже само војне тајне, већ и политичке процене, научна истраживања, технолошке иновације, податке о јавним политикама, податке о цивилном друштву и информације које могу имати стратешку вредност у међународном надметању.

Сајбер шпијунажа може да буде политичка, економска, војна, индустријска или научно-технолошка. Политичка шпијунажа усмерена је на дипломатске комуникације, изборне процесе, политичке странке, ставове влада и међународне преговоре. Војна шпијунажа усмерена је на одбрамбене системе, војне планове, командне структуре, наоружање, комуникационе канале и податке о оперативним капацитетима. Економска и индустријска шпијунажа усмерене су на пословне тајне, иновације, патенте, истраживачке пројекте, податке о набавкама, трговинске стратегије, финансијске информације и технолошку предност. Научно-технолошка шпијунажа односи се на прибављање резултата истраживања, техничких решења, алгоритама, софтверских решења, података из области вештачке интелигенције, биотехнологије, енергетике, телекомуникација и других области које имају стратешку вредност.[285]

Посебно важна димензија јесте економска и индустријска сајбер шпијунажа. У глобалној конкуренцији држава, приступ туђим научним, технолошким и пословним информацијама може да значи убрзани развој сопствене индустрије, смањење трошкова истраживања, предност у преговорима или јачање домаћих компанија. Због тога се сајбер шпијунажа не односи само на класичне државне тајне, већ и на податке приватног сектора. У томе је једна од њених најважнијих савремених карактеристика а то је да граница између националне безбедности, економске политике и технолошког надметања све је мање јасна.[286]

Посебан проблем код сајбер шпијунаже представља чињеница да државе ретко делују отворено и непосредно, већ се у пракси често ослањају на прикривене структуре, групе повезане са обавештајним службама, техничке посреднике или актере који формално нису део државног апарата. Такав модел деловања омогућава држави да прикупља поверљиве информације, а да истовремено задржи могућност порицања одговорности. Стога је сајбер шпијунажа један од најпогоднијих инструмената савременог међудржавног надметања испод прага оружаног сукоба. Њена вредност не огледа се само у прибављању података, већ и у могућности да се ти подаци касније користе за политички притисак, дипломатско позиционирање, економску предност, утицајне операције или припрему будућих сајбер активности.

Сајбер шпијунажа представља трајан облик прикривеног надметања држава, у коме информација постаје један од најважнијих стратешких ресурса. Овај облик активности треба разликовати од сајбер рата, иако у пракси може да постоји извесно преклапање. Сајбер шпијунажа не мора да има деструктивни карактер и не мора да резултира физичких последицама. Њен примарни циљ је

[284] Microsoft, *Microsoft Digital Defense Report 2025: Safeguarding Trust in the AI Era* (Redmond, WA: Microsoft, 2025), 43.
[285] Microsoft, *Microsoft Digital Defense Report 2025*, 43–47.
[286] Microsoft, *Microsoft Digital Defense Report 2025*, 43; Buchan, "The International Legal Regulation of Cyber Espionage," 12–18.

прибављање информација, а не уништавање система. Са друге стране, она може да буде припремна радња за касније сајбер операције, јер актер који дуже време има приступ систему може да прикупља податке о његовој структури, корисницима, слабостима и безбедносним механизмима. На тај начин сајбер шпијунажа може да створи предуслове за саботажу, утицајне операције, политички притисак или касније офанзивно деловање, али сама по себи не представља сајбер рат.[287]

2.7.3 Сајбер саботажа

Сајбер саботажа представља посебно опасан облик нелегалног деловања у сајбер простору, јер није усмерена само на неовлашћени приступ систему, крађу података или прибављање поверљивих информација, већ на онемогућавање, оштећење, прекид или озбиљно ометање рада информационих система.

Суштина сајбер саботаже је у нарушавању нормалног функционисања дигиталне инфраструктуре, било да се ради о уништавању или измени података, блокирању приступа систему, брисању садржаја, употреби деструктивног малвера или компромитовању индустријских контролних система. Сајбер саботажа може да се посматра као напад на доступност и интегритет система, а не само као напад на поверљивост података. Будимпештанска конвенција ову врсту радњи препознаје кроз дела ометања података и ометања система, односно кроз намерно оштећење, брисање, измену или прикривање рачунарских података, као и озбиљно ометање функционисања рачунарског система.[288]

За разлику од сајбер шпијунаже, чији је примарни циљ прикривено прибављање информација, сајбер саботажа има изразито деструктиван или ометајући карактер. Њен циљ није нужно да се подаци украду, већ да омогући прекид у раду система, да институција или предузеће изгубе оперативну способност, да се прекине испорука услуга или да се створи притисак на државу, организацију или јавност. Управо због тога сајбер саботажа има посебан безбедносни значај када су мете енергетика, јавна управа, саобраћај, телекомуникације, здравство, финансијски системи, војна инфраструктура или други сектори од којих зависи нормално функционисање друштва.[289]

Државе или актери повезани са државама могу да користе сајбер саботажу као средство за слабљење противника, тестирање његове отпорности, нарушавање поверења у институције, ометање војних или цивилних капацитета и демонстрацију технолошке моћи. И у таквим случајевима потребно је правити разлику између сајбер саботаже и сајбер рата. Сајбер саботажа може да буде део ширег политичког или безбедносног притиска, али сама по себи не мора да достигне праг оружаног сукоба.

Један од најпознатијих примера сајбер саботаже јесте Stuxnet, злонамерни софтвер откривен 2010. године, који је био усмерен на индустријске контролне системе и програмбилне логичке контролере. У стручним анализама Stuxnet се издваја као пример напада који није био усмерен само на крађу података, већ на измену начина рада индустријског процеса. Symantec је у техничком извештају указао да је крајњи циљ овог малвера био саботирање одређеног

[287] Vukelić, „Sukobi u sajber prostoru 'ispod praga rata,'" 52–55; NATO Cooperative Cyber Defence Centre of Excellence, "Peacetime Cyber Espionage."
[288] Council of Europe, *Convention on Cybercrime*, ETS No. 185, Budapest, November 23, 2001, arts. 4–5.
[289] Council of Europe, *Convention on Cybercrime*, arts. 4–5; Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier*, Version 1.4 (Symantec Security Response, February 2011), 2.

индустријског постројења путем репрограмирања контролера тако да уређаји раде ван предвиђених параметара.[290] У анализама NATO CCDCOE такође се наглашава да је Stuxnet мењао рад индустријских система на прикривен начин, уз истовремено приказивање оператерима да систем функционише нормално.[291] Овај пример је важан јер показује да сајбер саботажа може да пређе границу чисто дигиталне штете и утицати на физичке процесе у индустријском окружењу.

Сајбер саботажа у савременом окружењу може да буде део ширег притиска на државу, њене институције и критичне функције. Сајбер саботажа је посебно важна зато што спаја технички, правни и безбедносни аспект нелегалних активности у сајбер простору. Може да буде извршена од стране појединаца, криминалних група, инсајдера, конкурената, политички мотивисаних актера или државно повезаних група. Последице сајбер саботаже могу да буду локалне, али и транснационалне; могу да погоде једну организацију, али и читав сектор, могу да буду ограничене на податке, али могу да утичу и на физичке процесе. Попут сајбер шпијунаже, и сајбер саботажу треба разликовати од сајбер рата.

Сајбер саботажа не мора увек бити сајбер рат, али може бити његов увод, пратећи инструмент или део ширег стратешког деловања. Када је спроводе државно повезани актери, сајбер саботажа може да служи за слабљење противника, ометање критичних услуга, припрему терена за друге операције или слање политичке поруке. Ова нелегална активност показује да дигитални напад не мора бити усмерен само на информације, већ и на саму способност институција, система и држава да функционишу.

[290] Falliere, O Murchu, and Chien, *W32.Stuxnet Dossier*, 2

[291] Edoardo Falco, *Stuxnet Facts Report: A Technical and Strategic Analysis* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012), 11–13.

3. Концепт сајбер ратовања

3. 1 Дефинисање појма „сајбер ратовање“

Од настанка првих организованих политичких заједница, рат је представљао једног од сталних пратилаца историјског развоја држава и међудржавних односа.

Од античких полиса и средњовековних краљевстава до модерних националних држава, сукоби су се јављали као средство одбране, освајања, очувања утицаја и наметања политичке воље. Због тога је рат веома рано постао и предмет теоријског промишљања, па су бројни мислиоци настојали да објасне његове узроке, природу, циљеве и место у политичком животу. Посебно је значајно становиште Карла фон Клаузевица, према којем је рат наставак политике другим средствима, јер управо такво схватање омогућава да се рат не посматра само као оружана борба, већ и као шири облик организованог политичког сукоба.[292]

После Другог светског рата, оснивањем Уједињених нација и успостављањем савременог међународноправног поретка, употреба силе је начелно забрањена, али рат није нестао из међународне политике, већ је временом мењао своје облике, средства и просторе испољавања. Савремени развој технологије, глобалних комуникација и дигиталних мрежа довео је до тога да се сукоби више не воде искључиво на копну, мору и у ваздуху, већ и у информационом и сајбер простору. У том контексту постаје јасно да савремене државе не настоје само да противника поразе на традиционалном војном бојишту, већ и да га изненаде, ослабе, паралишу или потчине деловањем на његове информационе системе, инфраструктуру и процесе одлучивања. Зато се сајбер ратовање може разумети као један од савремених облика испољавања старе тежње држава да политичке циљеве остваре употребом нових средстава у трансформисаном безбедносном окружењу.[293]

Дефинисање појма сајбер ратовања представља једно од најсложенијих питања савремених студија међународних односа, безбедности и права. Разлог томе је у чињеници да је реч о релативно новом феномену, чији се технолошки облици, оперативне могућности и политичке импликације развијају брже него што наука и правна теорија успевају да изграде јединствен и општеприхваћен појмовни оквир. У домаћој литератури се с правом указује да се појам сајбер ратовања често меша са сродним категоријама, као што су сајбер криминал, сајбер шпијунажа, информационе операције, хактивизам и сајбер тероризам, па без јасног разграничења ових појава није могуће ни прецизно одредити шта се под сајбер ратовањем заиста подразумева.[294]

---

[292] Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 87; Nenad R. Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata* (докторска дисертација, Универзитет у Београду, Факултет безбедности, 2012), 3–4.

[293] *Charter of the United Nations*, June 26, 1945, arts. 2(4), 51.

[294] Dragan D. Mladenović, Danko M. Jovanović, and Mirjana S. Drakulić, “Definisanje sajber ratovanja,” *Vojnotehnički glasnik / Military Technical Courier* 60, no. 2 (2012): 84–85, 88–89; Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata*, 3–4.

Један од првих корака у појмовном разјашњењу ове области јесте јасно разликовање између израза сајбер рат, сајбер ратовање, сајбер операције и информационо ратовање.[295] Иако се ови термини у јавном говору често користе као синоними, у научној и стручној литератури они немају исто значење, нити се односе на исти ниво конфликтног деловања.[296] Реч је, заправо, о појмовима који означавају различите степене, облике и домене сукоба у дигиталном окружењу. Њихово разграничење је важно како би се избегла појмовна нејасноћа и претерана неоснована употреба израза „сајбер рат“ на сваки напад или инцидент у сајбер простору.[297]

Појам сајбер рат у ужем и строжем смислу најчешће се користи за означавање ситуације у којој дигитално деловање достиже такав интензитет, политички значај и врсту последица да се може поредити са оружаним сукобом.[298] То значи да се не ради о сваком злонамерном продору у систем, већ о деловању које има јасну политичку позадину, инструменталну функцију и способност да произведе озбиљне последице по државу, инфраструктуру или друштво.[299] Томас Рид управо на том месту уводи једну од најпознатијих рестриктивних позиција у литератури, истичући да би се о сајбер рату могло да се говори тек онда када дигитални напад има карактер политичког акта силе, односно када је способан да изазове последице упоредиве са традиционалним облицима насиља.[300] Из тог угла, многи догађаји које политичари, медији или јавност називају „сајбер ратом“ у научном смислу пре би се могли одредити као саботажа, шпијунажа или субверзија.[301]

Сајбер ратовање представља шири појам и означава начин вођења сукоба у сајбер простору, односно употребу дигиталних средстава у офанзивне и дефанзивне сврхе, било као самосталног вида деловања, било као подршке класичним војним, политичким, безбедносним или обавештајним активностима.[302] У том смислу, сајбер ратовање не мора увек достићи праг сајбер рата у ужем значењу, али обухвата читав спектар активности којима се противник слаби, омета, надзире, збуњује, исцрпљује или припрема за шири сукоб.[303] У домаћој литератури посебно се наглашава да сајбер ратовање може да има и директне и посредне ефекте јер може да буде усмерено на информације и информационе системе, али и на процесе, институције, инфраструктуру и друштво које од тих система зависи.[304] Управо зато је овај појам аналитички кориснији од појма сајбер рата, јер обухвата и ширу „сиву зону“ сукоба испод прага отвореног оружаног рата.[305]

Сајбер операције представљају најужи појам у овом низу и означавају појединачне, конкретне активности као што су продор у систем, постављање злонамерног кода, ометање комуникација, крађа података, манипулација информацијама, саботажа одређене мреже или привремено

[295] Nenad R. Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata* (докторска дисертација, Универзитет у Београду, Факултет безбедности, 2012), 3–4.
[296] Dragan D. Mladenović, Danko M. Jovanović, and Mirjana S. Drakulić, “Definisanje sajber ratovanja,” *Vojnotehnički glasnik / Military Technical Courier* 60, no. 2 (2012): 84–89.
[297] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 3–8.
[298] Thomas Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies* 35, no. 1 (2012): 6–15.
[299] Lucas Kello, “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft,” *International Security* 38, no. 2 (2013): 7–40.
[300] Rid, “Cyber War Will Not Take Place,” 5–15.
[301] Rid, “Cyber War Will Not Take Place,” 15–22.
[302] Dejan V. Vuletić, “Upotreba sajber prostora u kontekstu hibridnog ratovanja,” *Vojno delo* 69, no. 7 (2017): 312–313.
[303] Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata*, 457.
[304] Mladenović, Jovanović, and Drakulić, “Definisanje sajber ratovanja,” 88–89, 106–109.
[305] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 2–6.

онемогућавање дигиталних сервиса.[306] Другим речима, сајбер операција је појединачан акт или низ технички повезаних радњи, док је сајбер ратовање шири образац у који такве операције могу бити уклопљене.[307] Из тога следи да свака сајбер операција не мора нужно бити део сајбер ратовања, неке су криминалне, неке шпијунске, неке обавештајне, а неке тек у одређеном политичком и стратешком контексту постају елемент ширег конфликтног деловања.[308]

Информационо ратовање представља шири концепт од сајбер ратовања, јер обухвата деловање усмерено не само на информационе системе, већ и на свест, перцепцију, јавно мњење, психолошко стање противника, медијски простор и процесе одлучивања.[309] У том оквиру, сајбер ратовање се може разумети као један, технолошки и дигитални сегмент ширег информационог ратовања.[310] Док је сајбер ратовање чешће усмерено на мреже, системе, инфраструктуру и податке, информационо ратовање обухвата и пропаганду, психолошке операције, дезинформације, манипулацију наративима и друге облике утицаја на начин на који друштво, институције или политички актери тумаче стварност.[311] Управо због тога се у пракси ова два појма често преплићу: једна те иста операција може истовремено имати техничку, психолошку, медијску и политичку димензију.[312] Разликовање ових појмова је неопходно како би анализа сајбер конфликта била прецизна.[313] Ако се сваки напад аутоматски назове сајбер ратом, губи се могућност да се разумеју разлике између техничког инцидента, шпијунске операције, хибридног притиска и правог дигиталног конфликта са стратешким последицама.[314]

У домаћој стручној литератури значајно место има одређење према коме сајбер ратовање представља офанзивну и дефанзивну примену сајбер оружја и информација, коју покрећу или организују државни актери ради уништавања или онеспособљавања противничког циља директним дејством на информације и информационе системе, али и посредним дејством на системе, сервисе, процесе, друштво и појединце који зависе од тих инфраструктура. Ово одређење је значајно јер не своди појам само на технички напад на рачунарске мреже, већ у њега укључује и стратешки контекст, државне актере и шире друштвене последице. Уједно, оно показује да сајбер ратовање треба разумети као посебан облик савременог конфликта у коме дигитална средства служе производњи реалних политичких, војних, економских или друштвених ефеката.[315]

Поред овог ширег приступа, у литератури се појављују и уже дефиниције које тежиште стављају на конкретне облике дејства. Тако се сајбер ратовање понекад одређује као неовлашћено упадање од стране, за рачун или уз подршку владе у рачунаре или мреже друге државе, с циљем додавања, измене или фалсификовања података, као и изазивања прекида или оштећења рачунарских и контролних система. Овакво одређење има предност у практичној јасноћи, јер издваја државни елемент, намеру и конкретан облик напада, али је уже од стратешког разумевања појма, јер мање пажње посвећује психолошким, политичким и друштвеним ефектима. Због тога се у теорији и

[306] *Joint Publication 3-12: Cyberspace Operations* (Washington, DC: Joint Chiefs of Staff, 2018), I-1.
[307] Mladenović, Jovanović, and Drakulić, "Definisanje sajber ratovanja," 88–89.
[308] Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata*, 206–207.
[309] Martin C. Libicki, *What Is Information Warfare?* (Washington, DC: National Defense University Press, 1995), x–xii.
[310] Vuletić, "Upotreba sajber prostora u kontekstu hibridnog ratovanja," 312–313.
[311] Libicki, *What Is Information Warfare?*, 1–7.
[312] Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata*, 206–207.
[313] Kello, "The Meaning of the Cyber Revolution," 7–40.
[314] Rid, "Cyber War Will Not Take Place," 5–15.
[315] Dejan V. Vuletić, "Upotreba sajber prostora u kontekstu hibridnog ratovanja," *Vojno delo* 69, no. 7 (2017): 312–313.

јављају различите дефиниције, неке појам схватају у техничко-оперативном, а друге у ширем стратешко-политичком смислу.[316]

Посебно је важно разликовати сајбер ратовање од информационог ратовања. Док сајбер ратовање подразумева деловање на дигиталне системе, мреже, инфраструктуре и податке, информационо ратовање обухвата и много шири спектар активности усмерених на контролу, манипулацију, нарушавање или заштиту информација, перцепција, комуникационих токова и одлучивања. Информационо ратовање укључује пропаганду, психолошке операције, дезинформације, медијску манипулацију, електронско ратовање и сајбер операције. Због тога се може рећи да је сајбер ратовање једна од савремених форми информационог ратовања, али не и његов једини облик. У пракси се ова два појма често преплићу јер упад у сервер политичке странке, праћен контролисаним објављивањем украдених података и појачавањем пропагандне кампање на друштвеним мрежама, истовремено има и сајбер и информациону димензију.[317]

Још један важан спор у литератури односи се на питање да ли се уопште може говорити о „рату" у сајбер простору. Томас Рид је тврдио да би нека активност могла бити названа ратом само ако је политичка, инструментална и потенцијално насилна, односно ако може да произведе стварну штету и да служи принуди противника. Из тог угла, велики број познатих сајбер инцидената не достиже праг рата, већ остаје у пољу шпијунаже, саботаже, субверзије или обавештајног надметања. Овај став је значајан зато што спречава олако ширење појма сајбер рата на сваки дигитални инцидент.[318]

С друге стране, бројни аутори у домаћој литератури наглашавају да је сувише уско везивање сајбер рата искључиво за физичко разарање или људске жртве недовољно за разумевање савремених конфликата. Ненад Путник истиче да кибер ратовање има смисла тек када производи ефекте у реалном свету, односно када таргетира институције, инфраструктуре, процесе одлучивања или шири друштвени поредак. Милош Вукелић указује да се већина досадашњих државних сукоба у сајбер простору одвијала „испод прага рата", у зони између мира и оружаног конфликта, у којој доминирају саботаже, шпијунажа, субверзија и обавештајно надметање. То значи да је за савремену анализу потребан појам довољно широк да обухвати ову сиву зону, али довољно прецизан да не обухвати сваки облик дигиталне злоупотребе.[319]

Због тога је корисно појам сајбер ратовања одредити као облик политички и стратешки мотивисаног, претежно државног или државно подржаног конфликтног деловања у сајбер простору, које обухвата офанзивне и дефанзивне активности усмерене на нарушавање, онеспособљавање, контролу, експлоатацију или заштиту информација, информационих система и инфраструктура, са циљем остваривања предности над противником и производње конкретних ефеката у реалном политичком, војном, економском или друштвеном окружењу. У том одређењу су кључни следећи елементи: политичка намера, конфликтни контекст, државни или квазидржавни карактер актера, употреба дигиталних средстава и постојање ефекта који

[316] Vuletić, "Upotreba sajber prostora u kontekstu hibridnog ratovanja," 312; Mladenović, Jovanović, and Drakulić, "Definisanje sajber ratovanja," 88–89.
[317] Vuletić, "Upotreba sajber prostora u kontekstu hibridnog ratovanja," 312–313; Ivana S. Damnjanović, *Odnos politike i tehnologije u savremenoj političkoj teoriji* (докторска дисертација, Универзитет у Београду, Факултет политичких наука, 2013), 255–257.
[318] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–15.
[319] Nenad R. Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata* (докторска дисертација, Универзитет у Београду, Факултет безбедности, 2012), 206–207, 457; Miloš Vukelić, "Sukobi u sajber prostoru 'ispod praga rata': sajber oružje u obaveštajnom nadmetanju država," *Međunarodni odnosi* 74, no. 1183 (2023): 52–55, 68–69.

превазилази чисто техничку раван. Таква дефиниција омогућава да се сајбер ратовање разликује и од сајбер криминала, и од сајбер тероризма, и од уобичајених техничких инцидената.[320]

Другим речима, суштина проблема није само у томе да ли се неки напад одиграо у сајбер простору, већ ко га је покренуо, против каквог циља, са којом намером, са каквим последицама и у ком ширем политичком контексту. Зато је појам сајбер ратовања истовремено технички, правни, политички и стратешки појам. Управо због тога његово дефинисање не може бити сведено на једну једину формулу, већ мора бити резултат пажљивог разликовања блиских појмова и разумевања да се савремени конфликти све чешће воде у хибридној, мрежној и често прикривеној средини дигиталног доба.[321]

3.1.1 Кључни елементи и обележја сајбер ратовања

Уколико се сајбер ратовање посматра само као технички напад на информационе системе, онда се његова суштина своди на ниво оперативне радње и губи се из вида његов шири политички и безбедносни значај. Због тога је за научно разумевање овог феномена неопходно издвојити његове кључне елементе као и основна обележја. Кроз такву анализу постаје јасно по чему се сајбер ратовање разликује од других облика дигиталног насиља и због чега заузима посебно место у савременим студијама безбедности. У домаћој литератури с правом се наглашава да сајбер ратовање није само питање технике, већ питање политичке намере, конфликта, државне моћи и ефеката који настају ван самог дигиталног простора.[322]

Политичка и стратешка усмереност представља једно од његових најважнијих обележја. За разлику од сајбер криминала, који је најчешће мотивисан нелегалним стицањем финансијске користи, сајбер ратовање има за циљ остваривање ширих политичких, геополитичких и војних интереса.[323] То значи да напад у сајбер простору није сам себи сврха, већ средство за слабљење противника, стицање предности, утицај на процесе одлучивања или измену односа снага у корист нападача. Стога се у литератури наглашава да се суштина сајбер ратовања не налази у самом техничком чину продора, већ у функцији коју тај чин има у ширем конфликтном контексту.[324] Из тога произлази да политичка намера нападача представља један од кључних критеријума за разликовање сајбер ратовања од сајбер шпијунаже, криминала или обичне техничке злоупотребе.[325]

Са тим је тесно повезан и државни или државно подржани карактер деловања. У најужем смислу, сајбер ратовање се везује за државе, њихове оружане снаге, обавештајне службе или актере који делују уз њихову сагласност, подршку или у њиховом интересу.[326] Иако у сајбер простору делују и бројни недржавни актери, присуство државне стратегије, политичке усмерености и

[320] Mladenović, Jovanović, and Drakulić, "Definisanje sajber ratovanja," 106–109; Vuletić, "Upotreba sajber prostora u kontekstu hibridnog ratovanja," 312–313; Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata*, 457.
[321] Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata*, 3–4, 457; Rid, "Cyber War Will Not Take Place," 5–15.
[322] Dragan D. Mladenović, Danko M. Jovanović, and Mirjana S. Drakulić, "Definisanje sajber ratovanja," *Vojnotehnički glasnik / Military Technical Courier* 60, no. 2 (2012): 106–109.
[323] Nenad R. Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata* (докторска дисертација, Универзитет у Београду, Факултет безбедности, 2012), 3,4
[324] Ибид., 457.
[325] Dragan D. Mladenović, Danko M. Jovanović, and Mirjana S. Drakulić, "Definisanje sajber ratovanja," *Vojnotehnički glasnik / Military Technical Courier* 60, no. 2 (2012): 88–89.
[326] Dejan V. Vuletić, "Upotreba sajber prostora u kontekstu hibridnog ratovanja," *Vojno delo* 69, no. 7 (2017): 312–313.

институционалних ресурса даје дигиталним нападима карактер ратовања.[327] У пракси, међутим, та државна улога често није отворена, већ се прикрива употребом посредника, неформалних група, „патриотских хакера“ или инфраструктуре смештене у другим јурисдикцијама, што додатно усложњава правну и политичку квалификацију оваквих активности.[328]

Посебно важно обележје сајбер ратовања јесте тешкоћа атрибуције. Док је у класичном оружаном сукобу много лакше идентификовати носиоца напада, у сајбер простору нападач може да прикрије свој идентитет коришћењем посредничких сервера, туђе инфраструктуре, заражених уређаја, украдених идентитета и техника лажног усмеравања трагова.[329] То значи да је често могуће технички уочити да је напад изведен, али много теже са довољном извесношћу доказати ко га је наредио, ко га је извео и у чије име је деловано. Ова нејасноћа омогућава државама да делују у „сивој зони“, односно испод прага јасно препознатљивог оружаног напада, што битно компликује примену међународног права, позивање на одговорност и предузимање противмера.[330]

Сајбер ратовање одликује и асиметричност. У традиционалном ратовању војна снага државе најчешће се огледа у величини оружаних снага, индустријским и логистичким капацитетима, географском положају и количини класичног наоружања. У сајбер простору та равнотежа може бити нарушена, јер и актери са ограниченијим материјалним ресурсима могу да нанесу значајну штету далеко моћнијем противнику.[331] Сајбер ратовање се често описује као простор у коме релативно ограничена улагања могу да произведу несразмерно велике последице.[332] То је нарочито значајно за мање државе, али и за све актере који у сајбер простору виде могућност да надокнаде недостатак конвенционалне војне моћи.[333]

Посебно значајно обележје сајбер ратовања јесте мрежноцентричност и зависност модерног друштва од дигиталних система. Сајбер операције су ефикасне управо зато што савремене државе, економије и оружане снаге у великој мери зависе од умрежених информационих инфраструктура.[334] Због тога мета сајбер ратовања нису само војни системи у ужем смислу, већ и телекомуникације, енергетске мреже, системи командовања и контроле, државни регистри, логистичке платформе, банкарске мреже и здравствени системи.[335] У сајбер ратовању се замагљује класична граница између цивилног и војног, јер оно што је у миру цивилна инфраструктура, у конфликту може да постане стратешки циљ.[336]

Из тог разлога, важан елемент сајбер ратовања јесте и способност да дигитално деловање произведе реалне, физичке и друштвене последице. Напад злонамерним кодом *Stuxnet* показао је да сајбер операција може довести до конкретног оштећења индустријске инфраструктуре.[337] У овом случају, напад је био усмерен на системе који управљају радом центрифуга у иранском

[327] Ибид.
[328] Thomas Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies* 35, no. 1 (2012): 10–15.
[329] Mladenović, Jovanović, and Drakulić, “Definisanje sajber ratovanja,” 107.
[330] Rid, “Cyber War Will Not Take Place,” 5–15.
[331] Mladenović, Jovanović, and Drakulić, “Definisanje sajber ratovanja,” 107–108.
[332] Ибид., 108.
[333] Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata*, 206–207.
[334] Mladenović, Jovanović, and Drakulić, “Definisanje sajber ratovanja,” 106–108.
[335] Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata*, 206–207.
[336] Mladenović, Jovanović, and Drakulić, “Definisanje sajber ratovanja,” 107–108
[337] Miloš Vukelić, “Sukobi u sajber prostoru ‘ispod praga rata’: sajber oružje u obaveštajnom nadmetanju država,” *Međunarodni odnosi* 74, no. 1183 (2023): 58–59

нуклеарном програму, а последица није била само компромитација података, већ и реално онеспособљавање индустријске опреме.[338] Слично томе, напади на електроенергетску мрежу Украјине показали су да последице сајбер деловања могу захватити и свакодневни живот становништва, снабдевање струјом и функционисање критичних јавних служби.[339] Такви примери потврђују да се сајбер ратовање не може свести само на манипулацију подацима, већ да његови ефекти могу бити материјални, безбедносни и друштвени.[340]

Сајбер ратовање одликују и прикривеност, постепеност и дуготрајност деловања. За разлику од класичног напада који је често тренутан, видљив и временски одређен, сајбер операција може да буде припремана током дужег периода. Нападач може да месецима непримећено борави у мрежи противника, да прикупља податке, мапира инфраструктуру, убацује „успавани“ злонамерни код и чека погодан политички тренутак за активирање.[341] Сајбер ратовање је често процес, а не једнократан догађај. Та одложеност напада отежава одбрану, јер се граница између мира и конфликта стално помера и постаје тешко утврдити када је сукоб заправо почео.[342]

Хибридни карактер сајбер ратовања такође представља његово обележје. У пракси се оно веома ретко појављује изоловано. Најчешће је део ширег спектра деловања који укључује информационе операције, психолошки утицај, дезинформације, економске притиске, дипломатске сигнале и обавештајне активности.[343] Зато се с разлогом наглашава да употреба сајбер простора у великој мери припада ширем обрасцу хибридног ратовања. На пример, упад у сервере политичких или државних институција, праћен селективним објављивањем украденог материјала и појачавањем одређених наратива на друштвеним мрежама, истовремено представља и сајбер и информациону операцију.[344] Уклопљеност у шири дијапазон средстава принуде и утицаја чини сајбер ратовање сложеним и вишеслојним обликом савременог конфликта.[345]

До сада су се већина државних сукоба у сајбер простору одвијали без формалне објаве рата и без недвосмисленог преласка у отворени оружани сукоб.[346] Милош Вукелић оправдано указује да досадашња пракса више личи на трајно обавештајно, субверзивно и саботажно надметање у „сивој зони“ него на класичан рат у правом смислу те речи.[347] То значи да сајбер ратовање омогућава државама да делују агресивно, а да притом избегну формалне и правне последице које би пратиле отворени оружани напад.[348] Управо у томе лежи једна од његових највећих стратешких предности, али истовремено и један од највећих ризика по међународну стабилност.[349]

[338] Nenad R. Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata* (докторска дисертација, Универзитет у Београду, Факултет безбедности, 2012), 236.
[339] Vukelić, “Sukobi u sajber prostoru ‘ispod praga rata’,” 58–59
[340] Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata*, 236.
[341] Ибид., 206–207
[342] Thomas Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies* 35, no. 1 (2012): 5–15.
[343] Dejan V. Vuletić, “Upotreba sajber prostora u kontekstu hibridnog ratovanja,” *Vojno delo* 69, no. 7 (2017): 308–313.
[344] Ибид., 312–313
[345] Nenad R. Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata*, 457
[346] Miloš Vukelić, “Sukobi u sajber prostoru ‘ispod praga rata’: sajber oružje u obaveštajnom nadmetanju država,” *Međunarodni odnosi* 74, no. 1183 (2023): 52–55.
[347] Ибид., 68–69
[348] Thomas Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies* 35, no. 1 (2012): 5–15.
[349] Vukelić, “Sukobi u sajber prostoru ‘ispod praga rata’,” 68–69.

Када се анализирају сва наведена обележја, постаје јасно да сајбер ратовање није једнодимензионалан феномен. Оно истовремено садржи техничку, војну, правну, политичку, обавештајну, психолошку и друштвену компоненту.[350] Та вишеслојност га чини различитим од класичних облика оружаног сукоба. У њему су средства често невидљива, актери прикривени, последице распоређене у више домена, док су границе између цивилног и војног, мира и рата, одбране и напада далеко нејасније него у традиционалном ратовању.[351] Зато је за правилно разумевање сајбер ратовања неопходно истовремено посматрати и његову техничку основу и његов шири политички смисао.[352]

Управо спој ових елемената чини сајбер ратовање посебним обликом савременог конфликта и објашњава због чега је оно постало једно од кључних питања савремене безбедносне теорије и праксе.[353]

3.1.2 Облици и типологија сајбер ратовања

Сајбер ратовање у пракси не испољава у једном једином, униформном облику, већ као читав спектар активности које се разликују према циљу, интензитету, мети, начину извођења и врсти последица које производе. У литератури не постоји потпуно јединствен модел класификације, али је могуће уочити неколико релативно стабилних критеријума који омогућавају аналитичко груписање ових појава. Сајбер ратовање се, стога, може типолошки разматрати према доминантном циљу деловања, према врсти мете, према природи ефекта који се жели постићи, као и према односу дигиталне операције према ширем политичком или војном сукобу.[354]

Један од најкориснијих начина типолошког разликовања сајбер ратовања јесте класификација према доминантној сврси операције. У том смислу могу се издвојити експлоататативни, дестабилизациони, деструктивни, принудни и подржавајући облици сајбер деловања. Експлоататативни облик усмерен је пре свега на продор у систем, тајно задржавање у њему, прикупљање података и стицање увида у противничке капацитете. Дестабилизациони облик тежи ометању или привременом онеспособљавању система, најчешће без трајног физичког оштећења. Деструктивни облик подразумева намеру да се изазове трајнија штета, било на подацима, било на инфраструктури, док принудни облик има за циљ да изврши политички или стратешки притисак на противника. Подржавајући облик сајбер ратовања, пак, најчешће је уклопљен у шири војни или хибридни оквир и служи као припрема или допуна класичним операцијама.[355]

Експлоататативни облик сајбер ратовања најближи је сајбер шпијунажи, али се од ње разликује онда када прикупљање података постаје део ширег стратешког надметања између држава. У овом облику нагласак није на тренутној деструкцији, већ на дугорочном продору, прикривеном присуству и стицању предности кроз контролу информација. Дестабилизациони облик сајбер ратовања усмерен је на ометање рада институција, комуникација, јавних сервиса и критичне инфраструктуре, без нужне намере да се изазове трајно материјално разарање. Његов циљ је да

[350] Mladenović, Jovanović, and Drakulić, "Definisanje sajber ratovanja," 107–109.
[351] Rid, "Cyber War Will Not Take Place," 5–15.
[352] Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata*, 457
[353] Mladenović, Jovanović, and Drakulić, "Definisanje sajber ratovanja," 106–109; Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata*, 457; Vukelić, "Sukobi u sajber prostoru 'ispod praga rata'," 68–69.
[354] Nenad R. Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata* (докторска дисертација, Универзитет у Београду, Факултет безбедности, 2012), 457; Miloš Vukelić, "Sukobi u sajber prostoru 'ispod praga rata': sajber oružje u obaveštajnom nadmetanju država," *Međunarodni odnosi* 74, no. 1183 (2023): 52–55.
[355] Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata*, 206–207, 457.

произведе пометњу, успори одлучивање, ослаби способност координације или подрије поверење у институционалну стабилност. Напади на Естонију 2007. године представљају класичан пример оваквог деловања: током више недеља нападнути су портали државних органа, парламента, министарстава, медија, интернет провајдера и банака, што је изазвало озбиљне поремећаје у дигиталном функционисању државе. Овај случај је важан зато што показује да сајбер ратовање не мора одмах да произведе физичко уништење да би имало стратешки значај; довољно је да привремено паралише кључне токове комуникације и управљања. Сродан образац виђен је и током напада на Грузију 2008. године, када су дигиталне операције деловале упоредо са класичним војним сукобом, продубљујући институционалну и комуникациону рањивост државе.[356]

Деструктивни облик сајбер ратовања обухвата операције чији је циљ трајније уништавање или озбиљно оштећење система, података или инфраструктуре. Најпознатији пример у том смислу јесте поменути вирус Stuxnet, који се у литератури често наводи као парадигматичан случај дигиталне операције са физичким последицама. Stuxnet има посебно место у типологији сајбер ратовања јер показује да злонамерни код може деловати као средство саботаже које прелази из дигиталног у материјални домен. У исту ширу категорију могу се сврстати и операције усмерене на брисање података или онеспособљавање великих мрежа, посебно када је циљ да се противнику ускрате ресурси или да се трајно наруши способност функционисања.[357]

Посебно важан подтип деструктивног деловања представљају напади на индустријске контролне системе и критичну инфраструктуру. Они показују да сајбер ратовање није ограничено на сферу података, већ може захватити енергетске, транспортне, производне и телекомуникационе системе. Напад на украјинску електроенергетску мрежу из 2015. године био је један од првих широко документованих случајева у којем је дигитална операција довела до стварног прекида снабдевања електричном енергијом за велики број корисника. Анализе тог инцидента показале су да је реч о добро припремљеној операцији која је укључивала продор у корпоративне мреже, злоупотребу легитимних приступа, даљинско управљање, брисање података и ометање процеса опоравка. Овакви случајеви су посебно значајни за типологију сајбер ратовања зато што показују прелаз са експлоатације и ометања на физичко и функционално нарушавање критичних јавних система.[358]

У оквиру деструктивне типологије посебно место заузимају и операције које су формално представљене као нешто друго, на пример као рансомвер, а у суштини имају разарајућу сврху. NotPetya је управо такав пример. Иако је у почетку деловао као типичан изнуђивачки малвер, накнадне анализе показале су да је његова суштина била деструкција, а не финансијска добит. Напад је првобитно погодио украјинско окружење, али се брзо проширио и на глобалне корпоративне мреже, изазивајући тешке поремећаје у логистици, транспорту, пословању и међународним ланцима снабдевања. Типолошки значај NotPetya је да сајбер ратовање може да

[356] Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010), 14–18; Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–15.
[357] Dragan D. Mladenović, Danko M. Jovanović, and Mirjana S. Drakulić, "Definisanje sajber ratovanja," *Vojnotehnički glasnik / Military Technical Courier* 60, no. 2 (2012): 107–108.
[358] Robert M. Lee, Michael J. Assante, and Tim Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid* (Washington, DC: Electricity Information Sharing and Analysis Center and SANS Industrial Control Systems, 2016), 5, 9–15.

буде деструктивно чак и онда када је његов спољашњи облик камуфлиран у нешто друго, а да се стварни циљ открива тек кроз обим и природу последица.[359]

Поред експлоататативних, дестабилизационих и деструктивних, могу се издвојити и принудни облици сајбер ратовања, односно операције чији је циљ да се противник натера на одређено понашање, да се одврати од неке политичке одлуке или да се изложи притиску без отвореног војног напада. У тим случајевима дигитално деловање има функцију сигнализирања моћи, демонстрације рањивости противника или производње контролисане штете која треба да делује као политичка порука. Иако у пракси није увек лако раздвојити принудни облик од дестабилизационог, разлика лежи у томе што је код принуде нагласак на политичком ефекту и промени понашања, док је код дестабилизације нагласак на нарушавању функционисања. Ова врста типологије је важна у анализи државног надметања испод прага рата, где су последице често намерно ограничене, али политичка порука снажна.[360]

Типологија сајбер ратовања може да се разматра и према врсти мете. У том смислу разликују се напади на војне системе, напади на државну управу и институције, напади на критичну инфраструктуру, напади на привредне и логистичке системе, као и напади на друштвено-когнитивну сферу.[361]

Још један могућ начин типолошког разликовања односи се на темпо и фазу деловања. У том смислу могу се издвојити припремне, активне и експлоатационе фазе сајбер ратовања. Припремне операције подразумевају продор, мапирање система, успостављање приступа и постављање техничких предуслова за будуће деловање. Активна фаза обухвата непосредно ометање, уништавање, манипулацију или експлоатацију система у тренутку када се жели постићи политички или војни ефекат. Експлоатациона фаза односи се на коришћење стечене предности, било кроз извлачење података, наставак контроле над компромитованим системом или интеграцију добијених информација у ширу стратегију. Ова типологија је посебно корисна зато што показује да сајбер ратовање није увек једнократан напад, већ често низ повезаних активности које тек у својој целини добијају стратешки смисао.[362]

Посматрано у целини, типологија сајбер ратовања открива да овај феномен не може да се сведе ни на једну једину шему. Поједине операције имају претежно експлоатативан карактер, друге су деструктивне, треће су подршка класичним војним акцијама, а четврте служе дугорочној дестабилизацији или принуди. Поред тога, исте операције често истовремено припадају у више категорија јер могу бити и експлоатативане и деструктивне, и техничке и информационе, и ограничене и стратешки дубоке. Управо зато је аналитички најкорисније говорити о типологији као о низу преклапајућих образаца, а не као о круто затвореним класама. Такав приступ омогућава да се различити историјски и савремени случајеви (од Естоније и Stuxnet-а до украјинске

[359] *Case Study: The NotPetya Campaign* (Budapest: Ludovika University of Public Service, 2024), 9–10; Sandor Boyson et al., *NotPetya: A Columbia University Case Study* (New York: Columbia University, 2022), 1–6.
[360] Thomas Rid, "Cyber War Will Not Take Place," 15–22; Dejan V. Vuletić, "Upotreba sajber prostora u kontekstu hibridnog ratovanja," *Vojno delo* 69, no. 7 (2017): 308–313.
[361] Vuletić, "Upotreba sajber prostora u kontekstu hibridnog ratovanja," 312–313; Miloš Vukelić, "Sukobi u sajber prostoru 'ispod praga rata'," 52–71.
[362] Danish Centre for Cyber Security, *State-Sponsored Global Software Supply Chain Attack* (Copenhagen: CFCS, 2021), 4–9; Office of the Director of National Intelligence, National Counterintelligence and Security Center, *Cyber Aware Case Study: OPM Data Breach* (Washington, DC: ODNI/NCSC, n.d.), 2.

електромреже, NotPetya-е и итд.) правилно разумеју у складу са циљем, методом и последицама које су производили.[363]

3.1.3 Средства и методе сајбер ратовања

Ако се у претходним разматрањима показало да је сајбер ратовање посебан облик савременог конфликта, онда је за његово потпуније разумевање неопходно анализирати и средства и методе кроз које се оно практично испољава. Под средствима сајбер ратовања спадају технички, софтверски, мрежни, организациони и обавештајни ресурси који омогућавају продор, контролу, ометање, манипулацију или уништавање противничких информационих система. Под методама се, пак, подразумевају начини на које се та средства употребљавају у циљу постизања одређеног стратешког, војног, политичког или друштвеног ефекта. Ово разликовање је важно јер показује да сајбер ратовање није само скуп техничких алата, већ организован процес у коме се дигитална средства уклапају у шири образац деловања државе или државно подржаних актера.[364]

У техничком смислу, једно од најважнијих средстава сајбер ратовања јесу различити облици злонамерног софтвера. У ту категорију спадају вируси, црви, тројанци, логичке бомбе, шпијунски програми, разарајући кодови, рансомвери, односно програми чији је циљ брисање, преузимање или неповратно оштећивање података. Посебну опасност представљају злонамерни кодови који су прилагођени индустријским контролним системима, јер у том случају последице не остају у домену дигиталног, већ могу да захвате и физичку инфраструктуру. Управо је Stuxnet показао како софтвер може да буде употребљен као средство саботаже које производи реално оштећење индустријске опреме, чиме се брише граница између виртуелног напада и физичког дејства.[365]

Поред злонамерног софтвера, важна средства сајбер ратовања представљају и ботнети и системи за извођење дистрибуираних напада ускраћивања услуге (DDoS). Ботнет је мрежа компромитованих уређаја којом нападач може централно управљати и користити је за преоптерећење сервера, мрежних капацитета или јавних сервиса. Ови напади су нарочито ефикасни када је циљ привремена парализа државних портала, медија, банкарских система или комуникационих платформи. Напади на Естонију 2007. године често се наводе као пример управо оваквог облика дејства, у којем је масовно преоптерећење дигиталне инфраструктуре имало значајне политичке и институционалне последице, иако није произвело класично физичко разарање.[366]

Једно од најсофистицираних средстава сајбер ратовања јесу и експлоатације рањивости, нарочито такозваних „zero-day“ пропуста, односно безбедносних слабости за које произвођач у тренутку напада још увек нема закрпу. Употреба таквих рањивости омогућава нападачу да стекне приступ систему пре него што се одбрана уопште успостави. Иако сама рањивост није оружје у класичном смислу, њена експлоатација постаје кључно средство за извођење даљих фаза операције. То је једна од највећих специфичности сајбер ратовања јер његова средства често нису

[363] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014), 5–6, 118–19, 143–45; Tikk, Kaska, and Vihul, *International Cyber Incidents*, 14–18

[364] Nenad R. Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata* (докторска дисертација, Универзитет у Београду, Факултет безбедности, 2012), 206–207, 457; Dejan V. Vuletić, "Upotreba sajber prostora u kontekstu hibridnog ratovanja," *Vojno delo* 69, no. 7 (2017): 312–313.

[365] Dragan D. Mladenović, Danko M. Jovanović, and Mirjana S. Drakulić, "Definisanje sajber ratovanja," *Vojnotehnički glasnik / Military Technical Courier* 60, no. 2 (2012): 107–108.

[366] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014), 5–6, 118–119, 143–145.

материјална у традиционалном смислу, већ се заснивају на знању, откривеним слабостима, способности прикривеног приступа и временској предности над противником.[367]

Важну улогу имају и крађа акредитива, злоупотреба идентитета и социјални инжењеринг. Нападач не мора увек да „разбија“ техничку заштиту; често је ефикасније да наведе корисника да сам отвори врата систему. У том смислу, spear-phishing, лажне поруке, компромитовани прилози, злоупотреба поверења и отуђивање приступних података представљају уобичајена средства. У нападима на индустријске и државне системе овакав приступ је посебно важан, јер омогућава да сложена операција започне релативно једноставним механизмом обмане корисника. Напад на украјинску електроенергетску мрежу 2015. године показао је да чак и врло сложене операције над критичном инфраструктуром често почињу управо компромитацијом приступа и накнадним ширењем унутар мреже.[368]

Посебно значајно средство савременог сајбер ратовања представља и компромитација ланца снабдевања софтвером и услугама. Уместо директног напада на крајњу мету, нападач може компромитовати софтвер, добављача, платформу за ажурирање или услугу коју користи велики број организација. На тај начин једним улазом може се обухватити широк круг државних и корпоративних система.[369]

Када је реч о методама сајбер ратовања, прва и најчешћа метода јесте тихи продор и дуготрајно задржавање у систему. Ова метода се не заснива на тренутној деструкцији, већ на постепеном уласку, прикривеном присуству, мапирању система и стицању контроле над критичним тачкама мреже. Нападач настоји да остане непримећен, да стекне привилегије, да се креће кроз више подсистема и да тек у погодном тренутку активира наредну фазу деловања. У том смислу, сајбер ратовање често функционише као процес више фаза: иницијални приступ, успостављање присуства, ескалација привилегија, ширење кроз мрежу, прикупљање података, припрема за саботажу и тек потом активирање главног ефекта.[370]

Друга значајна метода јесте манипулација подацима и информационим токовима. За разлику од класичног уништавања, овде је циљ да се измени садржај, интегритет или поузданост података тако да противник доноси погрешне одлуке, губи ситуациону свест или делује на основу лажних информација. Ово је изразито опасно у војним, обавештајним и управљачким системима, где и најмања промена у подацима може произвести крупне последице. Метод сајбер ратовања не мора бити усмерен на „гашење“ система, већ на његово дискретно искривљавање. Стратешки ефекат тада произлази не из одсуства података, већ из њихове непоузданости.[371]

---

[367] Karen Scarfone et al., *Computer Security Incident Handling Guide*, NIST Special Publication 800-61 Revision 2 (Gaithersburg, MD: National Institute of Standards and Technology, 2012); Karen Stouffer et al., *Guide to Operational Technology (OT) Security*, NIST Special Publication 800-82 Revision 3 (Gaithersburg, MD: National Institute of Standards and Technology, 2023).

[368] Robert M. Lee, Michael J. Assante, and Tim Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid* (Washington, DC: Electricity Information Sharing and Analysis Center and SANS Industrial Control Systems, 2016), 5, 9–15.

[369] Office of the Director of National Intelligence, National Counterintelligence and Security Center, *Cyber Aware Case Study: OPM Data Breach* (Washington, DC: ODNI/NCSC, n.d.), 2; Danish Centre for Cyber Security, *State-Sponsored Global Software Supply Chain Attack* (Copenhagen: CFCS, 2021), 4–9.

[370] *Case Study: The NotPetya Campaign* (Budapest: Ludovika University of Public Service, 2024), 9–10.

[371] Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata*, 457.

Трећа важна метода јесте ометање и ускраћивање функционалности. Циљ оваквих операција није нужно уништење, већ привремена нефункционалност. Нападач тежи да противнику ускрати употребу ресурса у критичном тренутку, например, да прекине комуникацију, успори проток информација, онемогући приступ платформама или оптерети мрежу до нивоа нефункционалности. Такве операције су за нападаче нарочито корисне у кризним ситуацијама, током избора, политичких тензија, војних покрета или координације одбране. Практичан значај ове методе види се управо у нападима усмереним на јавне дигиталне сервисе, медије и институције, где је ефекат привремене неупотребљивости довољан да се произведе шире друштвено и политичко нарушавање.[372]

Четврта метода може се описати као саботажа критичне инфраструктуре. Овде је циљ да се деловањем на индустријске контролне системе, сензорске мреже, енергетске или транспортне процесе изазове функционални или физички поремећај. Ова метода има посебну тежину јер директно повезује сајбер домен са материјалним последицама. У таквим случајевима сајбер ратовање престаје да буде само питање дигиталног инцидента и постаје средство нарушавања свакодневног живота, јавне безбедности и друштвене стабилности.[373]

Пета метода јесте маскирање деструкције у друге облике напада. Нападач понекад формално представља операцију као рансомвер, криминални напад или технички инцидент, док је њена стварна сврха уништење, дестабилизација или стратешки притисак. NotPetya је управо такав пример: спољa је личио на изнуђивачки малвер, али је његова стварна функција била разарајућа, што се видело по ширини последица и ограниченој реалној могућности поврата података. Оваква метода је посебно значајна јер нападачу омогућава да замагли намеру, одложи политичку реакцију и отежа атрибуцију.[374]

Сајбер ратовање се ретко појављује изоловано; много чешће оно има улогу припреме, подршке или појачања других облика притиска. Дигитални напад може да претходи класичном нападу, може да ослаби комуникацију и координацију, али може и да буде упарен са дезинформационим кампањама и психолошким операцијама. Сајбер дејство се неретко користи ради нарушавања комуникационе инфраструктуре у критичном оперативном тренутку.[375]

Седма метода јесте деловање испод прага отвореног рата. Ово није само политичка карактеристика, већ и посебан метод приступа: штета се дозира, ефекти се ограничавају, операције остају прикривене или се изводе у облику који не изазива аутоматски класичан војни одговор. У таквом моделу циљ није једнократна одлучујућа победа, већ постепено исцрпљивање, тестирање граница, притисак, сигнализирање моћи и дугорочно слабљење противника. Ова

[372] Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010), 14–18.
[373] Lee, Assante, and Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, 9–15; Stouffer et al., *Guide to Operational Technology (OT) Security*.
[374] *Case Study: The NotPetya Campaign*, 9–10.
[375] Viasat, "KA-SAT Network cyber attack overview," March 30, 2022; Jaime Blasco and Juan Andres Guerrero-Saade, "Reviewing the 2022 KA-SAT Incident and Implications for Distributed Communication Environments," *Virus Bulletin Conference Proceedings* (2024).

метода нарочито одговара савременом државном надметању, јер омогућава агресивно деловање уз очување формалне могућности уверљивог порицања одговорности.[376]

Средства и методе сајбер ратовања чине јединствену, али веома разноврсну целину. У међусобном споју ових побројаних средстава и метода лежи суштина сајбер ратовања као савременог инструмента политичког и стратешког надметања међу државама.[377]

3.1.4 Циљеви сајбер ратовања

У савременим међудржавним односима сајбер ратовање представља средство којим се истовремено прикупљају подаци, слаби противник, обликује његово понашање и ремете његови институционални и инфраструктурни капацитети. То је суштински разлог зашто циљеви сајбер ратовања морају да се анализирају у ширем оквиру стратешког надметања, а не као збир изолованих дигиталних инцидената.[378]

Један од основних циљева сајбер ратовања јесте стицање обавештајне и информационе предности. Држава која успе да продре у информационе системе друге државе, њених министарстава, парламента, институција, критичне инфраструктуре или великих добављача дигиталних услуга добија увид у противничке капацитете, слабости, планове и обрасце деловања. Операција Cloud Hopper, која се у отвореним изворима доводи у везу са групом APT10, показује како циљ сајбер деловања може да буде стицање широког и дуготрајног приступа подацима клијената преко компромитованих managed service provider компанија. У овом случају није примарни циљ био тренутно разарање, већ стварање трајне обавештајне предности над великим бројем мета у различитим државама и секторима.[379]

Код сајбер ратовања долази до нарушавање функционисања државних институција и подривање политичког ауторитета. Када је 2015. године нападнут немачки Бундестаг, последице се нису исцрпеле у крађи података. Напад је погодио информациони систем парламента, утицао на његову способност рада током више дана и захватио комуникацију посланика, укључујући и налоге високих политичких личности. Такви напади имају двострук циљ: са једне стране, стицање осетљивих података, а са друге стране, демонстрацију институционалне рањивости и политички притисак на нападнуту државу. У овом типу деловања сајбер ратовање постаје средство ерозије државне самоуверености, поверења у институције и унутрашње политичке стабилности.[380]

Циљ сајбер ратовања може да буде и дестабилизација јавне комуникационе сфере и стварање симболичког удара на државу или друштво. Напад на француску телевизијску мрежу TV5Monde 2015. године представља упечатљив пример овакве логике. Емитовање програма телевизије је

[376] Miloš Vukelić, "Sukobi u sajber prostoru 'ispod praga rata': sajber oružje u obaveštajnom nadmetanju država," *Međunarodni odnosi* 74, no. 1183 (2023): 52–55, 68–69; Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–15.
[377] Mladenović, Jovanović, and Drakulić, "Definisanje sajber ratovanja," 106–109; Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata*, 457; Vukelić, "Sukobi u sajber prostoru 'ispod praga rata'," 68–69.
[378] Nenad R. Putnik, *Kiber ratovanje – novi oblik savremenih društvenih konflikata* (докторска дисертација, Универзитет у Београду, Факултет безбедности, 2012), 206–207, 457; Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 41–45.
[379] PwC UK and BAE Systems, *Operation Cloud Hopper* (London: PwC and BAE Systems, 2017), 3–5; Council on Foreign Relations, "APT10," *Cyber Operations Tracker*.
[380] Council of the European Union, "Malicious cyber-attacks: EU sanctions two individuals and one body over 2015 Bundestag hack," October 22, 2020.

било прекинуто неколико сати, компромитовани су налози на друштвеним мрежама, а сама операција је у првом тренутку представљена као напад џихадистичких актера, да би накнадне истраге указале на ширу и сложенију позадину. Циљ оваквог деловања није било само техничко ометање рада медијске куће, већ и производња страха, несигурности, забуне и симболичке поруке да је могуће погодити јавни информациони простор једне државе. У том случају сајбер ратовање захвата и психолошку и информациону димензију конфликта.[381]

Посебан циљ сајбер ратовања јесте економско исцрпљивање противника и нарушавање привредне отпорности. Напад малвером Shamoon на Saudi Aramco 2012. године, у којем је обрисан садржај на око 35.000 рачунара, јасно показује да циљ дигиталног удара може бити разарање пословне инфраструктуре, успоравање функционисања једне стратешки значајне компаније и изазивање ширег економског и симболичког ефекта. Када је мета енергетски сектор, последице напада излазе изван оквира једног предузећа и постају питање националне економске стабилности и геополитичке сигнализације. Овде је циљ сајбер ратовања да се противнику повећа цена функционисања, умањи економска отпорност и пошаље порука о његовој рањивости.[382]

Један од најопаснијих циљева сајбер ратовања јесте изазивање физичке штете, угрожавање безбедности процеса и потенцијално довођење у опасност људских живота. Напад познат као TRITON/TRISIS, откривен 2017. године, био је усмерен на сигурносне контролере у индустријском окружењу. Значајан је јер су званични безбедносни извори оценили да је реч о нападу који је био дизајниран тако да омогући физичку штету, еколошке последице и губитак живота у случају рада постројења у небезбедном режиму. Овде је циљ сајбер ратовања прешао границу између дигиталног и физичког и показао да сајбер операција може да буде употребљена као средство угрожавања индустријске безбедности и реалног живота. Такав тип циља представља најозбиљнији облик сајбер претње, јер директно приближава сајбер ратовање ефектима класичне саботаже и оружаног насиља.[383]

Сајбер ратовање може имати и циљ принуде, односно настојање да се противник наведе на промену понашања без формалног уласка у отворени оружани сукоб. У том случају, сајбер операције служе као средство сигнализације моћи, демонстрације рањивости и стварања политичког притиска. Напад не мора нужно да буде масован или трајно разоран да би био успешан, довољно је да противнику покаже да су његове институције, комуникације или критични системи подложни нарушавању. Из тог разлога сајбер ратовање постаје важно средство принуде у „сивој зони“, односно простору између мира и класичног рата.[384]

Још један важан циљ јесте припрема оперативног окружења за шири конфликт. Многе сајбер операције немају за циљ тренутни удар, већ претходно постављање услова за касније деловање: продор у мрежу, мапирање инфраструктуре, убацивање „успаваног“ кода, компромитацију налога и успостављање канала за будућу контролу. У том смислу, циљ сајбер ратовања може да буде и стварање прикривене предности која ће бити активирана тек у будућој кризи или оружаном

[381] Council on Foreign Relations, “Compromise of TV5 Monde,” *Cyber Operations Tracker*.
[382] Council on Foreign Relations, “Compromise of Saudi Aramco and RasGas,” *Cyber Operations Tracker*.
[383] Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, National Security Agency, and Department of Energy, *TRITON Malware Remains Threat to Global Critical Infrastructure* (Washington, DC, 2022), 1; UK National Cyber Security Centre, *TRITON Malware Targeting Safety Controllers* (London: NCSC, 2017), 2.
[384] Thomas Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies* 35, no. 1 (2012): 15–22; Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 41–45.

сукобу. Могућност дуготрајног прикривеног присуства разликује сајбер ратовање од већине класичних оружаних дејстава.[385]

С обзиром да су циљеви сајбер ратовања истовремено институционални, економски, безбедносни, психолошки и политички, морају се посматрати као део ширег обрасца државног надметања, а не као низ изолованих техничких епизода[386].

3.1.5 Актери сајбер ратовања

Када се говори о актерима сајбер ратовања, полазна претпоставка мора да буде да сајбер простор није искључиво државни домен, али да државе у њему и даље представљају централне и најмоћније носиоце конфликта.[387] Разлог за то лежи у чињеници да једино државе располажу правним овлашћењима, обавештајним структурама, институционалним апаратом, финансијским ресурсима и стратешком способношћу да дугорочно планирају, координишу и интегришу сложене сајбер операције у оквир своје националне безбедности и спољне политике.[388] Сајбер ратовање је, чак и када се формално изводи преко посредника, најчешће повезано са државним интересима, државним структурама или државном политичком вољом.[389]

Унутар државе, кључни носиоци сајбер ратовања најчешће су оружане снаге, војне сајбер команде, обавештајне и контраобавештајне службе, као и специјализоване техничке јединице.[390] Дражавни актери обезбеђују спој техничког знања, оперативне дисциплине и политичке усмерености који је потребан да би сајбер операција добила стратешки значај. Max Smeets с правом указује да развој војних сајбер снага није спонтан технички процес, већ институционални подухват који зависи од организационе структуре, доктрине, политичке подршке и способности државе да дигиталне капацитете уклопи у шири војни систем.[391] То значи да државни актери у сајбер ратовању нису само корисници техничких алата, већ носиоци целокупне архитектуре дигиталног конфликта. Државе у сајбер простору делују не само ради прикупљања података, већ и ради подривања институционалног суверенитета, демонстрације моћи и политичког притиска.[392]

Поред директно државних структура, важни актери сајбер ратовања су и државни посредници, односно прокси групе. То су актери који формално нису део државног апарата, али делују у складу са интересима неке државе, уз њену подршку, толерисање или прећутну координацију.[393] Michael Schmitt и аутори окупљени око *Tallinn Manual 2.0* посебно указују на проблем који настаје када држава делује преко посредника, јер се тиме замагљује линија између формално недржавног

---

[385] Dejan V. Vuletić, "Upotreba sajber prostora u kontekstu hibridnog ratovanja," *Vojno delo* 69, no. 7 (2017): 308–313; Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 2–6.
[386] Dejan V. Vuletić, "Upotreba sajber prostora u kontekstu hibridnog ratovanja," *Vojno delo* 69, no. 7 (2017): 308–313; Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–15.
[387] Niall Fick et al., *Confronting Reality in Cyberspace* (New York: Council on Foreign Relations, 2022), 34.
[388] Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (London: Hurst, 2022), 1–5, 51–54.
[389] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 2–6.
[390] Smeets, *No Shortcuts*, 51–54
[391] Ибид., 1–5.
[392] Niall Fick et al., *Confronting Reality in Cyberspace*, 34.
[393] Council on Foreign Relations, "Cyber Proxies in the Ukraine Conflict: Implications for International Norms," March 21, 2022.

деловања и суштински државне одговорности.[394] У савременим конфликтима ови актери су од посебног значаја, јер омогућавају државама да делују агресивно, а да истовремено смање политичку цену јавне атрибуције. Управо је рат у Украјини додатно показао колико су прокси и добровољачке дигиталне мреже постале важне у савременом сајбер конфликту.[395]

Важну улогу имају и хакери, односно појединци и групе који располажу техничким знањем и способношћу да се инфилтрирају у системе, наруше њихов рад, украду податке или спроведу дигиталну саботажу. Међутим, хакери нису јединствена категорија. Једни делују из финансијских побуда, други из идеолошких уверења, трећи из политичких мотива, а четврти у сарадњи са државним структурама.[396] Зато појам хакера у контексту сајбер ратовања мора да буде употребљен опрезно јер није сваки хакер актер сајбер ратовања, али одређене хакерске групе, уколико делују у политичком конфликту, у корист државе или са јасно израженим геополитичким циљем, али свакако могу да постану његов значајан чинилац.[397]

Посебну подкатегорију чине хактивисти, односно актери који комбинују техничко деловање са политичким активизмом. У пракси, њихове акције се често крећу од DDoS напада и defacement-а сајтова до крађе и објављивања података и симболичких кампања усмерених на одређене државе, институције или политичке актере. Група Anonymous представља најпознатији пример ове врсте актера: њено деловање током рата у Украјини, када је јавно објављен „сајбер рат“ Русији, показало је како хактивистичко деловање може постати део ширег конфронтационог амбијента, чак и када није формално интегрисано у државни апарат.[398] ENISA у својим проценама претњи бележи и да хактивистичке групе имају све већу улогу у масовним DDoS инцидентима и политички мотивисаним дигиталним нападима.[399]

Још једну специфичну категорију чине терористички актери. За разлику од држава, терористичке организације најчешће не располажу истим нивоом техничке, кадровске и организационе комплексности који је неопходан за дугорочне, дубоке и сложене операције против критичне инфраструктуре једне државе. Ипак, то не значи да су ирелевантне у сајбер домену. Напротив, бројна истраживања показују да терористичке групе интензивно користе интернет и дигиталне платформе ради пропаганде, регрутовања, радикализације, комуникације са симпатизерима, прикупљања средстава и ширења психолошког утицаја[400]. Europol је у прегледу џихадистичке пропаганде за 2023. годину посебно анализирао онлајн деловање Исламске државе, Ал Каиде и Хамаса, показујући да су дигиталне мреже постале важан оперативни простор за терористичку комуникацију и наративно деловање.[401] У том смислу, терористички актери најчешће нису носиоци класичног сајбер ратовања у смислу државне сајбер саботаже или напада на индустријске системе, али јесу важни актери информационог и психолошког конфликта у сајбер простору. Интернет је за терористичке организације пре свега средство оперативне комуникације, утицаја и мобилизације, али да та улога може имати озбиљне безбедносне последице и по државе

[394] Schmitt, *Tallinn Manual 2.0*, 2–6.
[395] Council on Foreign Relations, “Cyber Proxies in the Ukraine Conflict.”
[396] Thomas Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies* 35, no. 1 (2012): 5–15.
[397] Rid, “Cyber War Will Not Take Place,” 15–22
[398] Council on Foreign Relations, “Cyber Proxies in the Ukraine Conflict.”
[399] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2025* (Athens: ENISA, 2026), 8.
[400] Katarina Jonev, „Sajber terorizam i upotreba sajber prostora u terorističke svrhe,” *Bezbednost* 58, br. 2 (2016): 206–222,
[401] Europol, *Online Jihadist Propaganda: 2023 in Review* (The Hague: Europol, 2024), 9–10.

и по друштва.[402]То значи да су терористички актери релевантни у ширем екосистему сајбер конфликта, посебно тамо где се преплићу пропаганда, дигитална комуникација и радикализација.

Савремени сајбер простор отворио је место и за плаћенике, односно комерцијалне актере који производе, продају или изнајмљују офанзивне дигиталне капацитете. У традиционалном ратовању плаћеници су били борци који ратују за новац, а у сајбер домену та улога је трансформисана у приватне фирме и стручњаке који развијају шпијунски софтвер, exploit пакете, инфраструктуру за дигиталну компромитацију и системе надзора. Citizen Lab у својим анализама изричито користи појам mercenary spyware, указујући да је реч о глобалном тржишту на коме приватни субјекти државама и другим клијентима продају офанзивне способности које се могу употребити за надзор, инфилтрацију и компромитацију.[403] Такви актери представљају посебан изазов, јер уносе тржишну логику у домен који је некада био претежно резервисан за државне и обавештајне структуре. Илустративан пример оваквог актера представља Paragon Solutions, чији је spyware *Graphite* Citizen Lab почео детаљније да документује 2025. године. Анализа је показала да ова фирма не делује као класичан државни орган, али да њени производи и услуге могу да буду употребљени у операцијама које имају јасан политички и безбедносни значај.[404]

Поред актера који нападају, важну улогу имају и одбрамбени и нормативни актери. Национални CERT/CSIRT тимови, међународне организације, војни савези, истраживачки центри и компаније за threat intelligence често не изводе нападе, али значајно утичу на то како ће они бити откривени, тумачени, атрибутовани и политички квалификовани. NATO и CCDCOE, на пример, делују као важни актери у развоју доктрине, вежби, сарадње и заједничког разумевања претњи, док Уједињене нације покушавају да кроз рад експертских група обликују норме одговорног понашања држава у сајбер простору.[405] Ово показује да актере сајбер ратовања не чине само извршиоци, већ и субјекти који дефинишу правила, нуде одговоре и обликују политичко разумевање дигиталног конфликта.

Актери сајбер ратовања чине разуђен и вишеслојан систем. Државе остају централни носиоци, јер једино оне могу трајно спојити војно, обавештајно, правно и политичко деловање у јединствену стратегију. Битно је нагласити да анализа актера сајбер ратовања не треба да буде ограничена само на питање ко је технички извео напад, већ мора да обухвати и читав круг субјеката који га омогућавају, финансирају, усмеравају, прикривају или политички користе.[406]

3.2. Државе као кључни актери сукоба у сајбер простору

Развој информационо-комуникационих технологија у последњим деценијама довео је до стварања новог простора друштвене интеракције, економске активности и политичког надметања – сајбер простора. Иако је у почетним фазама развоја интернета овај домен био посматран пре

[402] Katarina Jonev, „Sajber terorizam i upotreba sajber prostora u terorističke svrhe," *Bezbednost* 58, br. 2 (2016): 206–222,
[403] Citizen Lab, "Submission to the UN Working Group on the Use of Mercenaries," March 25, 2026, 4–5.
[404] Bill Marczak et al., "Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations," Citizen Lab Report No. 183 (Toronto: University of Toronto, 2025).
[405] NATO Cooperative Cyber Defence Centre of Excellence, "About Us"; United Nations, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (New York: United Nations, 2021).
[406] Niall Fick et al., *Confronting Reality in Cyberspace*, 34; Citizen Lab, "Submission to the UN Working Group on the Use of Mercenaries," 4–5.

свега као комуникационо и технолошко окружење, постепено је постало јасно да има и изузетно значајну безбедносну и геополитичку димензију.

Као што је објашњено у претходном поглављу рада, сајбер простор представља релативно нову димензију међународних односа у којој се све више испољавају традиционални обрасци политичког и безбедносног надметања. Иако се у раним фазама развоја интернета често говорило о томе да дигитално окружење представља „простор без граница“ у којем државе губе контролу, развој савремених технологија и растућа зависност друштва од дигиталне инфраструктуре довели су до супротног процеса. Државе су постепено почеле да преузимају кључну улогу у контролисању, регулисању и одбрани дигиталног простора, што је довело до тога да се и у сајбер окружењу све више примењује концепт суверенитета.

Савремени међународни односи све више укључују дигиталне инструменте моћи, а сајбер простор се често описује као ново поље сукоба између држава. У оквиру тог процеса управо државе представљају најзначајније и најмоћније актере у сајбер ратовању. Иако у дигиталном окружењу делују и други субјекти попут криминалних група, хактивистички покрети, терористичких организација, појединачних хакера, државе се издвајају по својој способности да мобилишу институционалне ресурсе, финансијске капацитете и стратешке механизме за планирање и спровођење комплексних сајбер операција. Државе су носиоци суверене политичке власти и поседују монопол над легитимном употребом силе, што им омогућава да сајбер операције интегришу у шири систем националне безбедности и одбране.[407]

Концепт државног суверенитета традиционално подразумева врховну власт државе над сопственом територијом, становништвом и институцијама. Међутим, са појавом дигиталних мрежа поставило се питање како овај принцип може да се примени у простору који нема јасно дефинисане физичке границе. Упркос тој специфичности, већина савремених теоретичара међународних односа сматра да државе задржавају одређени степен суверенитета и у сајбер простору. То се пре свега односи на чињеницу да се кључна инфраструктура интернета као што су сервери, телекомуникационе мреже, дата центри и комуникациони каблови налази на територији одређених држава и подлежу њиховој правној и политичкој надлежности. На тај начин дигитална инфраструктура постаје део националног безбедносног система и предмет државне заштите, а може се рећи и контроле.[408]

Поред надзора инфраструктуре, државе остварују суверенитет у сајбер простору и путем законодавства и регулативе. Савремене државе доносе законе који регулишу област сајбер безбедности, заштите података, дигиталних комуникација и функционисања информационих система. На тај начин оне настоје да успоставе правни оквир који омогућава контролу над дигиталним процесима који се одвијају унутар њихове надлежности. Многи аутори указују да сајбер простор није потпуно „анархичан“ систем, већ домен у којем се постепено развијају нови облици дигиталног суверенитета.[409]

У научној литератури се често наглашава да је сајбер простор постао „пето оперативно окружење“ модерног оружаног сукоба, поред копна, мора, ваздуха и свемира.[410] У том контексту државе настоје да развију способности које ће им омогућити и офанзивно и дефанзивно деловање у

[407] Joseph S. Nye, Jr., *The Future of Power* (New York: PublicAffairs, 2011), 113–18.
[408] Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation, 2009.
[409] Nye, Joseph S. Jr. *The Future of Power*. New York: PublicAffairs, 2011.
[410] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 5–7.

дигиталном окружењу. Развој сајбер капацитета постао је један од приоритета националних безбедносних стратегија многих земаља, укључујући Сједињене Америчке Државе, Кину, Русију, Немачку, Израел и друге технолошки напредне државе. Улагање у сајбер одбрану и сајбер офанзивне способности постало је део ширег процеса модернизације војске и безбедносних структура.

Државе се сматрају кључним актерима у сајбер простору јер располажу значајним ресурсима неопходним за развој сложених технолошких система. Развој напредних сајбер способности захтева високо обучене стручњаке, значајна финансијска улагања, приступ технолошкој инфраструктури и институционалну подршку. Све ове факторе најчешће могу да обезбеде управо државе, јер располажу буџетским средствима, образовним системом и институцијама које омогућавају развој технолошких капацитета. Због тога су државе у стању да развијају офанзивне и дефанзивне сајбер способности које су далеко сложеније од активности недржавних актера.[411]

Један од основних разлога због којих су државе доминантни актери у сајбер сукобима лежи у њиховој способности да интегришу сајбер операције у свеобухватну стратегију националне моћи. За разлику од недржавних актера, државе могу комбиновати сајбер инструменте са дипломатским, економским, обавештајним и војним средствима. Такав приступ омогућава употребу сајбер операција као дела ширег концепта такозваног хибридног ратовања, у којем се традиционалне и нетрадиционалне методе сукоба међусобно допуњују.[412]

Посебно значајну улогу у развоју државних сајбер капацитета имају војне структуре и обавештајне агенције. У многим државама формиране су специјализоване јединице које су задужене за планирање и извођење сајбер операција. Сједињене Америчке Државе су, на пример, 2009. године формирале Команду за сајбер операције (U.S. Cyber Command), чији је задатак да координише офанзивне и дефанзивне активности америчких оружаних снага у сајбер простору.[413] Сличне структуре постоје и у другим државама, што указује на растући значај дигиталног домена у савременим безбедносним стратегијама.

Један од првих догађаја који је указао на потенцијал сајбер напада као инструмента државне моћи била је војна вежба „Eligible Receiver 97“ у Сједињеним Америчким Државама. Током ове симулације тим стручњака успео је да продре у бројне војне и цивилне системе и да демонстрира на који начин и у којој мери би сајбер напади могли да угрозе функционисање националне инфраструктуре. Резултати ове вежбе показали су да релативно малобројна група стручњака може да изазове озбиљне поремећаје у функционисању државних институција, што је значајно утицало на касније формирање америчких сајбер стратегија.[414]

Поред војних структура, важну улогу у сајбер операцијама имају и обавештајне службе. У Руској Федерацији, на пример, Главна обавештајна управа (ГРУ) развила је значајне капацитете за дигиталну шпијунажу и сајбер операције усмерене на прикупљање обавештајних података и утицај на политичке процесе.[415] Сајбер операције овог типа често укључују продор у

[411] Rid, Thomas. *Cyber War Will Not Take Place*. London: Hurst & Company, 2013
[412] Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst & Company, 2013), 54–58.
[413] Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016), 188–90; U.S. Cyber Command, “Command History,”, прегледано 10.априла 2026
[414] Kaplan, *Dark Territory*, 89–92.
[415] Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia’s Digital Dictators and the New Online Revolutionaries* (New York: PublicAffairs, 2015), 312–18; U.S. Department of Justice, “Grand Jury Indicts 12 Russian

информационе системе, прикупљање осетљивих података или спровођење кампања дезинформација.

Једна од специфичних карактеристика државних сајбер операција јесте и могућност деловања у условима релативне анонимности. За разлику од традиционалних војних напада, код сајбер операција често је тешко са сигурношћу утврдити ко је одговоран за одређени напад. Овај проблем, познат као проблем атрибуције, представља један од највећих изазова у савременом сајбер ратовању.[416] Због тога државе понекад користе посреднике, као што су хакерске групе или такозвани „патриотски хакери“, који формално делују као независни актери, али у пракси често следе интересе одређене државе.

Атрибуција сајбер напада представља процес утврђивања ко стоји иза одређене злонамерне активности у сајбер простору, односно да ли је реч о појединцу, криминалној групи, недржавном актеру или држави.[417] Атрибуција је једно од најсложенијих питања сајбер безбедности, јер нападачи могу да прикрију свој идентитет коришћењем посредничких сервера, заражених уређаја, лажних трагова и инфраструктуре распоређене у више држава. У стручној литератури се обично разликују техничка, правна и политичка атрибуција.[418] Техничка атрибуција односи се на анализу дигиталних трагова и злонамерног кода, правна на утврђивање одговорности у складу са правилима међународног права, а политичка на одлуку државе да јавно именује одговорног актера.[419] Управо због тога атрибуција није само техничко питање, већ и питање процене, интереса и последица које таква квалификација може произвести у међународним односима.[420] Уколико држава не може поуздано да утврди ко стоји иза напада, отежано је и предузимање противмера, позивање на одговорност и примена концепта одвраћања у сајбер простору.[421] Зато се атрибуција данас сматра једним од кључних предуслова за ефикасну сајбер безбедност, примену међународног права и очување стабилности у дигиталном окружењу.[422]

Сајбер операције држава често имају и значајну улогу у обавештајном деловању. Сајбер шпијунажа омогућава државама да прикупљају велике количине података о политичким, економским и војним активностима других држава. За разлику од традиционалне шпијунаже, која подразумева физичко присуство агената, дигитална шпијунажа омогућава приступ осетљивим информацијама са велике удаљености и уз знатно мањи ризик од откривања.[423]

Поред прикупљања података, државе користе сајбер простор и за спровођење операција усмерених на критичну инфраструктуру. Енергетски системи, телекомуникационе мреже, транспортна инфраструктура и финансијски системи представљају потенцијалне мете сајбер

Intelligence Officers for Hacking Offenses Related to the 2016 Election," July 13, 2018. https://www.justice.gov/archives/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election?utm_source=chatgpt.com

[416] Libicki, *Cyberdeterrence and Cyberwar*, 39–41; Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 82–95.

[417] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37.

[418] Ибид, 4-37

[419] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 82–95.

[420] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37

[421] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 82–95.

[422] Ибид, 82-95

[423] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 67–75.

напада јер њихово нарушавање може имати озбиљне последице по функционисање друштва и државе. Ови системи су често у фокусу државних сајбер операција, јер њихово ометање или изазивање прекида у раду може да доведе до економске нестабилности и политичког притиска на противничку државу.[424]

У савременим оружаним конфликтима сајбер операције се све чешће користе као подршка класичним војним акцијама. Напади на комуникационе системе, радарске мреже или системе командовања могу да значајно ослабе способност противника да координише своје војне снаге. На тај начин сајбер операције постају важан елемент модерних војних стратегија, јер омогућавају постизање војних циљева без непосредне употребе кинетичке силе.[425]

Поред војних аспеката, државе користе сајбер простор и као средство политичког утицаја. Кампање дезинформација, манипулација информацијама и дигитална пропаганда представљају важан инструмент савременог информационог ратовања. У таквим операцијама циљ није директно уништавање инфраструктуре, већ утицај на јавно мњење, политичке процесе или стабилност институција у другој држави.

Сајбер простор је тиме постао нова арена геополитичког надметања, у којој се традиционалне категорије моћи попут војне, политичке и економске, преплићу са технолошким факторима. Разумевање улоге држава као кључних актера у овом домену представља неопходан предуслов за анализу савремених безбедносних изазова и будућег развоја међународних односа.

Државе су одговорне за заштиту сопствене националне инфраструктуре и становништва. Савремена друштва у великој мери зависе од дигиталних система који управљају енергетиком, финансијама, транспортом, здравством и комуникацијама. Напади на ове системе могу да имају озбиљне последице по функционисање државе, што захтева системску заштиту и координацију различитих институција.

Управо државе имају капацитет да организују националне системе сајбер одбране и да координишу активности војске, обавештајних служби и цивилних институција у циљу заштите критичне националне инфраструктуре.[426]

3.3 Концепт традиционалног и дигиталног суверенитета држава

Концепт суверенитета представља један од основних принципа модерних међународних односа и темељ функционисања савременог међународног правног поретка. Традиционално посматрано, суверенитет подразумева врховну власт државе над сопственом територијом, становништвом и институцијама, као и право да самостално доноси одлуке без мешања спољних актера. Овај принцип је јасно формулисан још у периоду након Вестфалског мира 1648. године, када је успостављен систем суверених националних држава као основа међународног поретка. Суверенитет је дуго био тесно повезан са физичком територијом, географским границама и контролом над материјалним ресурсима који се налазе унутар тих граница.[427]

[424] Henry Durojaye and Oluwaukola Raji, "Impact of State and State-Sponsored Actors on the Cyber Environment and the Future of Critical Infrastructure," *arXiv* (2022): 6–7.
[425] Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst & Company, 2013), 73–79.
[426] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND, 2009), 39.
[427] Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (Princeton, NJ: Princeton University Press, 1999), 20–25.

Међутим, развој информационо-комуникационих технологија и ширење интернета довели су до трансформације начина на који се суверенитет испољава у савременом свету. Појава глобалних дигиталних мрежа створила је нови простор интеракције који не поседује јасно дефинисане географске границе и у којем се комуникација и размена података одвијају готово тренутно. Овај развој довео је до питања да ли традиционални концепт суверенитета може бити примењен на дигитално окружење, или је неопходно развити нове концепте који би одражавали специфичности савремене технолошке реалности.

У том контексту, у научној и политичкој литератури појавио се појам дигиталног или сајбер суверенитета. Овај концепт се најчешће односи на способност државе да контролише, регулише и штити дигиталну инфраструктуру, информационе токове и податке који се налазе у оквиру њене надлежности. Дигитални суверенитет подразумева и способност државе да развија сопствене технолошке капацитете, да управља сајбер безбедносним системима и да доноси политике које регулишу функционисање дигиталног простора.[428]

Паралела између традиционалног и дигиталног суверенитета може се посматрати кроз неколико основних елемената. У класичном схватању, суверенитет је тесно повезан са контролом над физичком територијом. Држава има право да контролише границе, инфраструктуру и ресурсе који се налазе на њеној територији. У дигиталном контексту, овај принцип се трансформише у контролу над информационом инфраструктуром која се налази унутар државе, као што су дата центри, сервери, телекомуникационе мреже и други системи који омогућавају функционисање интернета. Иако се интернет често описује као глобална мрежа без граница, у стварности се његова физичка инфраструктура налази на територији конкретних држава и подлеже њиховом правном и регулаторном оквиру.[429]

Други важан аспект традиционалног суверенитета односи се на правну власт државе. Суверена држава има право да доноси законе који се примењују на њеној територији и на становништво које у њој живи. У дигиталном окружењу овај принцип се огледа у доношењу закона и регулатива које регулишу област сајбер безбедности, заштите података, електронских комуникација и дигиталне економије. Државе све више настоје да успоставе правни оквир који ће им омогућити контролу над дигиталним процесима, укључујући складиштење података, рад технолошких компанија и функционисање онлајн платформи. На тај начин дигитални простор постаје предмет државне регулације, слично као и традиционални економски или политички системи.[430]

Суверенитет се односи и на безбедност. Једна од основних функција државе јесте заштита територије и становништва од спољних претњи. У традиционалном контексту ова улога се остварује кроз војску, полицију и друге безбедносне институције. У дигиталном добу, ова функција се проширује на заштиту информационих система и критичне инфраструктуре од сајбер напада. Савремена друштва у великој мери зависе од дигиталних система који управљају енергетиком, транспортом, здравством, финансијама и комуникацијама. Напади на ове системе

[428] Luciano Floridi, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU," *Philosophy & Technology* 33, no. 3 (2020): 369–78.
[429] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 9–12
[430] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 11–14.

могу да имају озбиљне последице по функционисање државе и друштва, што доводи до потребе за развојем националних система сајбер одбране.[431]

Још једна важна димензија дигиталног суверенитета односи се на контролу над подацима грађана. У савременом свету подаци представљају један од најзначајнијих ресурса, јер омогућавају развој технологија, економских активности и политичких стратегија. Државе све више настоје да осигурају да се подаци који се односе на њихове грађане, институције и економске активности налазе под њиховом надлежношћу. Овај процес често се описује као „суверенитет над подацима", који подразумева право државе да регулише начин на који се подаци прикупљају, складиште и користе.[432]

Иако постоје бројне сличности између традиционалног и дигиталног суверенитета, постоје и значајне разлике. Док је традиционални суверенитет углавном везан за јасно дефинисану територију, дигитални суверенитет се остварује у простору који је по својој природи транснационалан. Интернет мреже повезују кориснике и системе широм света, што значи да активности у једној држави могу имати директне последице у другој. Ова међусобна повезаност ствара нове изазове за примену традиционалних правних и политичких механизама.

Поред тога, дигитални простор карактерише и присуство снажних недржавних актера, као што су глобалне технолошке компаније које управљају великим делом интернет инфраструктуре и дигиталних услуга. Ове компаније често имају значајан утицај на функционисање дигиталног простора, што доводи до нових питања о односу између државне власти и корпоративне моћи. У том контексту државе настоје да успоставе механизме који ће им омогућити да задрже контролу над кључним аспектима дигиталног окружења.[433]

Упркос овим изазовима, све је више држава које настоје да развију сопствени модел дигиталног суверенитета. Неке земље нагласак стављају на технолошку независност и развој сопствених дигиталних платформи, док друге настоје да ојачају регулаторне механизме који ће им омогућити већу контролу над глобалним технолошким компанијама. Без обзира на различите приступе, заједничка карактеристика ових политика јесте тежња држава да задрже одређени степен контроле над дигиталним процесима који имају значајан утицај на националну безбедност, економију и друштво у целини.

Дигитални суверенитет представља еволуцију традиционалног концепта суверенитета, прилагођену условима савременог технолошког окружења. Иако сајбер простор по својој природи превазилази физичке границе држава, државе и даље остају централни актери у регулисању, заштити и обликовању овог простора. Разумевање концепта дигиталног суверенитета представља важан елемент анализе савремених безбедносних и политичких процеса у међународним односима.

[431] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 52–60.
[432] Luciano Floridi, *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality* (Oxford: Oxford University Press, 2014), 167–70.
[433] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (New York: Oxford University Press, 2020), 243–50.

3.4 Последице сајбер ратовања по функционисање државе и друштва

Током последњих неколико деценија дошло је до интензивне дигиталне трансформације готово свих сфера друштвеног живота. Информационо-комуникационе технологије постале су кључна инфраструктура модерних држава, јер омогућавају функционисање управних система, економских активности, безбедносних структура, али и свакодневне комуникације и интеракције грађана. Дигиталне мреже данас повезују институције, привреду и појединце у јединствен систем који функционише у реалном времену, што значајно повећава ефикасност управљања и економске продуктивности, али истовремено ствара и нове безбедносне ризике.[434]

Развој интернета, великих база података и аутоматизованих система управљања довео је до тога да државе све више ослањају своје функционисање на дигиталну инфраструктуру. Државне институције користе информационе системе за управљање административним процесима, чување података о грађанима, координацију јавних политика и комуникацију између различитих нивоа власти. Истовремено, економски системи све више зависе од дигиталних платформи које омогућавају финансијске трансакције, управљање логистичким процесима и глобалну трговину. Безбедносне структуре, укључујући војску и обавештајне службе, такође се у великој мери ослањају на дигиталне системе за комуникацију, анализу података и оперативно планирање.[435]

Овај процес свеобухватне дигитализације довео је до стварања новог безбедносног окружења у којем се појављују нове врсте претњи. Сајбер простор, као глобална мрежа информационих система и комуникационих канала, постао је важан домен у којем се одвијају различити облици политичког, економског и безбедносног надметања. За разлику од ранијих периода у којима су главне безбедносне претње биле повезане са физичким просторима (копно, море и ваздух), савремене претње се све чешће јављају у дигиталном окружењу. Управо због тога многи аутори указују да је сајбер простор постао нова димензија савремених сукоба и један од кључних елемената националне и међународне безбедности.[436]

У таквом контексту сајбер ратовање се све чешће описује као један од најзначајнијих безбедносних изазова савременог доба. За разлику од традиционалних облика ратовања, који су углавном подразумевали употребу физичке силе и уништавање материјалних ресурса, сајбер ратовање се одвија у дигиталном окружењу и заснива се на употреби информационих технологија као инструмента сукоба. Ове операције могу бити усмерене на различите системе и структуре, укључујући државне институције, економске системе, критичну инфраструктуру и комуникационе мреже. Због тога потенцијалне последице сајбер конфликата не морају бити ограничене искључиво на безбедносне и војне структуре, већ се могу проширити и на друге сегменте функционисања државе и друштва.[437]

Поред тога, специфичност сајбер ратовања огледа се и у чињеници да се оно често одвија испод прага отвореног оружаног конфликта. Сајбер операције могу се спроводити у мирнодопским условима, без формалног проглашења рата и без директне употребе војне силе. Управо због тога оне представљају посебно погодан инструмент за остваривање политичких и стратегијских циљева у међународним односима. Дигитални напади могу бити усмерени на различите системе

[434] Manuel Castells, *The Rise of the Network Society*, 2nd ed. (Oxford: Wiley-Blackwell, 2010), 69–75.
[435] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 28–35.
[436] Joseph S. Nye, Jr., *The Future of Power* (New York: PublicAffairs, 2011), 113–20.
[437] Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst & Company, 2013), 11–16.

и институције, при чему њихов ефекат може бити постепен и дугорочан, што додатно отежава њихово откривање и спречавање.[438]

За разлику од традиционалних оружаних сукоба, чије су последице најчешће ограничене на физичку инфраструктуру и војне циљеве, сајбер ратовање има потенцијал да истовремено захвати више различитих система који су међусобно повезани у оквиру дигиталне инфраструктуре једне државе. Савремени информациони системи често функционишу као интегрисане мреже у којима су административни, економски и комуникациони системи тесно повезани. Управо због те међузависности, поремећаји у једном сегменту дигиталне инфраструктуре могу имати шире последице по функционисање других система.[439]

Дигитални напади могу довести до поремећаја у функционисању институција, економских система, комуникационих мрежа и јавних служби. Уколико дође до нарушавања ових система, последице могу бити вишеструке и сложене, јер савремене државе у великој мери зависе од информационих технологија за управљање ресурсима, координацију институција и пружање јавних услуга грађанима. У том смислу, сајбер конфликти имају потенцијал да утичу на различите аспекте функционисања државе и друштва, укључујући политичке, економске и социјалне процесе.[440]

Управо због ових карактеристика сајбер ратовање се све више посматра као специфичан облик савременог конфликта који одражава трансформацију међународног безбедносног окружења у условима технолошког развоја. Док су у прошлости оружани сукоби углавном били повезани са контролом над територијом и физичким ресурсима, у савременом добу све већу улогу има контрола над информацијама, комуникационим системима и дигиталном инфраструктуром. Управо ова трансформација безбедносног окружења доводи до тога да сајбер простор постаје једно од кључних поља савремених геополитичких надметања.[441]

3.4.1 Утицај на државне институције и управљање

Једна од најзначајнијих последица сајбер ратовања огледа се у потенцијалу да се наруши функционисање државних институција и механизама управљања. У савременим државама, административни системи, министарства, агенције за безбедност, као и бројне јавне институције у великој мери зависе од дигиталних информационих система. Ови системи омогућавају обраду великих количина података, координацију активности различитих институционалних структура и ефикасно доношење политичких и управљачких одлука. Међутим, управо та зависност од информационо-комуникационих технологија ствара нове безбедносне ризике који могу бити искоришћени у оквиру сајбер конфликата.[442]

Дигитална трансформација јавне управе довела је до тога да се велики број административних процедура, регистара и база података води у електронском облику. Ово укључује системе за

[438] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 21–26.
[439] Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016), 45–50
[440] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 15–18.
[441] P. W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (Boston: Houghton Mifflin Harcourt, 2018), 23–30.
[442] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 14–16, 23–25.

управљање становништвом, изборне регистре, пореске евиденције, као и базе података које користе безбедносне службе и правосудне институције. Уколико дође до сајбер напада усмереног на ове системе, последице могу бити озбиљне и вишеструке. Нападачи могу ометати функционисање информационих система, манипулисати подацима или привремено онемогућити приступ критичним информацијама. Такви поремећаји могу довести до значајних проблема у функционисању државне администрације и спровођењу јавних политика.[443]

Илустративан пример представља сајбер напад на Естонију 2007. године, који је уследио након политичких тензија са Руском Федерацијом. Током овог напада, државне институције, укључујући парламент, министарства и банкарски систем, биле су изложене масовним дистрибуираним нападима ускраћивања услуге (DDoS), што је довело до привременог прекида функционисања бројних јавних сервиса. Овај догађај показао је колико сајбер напади могу парализовати функционисање државе без употребе класичне војне силе.[444]

Посебно је значајан ризик од компромитовања осетљивих информација које се налазе у системима државне управе. Савремене државе прикупљају и обрађују велике количине података који могу имати стратешки значај, укључујући дипломатску преписку, војне планове, обавештајне процене и економске стратегије. Уколико такви подаци постану доступни страним актерима, то може довести до нарушавања националне безбедности и слабљења међународне позиције државе. Сајбер шпијунажа, која подразумева тајно прикупљање података путем дигиталних средстава, представља један од најчешћих облика сајбер активности усмерених на државне институције.[445]

У том контексту, посебно значајан пример представља афера позната као „SolarWinds“ из 2020. године, у којој су бројне америчке државне институције, укључујући Министарство финансија и Министарство трговине, биле компромитоване путем софистицираног сајбер напада на ланац снабдевања софтвером. Нападачи су успели да приступе осетљивим подацима и комуникацијама државних органа, што је указало на висок ниво рањивости чак и најразвијенијих система сајбер безбедности.[446]

Поред безбедносних последица, сајбер напади на институције могу имати и значајну политичку димензију. Уколико дође до озбиљног нарушавања информационих система државне управе, то може довести до пада поверења грађана у институције и способност државе да обезбеди ефикасно управљање и заштиту јавних ресурса. Поверење грађана представља један од кључних елемената стабилности сваког политичког система и његово нарушавање може да има далекосежне последице по легитимитет власти. У том смислу, сајбер напади на институције не представљају само технички или безбедносни проблем, већ и изазов за политичку стабилност државе.[447]

Посебно је илустративан случај сајбер активности усмерених на изборне процесе у Сједињеним Америчким Државама 2016. године, када је дошло до хаковања и објављивања података политичких организација. Овај догађај је показао да сајбер операције могу да директно утичу на

[443] Singer and Friedman, *Cybersecurity and Cyberwar*, 23–25, 119–21.
[444] Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010), 18–25, 98–100.
[445] Singer and Friedman, *Cybersecurity and Cyberwar*, 67–75.
[446] Massimo Marelli, "The SolarWinds Hack: Lessons for International Humanitarian Organizations," *International Review of the Red Cross* 104, no. 919 (2022): 1267–69.
[447] Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017), 141–45.

политичке процесе, изборе и јавно мњење, чиме се проширује домен деловања сајбер ратовања са техничког на политички ниво.[448]

Додатни ризик представља могућност манипулације информацијама у оквиру државних система. У случају успешног упада у информационе системе, нападачи могу да измене, избришу или фалсификују податке који се користе у процесима доношења одлука. Овакве активности могу довести до доношења погрешних политичких или административних одлука, што може да има значајне последице по функционисање државе. У савременим условима, када се многе одлуке доносе на основу дигитално обрађених података, интегритет информационих система постаје кључни елемент безбедности управљачких структура.[449]

Због свих ових фактора, државе све више улажу у развој механизама заштите својих информационих система, укључујући националне стратегије сајбер безбедности, специјализоване агенције и механизме међународне сарадње. Циљ ових мера јесте јачање отпорности институционалних система на сајбер претње и очување стабилности државног управљања у условима све интензивније дигитализације друштва[450].

3.4.2 Утицај на критичну инфраструктуру

Једна од најозбиљнијих претњи које произилазе из сајбер ратовања односи се на могућност напада на критичну националну инфраструктуру. Под појмом критичне инфраструктуре подразумевају се системи, мреже и објекти чије функционисање има кључни значај за стабилност и безбедност државе, као и за свакодневни живот становништва. У ову категорију обично спадају енергетски системи, водоснабдевање, телекомуникационе мреже, транспортни системи, финансијске институције и здравствени систем. Ови системи представљају основу функционисања модерних друштава и нарушавање њиховог рада може да има озбиљне последице.[451]

Савремена критична инфраструктура у великој мери се ослања на дигиталне контролне системе, као што су индустријски контролни системи (ICS) и SCADA платформе. Ови системи омогућавају управљање сложеним техничким процесима на даљину и у реалном времену. Међутим, интеграција информационих технологија у инфраструктурне системе истовремено повећава њихову рањивост на сајбер нападе. Уколико нападачи успеју да приступе овим системима, могу да изазову прекиде у функционисању инфраструктуре или да манипулишу њеним радом.[452]

Један од најзначајнијих и најчешће анализираних примера сајбер напада на критичну инфраструктуру представља операција позната као „Stuxnet“, откривена 2010. године. Овај злонамерни софтвер био је усмерен на ирански нуклеарни програм, конкретно на постројења за обогаћивање уранијума у Натанзу. Напад је довео до физичког оштећења центрифуга, што представља јединствен пример у коме је сајбер операција изазвала директне материјалне

[448] Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections* (Washington, DC: ODNI, 2017), 1, 6, 10–11.
[449] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 13–18.
[450] ENISA, *National Cyber Security Strategies in the World* (Athens: European Union Agency for Cybersecurity, 2019), 22–27.
[451] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 24.
[452] Keith Stouffer, Joe Falco, and Karen Scarfone, *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication 800-82 Revision 1 (Gaithersburg, MD: National Institute of Standards and Technology, 2011), 1–2, 16–18.

последице у индустријском систему. У научној и стручњачкој јавности широко је прихваћено становиште да су иза ове операције стајале државе, пре свега Сједињене Америчке Државе и Израел, што указује на нову фазу милитаризације сајбер простора.[453]

Један од најчешће навођених сценарија у литератури о сајбер безбедности односи се на могућност напада на електроенергетску мрежу. Електрична енергија представља основу функционисања готово свих других инфраструктурних система, укључујући телекомуникације, транспорт и здравствене установе. Уколико би дошло до масовног прекида снабдевања електричном енергијом као последице сајбер напада, последице би се брзо проширile на друге секторе друштва. Болнице би могле остати без електричне енергије, комуникационе мреже би могле престати да функционишу, а транспортни системи могли би бити парализовани.[454]

Практичну потврду оваквог сценарија представља сајбер напад на електроенергетску мрежу Украјине 2015. године. Током овог напада, који се приписује руским сајбер јединицама, хакери су успели да преузму контролу над електроенергетским системом и изазову прекид снабдевања електричном енергијом за стотине хиљада грађана Украјине. Овај догађај представља први познати случај успешног сајбер напада који је довео до нестанка струје на великој територији. Овим је потврђена способност сајбер операција да произведу ефекте упоредиве са класичним, традиционалном нападима на инфраструктуру.[455]

Поред енергетских система, значајну улогу у функционисању друштва имају и телекомуникационе мреже. Ове мреже омогућавају комуникацију између државних институција, привредних субјеката и грађана. У случају успешног сајбер напада на телекомуникациону инфраструктуру, може доћи до прекида комуникације, што би значајно отежало координацију активности институција у кризним ситуацијама. У савременим условима, где се многи процеси ослањају на дигиталну комуникацију, поремећаји у раду телекомуникационих система могу имати озбиљне последице по функционисање државе.[456]

Посебно је значајан и пример злонамерног софтвера „NotPetya“из 2017. године, који је иницијално био усмерен на украјинске институције и инфраструктуру, али се брзо проширио на глобалном нивоу. Иако је формално представљен као рансомвер, анализа је показала да је његова основна функција била деструктивна. Напад је изазвао озбиљне поремећаје у функционисању транспортних система, логистичких компанија и државних институција, при чему су поједине државе овај напад јавно приписале Руској Федерацији. Овај случај показује да сајбер напади на инфраструктуру могу да имају не само локалне, већ и глобалне последице.[457]

Истраживања у области сајбер безбедности показују да је један од проблема у заштити критичне инфраструктуре чињеница да су многи инфраструктурни системи пројектовани у периоду када сајбер претње нису представљале значајан безбедносни фактор. Као резултат тога, поједини

[453] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014), 5–6, 118–19, 143–45.
[454] Singer and Friedman, *Cybersecurity and Cyberwar*, 24.
[455] Robert M. Lee, Michael J. Assante, and Tim Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid* (Washington, DC: Electricity Information Sharing and Analysis Center and SANS Industrial Control Systems, 2016), 5, 9–15, 25.
[456] Robert M. Lee, Michael J. Assante, and Tim Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid* (Washington, DC: Electricity Information Sharing and Analysis Center and SANS Industrial Control Systems, 2016), 5, 9–15, 25.
[457] *Case Study: The NotPetya Campaign* (Budapest: Ludovika University of Public Service, 2024), 9–10

индустријски системи и даље користе застареле технологије које не поседују адекватне механизме заштите од сајбер напада. Ово повећава ризик да критична инфраструктура постане мета актера који настоје да остваре политичке, војне или економске циљеве путем сајбер операција.[458]

Због потенцијалних последица које могу да настану услед нарушавања инфраструктурних система, заштита критичне инфраструктуре постала је један од приоритета националних стратегија сајбер безбедности. Државе настоје да унапреде механизме заштите инфраструктуре кроз развој техничких мера безбедности, јачање институционалних капацитета и унапређење сарадње између јавног и приватног сектора. Ови напори имају за циљ да повећају отпорност инфраструктурних система на сајбер претње и обезбеде континуитет функционисања друштва у условима потенцијалних сајбер конфликата.

3.4.3 Економске последице сајбер ратовања

Сајбер ратовање може да има значајне економске последице по државе и друштва. Савремена глобална економија у великој мери зависи од дигиталних информационих система који омогућавају функционисање финансијских тржишта, електронску трговину, логистичке процесе и управљање индустријском производњом. Банкарски сектор, берзе, платни системи и међународне финансијске трансакције ослањају се на сложене мреже информационих технологија које омогућавају брз и ефикасан проток капитала. У таквим условима, сајбер напади усмерени на финансијске институције или дигиталну економску инфраструктуру могу да доведу до озбиљних поремећаја у функционисању економског система.[459]

Један од најочигледнијих облика економских последица сајбер ратовања односи се на директне финансијске губитке. Напади на банкарске системе, платне платформе или берзанске институције могу да доведу до крађе финансијских средстава, блокирања трансакција или привременог прекида функционисања финансијских тржишта. Поред тога, сајбер напади могу да изазову значајне трошкове за компаније и институције које морају да уложе додатна средства у обнову система, истрагу инцидената и јачање безбедносних механизама. Илустративан пример представља напад на Централну банку Бангладеша 2016. године, када су актери повезани са Северном Корејом злоупотребили SWIFT систем и покушали да изврше трансфере у износу близу милијарду долара, при чему је успешно украдено 81 милион долара. Овај случај је показао да сајбер операције могу бити употребљене као инструмент директног финансијског подривања државних и међународних финансијских токова.[460]

Поред директних финансијских губитака, сајбер напади могу да доведу и до ширих економских последица које утичу на стабилност тржишта и економски развој државе. Нарушавање поверења у дигиталне системе може да утиче на функционисање финансијских институција и инвестициону климу. Уколико инвеститори и привредни субјекти процене да постоји висок ризик од сајбер напада на финансијску инфраструктуру, то може да доведе до смањења инвестиција, повећања трошкова пословања и успоравања економског раста. Поверење у стабилност и безбедност

[458] Stouffer, Falco, and Scarfone, *Guide to Industrial Control Systems (ICS) Security*, 1–2, 16–18.
[459] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 119–21.
[460] United States Department of Justice, "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," September 6, 2018

финансијског система представља један од кључних предуслова функционисања модерне економије, па његово нарушавање може имати дугорочне негативне ефекте.[461]

Сајбер ратовање може да има значајан утицај и на функционисање глобалних ланаца снабдевања. Савремена производња и трговина ослањају се на дигиталне системе за управљање логистиком, транспортом и складиштењем робе. Уколико дође до сајбер напада на ове системе, може да уследи прекид у снабдевању, кашњења у производњи и поремећаја у међународној трговини. У условима глобализоване економије, где су производни процеси често распоређени у више држава, чак и ограничени поремећаји у функционисању дигиталних система могу имати значајне последице по економске активности на ширем нивоу. У том смислу, напад „Shamoon“ на Saudi Aramco 2012. године имао је шири економски значај од непосредне штете нанете једној компанији јер су брисањем података на десетинама хиљада рачунара нападачи показали колико су рањиви енергетски и логистички системи који подржавају једну од кључних индустрија светске економије.[462]

Посебно значајан аспект економских последица сајбер ратовања представља индустријска и технолошка шпијунажа. У савременим условима, технолошке иновације, истраживање и развој, као и интелектуална својина представљају један од најважнијих извора економске конкурентности. Државе могу користити сајбер операције како би дошле до технолошких решења, индустријских тајни и пословних стратегија конкурената. Овакве активности могу омогућити бржи технолошки развој или економску предност без улагања у дуготрајне истраживачке процесе. У том смислу, сајбер шпијунажа представља инструмент економског надметања између држава и компанија у глобалној економији. Веома упечатљив пример представља оптужница Министарства правде Сједињених Америчких Држава из 2014. године против петорице припадника кинеске Народноослободилачке војске, који су оптужени за сајбер шпијунажу усмерену против америчких компанија из нуклеарног, металског и соларног сектора.[463]

Слично томе, економске последице се не исцрпљују само у непосредној крађи новца или података. Када држава или актери повезани са њом успеју да приступе у пословне системе, истраживачко-развојне програме или преузму податке о трговинским преговорима, последице могу дс буду дугорочне и структурне. Такве операције могу да утичу на пад конкурентности, губитак тржишне предности и слабљење технолошког суверенитета нападнуте државе или компаније. Због тога економска димензија сајбер ратовања данас обухвата читав спектар последица: од непосредне крађе средстава, преко парализе пословних процеса, до стратешког слабљења привредних капацитета друге државе.[464]

Због потенцијалних економских последица сајбер напада, све већи број држава посвећује значајну пажњу заштити економских система и финансијске инфраструктуре. Националне стратегије сајбер безбедности све чешће укључују мере за заштиту банкарског сектора, финансијских тржишта и индустријских система од сајбер претњи. Ове мере обухватају развој техничких

[461] Joseph S. Nye, Jr., “Deterrence and Dissuasion in Cyberspace,” *International Security* 41, no. 3 (2017): 61–63.
[462] James A. Lewis, “Iran’s Threat to Saudi Critical Infrastructure: The Implications for U.S.-Iranian Escalation” (Washington, DC: Center for Strategic and International Studies, 2019); Council on Foreign Relations, “Compromise of Saudi Aramco and RasGas,” *Cyber Operations Tracker*.
[463] United States Department of Justice, “U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization,” May 19, 2014.
[464] Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017), 156–60.

механизама заштите, унапређење регулаторних оквира и јачање сарадње између државних институција и приватног сектора. Савремена искуства показују да је економска безбедност државе све теже одвојити од безбедности њене дигиталне инфраструктуре.[465]

3.4.4 Утицај на друштво и јавно мњење

Поред институционалних, безбедносних и економских последица, сајбер ратовање има дубок и све израженији утицај на друштво и јавно мњење. Савремени дигитални комуникациони системи, пре свега друштвене мреже, онлајн медији и платформе за размену информација, постали су кључни канали кроз које се обликује перцепција стварности, политички ставови и друштвене вредности. У таквом окружењу, сајбер простор не представља само технички домен, већ и простор у којем се одвијају информационе и психолошке операције са потенцијално далекосежним последицама по стабилност држава.[466]

Један од кључних аспеката утицаја сајбер ратовања на друштво односи се на ширење дезинформација и манипулацију информацијама. Државе и актери повезани са њима све чешће користе дигиталне платформе за ширење лажних или обмањујућих информација са циљем обликовања јавног мњења у складу са сопственим политичким интересима. Ове активности укључују креирање лажних профила, координисане кампање на друштвеним мрежама, као и употребу алгоритама за појачавање одређених наратива.[467] Илустративан пример представља случај Cambridge Analytica, који је показао како подаци прикупљени са друштвених мрежа могу да се користе за прецизно циљање бирача и утицај на политичке ставове. Иако овај случај није класичан пример државног сајбер напада, он јасно указује на потенцијал злоупотребе дигиталних података у политичке сврхе. У комбинацији са државно подржаним информационим операцијама, овакве технике могу да постану снажан инструмент утицаја на демократске процесе.[468]

Поред тога, значајан пример представљају информационе операције које се приписују Кини, а које су биле усмерене на обликовање јавног мњења у вези са пандемијом COVID-19. Истраживања су показала да су коришћене координисане кампање на друштвеним мрежама како би се промовисале одређене интерпретације догађаја, ублажиле критике и ојачала међународна позиција државе. Овакве активности указују на све већу улогу информационог простора као продужетка геополитичког надметања.[469]

Утицај на друштво огледа се и у способности сајбер операција да подстакну друштвене поделе. Ширењем контроверзних или поларизујућих садржаја, актери могу да продубе постојеће друштвене тензије и ослабе социјалну кохезију. У том смислу, сајбер ратовање не мора да има за циљ директно уништавање инфраструктуре, већ дестабилизацију друштва кроз утицај на међуљудске односе, политичке ставове и поверење у институције.[470]

---

[465] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 63–67.
[466] Samantha Bradshaw and Philip N. Howard, *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*, Working Paper 2019.2 (Oxford: Project on Computational Propaganda, 2019), i, 1, 22.
[467] Bradshaw and Howard, *The Global Disinformation Order*, i, 1, 18, 22.
[468] Government of Canada, Rapid Response Mechanism Canada, "October 23 Statement on Spamouflage," October 23, 2023, 1–3.
[469] National Security Bureau, Republic of China (Taiwan), *China's Disinformation Dissemination Patterns in 2024* (Taipei: National Security Bureau, 2024), 1–6.
[470] Office of the Director of National Intelligence, National Counterintelligence and Security Center, *Cyber Aware Case Study: OPM Data Breach* (Washington, DC: ODNI/NCSC, n.d.), 2.

Посебно је значајан и пример из 2015. године, када је дошло до масовног сајбер напада на америчку Канцеларију за управљање кадровима (Office of Personnel Management – OPM), који се приписује кинеским актерима. У овом нападу компромитовани су подаци милиона државних службеника, укључујући осетљиве информације о безбедносним проверама. Иако је примарни циљ био прикупљање обавештајних података, овај случај је показао како компромитовање личних података може да има и шири друштвени утицај, укључујући осећај несигурности међу грађанима и слабљење поверења у државне институције.[471]

Још један важан аспект односи се на улогу алгоритама и аутоматизованих система у ширењу информација. Друштвене мреже користе алгоритме који фаворизују садржај који изазива снажне реакције, што може да доведе до брзог ширења сензационалистичких или нетачних информација. Уколико се овакви механизми злоупотребе у оквиру координисаних информационих операција, ефекат на јавно мњење може да буде значајан и дуготрајан.[472]

Утицај на јавно мњење има директне политичке последице. Уколико грађани изгубе поверење у медије, институције или изборне процесе, то може да доведе до смањења политичке стабилности и легитимитета власти. У екстремним случајевима, овакве активности могу да изазову политичке кризе или друштвене немире. Због тога се сајбер ратовање све више посматра као инструмент „меке моћи“, који омогућава државама да остваре своје циљеве без директне употребе војне силе.[473]

Поред политичких последица, сајбер операције могу да имају и психолошки утицај на становништво. Континуирано излагање дезинформацијама, осећај несигурности и неповерење у институције могу да доведу до повећања анксиозности и друштвене фрагментације. У том смислу, сајбер ратовање обухвата не само техничке и политичке, већ и психолошке димензије које утичу на свакодневни живот грађана[474].

Због свих ових фактора, заштита информационог простора постаје један од кључних изазова савремених држава. Поред техничких мера безбедности, неопходно је развијати и механизме за јачање медијске писмености, критичког мишљења и отпорности друштва на манипулацију информацијама. У условима дигиталног доба, способност друштва да препозна и одговори на информационе претње постаје један од кључних елемената националне безбедности.

3.4.5 Безбедносне и војне последице

Сајбер ратовање има значајне импликације по војне и безбедносне системе савремених држава. Развој информационо-комуникационих технологија довео је до дубоке трансформације начина на који функционишу војне организације, као и начина на који се планирају и изводе војне операције. Савремене оружане снаге све више зависе од дигиталних система који омогућавају комуникацију између јединица, управљање војним ресурсима, прикупљање обавештајних података и координацију сложених војних активности. Услед ове технолошке зависности, сајбер простор постаје важан домен савремених војних конфликата.[475]

[471] Bradshaw and Howard, *The Global Disinformation Order*, 22.
[472] National Security Bureau, Republic of China (Taiwan), *China's Disinformation Dissemination Patterns in 2024*, 5–6.
[473] Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2017): 60–63.
[474] Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017), 167–73.
[475] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 190–91.

Један од основних аспеката безбедносних последица сајбер ратовања односи се на могућност нарушавања система командовања и контроле (Command and Control – C2) који представљају основу функционисања војних структура. Ови системи омогућавају координацију активности различитих јединица, размену информација између командних структура и доношење оперативних одлука у реалном времену. Уколико би сајбер напад успео да наруши функционисање ових система, то би могло довести до значајног смањења способности војске да ефикасно управља својим снагама и реагује на кризне ситуације.[476]

Савремене војске у великој мери користе дигиталне системе за навигацију, извиђање и прикупљање обавештајних података. Сателитски системи, беспилотне летелице, радарске мреже и различити сензорски системи омогућавају прикупљање информација које су кључне за планирање војних операција. Сајбер напади усмерени на ове системе могу довести до губитка или манипулације подацима, што може значајно утицати на способност војних команданата да донесу правовремене и тачне одлуке. У таквим условима, сајбер операције могу постати средство за нарушавање информационе надмоћи противника.[477]

Поред директног утицаја на функционисање војних система, сајбер ратовање може имати значајну улогу у оквиру ширих војних стратегија. У савременим конфликтима сајбер операције се често користе као средство припреме за традиционалне војне акције. Напади на комуникационе системе, системе командовања, радарске системе или логистичке мреже могу да ослабе способност противника да координише своје снаге и организује одбрану. На тај начин сајбер операције стварају повољније услове за извођење конвенционалних војних операција.[478]

Још један важан аспект безбедносних последица сајбер ратовања односи се на могућност угрожавања савремених оружаних система који се ослањају на софтвер и дигиталне контролне механизме. Многи савремени системи наоружања, укључујући системе противваздушне одбране, ракетне системе и беспилотне летелице, функционишу на основу сложених информационих система. Уколико би нападачи успели да компромитују ове системе, могли би изазвати њихово неисправно функционисање или чак преузети контролу над појединим системима. Овај аспект сајбер ратовања отвара нове безбедносне изазове који раније нису постојали у традиционалним облицима оружаних сукоба.[479]

Сајбер ратовање такође може да утиче на стратегијску стабилност између држава. Уколико државе процене да њихови критични војни системи могу да буду рањиви на сајбер нападе, то може довести до повећаног нивоа неповерења и нестабилности у међународним односима. Нејасноћа у погледу порекла сајбер напада, као и потешкоће у приписивању одговорности за такве активности, додатно компликују ситуацију и могу повећати ризик од ескалације конфликата. У том контексту, сајбер простор постаје ново поље стратешког надметања између држава.[480]

Због растућег значаја сајбер претњи, многе државе развијају специјализоване војне јединице и командне структуре задужене за сајбер операције. Ове структуре имају задатак да штите војне

[476]Ibid, 171, 177–78.
[477] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 308, 487.
[478] Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst & Company, 2013), 14–16.
[479] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 171
[480] Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2017): 60–64.

информационе системе, али и да спроводе офанзивне сајбер операције у случају конфликта. Увођење сајбер домена као посебне области војног деловања представља једну од најзначајнијих трансформација савремених војних стратегија. Савремене доктрине све чешће препознају сајбер простор као равноправан домен ратовања, уз копно, море, ваздух и космос.[481]

3.5 Стратегијско-доктринарни оквир сајбер безбедности

Стратегијско-доктринарна документа представљају полазну основу за развој националних политика у области сајбер безбедности. У условима интензивне дигитализације савременог друштва, државе све више препознају потребу за систематским приступом управљању ризицима који произилазе из сајбер простора. Управо због тога стратегијски документи имају кључну улогу у дефинисању националних приоритета, идентификацији главних претњи и одређивању механизама заштите критичне информационе инфраструктуре. Националне стратегије сајбер безбедности обично обухватају свеобухватну процену ризика, идентификацију кључних актера у систему безбедности, као и успостављање механизама координације између државних институција, приватног сектора и међународних партнера.[482]

Развој стратегијских докумената у области сајбер безбедности повезан је са растућим значајем информационих система у функционисању савремених држава. Државне институције, енергетски системи, транспортна инфраструктура, финансијски сектор и здравствени систем у великој мери зависе од дигиталних технологија и информационих мрежа. Ова зависност истовремено повећава и рањивост ових система на различите облике сајбер претњи, укључујући сајбер криминал, индустријску шпијунажу, сајбер саботажу и сајбер операције које спроводе државни актери. У том контексту, националне стратегије имају задатак да успоставе интегрисан систем управљања сајбер ризицима који обухвата превенцију, заштиту, реаговање и опоравак након сајбер инцидената.[483]

Овај приступ јасно се може уочити на примеру Естоније, која је након масовних сајбер напада 2007. године развила један од најнапреднијих националних система сајбер безбедности у Европи. Естонска стратегија ставља посебан акценат на отпорност дигиталних националних система, развој капацитета за одговор на инциденте и блиску сарадњу са НАТО структурама, што је довело до оснивања НАТО Центра изврсности за сајбер одбрану у Талину. Овај пример показује конкретно како искуство сајбер напада може директно да утиче на обликовање стратегијских приоритета једне државе.[484]

Један од основних циљева стратегијских докумената јесте јачање отпорности државе на сајбер претње. Концепт отпорности подразумева способност институција и инфраструктуре да издрже, апсорбују и брзо и ефикасно се опораве од последица сајбер напада. То подразумева развој капацитета за превенцију, детекцију и реаговање на сајбер инциденте, као и изградњу

[481] Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (London: Hurst, 2022); NATO, "Warsaw Summit Communiqué," July 9, 2016, para. 70.
[482] European Union Agency for Network and Information Security (ENISA), *National Cyber Security Strategies: Practical Guide on Development and Execution* (Heraklion: ENISA, 2012), 12–13.
[483] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 28–35; ENISA, *National Cyber Security Strategies*, 12–14.
[484] Government Office of Estonia, *Cyber Security Strategy 2014–2017* (Tallinn: Government Office of Estonia, 2014), 2–3; Republic of Estonia, *Cybersecurity Strategy 2019–2022* (Tallinn: Ministry of Economic Affairs and Communications, 2019), 3–4; NATO Cooperative Cyber Defence Centre of Excellence, "About Us," accessed April 18, 2026.

институционалних механизама који омогућавају ефикасну координацију различитих актера у систему националне безбедности.

Стратегије често наглашавају значај развоја националних система за рано упозоравање, као и унапређење механизама за размену информација о сајбер претњама између различитих институција и организација.[485] Сличан приступ може да се уочи и у стратегији Израела, који је развио високо централизован модел управљања сајбер безбедношћу кроз Националну сајбер дирекцију. Израелски модел комбинује војне, цивилне и приватне капацитете, са посебним нагласком на иновације и брз одговор на претње. Овај приступ омогућио је Израелу да постане један од глобалних лидера у области сајбер безбедности, што показује значај интегрисаног стратегијског планирања.[486]

Посебан значај у стратегијским документима има и питање заштите критичне информационе инфраструктуре. Као што је већ наглашено, под овим појмом подразумевају се информациони системи чије би нарушавање могло имати озбиљне последице по функционисање државе, економску стабилност или безбедност становништва. У такве системе спадају енергетске мреже, телекомуникационе инфраструктуре, системи управљања саобраћајем, банкарски системи и здравствене информационе мреже. Због њиховог стратешког значаја, националне стратегије сајбер безбедности често предвиђају посебне механизме заштите критичне инфраструктуре, укључујући примену високих безбедносних стандарда, редовне процене ризика и развој планова за управљање кризним ситуацијама.[487] Добар пример представља Немачка, која је усвојила свеобухватну стратегију заштите критичне инфраструктуре и успоставила Федералну канцеларију за информациону безбедност (BSI) као централну институцију у овој области. Немачки приступ посебно наглашава сарадњу са приватним сектором, с обзиром на то да велики део критичне инфраструктуре није у директном власништву државе. Ово указује на значај јавно-приватног партнерства у савременим системима сајбер безбедности.[488]

Поред националних стратегија, значајну улогу у обликовању стратегијског оквира сајбер безбедности имају и војне доктрине. Са развојем дигиталних технологија и све већом зависношћу војних система од информационих мрежа, сајбер простор је постепено постао један од кључних домена савремених војних операција. У савременим безбедносним концептима сајбер простор се све чешће третира као равноправан домен ратовања, уз копно, море, ваздух и космос. У складу са тим, многе државе у својим војним доктринама предвиђају развој офанзивних и дефанзивних сајбер способности као важан елемент националне безбедности.[489] Увођење сајбер простора као новог домена војног деловања довело је до значајних промена у војним стратегијама и доктринама. На пример, Француска је у својим одбрамбеним документима јасно дефинисала могућност употребе офанзивних сајбер капацитета као дела националне одбрамбене политике.

[485] ENISA, *National Cyber Security Strategies*, 12–14
[486] Government of Israel, *National Cybersecurity Strategy 2025* (Jerusalem: Israel National Cyber Directorate, 2025), 7–11.
[487] European Union Agency for Network and Information Security (ENISA), *National Cyber Security Strategies: Practical Guide on Development and Execution* (Heraklion: ENISA, 2012), 12–14.
[488] Federal Ministry of the Interior and Community, *Cyber Security Strategy for Germany 2021* (Berlin: Federal Ministry of the Interior and Community, 2021); Federal Office for Information Security, "Federal Office for Information Security," accessed April 18, 2026.
[489] Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (London: Hurst, 2022), 51–54; NATO, "Warsaw Summit Communiqué," July 9, 2016, para. 70.

Овај приступ указује на све већу интеграцију сајбер операција у класичне војне концепте и стратегије.[490]

Стратегијско планирање у области сајбер безбедности подразумева и развој механизама сарадње са међународним организацијама и партнерским државама. Сајбер претње имају изразито транснационални карактер, што значи да ниједна држава не може ефикасно да се суочи са њима искључиво сопственим капацитетима. Напади на информационе системе често се изводе преко глобалних мрежа, уз коришћење инфраструктуре која се налази у више различитих држава. Због тога је међународна сарадња постала један од кључних елемената савремених политика сајбер безбедности.[491]

У том контексту, Европска унија представља значајан пример наднационалног приступа сајбер безбедности кроз директиву о безбедности мрежа и информационих система (NIS директива), која обавезује државе чланице да развију националне капацитете и успоставе механизме сарадње. Овакав модел указује на значај регионалних иницијатива у јачању отпорности дигиталног простора.[492]

Иако су Сједињене Америчке Државе и Кина међу најразвијенијим актерима у области сајбер безбедности, њихови модели се разликују. Док САД наглашавају партнерство са приватним сектором и развој офанзивних способности, Кина развија централизовани систем контроле и управљања сајбер простором. Ове разлике показују да не постоји јединствен модел, већ да стратегијски приступи зависе од политичког система, економске структуре и безбедносних приоритета државе.[493]

Све наведено указује на то да стратегијско-доктринарни оквир представља један од најважнијих елемената националних система сајбер безбедности. Он омогућава државама да систематски приступе управљању сајбер ризицима, дефинишу приоритете националне безбедности и развију институционалне капацитете неопходне за заштиту дигиталног простора. У условима све већег значаја информационих технологија, развој свеобухватних стратегијских докумената постаје један од кључних предуслова за очување стабилности, безбедности и суверенитета савремених држава.

3.6 Нормативно-правни оквир сајбер безбедности

Нормативно-правни оквир представља један од кључних елемената националних система сајбер безбедности. У условима све веће зависности савремених држава од информационо-комуникационих технологија, правна регулатива има значајну улогу у успостављању правила

[490] French Ministry for the Armed Forces, *Droit international appliqué aux opérations dans le cyberespace* (Paris: Ministry for the Armed Forces, 2019), 7–9.
[491] European Union Agency for Network and Information Security (ENISA), *National Cyber Security Strategies: Practical Guide on Development and Execution* (Heraklion: ENISA, 2012), 12–14; Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2017): 58–60.
[492] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), *Official Journal of the European Union* L333 (2022): 80–152, esp. 84–86, 98–101.
[493] U.S. Department of Defense, *2023 Department of Defense Cyber Strategy Summary* (Washington, DC: Department of Defense, 2023), 2–3; The State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era* (Beijing: State Council Information Office, 2023), 3–6.

понашања у сајбер простору и дефинисању механизама заштите информационих система. Законодавство у овој области има за циљ да уреди одговорности државних институција, приватних организација и појединаца у погледу безбедног коришћења дигиталних технологија, као и да обезбеди ефикасне механизме за спречавање, откривање и санкционисање сајбер инцидената.[494]

Развој нормативно-правног оквира сајбер безбедности условљен је специфичностима сајбер простора као глобалног и динамичног окружења. За разлику од традиционалних области права, које се заснивају на јасно дефинисаним територијалним границама, сајбер простор карактерише висок степен транснационалности. Сајбер напади се често изводе преко инфраструктуре која се налази у више различитих држава, што отежава утврђивање надлежности и спровођење правних мера. Управо због тога савремене државе настоје да развију законодавне оквире који омогућавају ефикасно реаговање на сајбер претње, али и подстичу међународну сарадњу у области сајбер безбедности.[495]

Државе најчешће доносе посебне законе о информационој безбедности, критичној инфраструктури и заштити података. Ови прописи регулишу обавезе организација које управљају критичним информационим системима, укључујући обавезу примене одређених безбедносних стандарда, редовно спровођење процене ризика, пријављивање сајбер инцидената и сарадњу са надлежним институцијама. У многим државама законодавство предвиђа и успостављање система националних CERT или CSIRT тимова који имају задатак да прате сајбер претње и координишу одговор на безбедносне инциденте.[496]

Посебан сегмент нормативно-правног оквира односи се на регулисање заштите критичне инфраструктуре. Нарушавање функционисања ових система може имати озбиљне последице по националну безбедност и јавну безбедност, због чега законодавство у овој области често предвиђа строге безбедносне стандарде и посебне механизме надзора.[497]

Један од важних аспеката нормативно-правног оквира односи се и на кривичноправну регулацију сајбер криминала. Сајбер напади могу да укључују различите облике незаконитих активности, као што су неовлашћен приступ информационим системима, крађа података, саботажа дигиталне инфраструктуре, финансијске преваре или ширење злонамерног софтвера. Законодавство у овој области има за циљ да обезбеди ефикасно кривично гоњење починилаца и спречи злоупотребу информационих технологија. У том контексту, многе државе су у своје кривичне законе увеле

[494] European Union Agency for Network and Information Security (ENISA), *National Cyber Security Strategies: Practical Guide on Development and Execution* (Heraklion: ENISA, 2012), 12–14.
[495] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 62–63, 101, 115–16.
[496] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), *Official Journal of the European Union* L333 (2022): 80–152, esp. 84–86, 98–101.
[497] Directive (EU) 2022/2555, *Official Journal of the European Union* L333 (2022): 84–86, 98–101; European Union Agency for Network and Information Security (ENISA), *National Cyber Security Strategies: Practical Guide on Development and Execution* (Heraklion: ENISA, 2012), 12–14

посебна кривична дела која се односе на злоупотребу информационих система и дигиталних података.[498]

Поред кривичноправне регулативе, нормативно-правни оквир сајбер безбедности обухвата и прописе који се односе на заштиту личних података и приватности. Савремене информационе технологије омогућавају прикупљање, обраду и складиштење огромних количина података о појединцима, што отвара бројна питања у вези са заштитом приватности и безбедности личних информација. Због тога су многе државе усвојиле законодавство које регулише обраду личних података и прописује обавезе организација које управљају овим подацима. Ови прописи имају за циљ да обезбеде баланс између развоја дигиталних технологија и заштите основних права грађана.[499]

Поред националног законодавства, значајну улогу имају и међународни правни инструменти који регулишу понашање држава у сајбер простору. Иако још увек не постоји свеобухватни међународни уговор који се искључиво бави сајбер ратовањем, постоје бројне иницијативе које имају за циљ развој међународних норми у овој области. Један од најзначајнијих докумената у том контексту је Будимпештанска конвенција о сајбер криминалу, која представља први међународни правни инструмент посвећен борби против сајбер криминала и јачању међународне сарадње у истрагама ових кривичних дела.[500]

Будимпештанска конвенција има посебан значај јер успоставља заједничке стандарде у области криминализације одређених облика сајбер криминала, као што су незаконит приступ информационим системима, пресретање података, злоупотреба уређаја и рачунарске преваре. Поред тога, ова конвенција предвиђа механизме међународне сарадње који омогућавају бржу размену информација и координацију истрага између различитих држава. Ови механизми су од посебног значаја у борби против сајбер криминала, с обзиром на то да се многе незаконите активности у сајбер простору одвијају преко више националних јурисдикција.[501]

Поред Будимпештанске конвенције, значајну улогу у развоју међународних норми у области сајбер безбедности имају и иницијативе Уједињених нација, као и бројни регионални механизми сарадње. У оквиру Уједињених нација формиране су експертске групе које се баве питањем примене међународног права у сајбер простору и развојем норми одговорног понашања држава у дигиталном окружењу. Ове иницијативе имају за циљ да допринесу стабилности међународног система и спрече ескалацију конфликата у сајбер простору.[502]

[498] Council of Europe, *Convention on Cybercrime*, ETS No. 185 (Budapest: Council of Europe, 2001), arts. 2–10; Susan W. Brenner, "U.S. Cybercrime Law: Defining Offenses," *Information & Communications Technology Law* 13, no. 3 (2004): 231–32.

[499] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), *Official Journal of the European Union* L119 (2016): 1–88, recitals 1–13, arts. 5, 24, 32.

[500] Council of Europe, *Convention on Cybercrime*, ETS No. 185 (Budapest: Council of Europe, 2001), preamble, arts. 2–10, 23–25

[501] Council of Europe, *Convention on Cybercrime*, ETS No. 185 (Budapest: Council of Europe, 2001), arts. 2–10, 23–35; Council of Europe, *Explanatory Report to the Convention on Cybercrime*, paras. 44–54, 245–270.

[502] United Nations, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, 2021; United Nations, *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, final report, 2021, paras. 34–39.

Нормативно-правни оквир представља један од основних предуслова за ефикасно функционисање националних система сајбер безбедности. Развој свеобухватног законодавства, усклађеног са међународним стандардима, омогућава државама да успоставе јасна правила понашања у сајбер простору, заштите критичну инфраструктуру и обезбеде ефикасно реаговање на сајбер претње. У условима све веће дигиталне повезаности савременог друштва, правна регулатива постаје један од кључних инструмената за очување безбедности и стабилности у сајбер простору.

3.7 Организационе и институционалне структуре држава у систему сајбер безбедности

Поред стратегијско-доктринарних докумената и нормативно-правног оквира, ефикасна заштита сајбер простора захтева и развој одговарајућих организационих и институционалних структура. Савремене државе све више препознају да сајбер безбедност представља комплексну и мултидисциплинарну област која захтева координисано деловање различитих институција, укључујући органе државне управе, безбедносне службе, војне структуре, регулаторна тела, као и приватни и академски сектор. Управо због тога изградња функционалног институционалног система представља један од кључних предуслова за ефикасно управљање сајбер претњама и одржавање стабилности дигиталног простора.[503]

Организационе структуре у области сајбер безбедности обично се заснивају на принципу мултисекторског приступа, који подразумева сарадњу између различитих институционалних актера. Овај приступ произилази из чињенице да значајан део критичне информационе инфраструктуре није у директном власништву државе, већ приватних компанија. Енергетски системи, телекомуникационе мреже, банкарски сектор и транспортна инфраструктура у великој мери зависе од приватних оператера, што значи да ефикасна заштита ових система није могућа без блиске сарадње између јавног и приватног сектора.[504] Добар пример оваквог приступа представља Уједињено Краљевство, које је успоставило Национални центар за сајбер безбедност (NCSC) као кључну институцију за координацију између државе и приватног сектора. Ова институција делује као централна тачка за размену информација, реаговање на инциденте и подршку критичној инфраструктури, што показује значај интегрисаног институционалног приступа.[505]

Један од кључних елемената организационе структуре система сајбер безбедности представљају национални тимови за реаговање на рачунарске инциденте, познати као Computer Emergency Response Team (CERT) или Computer Security Incident Response Team (CSIRT). Ове институције имају задатак да прате сајбер претње, анализирају безбедносне инциденте и пружају техничку подршку организацијама које су погођене сајбер нападима. Поред тога, CERT/CSIRT тимови имају важну улогу у размени информација о безбедносним претњама и координацији одговора на сајбер инциденте на националном и међународном нивоу.[506] На пример, Финска је развила један од најефикаснијих националних CERT система у Европи, који функционише у оквиру

[503] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 88–92.
[504] European Union Agency for Network and Information Security (ENISA), *National Cyber Security Strategies: Practical Guide on Development and Execution* (Heraklion: ENISA, 2012), 12–14.
[505] National Cyber Security Centre, *The Launch of the National Cyber Security Centre* (London: NCSC, 2016), 8; National Cyber Security Centre, "The National Cyber Security Centre," accessed April 18, 2026.
[506] European Union Agency for Cybersecurity (ENISA), *How to Setup Up CSIRT and SOC* (Athens: ENISA, 2020), 9–12, 20–24.

Транспортно-комуникационе агенције (Traficom). Фински модел карактерише висок ниво поверења између државе и приватног сектора, као и брза размена информација о претњама, што значајно доприноси отпорности националног система.[507]

Национални CERT центри често делују као централне институције за управљање сајбер инцидентима, јер прикупљају и анализирају податке о сајбер претњама и координишу активности различитих институција које учествују у систему сајбер безбедности. Ове институције такође играју значајну улогу у едукацији организација и грађана о ризицима у сајбер простору, као и у развоју препорука и стандарда за заштиту информационих система.[508]

Поред цивилних институција, значајну улогу у систему сајбер безбедности имају и безбедносне и обавештајне службе. Ове институције су задужене за праћење активности потенцијалних противника у сајбер простору, идентификацију напредних претњи и прикупљање обавештајних података који могу бити од значаја за националну безбедност. У многим државама обавештајне агенције имају кључну улогу у откривању сложених сајбер операција које спроводе државни актери.[509] Илустративан пример представља Израел, где обавештајне структуре, посебно јединица 8200, играју значајну улогу у развоју сајбер капацитета и интеграцији обавештајних и технолошких ресурса. Овај модел показује како се сајбер безбедност може развити као спој обавештајних активности, технолошке експертизе и националне стратегије.[510]

Све већи значај сајбер простора као домена безбедности довео је и до развоја војних капацитета за сајбер операције. Многе државе су у оквиру својих оружаних снага успоставиле специјализоване јединице задужене за сајбер безбедност и сајбер операције. Ове јединице имају задатак да штите војне информационе системе, али и да развијају способности за извођење офанзивних операција у сајбер простору у случају оружаног конфликта.[511] Француска, на пример, има развијену Команду за сајбер одбрану (COMCYBER), која делује у оквиру оружаних снага и има задатак да штити војне системе, али и да спроводи офанзивне операције када је то неопходно. Слично томе, Немачка је формирала посебну сајбер команду (Cyber and Information Space Command), чиме је сајбер простор институционализован као засебан домен војног деловања.[512]

Поред националних институција, значајну улогу у систему сајбер безбедности имају и регулаторна тела која надзиру примену безбедносних стандарда у одређеним секторима. Ова тела имају задатак да прате примену законодавства у области информационе безбедности, контролишу рад оператера критичне инфраструктуре и обезбеде да организације које управљају осетљивим информационим системима примењују прописане безбедносне мере. У појединим државама, ова

[507] Finnish Transport and Communications Agency (Traficom), "Aviation Cyber Security," accessed April 18, 2026; Finnish Transport and Communications Agency (Traficom), "Glossary of Central Cyber Security Terms," accessed April 18, 2026.
[508] ENISA, *How to Setup Up CSIRT and SOC*, 20–24
[509] Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017), 141–45.
[510] Michael Raska, *Israel's Evolving Cyber Defense Strategy* (Singapore: S. Rajaratnam School of International Studies, 2015), 5–6; Stéphane Cordey, *The Israeli Unit 8200: An OSINT-Based Study* (Zurich: Center for Security Studies, ETH Zürich, 2019), 10–11, 14.
[511] Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (London: Hurst, 2022), 51–54.
[512] French Ministry for the Armed Forces, "Le Commandement de la cyberdéfense (COMCYBER)," accessed April 18, 2026; German Federal Armed Forces (Bundeswehr), "The Cyber and Information Domain Service," December 8, 2020.

тела имају и овлашћења за изрицање санкција, што додатно јача њихову улогу у систему сајбер безбедности.[513]

Организационе структуре у области сајбер безбедности често укључују и механизме координације на највишем нивоу државне управе. У многим државама успостављени су национални савети или координациона тела за сајбер безбедност која окупљају представнике различитих институција. На пример, Аустралија је успоставила Аустралијски центар за сајбер безбедност (ACSC), који делује као централна тачка за координацију активности владе, безбедносних служби и индустрије.[514]

Важан елемент институционалног система представља и сарадња са академском заједницом и истраживачким институцијама. Универзитети и научни центри имају значајну улогу у развоју нових технологија, анализа сајбер претњи и едукацији стручњака у области информационе безбедности. На пример, Холандија је развила снажан модел сарадње између државе, универзитета и приватног сектора кроз иницијативе као што је The Hague Security Delta, што представља пример успешне интеграције различитих актера.[515]

Ефикасан институционални оквир омогућава координисано деловање различитих актера, брзо реаговање на сајбер инциденте и развој дугорочних стратегија заштите дигиталног простора. У условима све већег значаја информационих технологија, изградња снажних институционалних капацитета постаје један од основних предуслова за очување националне безбедности и стабилности савременог друштва.

3.8 Важност сајбер стратегија за безбедност држава

У савременом безбедносном окружењу, обележеном интензивном дигитализацијом и све већом зависношћу друштва од информационо-комуникационих технологија, сајбер стратегије представљају један од кључних инструмената заштите националне безбедности. Оне омогућавају државама да систематски идентификују претње, дефинишу приоритете и успоставе институционалне и оперативне механизме за реаговање на ризике који произилазе из сајбер простора. Без јасно дефинисане стратегије, активности у области сајбер безбедности остају фрагментиране, реактивне и недовољно координисане, што значајно повећава рањивост државе.[516]

Сајбер стратегије имају посебан значај јер омогућавају интеграцију различитих елемената система националне безбедности. За разлику од традиционалних облика безбедности, који су били јасно подељени између војних и цивилних структура, сајбер простор захтева тесну сарадњу између државних институција, приватног сектора, академске заједнице и међународних партнера.

---

[513] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), *Official Journal of the European Union* L333 (2022): 84–86, 98–101.

[514] Australian Signals Directorate, Australian Cyber Security Centre, *Supporting Australian Organisations through a Cyber Security Incident* (Canberra: ASD/ACSC, 2024), 2–3.

[515] Security Delta (HSD), "The Dutch Security Cluster," accessed April 18, 2026.

[516] European Union Agency for Network and Information Security (ENISA), *National Cyber Security Strategies: Practical Guide on Development and Execution* (Heraklion: ENISA, 2012), 12–14.

Управо стратегијски документи омогућавају успостављање оваквог мултисекторског приступа, дефинишући улоге и одговорности различитих актера у систему сајбер безбедности.[517]

Један од кључних аспеката значаја сајбер стратегија огледа се у њиховој улози у управљању ризицима. Савремене сајбер претње карактерише висок степен комплексности, динамичности и непредвидивости, што захтева систематски и проактиван приступ. Сајбер стратегије омогућавају државама да идентификују критичне рањивости, процене потенцијалне последице напада и развију механизме за превенцију, детекцију и реаговање. Овај процес управљања ризицима представља основу за изградњу отпорности система и смањење потенцијалних последица сајбер инцидената.[518]

Посебно значајна улога сајбер стратегија односи се на заштиту критичне информационе инфраструктуре. У условима све веће зависности од дигиталних система, функционисање државе у великој мери зависи од стабилности енергетских мрежа, телекомуникационих система, транспортне инфраструктуре и јавних услуга. Сајбер напади усмерени на ове системе могу довести до озбиљних поремећаја у функционисању државе, укључујући прекиде у снабдевању, угрожавање јавне безбедности и друштвену нестабилност. Сајбер стратегије омогућавају идентификацију ових система као приоритетних и дефинисање посебних мера за њихову заштиту.[519]

Поред заштите инфраструктуре, сајбер стратегије имају значајну улогу у развоју националних капацитета за одговор на сајбер претње. Ово укључује изградњу техничких капацитета, развој институција, обуку стручњака и унапређење законодавног оквира. Без стратегијског приступа, ови процеси се одвијају спорадично и без јасне координације, што доводи до неефикасности и дуплирања ресурса. Стратегије омогућавају рационално коришћење ресурса и дугорочно планирање развоја капацитета.[520]

Као што је истакнуто у раду, сајбер простор је данас препознат као пети домен ратовања, уз копно, море, ваздух и космос. У том контексту, сајбер стратегије омогућавају државама да дефинишу своје позиције у односу на офанзивне и дефанзивне способности, као и да утврде услове под којима се сајбер напади могу сматрати претњом националној безбедности. Ово је посебно важно у контексту развоја концепта сајбер одвраћања, који подразумева способност државе да одговори на сајбер претње на начин који ће одвратити потенцијалне нападаче.[521]

Сајбер стратегије такође имају значајну улогу у јачању међународне сарадње. Сајбер претње имају транснационални карактер, што значи да ниједна држава не може самостално да обезбеди потпуну заштиту својих система. Стратегијски документи омогућавају дефинисање оквира за сарадњу са другим државама и међународним организацијама, укључујући размену информација,

[517] ENISA, *National Cyber Security Strategies*, 12–14.
[518] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 41–45.
[519] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 102–106.
[520] ENISA, *National Cyber Security Strategies*, 12–14; Singer and Friedman, *Cybersecurity and Cyberwar*, 91–94.
[521] Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2017): 58–60; NATO, "Warsaw Summit Communiqué," July 9, 2016, para. 70

заједничке вежбе и координацију одговора на сајбер инциденте. Ова сарадња је од кључног значаја за ефикасно суочавање са глобалним сајбер претњама.[522]

Упоредна анализа показује да државе које су раније усвојиле свеобухватне сајбер стратегије имају развијеније институционалне механизме и већу отпорност на сајбер претње. На пример, Естонија је након сајбер напада 2007. године развила један од најнапреднијих система сајбер безбедности, заснован на јасно дефинисаној националној стратегији и снажној институционалној координацији. Слично томе, Израел је кроз интегрисани стратегијски приступ успео да развије висок ниво технолошких и одбрамбених капацитета у сајбер домену.[523] Са друге стране, недостатак јасно дефинисаних сајбер стратегија може да доведе до значајних безбедносних пропуста. Државе које немају развијене стратегијске оквире често се суочавају са некоординисаним институционалним деловањем, недовољном заштитом критичне инфраструктуре и слабом способношћу реаговања на сложене сајбер претње. Ово указује на то да сајбер стратегије нису само формални документи, већ кључни инструменти за ефикасно функционисање система националне безбедности.[524]

Поред оперативне и безбедносне димензије, сајбер стратегије имају и важну политичку и нормативну улогу. Оне одражавају став државе према питањима као што су дигитални суверенитет, заштита података, слобода интернета и међународна правила понашања у сајбер простору. На тај начин, сајбер стратегије постају инструмент не само безбедносне, већ и спољне политике државе.[525]

Значај сајбер стратегија огледа се у њиховој способности да повежу различите аспекте националне безбедности у јединствен и функционалан систем. Оне омогућавају државама да пређу са реактивног на проактивни модел деловања, да унапреде отпорност својих система и да се ефикасније суоче са изазовима савременог дигиталног окружења.

У условима све већег значаја сајбер простора, постојање свеобухватне и добро имплементиране сајбер стратегије постаје један од основних предуслова за очување безбедности, стабилности и суверенитета држава.

[522] European Union Agency for Network and Information Security (ENISA), *National Cyber Security Strategies: Practical Guide on Development and Execution* (Heraklion: ENISA, 2012), 12–14; European Union Agency for Network and Information Security (ENISA), *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches* (Heraklion: ENISA, 2015), 8–12.
[523] Republic of Estonia, *Cybersecurity Strategy 2019–2022* (Tallinn: Ministry of Economic Affairs and Communications, 2019), 3–4; Government of Israel, *National Cybersecurity Strategy 2025* (Jerusalem: Israel National Cyber Directorate, 2025), 7–11.
[524] European Union Agency for Network and Information Security (ENISA), *National Cyber Security Strategies: Practical Guide on Development and Execution* (Heraklion: ENISA, 2012), 12–14; European Union Agency for Network and Information Security (ENISA), *Updated Good Practice Guide on National Cyber Security Strategies* (Heraklion: ENISA, 2016), 10–13.
[525] Luciano Floridi, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU," *Philosophy & Technology* 33, no. 3 (2020): 369–78; Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017), 121–23.

4. Информациона безбедност Руске Федерације

4.1. Појам, стратешки оквир и руски приступ информационој безбедности

Разматрање појма информационе безбедности у Руској Федерацији везује за период након окончања Хладног рата, а нарочито за последњу деценију XX века, када питања контроле информационог простора, заштите државних комуникација и очувања политичке стабилности добијају изразито безбедносну димензију.[526] Иако су поједини елементи оваквог приступа постојали и раније, тек је са институционалном консолидацијом руске државе почетком XXI века информациона безбедност постала јасно профилисана стратешка категорија.[527]

За разлику од ужег, техничког разумевања сајбер безбедности, руски приступ је знатно шири, јер обухвата не само заштиту информационо-комуникационих система, већ и заштиту друштвене свести, политичке стабилности, државног суверенитета и институционалног поретка од штетних информационих утицаја.[528] Управо је то једна од кључних одлика руског концепта: информациона сфера се не посматра само као технолошко окружење, већ и као простор стратешког надметања у којем се укрштају политички, безбедносни, медијски, психолошки и војни утицаји.[529]

У руској стратешкој мисли, информатизација друштва није схваћена само као процес модернизације, већ и као извор нових рањивости које могу бити злоупотребљене од стране спољних актера.[530] Због тога се питање информационе безбедности у руском контексту неретко повезује са питањем државног опстанка, очувања унутрашњег поретка и способности државе да контролише токове информација од значаја за националне интересе.[531]

---

[526] Руска Федерација, Указ Президента Российской Федерации от 10 января 2000 г. № 24, „О Концепции национальной безопасности Российской Федерации"; Michelle Grisé, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn, and Khrystyna Holynska, *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation* (Santa Monica, CA: RAND Corporation, 2022), 9–10; Катарина Јонев, Хатица Бериша и Александар Ђираковић, „Информациона безбедност Руске Федерације," *Војно дело* 2/2018: 104–106.

[527] Michelle Grisé, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn, and Khrystyna Holynska, *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation* (Santa Monica, CA: RAND Corporation, 2022), 9–10.

[528] Руска Федерација, *Доктрина информационной безопасности Российской Федерации*, утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895; Michelle Grisé et al., *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation* (Santa Monica, CA: RAND Corporation, 2022), 9–10; Катарина Јонев, Хатица Бериша и Александар Ђираковић, „Информациона безбедност Руске Федерације," *Војно дело* 2/2018: 105–106.

[529] Grisé et al., *Rivalry in the Information Sphere*, 9–10.

[530] Ибид, 60–61, 74–75.

[531] Руска Федерација, *Доктрина информационной безопасности Российской Федерации*, утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.

Руску Федерацију одликује изразито развијен и хијерархијски уређен систем стратегијско-доктринарних докумената у области безбедности, у оквиру којих питање информационе безбедности заузима важно место.[532]

Највиши стратешки документ у овој области у посматраном периоду представљала је Стратегија националне безбедности Руске Федерације до 2020. године, донета Указом председника Руске Федерације бр. 537 од 12. маја 2009. године, који је потписао тадашњи председник Дмитриј Медведев.[533] Ова стратегија представља континуитет у односу на Концепцију националне безбедности Руске Федерације из 2000. године, али истовремено доноси шири, систематичнији и разрађенији приступ одређењу националних интереса, приоритета али и претњи.[534] За разлику од ранијих решења, документ из 2009. године безбедност не своди само на војну моћ или заштиту територије, већ је посматра као резултат способности државе да обезбеди политичку стабилност, институционалну ефикасност, социјални развој, економски раст и заштиту кључних националних ресурса.[535] Руски концепт националне безбедности почива на схватању да су безбедност државе и њен унутрашњи развој међусобно условљени и нераздвојиви.[536]

На самом врху хијерархије стратегијских докумената, поред наведене Стратегије националне безбедности, налази се и Концепција дугорочног социјално-економског развоја Руске Федерације до 2020. године, усвојена 2008. године, што јасно показује да се у руском стратешком мишљењу безбедност не темељи искључиво на делотворности органа безбедности, већ и на економском потенцијалу државе, степену њене модернизације и способности да обезбеди одржив друштвени развој.[537] Стога се као један од стратешких циљева у остваривању националне безбедности у економској сфери одређује и средњорочни задатак да Русија, према обиму бруто домаћег производа, постане једна од пет водећих држава света.[538] Ова одредница није само економске природе, већ има и изразиту безбедносну функцију, јер се економска снага у руској стратешкој мисли сматра нужним предусловом државне отпорности, међународног утицаја и заштите суверенитета.[539] На тај начин, безбедност се дефинише као интегрална категорија која обухвата и материјалне и нематеријалне основе државне моћи. Такав приступ уједно показује да је руска

[532] Руска Федерација, Указ Президента Российской Федерации от 12 мая 2009 г. № 537, „О Стратегии национальной безопасности Российской Федерации до 2020 года"; Правительство Российской Федерации, Распоряжение от 17 ноября 2008 г. № 1662-р, „О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года".
[533] Руска Федерација, Указ Президента Российской Федерации от 12 мая 2009 г. № 537, „О Стратегии национальной безопасности Российской Федерации до 2020 года".
[534] Руска Федерација, Указ Президента Российской Федерации от 10 января 2000 г. № 24, „О Концепции национальной безопасности Российской Федерации"; Руска Федерација, Указ Президента Российской Федерации от 12 мая 2009 г. № 537, „О Стратегии национальной безопасности Российской Федерации до 2020 года".
[535] Руска Федерација, Указ Президента Российской Федерации от 12 мая 2009 г. № 537, „О Стратегии национальной безопасности Российской Федерации до 2020 года".
[536] Ибид
[537] Правительство Российской Федерации, Распоряжение от 17 ноября 2008 г. № 1662-р, „О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года".
[538] Руска Федерација, Указ Президента Российской Федерации от 12 мая 2009 г. № 537, „О Стратегии национальной безопасности Российской Федерации до 2020 года".
[539] Правительство Российской Федерации, Распоряжение от 17 ноября 2008 г. № 1662-р, „О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года"; Руска Федерација, Указ Президента Российской Федерации от 12 мая 2009 г. № 537, „О Стратегии национальной безопасности Российской Федерации до 2020 года".

стратегијска култура дубоко ослоњена на идеју снажне државе, способне да контролише кључне процесе унутар сопственог политичког, економског и информационог простора.[540]

Највећи део Стратегије националне безбедности из 2009. године усмерен је на одређивање националних интереса и изградњу система националне безбедности, при чему се информациона сфера појављује као једно од подручја од посебног значаја за државу.[541] Стратегија, као документ општег усмерења, даје смернице државној политици у области одбране, економије, спољних послова и социјалне политике за период од десет година. Значај Стратегије за информациону безбедност лежи у чињеници да информациони простор препознаје као један од кључних ресурса националне моћи.[542] Основни концепт овог документа почива на становишту да се национална безбедност земље обезбеђује пре свега кроз развој економије, социјалне сфере, технологије, науке и институционалних капацитета државе.[543] У том оквиру, заштита информационог простора не подразумева само одбрану од техничких упада, саботажа или нарушавања рада информационих система, већ и заштиту јавног поретка, вредносног система и политичке стабилности од спољних информационих утицаја.[544] То је и разлог због чега руска држава у каснијим документима, нарочито у Стратегији националне безбедности из 2015. године и Доктрини информационе безбедности из 2016. године, додатно разрађује питање заштите националног информационог простора, јачања суверенитета у дигиталној сфери и супротстављања информационо-психолошким операцијама.[545] Додатан континуитет оваквог правца развоја представља и Стратегија националне безбедности Руске Федерације из 2021. године, у којој се заштита друштвене стабилности, националних вредности и информационог суверенитета још изразитије повезује са општим концептом националне безбедности.[546]

4.1.2 Специфичности Руске Федерације по питању информационе безбедности

Као што је је истакнуто у претходним редовима, информациона безбедност у Руској Федерацији није споредна или искључиво техничка компонента безбедносног система, већ један од његових темељних стубова.[547] Модел Руске Федерације представља значајан пример државе која је информациону сферу уздигла на ниво једног од кључних поља савременог безбедносног и геополитичког деловања.[548]Став Руске Федерације према безбедности у сајбер простору у значајној мери се разликује од америчког и европског приступа, пре свега због различитог

[540] Grisé et al., *Rivalry in the Information Sphere,* 74–75.
[541] Руска Федерација, Указ Президента Российской Федерации от 12 мая 2009 г. № 537, „О Стратегии национальной безопасности Российской Федерации до 2020 года".
[542] Ибид
[543] Ибид
[544] Руска Федерација, *Доктрина информационной безопасности Российской Федерации*, утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895; Michelle Grisé et al., *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation* (Santa Monica, CA: RAND Corporation, 2022), 10–11; Јонев, Бериша и Ћираковић, „Информациона безбедност Руске Федерације," 105–106.
[545] Руска Федерација, Указ Президента Российской Федерации от 31 декабря 2015 г. № 683, „О Стратегии национальной безопасности Российской Федерации"; Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации".
[546] Руска Федерација, Указ Президента Российской Федерации от 2 июля 2021 г. № 400, „О Стратегии национальной безопасности Российской Федерации".
[547] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации".
[548] Michelle Grisé et al., *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation* (Santa Monica, CA: RAND Corporation, 2022), 99–100, 105–106; Јонев, Бериша и Ћираковић, „Информациона безбедност Руске Федерације," 105–106.

разумевања саме улоге државе, природе претњи и граница суверенитета у дигиталном окружењу.[549]

Док западне државе нагласак стављају на безбедност мрежа, система и критичне инфраструктуре, руски приступ полази од знатно ширег појма информационе безбедности, који обухвата и техничку заштиту и контролу садржаја, информационих токова и утицаја на друштвену и политичку сферу.[550] Због тога Москва са резервом посматра принцип неограниченог протока информација, као и став да су националне границе у сајбер простору од секундарног значаја.[551] У руском схватању, слободна циркулација информација није сама по себи вредносно неутрална, јер може да послужи као средство спољног утицаја, политичке дестабилизације и нарушавања институционалног поретка.[552]

Руски концепт безбедности у дигиталној сфери почива на уверењу да држава мора задржати кључну улогу у уређивању, надзору и заштити сопственог информационог простора.[553] У томе се огледа једна од суштинских разлика између руског и западног приступа: док Запад тежи отвореном, глобално повезаном и вишеактерском моделу управљања интернетом, Русија инсистира на примату државног суверенитета и нормативне контроле унутар националних граница.[554]

Руска Федерација је међу првим државама која је питање међународне безбедности у информационо-комуникационој сфери покушала да институционализује на глобалном нивоу. Током 1998. године Русија је у Првом комитету Генералне скупштине Уједињених нација покренула нацрт резолуције „Развој у области информација и телекомуникација у контексту међународне безбедности“, чиме је отворила дуготрајан дипломатски процес који траје до данас.[555] Од тог периода Москва доследно заговара потребу за посебним међународноправним режимом који би регулисао понашање држава у информационом простору, а не само решавањем техничких аспеката сајбер инцидената.[556] У руском приступу Уједињене нације имају централно место као форум за изградњу нових правила, мера поверења и евентуално обавезујућег правног инструмента у области међународне информационе безбедности.[557] Насупрот томе, западне државе су традиционално биле скептичније према руским иницијативама, сматрајући да би оне могле послужити као основ за ширење државне контроле над интернетом и ограничење слободног

[549] Keir Giles, “Russia’s Public Stance on Cyberspace Issues,” in *2012 4th International Conference on Cyber Conflict*, ed. Christian Czosseck, Rain Ottis, and Katharina Ziolkowski (Tallinn: NATO CCD COE Publications, 2012), 63–64; Michelle Grisé, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn, and Khrystyna Holynska, *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation* (Santa Monica, CA: RAND Corporation, 2022), 10–11.
[550] Катарина Јонев, Хатица Бериша и Александар Ћираковић, „Информациона безбедност Руске Федерације,” *Војно дело* 2/2018: 104–106; Grisé et al., *Rivalry in the Information Sphere*, 10–11.
[551] Giles, “Russia’s Public Stance on Cyberspace Issues,” 63–65.
[552] Ибид, 63–65.
[553] Grisé et al., *Rivalry in the Information Sphere*, 10–11; Јонев, Бериша и Ћираковић, „Информациона безбедност Руске Федерације,” 105–106.
[554] Elaine Korzak, *Russia’s Cyber Policy Efforts in the United Nations*, Tallinn Paper No. 11 (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2021), 4–5, 17–18.
[555] United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security: Russian Federation Draft Resolution*, A/C.1/53/3, September 30, 1998; Korzak, *Russia’s Cyber Policy Efforts in the United Nations*, 4–5.
[556] Korzak, *Russia’s Cyber Policy Efforts in the United Nations*, 4–5, 16–18.
[557] Ибид, 18–19

протока информација.[558] Руско-западно неслагање у овој области не испољава само на теоријском плану, већ и у домену међународне сајбер дипломатије, где се сударају две различите визије будућег поретка у информационом простору.[559]

Једна од кључних тачака разилажења у ставовима између Русије и држава Европе и Северне Америке односи се на само одређење појма претње у сајбер, односно информационом простору. У руској доктринарној и дипломатској пракси претњама се не сматрају само злонамерни код, неовлашћени приступ системима и деструктивне операције против инфраструктуре, већ и употреба садржаја ради утицаја на друштвено-хуманитарну сферу, манипулација информационим токовима, дезинформације и ширење садржаја који могу угрозити политичку, економску и социјалну стабилност државе.[560] Управо зато Русија снажно подржава концепт интернет суверенитета, односно право државе да у складу са сопственим законодавством уређује информациони простор, штити националне ресурсе и ограничава оне облике прекограничног протока информација које сматра безбедносно ризичним.[561] Тај став био је јасно видљив и у предлозима Међународног кодекса понашања за информациону безбедност, које је Русија са партнерским државама подносила у УН, наглашавајући да су питања јавне политике у вези са интернетом у суверености надлежности држава.[562] По том моделу, држава није само један у низу актера дигиталног окружења, већ је најзначајнији актер, што представља суштинску разлику у односу на либералнији западни приступ.[563] Руски концепт сајбер безбедности далеко изразитије повезује техничку заштиту са питањима политичке, идеолошке и културне отпорности друштва.[564]

Појам информационог рата у руској литератури и стратешким документима такође има шири смисао од оног који је уобичајен у западним анализама. Он не обухвата само операције усмерене на информационе системе и мреже, већ и деловање усмерено ка подривању политичког, економског и друштвеног система противника, као и психолошко деловање на становништво ради изазивања нестабилности и вршења притиска на органе власти.[565] У руском схватању сајбер компонента представља само један сегмент шире информационе конфронтације, која обједињује техничке, психолошке, политичке и медијске и инструменте.[566] Појам информационе безбедности у руским документима се одређује и као стање заштићености виталних интереса личности, друштва и државе у информационој сфери, што јасно показује да је реч о појму ширем од западног појма „cybersecurity“.[567] Управо ту се најјасније види дисциплинарна и концептуална разлика: западна тумачења, по правилу, остају у ужем пољу заштите података, мрежа и информационих

[558] Ибид, 17–18.
[559] Ибид, 18–19.
[560] Giles, "Russia's Public Stance on Cyberspace Issues," 64–66; Јонев, Бериша и Ћираковић, „Информациона безбедност Руске Федерације," 105–106.
[561] Giles, "Russia's Public Stance on Cyberspace Issues," 64–65; United Nations General Assembly, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, A/66/359, September 14, 2011, annex.
[562] United Nations General Assembly, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, A/66/359, September 14, 2011, annex; Korzak, *Russia's Cyber Policy Efforts in the United Nations*, 14–18.
[563] Korzak, *Russia's Cyber Policy Efforts in the United Nations*, 17–18.
[564] Grisé et al., *Rivalry in the Information Sphere*, 99–100, 105–106.
[565] Grisé et al., *Rivalry in the Information Sphere*, 67–70.
[566] Ибид, 67–70, 99–100
[567] Руска Федерација, *Доктрина информационной безопасности Российской Федерации*, утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895; Јонев, Бериша и Ћираковић, „Информациона безбедност Руске Федерације," 105–106.

система, док руски модел у исту аналитичку раван ставља и информационе утицаје на свест, вредности, јавни поредак и државни суверенитет.[568] Руски став о безбедности у сајбер простору није заснован искључиво на техничкој логици одбране инфраструктуре, већ и на широј геополитичкој и државноцентричној визији контроле информационог окружења.[569] Управо та ширина појма објашњава и зашто Русија питања сајбер безбедности доследно смешта у оквир националне безбедности, међународног права и стратешког надметања великих сила.[570]

4.2 Доктринарни развој и институционализација заштите информационе сфере

Доктрина информационе безбедности Руске Федерације из 2000. године представљала је, све до усвајања нове Доктрине 2016. године, основни доктринарни документ којим се руска држава руководила у области заштите своје информационе сфере.[571] Њен значај није био само у томе што је систематизовала главне циљеве, принципе и правце деловања државе у овој области, већ и у томе што је јасно показала да Русија питање информационе безбедности не своди на техничку заштиту података и мрежа, већ га повезује са заштитом државе, друштва и појединца у целини.[572] Сама намера документа била је, између осталог, да обезбеди остваривање уставних права и слобода човека и грађанина да тражи, прима, преноси, производи и шири информације.[573] Истовремено, Доктрина је полазила од становишта да су национални интереси у информационој сфери сложени и вишеслојни и да захтевају истовремено правне, институционалне, технолошке и политичке механизме заштите.[574] Посебно је значајно што се у овом документу информациона безбедност изричито одређује као једна од саставних компоненти националне безбедности Руске Федерације, уз напомену да ће са технолошким развојем та зависност постајати све снажнија.[575] На тај начин је још почетком XXI века постављена основа за каснији развој руског државноцентричног приступа информационој сфери, у којем безбедност информација, друштвена стабилност и заштита државног суверенитета чине јединствену целину.[576]

У Доктрини се издвајају четири кључне компоненте националних интереса Руске Федерације у информационој сфери.[577] Прва компонента односи се на поштовање уставних права и слобода човека и грађанина у области пријема, коришћења и ширења информација, али и на духовну

---

[568] Grisé et al., *Rivalry in the Information Sphere*, 10–11; Јонев, Бериша и Ћираковић, „Информациона безбедност Руске Федерације," 105–106.
[569] Grisé et al., *Rivalry in the Information Sphere*, 99–100, 105–106.
[570] Руска Федерација, Указ Президента Российской Федерации от 12 апреля 2021 г. № 213, „Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности"; Korzak, *Russia's Cyber Policy Efforts in the United Nations*, 18–19.
[571] Руска Федерација, *Доктрина информационной безопасности Российской Федерации*, утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895; Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации".
[572] Руска Федерација, *Доктрина информационной безопасности Российской Федерации*, утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895; Катарина Јонев, Хатица Бериша и Александар Ћираковић, „Информациона безбедност Руске Федерације," *Војно дело* 2/2018: 105–106.
[573] Руска Федерација, *Доктрина информационной безопасности Российской Федерации*, утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.
[574] Michelle Grisé, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn, and Khrystyna Holynska, *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation* (Santa Monica, CA: RAND Corporation, 2022), 10–11
[575] Руска Федерација, *Доктрина информационной безопасности Российской Федерации*, утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.
[576] Ибид; Јонев, Бериша и Ћираковић, „Информациона безбедност Руске Федерације," 105–106.
[577] Руска Федерација, *Доктрина информационной безопасности Российской Федерации*, утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.

обнову Русије, очување моралних вредности друштва, патриотизма, хуманизма и културног и научног потенцијала земље.[578] Друга компонента обухвата информациону подршку државној политици, односно потребу да се руској и међународној јавности преносе поуздане информације о државној политици Руске Федерације и њеним званичним ставовима о друштвено значајним догађајима, уз обезбеђивање приступа грађана отвореним државним информационим ресурсима.[579] Трећа компонента тиче се развоја савремених информационих технологија, јачања националне информационе индустрије, укључујући средства информатизације, телекомуникација и веза, што показује да Русија информациону безбедност повезује и са технолошком самосталношћу државе.[580] Четврта компонента обухвата заштиту информационих ресурса од неовлашћеног приступа, као и безбедност већ успостављених и будућих информационо-телекомуникационих система на територији Руске Федерације.[581] Овако постављена структура националних интереса показује да руска доктрина није ограничена само на класичну заштиту информација, већ обједињује права грађана, легитимитет државне политике, технолошки развој и заштиту инфраструктуре у јединствен концепт.[582]

Доктрина је, такође, посебну пажњу посветила улози медија и државне информационе политике, што додатно потврђује ширину руског разумевања информационе безбедности.[583] У документу се не полази од претпоставке да су медији искључиво простор слободне размене информација, већ и од тога да они могу бити средство обликовања јавне свести, политичког утицаја и ширења дезинформација.[584] Зато Доктрина предвиђа развој механизама за повећање ефикасности државног управљања активностима државних медија и спровођење државне информационе политике.[585] Као значајне претње у унутрашњој политичкој сфери наводе се ширење дезинформација о политици Руске Федерације и деловању федералних органа власти, као и потреба за јачањем контрапропагандних активности ради спречавања негативних последица таквих појава.[586]

Из ових формулација јасно се види да руска држава информациону безбедност посматра и као питање заштите јавног поретка, политичког ауторитета и симболичке стабилности државе.[587] Доктрина се, поред тога, осврће и на друге облике претњи, укључујући угрожавање уставних права и слобода у информационој сфери, претње усмерене против државне информационе политике, опасности по националну информациону и телекомуникациону индустрију, као и претње усмерене на саме информационе системе и ресурсе.[588] Сходно томе, информациона безбедност у руском доктринарном оквиру мора да се разумети као шири безбедносни, политички

[578] Исто; Јонев, Бериша и Ћираковић, „Информациона безбедност Руске Федерације," 106.
[579] Руска Федерација, *Доктрина информационной безопасности Российской Федерации*, утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.
[580] Ибид
[581] Ибид
[582] Ибид; Јонев, Бериша и Ћираковић, „Информациона безбедност Руске Федерације," 106.
[583] Руска Федерација, *Доктрина информационной безопасности Российской Федерации*, утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895; Јонев, Бериша и Ћираковић, „Информациона безбедност Руске Федерације," 106.
[584] Руска Федерација, *Доктрина информационной безопасности Российской Федерации*, утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.
[585] Ибид
[586] Исто; Јонев, Бериша и Ћираковић, „Информациона безбедност Руске Федерације," 106.
[587] Руска Федерација, *Доктрина информационной безопасности Российской Федерации*, утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.
[588] Ибид

и друштвени концепт.[589] Управо та ширина појма представља једну од трајних особености руског приступа и важну полазну основу за разумевање каснијег развоја њене стратегије у сајбер и информационом простору.[590]

Иако после усвајања Доктрине информационе безбедности Руске Федерације 2016. године није донета нова доктрина истог назива, званични акти из 2024, 2025. и 2026. године јасно показују да информациона безбедност остаје високо позиционирана у систему стратешког и нормативног деловања руске државе.[591] Уместо доношења потпуно новог доктринарног текста, уочава се другачији образац развоја: постојећа доктринарна основа се задржава, док се њене поставке даље разрађују кроз председничке указе, акте Владе Руске Федерације и институционално јачање институција надлежних за ову област.[592] То значи да се у посматраном периоду не мења темељна концепција информационе безбедности, већ се усмерава у правцу конкретнијих механизама заштите, управљања и координације.[593] Доктрина не представља изолован документ, већ полазну основу за читав низ каснијих нормативних и организационих мера.[594] Због тога се акти из 2024, 2025. и 2026. године могу тумачити као наставак, а не као напуштање, доктринарне логике успостављене 2016. године.[595]

У 2024. години посебно је значајно то што се питање информационе безбедности изричито појављује у оквиру највиших државних развојних и безбедносних циљева. Указом председника Руске Федерације од 7. маја 2024. године бр. 309, којим су утврђени национални циљеви развоја до 2030. године и перспективе до 2036. године, као један од приоритета наводи се и обезбеђивање мрежног суверенитета и информационе безбедности.[596] Ова формулација показује да се информациона безбедност више не третира само као ускостручна тема сектора безбедности, већ као саставни део опште државне стратегије развоја.[597] Истовремено, Указом од 13. јуна 2024. године бр. 500 извршене су измене у ранијем указу о додатним мерама за обезбеђивање информационе безбедности Руске Федерације, што потврђује да председнички ниво власти наставља да непосредно интервенише у нормативни оквир ове области.[598] Поред тога,

[589] Grisé et al., *Rivalry in the Information Sphere,* 10–11; Јонев, Бериша и Ћираковић, „Информациона безбедност Руске Федерације," 105–106.
[590] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации"; Grisé et al., *Rivalry in the Information Sphere,* 99–100, 105–106.
[591] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации"; Руска Федерација, Указ Президента Российской Федерации от 4 марта 2026 г. № 136, „О внесении изменений в некоторые акты Президента Российской Федерации".
[592] Руска Федерација, Указ Президента Российской Федерации от 4 марта 2026 г. № 136, „О внесении изменений в некоторые акты Президента Российской Федерации".
[593] Ибид
[594] Ибид; Руска Федерација, Указ Президента Российской Федерации от 16 февраля 2026 г. № 88, „О внесении изменений в состав Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям, утвержденный Указом Президента Российской Федерации от 10 ноября 2018 г. № 648".
[595] Руска Федерација, Указ Президента Российской Федерации от 4 марта 2026 г. № 136, „О внесении изменений в некоторые акты Президента Российской Федерации".
[596] Руска Федерација, Указ Президента Российской Федерации от 7 мая 2024 г. № 309, „О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года".
[597] Исто.
[598] Руска Федерација, Указ Президента Российской Федерации от 13 июня 2024 г. № 500, „О внесении изменений в Указ Президента Российской Федерации от 1 мая 2022 г. № 250 „О дополнительных мерах по обеспечению информационной безопасности Российской Федерации"".

Постановљењем Владе Руске Федерације од 17. децембра 2024. године бр. 1805 циљ обезбеђивања мрежног суверенитета и информационе безбедности део државне политике.[599] На тај начин 2024. година показује да је руски приступ информационој безбедности истовремено и стратешки и програмски: он се не исцрпљује у општим декларацијама, већ се везује за конкретне државне циљеве и механизме јавне политике.[600]

Током 2025. године тај континуитет добија још израженију институционалну и технолошку димензију. Најпре је Указом од 7. априла 2025. године бр. 214 измењен ранији указ о мерама за обезбеђивање технолошке независности и безбедности критичне информационе инфраструктуре Руске Федерације, што сведочи о томе да питање заштите критичне информационе инфраструктуре остаје у самом средишту државне безбедносне политике.[601] Истога дана, Указом бр. 219, извршене су измене у саставу Међуресорне комисије Савета безбедности Руске Федерације за информациону безбедност, а затим су нове измене у истом саставу уследиле и Указом од 5. новембра 2025. године бр. 815.[602] Ови акти су важни не само због кадровских промена, већ и зато што показују да Комисија за информациону безбедност задржава активну улогу у систему Савета безбедности као кључног координативног механизма у овој области.[603] Другим речима, 2025. година не доноси нову доктрину, али доноси видљиво одржавање и прилагођавање институционалне архитектуре која ту доктрину треба да спроводи.[604] Поред тога, Постановљењем Владе Руске Федерације од 19. децембра 2025. године бр. 2068 наставља се програмско разрађивање циља обезбеђивања мрежног суверенитета и информационе безбедности на интернету, при чему се у државном програмском оквиру наглашава пројекција да до 2030. године овај циљ буде институционално и технички обезбеђен.[605] Може се закључити да се од 2025. године политика информационе безбедности Руске Федерације развија у три правца: кроз технолошку независност, кроз институционалну координацију и кроз програмско мерење државних циљева у дигиталном простору.[606]

---

[599] Правительство Российской Федерации, Постановление от 17 декабря 2024 г. № 1805, „О внесении изменений в некоторые акты Правительства Российской Федерации".

[600] Руска Федерација, Указ Президента Российской Федерации от 7 мая 2024 г. № 309, „О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года"; Правительство Российской Федерации, Постановление от 17 декабря 2024 г. № 1805, „О внесении изменений в некоторые акты Правительства Российской Федерации".

[601] Руска Федерација, Указ Президента Российской Федерации от 7 апреля 2025 г. № 214, „О внесении изменения в Указ Президента Российской Федерации от 30 марта 2022 г. № 166 „О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации"".

[602] Руска Федерација, Указ Президента Российской Федерации от 7 апреля 2025 г. № 219, „О внесении изменений в состав Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям, утвержденный Указом Президента Российской Федерации от 10 ноября 2018 г. № 648"; Руска Федерација, Указ Президента Российской Федерации от 5 ноября 2025 г. № 815, „О внесении изменений в состав Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям, утвержденный Указом Президента Российской Федерации от 10 ноября 2018 г. № 648".

[603] Ибид

[604] Ибид

[605] Правительство Российской Федерации, Постановление от 19 декабря 2025 г. № 2068, „О внесении изменений в некоторые акты Правительства Российской Федерации".

[606] Руска Федерација, Указ Президента Российской Федерации от 7 апреля 2025 г. № 214, „О внесении изменения в Указ Президента Российской Федерации от 30 марта 2022 г. № 166"; Руска Федерација, Указ Президента Российской Федерации от 7 апреля 2025 г. № 219, „О внесении изменений в состав Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям"; Руска Федерација, Указ Президента Российской Федерации от 5 ноября 2025 г. № 815, „О внесении изменений в состав

Акти из 2026. године додатно потврђују да је Доктрина из 2016. године и даље део важећег стратешког оквира. Указом од 16. фебруара 2026. године бр. 88 поново су извршене измене у саставу Међуресорне комисије Савета безбедности Руске Федерације за информациону безбедност, што сведочи о наставку институционалног прилагођавања овог тела.[607] Ово указује да руска држава информациону безбедност не посматра као завршено нормативно питање, већ као област која захтева стално организационо усклађивање и обнову управљачких капацитета.[608] Још важнији је Указ председника Руске Федерације од 4. марта 2026. године бр. 136, у коме се изричито наводи да одређени основи државне политике конкретизују, између осталог, и одредбе Стратегије националне безбедности Руске Федерације, Доктрине информационе безбедности Руске Федерације, Стратегије развоја информационог друштва и Указа бр. 309 из 2024. године.[609] Овакво нормативно упућивање има велики значај за научну анализу, јер недвосмислено показује да Доктрина информационе безбедности није напуштена, већ да и даље служи као важећа основа за конкретизацију других сегмената државне политике.[610] Поред тога, у званично објављеним актима из фебруара и марта 2026. године наставља се позивање на мере које се односе на технолошку независност и безбедност критичне информационе инфраструктуре, што потврђује да се тежиште државне политике не задржава само на нормативном нивоу, већ и на практичној заштити кључних дигиталних ресурса државе.[611] Стога 2026. година представља снажан доказ континуитета али не само у смислу доношења нове доктрине, већ у даље уклапање информационе безбедности у шири систем националне, културне, друштвене и технолошке безбедности.[612]

Из наведеног произлази да акти из 2024, 2025. и 2026. године не представљају дисконтинуитет у односу на Доктрину информационе безбедности из 2016. године, већ њено даље нормативно, програмско и институционално разрађивање.[613] Уочава се јасно уздизање питања мрежног суверенитета и информационе безбедности на Интернету на ниво државних развојних циљева.[614] Нагласак на технолошкој независности и безбедности критичне информационе инфраструктуре указује да руско разумевање информационе безбедности све више спаја суверенитет, технолошки развој, безбедност државних система и контролу над информационим токовима у јединствен

Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям"; Правительство Российской Федерации, Постановление от 19 декабря 2025 г. № 2068, „О внесении изменений в некоторые акты Правительства Российской Федерации".

[607] Руска Федерација, Указ Президента Российской Федерации от 16 февраля 2026 г. № 88, „О внесении изменений в состав Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям, утвержденный Указом Президента Российской Федерации от 10 ноября 2018 г. № 648".

[608] Ибид

[609] Руска Федерација, Указ Президента Российской Федерации от 4 марта 2026 г. № 136, „О внесении изменений в некоторые акты Президента Российской Федерации".

[610] Ибид

[611] Руска Федерација, Указ Президента Российской Федерации от 7 апреля 2025 г. № 214, „О внесении изменения в Указ Президента Российской Федерации от 30 марта 2022 г. № 166"; Руска Федерација, Указ Президента Российской Федерации от 4 марта 2026 г. № 136, „О внесении изменений в некоторые акты Президента Российской Федерации".

[612] Ибид; Руска Федерација, Указ Президента Российской Федерации от 16 февраля 2026 г. № 88, „О внесении изменений в состав Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям".

[613] Ибид.

[614] Руска Федерација, Указ Президента Российской Федерации от 7 мая 2024 г. № 309, „О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года"; Правительство Российской Федерации, Постановление от 19 декабря 2025 г. № 2068, „О внесении изменений в некоторые акты Правительства Российской Федерации".

концепт.[615] За анализу руске политике у сајбер простору од посебног је значаја закључак да се после 2016. године није појавила нова доктрина која би заменила претходну, али да је управо кроз акте из 2024, 2025. и 2026. године видљиво њено даље учвршћивање у систему државне политике и стратешког планирања.[616]

У Војној доктрини Руске Федерације из 2014. године и Доктрини информационе безбедности Руске Федерације из 2016. године не доминирају термини са префиксом „сајбер", већ појмови као што су информациона безбедност, информациони простор, информационо супротстављање и информациони утицај.[617] То није терминолошка случајност, већ показатељ дубљег концептуалног опредељења. Као што је истакнуто, за руску државу безбедност у сајбер простору представља само једну димензију укупне информационе безбедности.[618]

Војна доктрина из 2014. године изричито указује на тенденцију премештања војних опасности и претњи у информациони простор и у унутрашњу сферу Руске Федерације, чиме се потврђује да се савремени сукоб не посматра искључиво кроз класичне оружане форме.[619] Доктрина информационе безбедности из 2016. године, са своје стране, утврђује да је реч о систему званичних погледа на обезбеђивање националне безбедности у информационој сфери, што још једном показује да руски приступ почиње од шире категорије информационог суверенитета, а не од ужег техничког појма сајбер заштите.[620] Такво решење омогућава руској држави да у јединствен аналитички и нормативни оквир смести и заштиту критичне инфраструктуре, и борбу против компјутерских напада, и супротстављање информационо-психолошком деловању споља.[621] У том смислу, руска терминологија није само различита од западне, већ одражава и другачији модел односа државе, друштва и информационог окружења.[622]

Посебну улогу у институционализацији овог приступа има период власти Владимира Путина, у коме питање заштите државних информационих ресурса добија изразитији организациони и безбедносни значај.[623] Почетком 2013. године, у контексту појачане пажње према компјутерским нападима на државне структуре, Путин је потписао Указ од 15. јануара 2013. године бр. 31, којим је Федералној служби безбедности поверено стварање државног система за откривање, спречавање и отклањање последица компјутерских напада на информационе системе Руске

[615] Руска Федерација, Указ Президента Российской Федерации от 7 апреля 2025 г. № 214, „О внесении изменения в Указ Президента Российской Федерации от 30 марта 2022 г. № 166"; Руска Федерација, Указ Президента Российской Федерации от 13 июня 2024 г. № 500, „О внесении изменений в Указ Президента Российской Федерации от 1 мая 2022 г. № 250".
[616] Руска Федерација, Указ Президента Российской Федерации от 4 марта 2026 г. № 136, „О внесении изменений в некоторые акты Президента Российской Федерации".
[617] Russian Federation, *Военная доктрина Российской Федерации*, approved by the President of the Russian Federation on December 25, 2014, No. Пр-2976; Russian Federation, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации".
[618] Grisé et al., *Rivalry in the Information Sphere*, 10–11.
[619] Russian Federation, *Военная доктрина Российской Федерации*, approved by the President of the Russian Federation on December 25, 2014, No. Пр-2976.
[620] Russian Federation, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации".
[621] Grisé et al., *Rivalry in the Information Sphere*, 99–114.
[622] Korzak, *Russia's Cyber Policy Efforts in the United Nations*, 14–16.
[623] Giles, "Russia's Public Stance on Cyberspace Issues," 63–68.

Федерације.[624] Према доступним извештајима, непосредно након откривања шпијунске операције „Црвени октобар“ (Red October), која је обухватила компјутерске системе влада и дипломатских мисија широм бившег совјетског простора, руска држава је додатно појачала напоре да заштити сопствене информационе ресурсе.[625] Посебно је значајно што су у оквир заштите, према том указу, укључене не само државне рачунарске и телекомуникационе мреже унутар саме Русије, већ и системи у њеним амбасадама и конзулатима у иностранству.[626] То показује да руска држава компјутерске нападе не посматра као изоловани технички инцидент, већ као питање националне безбедности које обухвата дипломатску, обавештајну и спољнополитичку сферу.[627]

Важно је разликовати овај указ од другог значајног документа из исте године а то је Основа државне политике Руске Федерације у области међународне информационе безбедности за период до 2020. године, које је председник одобрио 24. јула 2013. године.[628] Док је јануарски указ био усмерен на стварање конкретног државног система који ће омогућити заштиту од компјутерских напада, Основе из 2013. године представљале су шири стратешко-политички оквир за руско деловање у области међународне информационе безбедности.[629] Оба документа показују да је руски приступ био истовремено и институционалан и геополитички. Док су са једне стране грађени механизми оперативне заштите, са друге је развијана шира државна политика у области међународне информационе безбедности.[630]

У тим Основама, као и у каснијим руским актима и дипломатским ставовима, препознају се кључне опасности које Москва повезује са међународном информационом безбедношћу.[631]Међу њима се посебно издвајају: коришћење информационо-комуникационих технологија као оружја у војнополитичке сврхе ради агресије и нарушавања стратешке стабилности; употреба ИКТ у терористичке и екстремистичке сврхе; растући обим компјутерске и шире високотехнолошке криминалности; као и употреба информационих технологија за мешање у унутрашње послове суверених држава.[632] Оваква класификација је нарочито значајна зато што показује да Русија у исти безбедносни оквир смешта и међудржавну конфронтацију, и тероризам, и криминал, и

[624] Russian Federation, Указ Президента Российской Федерации от 15 января 2013 г. № 31, „О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации”.
[625] Steve Gutterman, “Putin Orders Russian Computers to Be Protected after Spy Attacks,” *Reuters*, January 21, 2013.
[626] Russian Federation, Указ Президента Российской Федерации от 15 января 2013 г. № 31, „О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации”; Gutterman, “Putin Orders Russian Computers to Be Protected after Spy Attacks.”
[627] Russian Federation, Указ Президента Российской Федерации от 15 января 2013 г. № 31, „О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации”.
[628] Russian Federation, *Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года*, approved by the President of the Russian Federation on July 24, 2013, No. Пр-1753.
[629] Исто.
[630] Korzak, *Russia's Cyber Policy Efforts in the United Nations*, 14–18.
[631] Russian Federation, *Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года*, approved by the President of the Russian Federation on July 24, 2013, No. Пр-1753; Russian Federation, Указ Президента Российской Федерации от 12 апреля 2021 г. № 213, „Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности”.
[632] Russian Federation, Указ Президента Российской Федерации от 12 апреля 2021 г. № 213, „Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности”.

политичко-информациони утицај споља.[633] Уједно, тиме се потврђује да су за руску страну кључни објекти заштите не само критична инфраструктура и државни информациони системи, већ и дипломатска представништва, обавештајне структуре, државна политика и унутрашња политичка стабилност.[634] У овом контексту, активности страних политичких, војних, обавештајних и информативних структура, тежња појединих држава ка доминацији у глобалној информационој сфери и развој концепата информационог ратовања у иностранству тумаче се као трајни спољни извори угрожавања руских интереса.[635] Руска концепција међународне информационе безбедности није дефанзивна само у техничком смислу, већ и у политичко-правном јер настоји да ограничи оне облике употребе ИКТ које Москва доживљава као инструменте притиска, поткопавања суверенитета или подстицања унутрашње нестабилности.[636]

4.2.1 Међународна сарадња Руске Федерације у области информационе безбедности

Руска Федерација се дугорочно залаже за развој међународне сарадње у области сајбер, односно, како сама наглашава, међународне информационе безбедности. Полазећи од становишта да употреба информационо-комуникационих технологија може имати последице по међународни мир, државни суверенитет и унутрашњу стабилност држава,[637] Русија је једна од првих држава која је ово питање систематски изнела пред Уједињене нације, подносећи током 53. заседања Генералне скупштине 1998. године нацрт резолуције који је касније усвојен као Резолуција 53/70 од 4. децембра 1998. године.[638] Ова резолуција бавила се развојем у области информација и телекомуникација у контексту међународне безбедности и позвала је државе да на мултилатералном нивоу разматрају постојеће и потенцијалне претње у информационој сфери.[639] Већ у тој раној фази руски приступ је полазио од уверења да развој науке и технологије, иако има изразите модернизацијске предности, истовремено ствара нове облике рањивости који могу бити злоупотребљени од стране држава, криминалних група и терористичких актера.[640] Значај ове иницијативе огледа се и у томе што је временом постала трајна тема дневног реда Генералне скупштине УН, а Русија ју је наредних година редовно обнављала и ширила круг држава које су подржавале њен приступ.[641] Међутим, прва Група владиних експерата у оквиру овог процеса није успостављена 2001. године, већ 2004. године, а заседања је одржала 2004–2005, чиме је расправа

[633] Korzak, *Russia's Cyber Policy Efforts in the United Nations*, 14–17.
[634] Russian Federation, Указ Президента Российской Федерации от 15 января 2013 г. № 31, „О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации".
[635] Russian Federation, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации"; Grisé et al., *Rivalry in the Information Sphere*, 99–114.
[636] Russian Federation, Указ Президента Российской Федерации от 12 апреля 2021 г. № 213, „Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности"; Korzak, *Russia's Cyber Policy Efforts in the United Nations*, 17–18.
[637] Elaine Korzak, *Russia's Cyber Policy Efforts in the United Nations*, Tallinn Paper No. 11 (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2021), 4–5, 14–18.
[638] United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/53/70, December 4, 1998; United Nations Office for Disarmament Affairs, "Developments in the Field of Information and Telecommunications in the Context of International Security."
[639] United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/53/70, December 4, 1998.
[640] Korzak, *Russia's Cyber Policy Efforts in the United Nations*, 4–5.
[641] United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/54/49, December 1, 1999; A/RES/59/61, December 3, 2004; United Nations Office for Disarmament Affairs, "Developments in the Field of Information and Telecommunications in the Context of International Security."

о информационој безбедности прешла из фазе општих резолуција у фазу стручнијег и институционално уобличенијег дијалога.[642] До 2008. године подршка руском приступу значајно је порасла. Предлог резолуције у овој области усвојен је у Генералној скупштини са 167 гласова за, док су Сједињене Америчке Државе биле једина држава која је гласала против.[643] Ова динамика показује да је руски став, иако оспораван у делу западних држава, током времена задобио ширу подршку међу државама глобалног југа и делом великих незападних сила.[644]

Русија доследно истиче да међународна сарадња у овој области не сме да буде заснована на решењима која, из њене перспективе, релативизују државни суверенитет. Због тога је дуго одбијала да приступи Будимпештанској конвенцији о сајбер криминалу, иако је прихватала потребу за сарадњом у борби против високотехнолошког криминала.[645] Главни разлог руске резерве према Конвенцији односио се на члан 32, односно на могућност прекограничног приступа одређеним подацима без сагласности друге државе, што је Москва тумачила као потенцијално нарушавање начела суверенитета.[646] Руска страна је годинама заговарала не регионални, већ универзални, међудржавни и под окриљем УН усвојен правни режим, у коме би сва правила била резултат преговора суверених држава, а не проширивања решења насталих у оквиру једне регионалне организације.[647] Тај став је задржан и у периоду након 2020. године, што се огледа усвајањем Основâ државне политике Руске Федерације у области међународне информационе безбедности, које су одобрене Указом председника Руске Федерације бр. 213 од 12. априла 2021. године.[648] У новом документу циљ државне политике у области међународне информационе безбедности изричито се везује за успостављање међународноправног режима који би спречавао сукобе у информационом простору и обезбеђивао суверену једнакост држава у процесу регулисања ове сфере.[649] Овим је руска позиција добила јаснији доктринарни облик а то је да је међународна сарадња прихватљива и пожељна, али само ако почива на принципима државног суверенитета, немешања у унутрашње послове и универзалности међународноправних правила.[650]

Период од 2020. до 2025. године посебно је значајан зато што је у оквиру Уједињених нација успостављен и развијан нови институционални формат расправе о безбедности информационо-комуникационих технологија. Генерална скупштина је Резолуцијом 75/240 успоставила Отворену радну групу о безбедности и употреби ИКТ за период од 2021 до 2025.године, чиме је настављен процес у ком Русија види погодан мултилатерални оквир за разматрање норми, мера поверења,

[642] United Nations Office for Disarmament Affairs, "Developments in the Field of Information and Telecommunications in the Context of International Security."
[643] United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/63/37, December 2, 2008; Korzak, *Russia's Cyber Policy Efforts in the United Nations*, 13–18.
[644] Korzak, *Russia's Cyber Policy Efforts in the United Nations*, 13–18.
[645] Keir Giles, "Russia's Public Stance on Cyberspace Issues," in *2012 4th International Conference on Cyber Conflict*, ed. Christian Czosseck, Rain Ottis, and Katharina Ziolkowski (Tallinn: NATO CCD COE Publications, 2012), 67; Parliamentary Assembly of the Council of Europe, *Opinion on the Draft Second Additional Protocol to the Convention on Cybercrime (ETS No. 185)*, Doc. 15379 (2021), 6–7.
[646]Giles, "Russia's Public Stance on Cyberspace Issues," 67; Cybercrime Convention Committee (T-CY), *T-CY Guidance Note #3: Transborder Access to Data (Article 32)* (Strasbourg: Council of Europe, 2014), 2.
[647] Korzak, *Russia's Cyber Policy Efforts in the United Nations*, 14–18; PIR Center, "International Information Security and Russia's National Interests," 2025.
[648] Russian Federation, Указ Президента Российской Федерации от 12 апреля 2021 г. № 213, „Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности".
[649] Ибид
[650] Ибид; Korzak, Russia's Cyber Policy Efforts in the United Nations, 18–19.

изградње капацитета и питања међународног права у дигиталној сфери.[651] Током 2022, 2023. и 2024. године усвајани су годишњи извештаји о напретку рада ове Радне групе, а расправа се постепено померала ка питању да ли постојећи механизам треба претворити у трајнији форум под окриљем УН.[652] Са становишта руске политике, то је било од посебног значаја, јер је Москва дуго заговарала управо модел сталног, отвореног и међудржавног дијалога унутар Уједињених нација, уместо фрагментираних или регионално ограничених механизама.[653] Истовремено, на колосеку кривичноправне сарадње настављен је рад на изради универзалне конвенције УН о сајбер криминалу, који је произашао из раније резолуције 74/247.[654] Тај процес је кулминирао крајем 2024. године, када је Генерална скупштина Резолуцијом 79/243 од 24. децембра 2024. године усвојила Конвенцију Уједињених нација против сајбер криминала. Конвенција охрабрује јачање међународне сарадње у борби против одређених кривичних дела учињених путем информационо-комуникационих система и ради прикупљања, чувања и размене електронских доказа за тешка кривична дела.[655] Овај акт је од изузетног значаја за руску позицију, јер представља први глобални и универзални кривичноправни инструмент у овој области усвојен под окриљем УН, што је у основи ближе руском моделу међународне регулације него регионални приступ Будимпештанске конвенције.[656] Руска дипломатија је крајем 2024. године ову конвенцију оценила као преломан резултат и ставила њено што брже ступање на снагу међу приоритете своје политике у области међународне информационе безбедности.[657]

Током 2025. и почетком 2026. године уочава се да Русија овај приступ не само да задржава, већ настоји да га додатно институционализује. Коначни извештај Отворене радне групе 2021–2025 усвојен је у јулу 2025. године, а генерални секретар УН поздравио је његово усвајање као важан резултат мултилатералног дијалога.[658] Истовремено, у документима Генералне скупштине из 2025. године указује се на припреме за прво суштинско пленарно заседање будућег сталног механизма који треба да наследи овај формат, што значи да се расправа о међународној информационој безбедности постепено претвара у трајнији институционални процес.[659] Руско

[651] United Nations General Assembly, *Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, A/RES/75/240, December 31, 2020.
[652] United Nations General Assembly, *Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, A/77/275, August 8, 2022; United Nations General Assembly, *Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, A/78/265, August 1, 2023; United Nations General Assembly, *Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, A/79/214, July 18, 2024.
[653] Elaine Korzak, *Russia's Cyber Policy Efforts in the United Nations*, Tallinn Paper No. 11 (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2021), 14–19.
[654] United Nations General Assembly, *Countering the Use of Information and Communications Technologies for Criminal Purposes*, A/RES/74/247, December 27, 2019.
[655] United Nations General Assembly, *United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*, A/RES/79/243, December 24, 2024.
[656] Korzak, *Russia's Cyber Policy Efforts in the United Nations*, 14–18; United Nations General Assembly, *United Nations Convention against Cybercrime*, A/RES/79/243, December 24, 2024.
[657] Ministry of Foreign Affairs of the Russian Federation, "Cyber Stability: Approaches, Prospects, Challenges," December 12, 2024.
[658] United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/80/257, July 24, 2025; United Nations Secretary-General, "Secretary-General Welcomes Adoption of Final Report of Open-ended Working Group on Security of and in the Use of Information and Communications Technologies," SG/SM/22726, July 14, 2025.
[659] United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/80/257, July 24, 2025; United Nations Office for Disarmament Affairs, "Global Mechanism on ICTs in the Context of International Security: Plenary 2026."

Министарство спољних послова је у јулу 2025. године, после завршетка рада Отворене радне групе, саопштило да ће Русија наставити да у УН доследно промовише идеју усаглашавања и усвајања универзалних правно обавезујућих договора у овој области.[660] Церемонија потписивања Конвенције УН против сајбер криминала одржала се у Ханоју у октобру 2025. године. Руска страна је и тада искористила прилику да позове све државе чланице УН да приступе документу и омогуће његово што брже ступање на снагу.[661]

Почетком 2026. године руски званичници су говорили о почетку унутрашње процедуре ратификације ове конвенције, док су и документи Комисије УН за превенцију криминала и кривично правосуђе у 2026. години полазили од чињенице да је Конвенција 2024. усвојена и да представља нову референтну тачку међународне сарадње у овој области.[662]

У периоду 2020–2026. године, руска политика међународне сарадње у информационој безбедности задржала је своја основна обележја — инсистирање на суверенитету, немешању у унутрашње послове и универзалним правилима под окриљем УН — али је истовремено ушла у фазу видљивије нормативне и институционалне консолидације.[663]

4.3 Доктрина информационе безбедности Руске Федерације из 2016. године

Дана 5. децембра 2016. године председник Руске Федерације Владимир Путин потписао је нову Доктрину информационе безбедности Руске Федерације, којом је замењена дотадашња Доктрина из 2000. године.[664] Нови документ није био тек формално ажурирање претходног текста, већ важан показатељ еволуције руског стратешког мишљења у условима убрзане дигитализације, погоршаних односа са Западом и све израженијег ослањања на информациони простор као поље државног надметања.[665]

У новој Доктрини изричито се наводи да она представља систем званичних погледа на обезбеђивање националне безбедности у информационој сфери, као и да припада кругу докумената стратешког планирања који се надовезују на Стратегију националне безбедности Руске Федерације из 2015. године.[666] Управо због те везе са ширим системом националне

[660] Ministry of Foreign Affairs of the Russian Federation, "On the Completion of the Activities of the UN Open-ended Working Group on Security in the Use of ICTs 2021–2025," July 14, 2025.
[661] Ministry of Foreign Affairs of the Russian Federation, "Press Release on the UN Convention against Cybercrime," October 26, 2025; Ministry of Foreign Affairs of the Russian Federation, "The Signing of a UN Convention against Cybercrime," October 24, 2025.
[662] Ministry of Foreign Affairs of the Russian Federation, "Briefing by Foreign Ministry Spokeswoman Maria Zakharova," January 30, 2026; United Nations Economic and Social Council, *Commission on Crime Prevention and Criminal Justice: Provisional Agenda for the Thirty-Fifth Session*, E/CN.15/2026/1, January 30, 2026.
[663] Russian Federation, Указ Президента Российской Федерации от 12 апреля 2021 г. № 213, „Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности"; United Nations General Assembly, *Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, A/80/257, July 24, 2025; United Nations General Assembly, *United Nations Convention against Cybercrime*, A/RES/79/243, December 24, 2024.
[664] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации".
[665] Katri Pynnöniemi and Martti J. Kari, *Russia's New Information Security Doctrine: Guarding a Besieged Cyber Fortress*, FIIA Comment 26/2016 (Helsinki: Finnish Institute of International Affairs, 2016).
[666] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации"; Руска Федерација, Указ Президента Российской Федерации от 31 декабря 2015 г. № 683, „О Стратегии национальной безопасности Российской Федерации".

безбедности, нова Доктрина из 2016. године задобила је изразито државноцентричан и геополитички тон. У поређењу са текстом из 2000. године, њен језик је оштрији, процена ризика експлицитнија, а спољне и унутрашње претње описане су знатно конкретније.[667] У литератури је с правом примећено да се реторички дух овог документа у великој мери поклапа са духом Стратегије националне безбедности из 2015. године, која Русију представља као државу изложену сложеним и вишеслојним облицима притиска и претњи.[668] Доктрина из 2016. године не само да дефинише циљеве информационе безбедности, већ и формулише шири наратив о угрожености државног суверенитета у условима савременог информационог надметања.[669] У том смислу, њен значај далеко превазилази уску сферу техничке заштите информационих система и прелази у домен опште стратегије очувања политичке стабилности, безбедности и међународног положаја Руске Федерације.[670]

Доктрина је описује информациону сферу као целину коју чине информације, објекти информатизације, информациони системи, интернет сајтове, комуникационе мреже, информационе технологије, субјекте који производе и обрађују информације, као и механизме којима се уређују друштвени односи у самој сфери.[671] Овакво одређење има важне теоријске и практичне последице, јер показује да руски приступ информационој безбедности није ограничен на одбрану техничке инфраструктуре, већ обухвата целокупно друштвено окружење у којем информације настају, циркулишу и делују.[672] У анализама Доктрине посебно се истиче значај појма информатизације, односно процеса кроз који информационе технологије постају саставни део друштвеног, економског и државног живота.[673] Та промена није само терминолошка. Она указује на то да руска држава информациону сферу схвата као простор који обликује друштвену структуру, политичку културу, јавну свест и могућности државног управљања.[674] Зато се у Доктрини подједнако наглашавају и технолошки аспекти развоја и безбедносне последице које произилазе из ширења информационих технологија.[675]

У оквиру националних интереса у информационој сфери Доктрина повезује заштиту уставних права и слобода грађана, стабилан рад критичне информационе инфраструктуре, развој сектора информационих технологија и обезбеђивање поузданих информација о државној политици, као и јачање информационог суверенитета Руске Федерације.[676] На тај начин се информациона

[667] Pynnöniemi and Kari, *Russia's New Information Security Doctrine*.
[668] Ибид
[669] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации"; Michelle Grisé, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn, and Khrystyna Holynska, *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation* (Santa Monica, CA: RAND Corporation, 2022), 99–100, 105–106.
[670] Pynnöniemi and Kari, *Russia's New Information Security Doctrine*; Grisé et al., *Rivalry in the Information Sphere*, 99–114.
[671] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации".
[672] Исто; Grisé et al., *Rivalry in the Information Sphere*, 10–11.
[673] Pynnöniemi and Kari, *Russia's New Information Security Doctrine*.
[674] Ибид.
[675] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации".
[676] Исто; Grisé et al., *Rivalry in the Information Sphere*, 99–100; Катарина Јонев, Хатиџа Бериша и Александар Ћираковић, „Информациона безбедност Руске Федерације," *Војно дело* 2/2018: 105–106.

безбедност у руском доктринарном оквиру појављује као јединствена спона између права, технологије, економије, државне политике и геополитике.[677]

Нова Доктрина истовремено садржи знатно развијенији и конкретнији опсег претњи. У њој се наглашава да су могућности трансграничног кретања информација све чешће инструментализоване ради геополитичких циљева, циљева војно-политичке природе, терористичких, екстремистичких и других незаконитих активности.[678] Као један од кључних негативних фактора издваја се чињеница да поједине стране државе развијају капацитете информационих технологија ради утицаја на информациону инфраструктуру у војне сврхе, док се истовремено појачавају активности техничке обавештајне делатности усмерене против руских државних органа, истраживачких организација и постројења одбрамбене индустрије.[679] Доктрина такође упозорава да обавештајне службе појединих држава све више користе информационо-психолошка средства са циљем дестабилизације унутрашње политичке и социјалне ситуације, подривања суверенитета и нарушавања територијалног интегритета других држава.[680] Поред тога, у тексту се изричито наводи да расте информациони притисак на становништво Руске Федерације, посебно на младе, с циљем поткопавања традиционалних духовних и моралних вредности.[681] Као значајна претња означен је и пораст компјутерског криминала, нарочито у кредитно-финансијској сфери, као и све већа сложеност, обим и координисаност напада на објекте критичне информационе инфраструктуре.[682] Овакво набрајање претњи показује да руска држава не раздваја строго техничке претње од политичких, психолошких и друштвених утицаја, већ их повезује у један јединствени модел угрожавања.[683]

Доктрина из 2016. године посебну пажњу посвећује и питању технолошке зависности Руске Федерације од страних информационих технологија. У економској сфери као један од кључних проблема наводи се недостатак конкурентних домаћих информационих технологија и висока зависност руске индустрије од страних електронских компоненти, рачунара, хардвера, софтвера и телекомуникационе опреме.[684] Сам документ изричито упозорава да таква зависност чини социоекономски развој Руске Федерације условљеним геополитичким интересима страних земаља.[685] Овај елемент Доктрине посебно је значајан, јер показује да Русија питање информационе безбедности не везује само за заштиту од напада, већ и за технолошки суверенитет. Из тог разлога као један од стратешких праваца деловања Доктрина предвиђа развој домаћег сектора информационих технологија и електронике, повећање удела домаћих решења у привреди,

[677] Grisé et al., *Rivalry in the Information Sphere*, 10–11, 99–100; Јонев, Бериша и Ћираковић, „Информациона безбедност Руске Федерације," 105–106.
[678] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации"; Katri Pynnöniemi and Martti J. Kari, *Russia's New Information Security Doctrine: Guarding a Besieged Cyber Fortress*, FIIA Comment 26/2016 (Helsinki: Finnish Institute of International Affairs, 2016).
[679] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации".
[680] Исто.
[681] Исто.
[682] Исто; Katri Pynnöniemi and Martti J. Kari, *Russia's New Information Security Doctrine: Guarding a Besieged Cyber Fortress*, FIIA Comment 26/2016 (Helsinki: Finnish Institute of International Affairs, 2016).
[683] Michelle Grisé, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn, and Khrystyna Holynska, *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation* (Santa Monica, CA: RAND Corporation, 2022), 99–114.
[684] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации".
[685] Исто

стварање конкурентне електронске компонентне базе и шире коришћење руских безбедносних решења.[686] У литератури је указано и на то да је у радној верзији Доктрине посебно место било посвећено проблему руског заостајања у развоју суперкомпјутера, али да је та тема потом ублажена или уклоњена из финалног текста.[687] Ипак, и без тог експлицитног помињања, коначан текст Доктрине јасно сведочи о свести државног врха да технолошка инфериорност може постати стратешка слабост.[688] То је разлог зашто развој домаћег хардвера, софтвера и безбедносних капацитета није представљен искључиво као економска политика, већ као нужан услов за очување статуса велике силе у XXI веку.[689]

Још једна значајна одлика Доктрине из 2016. године јесте настојање да се у истом нормативном оквиру помире права и слободе грађана са захтевима националне безбедности. У документу се међу националним интересима изричито наводи обезбеђивање и заштита уставних права и слобода човека и грађанина у погледу пријема и коришћења информација, као и заштита приватности при употреби информационих технологија.[690] Истовремено, Доктрина наглашава да је неопходно одржавати равнотежу између захтева грађана за слободном разменом информација и ограничења која произилазе из потребе очувања националне безбедности у информационој сфери.[691] Управо ова формулација показује да руски законодавац и државни апарат слободу информација не схватају као апсолутну вредност, већ као право које се мора подвести под шири оквир државне сигурности, јавног поретка и суверенитета.[692] Доктрина, даље, инсистира на континуираном мониторингу информационих претњи, процени стања информационе безбедности и централизованијем управљању снагама и средствима заштите.[693] У практичном смислу, то подразумева јачање улоге безбедносних органа, бољу координацију државних структура и даљу институционализацију надзора над руским сегментом информационог простора.[694] Због тога се Доктрина с правом може тумачити и као документ који поред заштитне има и управљачку функцију: она не прописује само одбрану од спољних и унутрашњих претњи, већ и јачање капацитета државе да трајно прати, усмерава и контролише процесе у информационој сфери.[695] Овде је јасно видљива једна од кључних оса савременог руског приступа: безбедност и слобода информација не постављају се у однос равнотежно распоређених вредности, већ у однос у коме држава задржава право да одреди границе те равнотеже.[696]

Посебно је важно што Доктрина из 2016. године није остала на нивоу опште стратегијске декларације, већ се временски надовезала на низ правних мера које су у пракси значајно ојачале

[686] Исто; Pynnöniemi and Kari, *Russia's New Information Security Doctrine*.
[687] Pynnöniemi and Kari, *Russia's New Information Security Doctrine*.
[688] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации"; Michelle Grisé et al., *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation* (Santa Monica, CA: RAND Corporation, 2022), 99–100.
[689] Pynnöniemi and Kari, *Russia's New Information Security Doctrine*; Martti J. Kari, "An Analytical Framework for Russian Cyber Threat Perception and Strategic Culture," *Journal of Information Warfare* 18, no. 3 (2019): 1–21.
[690] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации".
[691] Исто.
[692] Olga Chislova and Marina Sokolova, "Cybersecurity in Russia," *International Cybersecurity Law Review* 2, no. 2 (2021): 245–251.
[693] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации".
[694] Pynnöniemi and Kari, *Russia's New Information Security Doctrine*.
[695] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации".
[696] Chislova and Sokolova, "Cybersecurity in Russia," 245–251.

могућности државног надзора и безбедносне контроле. У том контексту, од великог значаја су такозвани „Јароваја закони“, односно пакет антитерористичких измена законодавства усвојен у јулу 2016. године.[697] Тај пакет, који чине Федерални закон бр. 374-ФЗ и Федерални закон бр. 375-ФЗ, проширио је овлашћења државних органа у сфери борбе против тероризма и јавне безбедности, али је истовремено увео и веома далеко сежуће обавезе за телекомуникационе операторе и интернет-компаније.[698] Према тим изменама, телекомуникациони и интернет субјекти били су дужни да на територији Руске Федерације чувају садржај комуникација током одређеног временског периода, као и метаподатке знатно дуже, а истовремено су морали да обезбеде приступ надлежним органима подацима и средствима неопходним за дешифровање електронских порука.[699] У практичном смислу, то је значило да су безбедносне агенције добиле још шири приступ дигиталним комуникацијама, уз значајно ниже прагове контроле него у класичним моделима судског надзора карактеристичним за либералне демократије.[700] Критичари овог пакета закона указивали су да таква решења драматично повећавају могућности масовног надзора, угрожавају право на приватност, слабе безбедност енкрипције и намећу огромне финансијске и техничке трошкове привредним субјектима.[701] Међутим, из перспективе руске државе, ове мере нису представљале пуко административно пооштравање, већ логичан наставак државне политике у којој се информациона безбедност третира као неодвојиви део националне безбедности, антитерористичке политике и очувања државног суверенитета.[702] Доктрина из 2016. године и „Јароваја пакет“ чине две комплементарне стране исте политике у ком прва поставља стратешки и идеолошки оквир, док друга обезбеђује конкретне инструменте правне и институционалне примене.[703]

Са научног становишта, Доктрина информационе безбедности Руске Федерације из 2016. године може се разумети као документ који је објединио неколико кључних тенденција руске државне политике: јачање информационог суверенитета, милитаризацију информационог простора, развој технолошког аутономизма, нормативно ограничавање слободе протока информација у корист државне безбедности и институционално ширење надзорних капацитета.[704] Она је, истовремено, означила прелазак са релативно опште формулације информационе безбедности из 2000. године на знатно конкретнији модел у коме су спољни противници, психолошко-информациони утицаји, технолошка зависност и критична инфраструктура препознати као међусобно повезани елементи

[697] Russian Federation, Federal Law of July 6, 2016 No. 374-FZ, „О внесении изменений в Федеральный закон ‘О противодействии терроризму’ и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности”; Russian Federation, Federal Law of July 6, 2016 No. 375-FZ, „О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности”.
[698] Ибид
[699] Russian Federation, Federal Law of July 6, 2016 No. 374-FZ; Katri Pynnöniemi and Martti J. Kari, “Russia’s New Information Security Doctrine: Guarding a Besieged Cyber Fortress,” *FIIA Comment* 12/2016 (Helsinki: Finnish Institute of International Affairs, 2016); Human Rights Watch, “Russia: ‘Big Brother’ Law Harms Security, Rights,” July 12, 2016.
[700] Human Rights Watch, “Russia: ‘Big Brother’ Law Harms Security, Rights,” July 12, 2016; United Nations Human Rights Special Procedures, *OL RUS 7/2016*, July 28, 2016.
[701] Human Rights Watch, “Russia: ‘Big Brother’ Law Harms Security, Rights,” July 12, 2016; United Nations Human Rights Special Procedures, *OL RUS 7/2016*, July 28, 2016.
[702] Russian Federation, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации”; Michelle Grisé, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn, and Khrystyna Holynska, *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation* (Santa Monica, CA: RAND Corporation, 2022), 99–114.
[703] Pynnöniemi and Kari, “Russia’s New Information Security Doctrine”; Grisé et al., *Rivalry in the Information Sphere*, 99–114.
[704] Grisé et al., *Rivalry in the Information Sphere*, 99–114.

јединственог поља ризика.[705] Због тога овај документ има посебан значај за разумевање савременог руског приступа сајбер и информационом простору: он показује да Русија дигиталну сферу не посматра као технички неутрално окружење, већ као арену стратешке конкуренције, политичког утицаја и државне самоодбране.[706]

Оштрији тон Доктрине, наглашена брига за контролу информационог простора и тежња ка домаћим технолошким решењима не представљају споредне елементе документа, већ његову суштину.[707] Зато се ова Доктрина може оценити као један од кључних нормативно-стратешких темеља савременог руског схватања информационе безбедности.[708]

4.4 Континуитет и релевантност руске политике информационе безбедности до 2026. године

Доктрина информационе безбедности Руске Федерације из 2016. године има значај који знатно превазилази оквир једног стратешког документа, јер је управо њоме коначно учвршћен модел руског разумевања информационе безбедности као широке државне, друштвене, технолошке и геополитичке категорије.[709] Она није само заменила Доктрину из 2000. године, већ је означила прелаз са релативно општег, програмског приступа на знатно конкретнији и безбедносно оштрији модел у коме су претње именоване прецизније, а улога државе у заштити информационе сфере дефинисана далеко експлицитније.[710] У том смислу, Доктрина из 2016. године представља нормативно-стратешки израз шире трансформације руске безбедносне политике после 2014. године, када су односи са Западом нагло погоршани, а дигитални и информациони простор дефинитивно препознати као једно од кључних поља савремене конфронтације.[711] Једна од најважнијих теоријских и практичних последица Доктрине из 2016. године јесте управо то што је потврдила руско становиште да је сајбер безбедност само један сегмент шире информационе безбедности.[712]

Руски стратешки документи, укључујући Војну доктрину, Доктрину информационе безбедности и касније основе државне политике, по правилу избегавају да у први план ставе терминологију са префиксом „сајбер“, већ доследно говоре о информационој сфери, информационом утицају,

[705] Russian Federation, *Доктрина информационной безопасности Российской Федерации*, approved by the President of the Russian Federation on September 9, 2000, No. Пр-1895; Russian Federation, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации”.
[706] Grisé et al., *Rivalry in the Information Sphere*, 10–11, 99–114.
[707] Pynnöniemi and Kari, “Russia’s New Information Security Doctrine.”
[708] Russian Federation, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации”; Grisé et al., *Rivalry in the Information Sphere*, 99–114.
[709] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации”; Michelle Grisé, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn, and Khrystyna Holynska, *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation* (Santa Monica, CA: RAND Corporation, 2022), 99–100, 105–106.
[710] Katri Pynnöniemi and Martti J. Kari, “Russia’s New Information Security Doctrine: Guarding a Besieged Cyber Fortress,” *FIIA Comment* 26/2016 (Helsinki: Finnish Institute of International Affairs, 2016).
[711] Руска Федерација, Указ Президента Российской Федерации от 31 декабря 2015 г. № 683, „О Стратегии национальной безопасности Российской Федерации”; Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации”.
[712] Grisé et al., *Rivalry in the Information Sphere*, 10–11; Катарина Јонев, Хатица Бериша и Александар Ћираковић, „Информациона безбедност Руске Федерације,” *Војно дело* 2/2018: 105–106.

информационој конфронтацији и међународној информационој безбедности.[713] Оваква разлика није само језичка, већ суштински концептуална: она показује да се у руском моделу заштита техничке инфраструктуре не може одвојити од питања политичког суверенитета и друштвене кохезије.[714] Због тога је Доктрина из 2016. године од пресудног значаја за разумевање начина на који Русија чита дигитални простор — не као неутрално техничко окружење, већ као арену сталне политичке, психолошке и стратешке борбе.[715] Управо на том месту овај документ најјасније одступа од уже, технички оријентисане западне концепције „cybersecurity“ и потврђује да руска држава информациону сферу посматра у оквиру много ширег поља државне моћи и одбране.[716]

Посебна вредност Доктрине из 2016. године огледа се у томе што она није остала на нивоу декларативног текста, већ је постала основ за читав низ институционалних и правних мера којима је руска држава настојала да практично ојача контролу и заштиту у информационој сфери.[717] Тај процес је нарочито видљив у законодавству и државној организацији после 2016. године. Већ Федералним законом бр. 187-ФЗ од 26. јула 2017. године о безбедности критичне информационе инфраструктуре створен је посебан правни оквир за идентификацију, категоризацију и заштиту значајних објеката критичне информационе инфраструктуре Руске Федерације.[718] Потом је Федералним законом бр. 90-ФЗ од 1. маја 2019. године додатно ојачана логика такозваног „сувереног интернета“, односно могућности државе да обезбеди стабилан, контролисан и, у крајњој линији, од спољних притисака отпорнији национални сегмент мреже.[719] У међународној равни овај развој добио је и доктринарну допуну у Основама државне политике Руске Федерације у области међународне информационе безбедности из 2021. године, где се изричито истиче потреба за међународноправним режимом заснованим на сувереној једнакости држава и немешању у унутрашње послове.[720] У унутрашњем безбедносном и технолошком смислу, ова линија је даље ојачана указима бр. 166 и бр. 250 из 2022. године, којима су државни органи и значајни субјекти обавезани на додатне мере у циљу обезбеђивања технолошке независности и информационе безбедности.[721] Све то показује да је Доктрина из 2016. године била не само концептуална основа, већ и нормативни покретач каснијег продубљивања државне политике у

[713] Руска Федерација, *Военная доктрина Российской Федерации*, approved by the President of the Russian Federation on December 25, 2014, No. Пр-2976; Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации”; Руска Федерација, Указ Президента Российской Федерации от 12 апреля 2021 г. № 213, „Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности”.
[714] Grisé et al., *Rivalry in the Information Sphere*, 10–11.
[715] Pynnöniemi and Kari, “Russia’s New Information Security Doctrine.”
[716] Grisé et al., *Rivalry in the Information Sphere*, 10–11, 99–100.
[717] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации”.
[718] Руска Федерација, Федеральный закон от 26 июля 2017 г. № 187-ФЗ, „О безопасности критической информационной инфраструктуры Российской Федерации”.
[719] Руска Федерација, Федеральный закон от 1 мая 2019 г. № 90-ФЗ, „О внесении изменений в Федеральный закон ‘О связи’ и Федеральный закон ‘Об информации, информационных технологиях и о защите информации’”.
[720] Руска Федерација, Указ Президента Российской Федерации от 12 апреля 2021 г. № 213, „Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности”.
[721] Руска Федерација, Указ Президента Российской Федерации от 30 марта 2022 г. № 166, „О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации”; Руска Федерација, Указ Президента Российской Федерации от 1 мая 2022 г. № 250, „О дополнительных мерах по обеспечению информационной безопасности Российской Федерации”.

правцу технолошке аутономије, заштите критичне инфраструктуре и јачања безбедносне контроле над националним информационим простором.[722]

Једно од најважнијих аналитичких питања које овај документ отвара јесте однос између права и слобода грађана у информационој сфери и државне безбедности.[723] Доктрина из 2016. године међу националним интересима у информационој сфери признаје заштиту уставних права и слобода човека и грађанина, укључујући право на приступ информацијама и употребу информационих технологија.[724] Међутим, сама Доктрина полази од потребе да се успостави равнотежа између слободног кретања информација и ограничења условљених очувањем националне безбедности, док пракса која је уследила показује да се у руском моделу у случају сукоба између индивидуалних слобода и државне безбедности предност даје безбедности, надзору и суверенитету.[725] У том смислу посебно су значајни такозвани „Јароваја закони“ из 2016. године, односно Федерални закони бр. 374-ФЗ и 375-ФЗ, којима су операторима и другим субјектима наметнуте обавезе чувања података и садржаја комуникација, као и омогућавања приступа надлежним органима.[726] Према оценама међународних стручних тела и организација за заштиту људских права, ова решења су значајно проширила могућности државног надзора, укључујући чување садржаја комуникација до шест месеци и метаподатака и корисничких података у дужим роковима, што је изазвало озбиљне критике у погледу приватности, слободе изражавања и безбедности енкрипције.[727] Отуд се може закључити да је једна од најважнијих практичних последица Доктрине из 2016. године управо учвршћивање нормативног оквира у коме држава задржава право да широким позивањем на безбедност ограничава обим слободне и приватне комуникације.[728] То је важан научни закључак, јер показује да руски концепт информационе безбедности није само одбрамбени, већ и управљачки и дисциплинарни: он не штити само од претњи, већ и проширује капацитет државе да трајно надзире и усмерава информациону сферу.[729]

[722] Руска Федерација, Указ Президента Российской Федерации от 13 июня 2024 г. № 500, „О внесении изменений в Указ Президента Российской Федерации от 1 мая 2022 г. № 250”; Руска Федерација, Указ Президента Российской Федерации от 7 апреля 2025 г. № 214, „О внесении изменения в Указ Президента Российской Федерации от 30 марта 2022 г. № 166”.

[723] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации”; Olga Chislova and Marina Sokolova, “Cybersecurity in Russia,” *International Cybersecurity Law Review* 2, no. 2 (2021): 245–251.

[724] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации”.

[725] Исто; Chislova and Sokolova, “Cybersecurity in Russia,” 245–251.

[726] Russian Federation, Федеральный закон от 6 июля 2016 г. № 374-ФЗ, „О внесении изменений в Федеральный закон ‘О противодействии терроризму’ и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности”; Russian Federation, Федеральный закон от 6 июля 2016 г. № 375-ФЗ, „О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности”.

[727] Human Rights Watch, “Russia: ‘Big Brother’ Law Harms Security, Rights,” July 12, 2016; United Nations Human Rights Special Procedures, *OL RUS 7/2016*, July 28, 2016.

[728] Chislova and Sokolova, “Cybersecurity in Russia,” 245–251; Human Rights Watch, “Russia: ‘Big Brother’ Law Harms Security, Rights,” July 12, 2016.

[729] Michelle Grisé, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn, and Khrystyna Holynska, *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation* (Santa Monica, CA: RAND Corporation, 2022), 99–114; Chislova and Sokolova, “Cybersecurity in Russia,” 245–251.

Друга крупна тема коју је Доктрина из 2016. године учинила стратешки централном јесте технолошки суверенитет.[730] У самом тексту Доктрине наглашава се да зависност од страних информационих технологија и електронских компоненти представља безбедносни ризик, јер социоекономски развој Русије чини подложним геополитичким интересима страних држава.[731] Из тог разлога, развој домаћих софтверских, хардверских и инфраструктурних решења представља један од аспеката безбедносне и државотворне политике.[732] Управо та логика технолошке самосталности наставља се и у периоду до 2026. године. Указ председника Руске Федерације бр. 309 од 7. маја 2024. године, којим су утврђени национални циљеви развоја до 2030. године и перспектива до 2036. године, изричито повезује развој државе са задацима мрежног суверенитета и информационе безбедности.[733] Указом бр. 500 од 13. јуна 2024. године унете су измене у ранији указ о додатним мерама обезбеђивања информационе безбедности, што имплицира да ова тема остаје на нивоу највише политичке пажње.[734]

У 2025. години додатно су ојачане везе између информационе безбедности, технолошке независности и критичне инфраструктуре, нарочито кроз Указ бр. 214 од 7. априла 2025. године, који мења претходни указ о технолошкој независности и безбедности критичне информационе инфраструктуре.[735] Стога се може рећи да је један од најтрајнијих ефеката Доктрине из 2016. године управо то што је она технолошку самосталност уздигла на ниво безбедносног императива, а до 2026. године тај императив је већ постао саставни део ширег државног развојног и безбедносног програма.[736]

Релевантност Доктрине из 2016. године у периоду до 2026. године посебно се види у даљој институционалној и техничкој конкретизацији механизама заштите. Она се не огледа само у програмским и политичким документима, већ и у прецизнијем уређивању начина деловања државних и кључних инфраструктурних субјеката. Тако су крајем 2025. године и почетком 2026. године објављени нови акти Федералне службе безбедности, којима се ближе уређује рад и повезивање субјеката критичне информационе инфраструктуре са државним системом за

[730] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации"; Katri Pynnöniemi and Martti J. Kari, "Russia's New Information Security Doctrine: Guarding a Besieged Cyber Fortress," *FIIA Comment* 26/2016 (Helsinki: Finnish Institute of International Affairs, 2016).
[731] Руска Федерација, Указ Президента Российской Федерации от 5 декабря 2016 г. № 646, „Об утверждении Доктрины информационной безопасности Российской Федерации".
[732] Pynnöniemi and Kari, "Russia's New Information Security Doctrine: Guarding a Besieged Cyber Fortress"; Martti J. Kari, "An Analytical Framework for Russian Cyber Threat Perception and Strategic Culture," *Journal of Information Warfare* 18, no. 3 (2019): 1–21.
[733] Руска Федерација, Указ Президента Российской Федерации от 7 мая 2024 г. № 309, „О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года".
[734] Руска Федерација, Указ Президента Российской Федерации от 13 июня 2024 г. № 500, „О внесении изменений в Указ Президента Российской Федерации от 1 мая 2022 г. № 250".
[735] Руска Федерација, Указ Президента Российской Федерации от 7 апреля 2025 г. № 214, „О внесении изменения в Указ Президента Российской Федерации от 30 марта 2022 г. № 166".
[736] Руска Федерација, Указ Президента Российской Федерации от 12 апреля 2021 г. № 213, „Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности"; Руска Федерација, Указ Президента Российской Федерации от 7 мая 2024 г. № 309, „О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года"; Руска Федерација, Указ Президента Российской Федерации от 13 июня 2024 г. № 500, „О внесении изменений в Указ Президента Российской Федерации от 1 мая 2022 г. № 250"; Руска Федерација, Указ Президента Российской Федерации от 7 апреля 2025 г. № 214, „О внесении изменения в Указ Президента Российской Федерации от 30 марта 2022 г. № 166".

откривање, спречавање и отклањање последица компјутерских напада.[737] Међу њима су нарочито важни: Приказ ФСБ бр. 548 од 25. децембра 2025. године, којим се уређује континуирано међудејство субјеката критичне информационе инфраструктуре са државним системом; Приказ ФСБ бр. 539 од 23. децембра 2025. године, који прописује начин добијања информација о средствима и методама компјутерских напада и начинима њиховог откривања и спречавања; као и прикази бр. 553 и 554 од 26. децембра 2025. године, који се односе на техничке услове инсталације и рада средстава за откривање, спречавање и отклањање последица компјутерских напада и реаговање на инциденте.[738] Значај ових аката је у томе што показују да се до краја 2025. и уласка у 2026. годину руска политика информационе безбедности креће ка још детаљнијем, практично оперативном уређењу односа између државе, ФСБ, критичне инфраструктуре и система раног откривања напада и реаговања.[739] Доктрина из 2016. године до 2026. више није само оквирна стратегија, већ основа из које се изводе конкретна техничка и организациона правила државне безбедносне праксе.[740]

Коначно, посебно је важно нагласити да и 2026. године Доктрина из 2016. остаје нормативно релевантна и политички активна. То се види по томе што се у новијим председничким актима она и даље наводи уз Стратегију националне безбедности и Стратегију развоја информационог друштва као једног од основних праваца државне политике.[741] Указ председника Руске Федерације бр. 136 од 4. марта 2026. године се изричито позива на Доктрину информационе безбедности Руске Федерације, што представља снажан доказ њеног континуитета у систему стратешког планирања.[742] Поред тога, кадровске и организационе измене у саставу Међуресорне комисије Савета безбедности Руске Федерације за информациону безбедност, укључујући Указ

[737] Руска Федерација, Приказ Федеральной службы безопасности Российской Федерации от 25 декабря 2025 г. № 548, „Об утверждении Порядка осуществления непрерывного взаимодействия субъектов критической информационной инфраструктуры Российской Федерации …"; Руска Федерација, Приказ Федеральной службы безопасности Российской Федерации от 23 декабря 2025 г. № 539, „Об утверждении Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения"; Руска Федерација, Приказ Федеральной службы безопасности Российской Федерации от 26 декабря 2025 г. № 553, „Об утверждении Порядка и Технических условий установки и эксплуатации средств …"; Руска Федерација, Приказ Федеральной службы безопасности Российской Федерации от 26 декабря 2025 г. № 554, „Об установлении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты …".

[738] Руска Федерација, Приказ Федеральной службы безопасности Российской Федерации от 25 декабря 2025 г. № 548, „Об утверждении Порядка осуществления непрерывного взаимодействия субъектов критической информационной инфраструктуры Российской Федерации …"; Руска Федерација, Приказ Федеральной службы безопасности Российской Федерации от 23 декабря 2025 г. № 539, „Об утверждении Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения"; Руска Федерација, Приказ Федеральной службы безопасности Российской Федерации от 26 декабря 2025 г. № 553, „Об утверждении Порядка и Технических условий установки и эксплуатации средств …"; Руска Федерација, Приказ Федеральной службы безопасности Российской Федерации от 26 декабря 2025 г. № 554, „Об установлении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты …".

[739] Ибид

[740] Руска Федерација, Приказ Федеральной службы безопасности Российской Федерации от 25 декабря 2025 г. № 548; Приказ Федеральной службы безопасности Российской Федерации от 23 декабря 2025 г. № 539; Приказ Федеральной службы безопасности Российской Федерации от 26 декабря 2025 г. № 553; Приказ Федеральной службы безопасности Российской Федерации от 26 декабря 2025 г. № 554.

[741] Руска Федерација, Указ Президента Российской Федерации от 4 марта 2026 г. № 136, „О внесении изменений в некоторые акты Президента Российской Федерации".

[742] Ибид

бр. 88 од 16. фебруара 2026. године, показују да држава ову област и даље третира као трајно и високо приоритетно безбедносно питање.[743]

Релевантност Доктрине из 2016. године до 2026. године је вишеструка. Она је истовремено концептуална, јер дефинише руско разумевање информационе безбедности; нормативна, јер служи као основ за касније акте; институционална, јер усмерава рад државних органа и координационих тела; и политичка, јер оправдава јачање државне контроле, технолошког суверенитета и безбедносне интервенције у дигиталном простору.[744] Управо зато ова Доктрина није само један од докумената у низу, већ један од кључних текстова за разумевање савременог руског приступа односу између државе, технологије, друштва и безбедности.[745]

Пуно значење руског приступа информационој безбедности најјасније се уочава у конкретним кризним и конфликтним ситуацијама, због чега је потребно посебно размотрити случај Естоније 2007. године и руско-украјински сукоб у сајбер простору.

4.5 Први међународни сајбер сукоб – напад на информационе системе у Естонији

Естонија је уочи напада из 2007. године важила за једну од најдигитализованијих држава у Европи и свету, а њен модел развоја често је навођен као пример успешне трансформације у е-државу.[746] Она је већ 2005. године постала прва држава која је спровела правно обавезујуће гласање на изборима путем интернета, док су банкарство, јавне услуге, комуникација са државом и велики део свакодневних друштвених и економских активности били снажно ослоњени на мрежну инфраструктуру.[747] Управо се та висока дигитална интегрисаност, која је представљала њену развојну предност, показала и као значајна безбедносна рањивост.[748]

У периоду од 27. априла до средине, односно краја маја 2007. године, Естонија је била изложена координисаној кампањи напада, пре свега у облику ускраћивања услуге и дистрибуираног ускраћивања услуге, усмерених на владине институције, парламент, министарства, банке, интернет провајдере, медије и друге приватне и јавне субјекте.[749] Напади су уследили после одлуке естонских власти да из центра Талина преместе споменик совјетским војницима, што је изазвало снажне политичке, друштвене и етничке тензије у самој Естонији, али и озбиљно погоршање односа са Москвом.[750] Напади су ескалирали у периоду око 9. маја, датума који у Русији има снажно симболичко значење као Дан победе над фашизмом у Другом светском рату. Мете напада су обухватиле не само информативне портале и веб-сајтове, већ и кључне услуге,

[743] Руска Федерација, Указ Президента Российской Федерации от 16 февраля 2026 г. № 88, „О внесении изменений в состав Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям, утвержденный Указом Президента Российской Федерации от 10 ноября 2018 г. № 648".
[744] Руска Федерација, Указ Президента Российской Федерации от 4 марта 2026 г. № 136; Руска Федерација, Указ Президента Российской Федерации от 16 февраля 2026 г. № 88.
[745] Ибид
[746] Vincent Joubert, *Five Years After Estonia's Cyber Attacks: Lessons Learned for NATO?* (Rome: NATO Defense College, 2012), 1–2.
[747] Fabian Breuer and Alexander H. Trechsel, *E-Voting in the 2005 Local Elections in Estonia* (Strasbourg: Council of Europe, 2006), 3–4.
[748] Joubert, *Five Years After Estonia's Cyber Attacks*, 1–2.
[749] Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," in *Proceedings of the 7th European Conference on Information Warfare and Security* (Plymouth, 2008), 163–168.
[750] Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia," 163–164.

укључујући електронско банкарство и DNS инфраструктуру.[751] Иако напади нису изазвали физичко разарање у класичном смислу, они су показали да чак и релативно „неконвенционалне“ дигиталне операције могу да привремено поремете функционисање високо дигитализоване државе.[752] Политички и правни контекст овог догађаја био је додатно усложен проблемом атрибуције, односно тешкоћом да се у сајбер простору поуздано утврди идентитет извршиоца, стварни налогодавац и степен државне одговорности за изведени напад.

Естонски званичници су у првим реакцијама сумњу усмерили ка Русији и окривили званичнике да су одговорни за напад. Међутим, упркос бројним сумњама и политичким оптужбама, у извештајима естонских и међународних извора нису били јавно представљени коначни и правно неспорни докази који би потврдили да је Кремљ непосредно руководио овим нападима.[753] Управо је та околност показала колико је у сајбер простору тешко са довољним степеном извесности утврдити ко је стварни организатор операције, нарочито када се напади изводе преко ботнета, инфраструктуре распоређене у више држава и великог броја компромитованих система.[754]

Истраге су довеле само до ограничених процесних резултата, па је тако у Естонији правноснажно осуђен један учесник, док је шира кривична и међудржавна одговорност остала нерасветљена.[755] У стручним анализама управо је овај случај често навођен као класичан пример јаза између политичке сумње, техничких индиција и правног стандарда доказивања.[756] Он је, истовремено, показао да сајбер инцидент може имати озбиљне националне, безбедносне и економске последице чак и када праг класичног оружаног напада није достигнут.[757] То је уједно био и један од разлога због којих је естонски случај постао толико значајан у каснијим правним и стратешким расправама о сајбер операцијама.[758]

Импликације напада у Естонији биле су вишеструке и далекосежне. Пре свега, естонски случај је показао да висок степен дигитализације, сам по себи, не значи и висок степен отпорности, већ да модерна е-држава може постати посебно осетљива ако развој електронских услуга не прати истовремено развој одбрамбених механизама, планова континуитета пословања и координације са приватним сектором.[759] Даље, напади су показали да је граница између јавног и приватног сектора у сајбер кризи знатно слабија него у класичним безбедносним сценаријима, јер су истовремено погођени државни органи, банке, провајдери, медији, и комуникациона инфраструктура.[760] Тако је постало јасно да заштита сајбер простора не може бити искључиво задатак безбедносних структура једне државе попут војске или полиције, већ захтева

[751] Исто, 164–166.
[752] Joubert, *Five Years After Estonia's Cyber Attacks*, 1–2; Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia," 164–166.
[753] Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia," 165–166.
[754] Исто, 165–166.
[755] Исто, 166.
[756] Michael N. Schmitt, gen. ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), foreword, xxiii–xxiv.
[757] Joubert, *Five Years After Estonia's Cyber Attacks*, 1–2.
[758] Schmitt, *Tallinn Manual 2.0*, foreword, xxiii–xxiv.
[759] Vincent Joubert, *Five Years After Estonia's Cyber Attacks: Lessons Learned for NATO?* (Rome: NATO Defense College, 2012), 1–2.
[760] Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," in *Proceedings of the 7th European Conference on Information Warfare and Security* (Reading: Academic Publishing Limited, 2008), 163–168.

свеобухватни модел у коме се повезују државни органи, технички експерти, финансијске институције и цивилни телекомуникациони актери.[761]

Естонски случај је наметнуо и питање правне квалификације сајбер напада: иако су напади били снажни, координисани и политички мотивисани, они нису јавно квалификовани као оружани напад у смислу међународног права, што је касније потврђено и у правној литератури окупљеној око Талинског приручника.[762] То је значило да су сајбер операције против Естоније откриле озбиљну празнину између стварне штете коју дигитални напади могу да произведу и постојећих правних прагова за примену самоодбране и колективне одбране.[763] У политичком смислу, случај је отворио и питање домета члана 5. Вашингтонског уговора, јер је Естонија као чланица НАТО-а очекивала снажнију реакцију савезника, али је Алијанса у том тренутку још увек била нормативно и институционално недовољно припремљена за сајбер кризе овог типа.[764] Ипак, управо је та неспремност постала снажан подстицај за промене унутар НАТО-а.[765] Савезнички министри одбране су већ 2007. године закључили да је неопходно хитно јачање способности заштите информационих система од критичног значаја, а НАТО је у јануару 2008. усвојио своју прву Политику сајбер одбране.[766] Непосредно затим, на иницијативу Естоније и више савезничких држава, 14. маја 2008. године основан је НАТО Центар изузетности за кооперативну сајбер одбрану у Талину, што представља једну од највидљивијих институционалних последица напада из 2007. године.[767] На националном нивоу, Естонија је 2008. године усвојила прву националну Стратегију сајбер безбедности, у којој су наглашени заштита критичне инфраструктуре, организациона сарадња, обука, развој и истраживање, као и активна међународна сарадња.[768] Напади су, дакле, деловали као катализатор за трансформацију сајбер безбедности из техничког питања у питање државне стратегије, јавне политике и међународне сарадње.[769] Они су такође показали да будући конфликти вероватно неће бити искључиво конвенционални, већ да ће сајбер операције све чешће деловати као допуна политичком притиску, информационим кампањама и, потенцијално, класичним војним средствима.[770] Са тог становишта, естонски случај је постао важна рана најава каснијих хибридних модела деловања, у којима се дигитални утицај комбинује са информационим, друштвеним и дипломатским инструментима. Суштина оваквих модела лежи у координисаној примени различитих облика моћи, како би се истовремено нарушили безбедност, стабилност институција и поверење јавности.[771] Овај случај је снажно подстакао развој међународноправне расправе о примени постојећег права на сајбер операције, а из тог процеса је проистекао и Талински приручник, чији је утицај на глобалну правну дебату остао снажан и деценију касније.[772] Чињеница да је CCDCOE 2021. покренуо и пројекат Tallinn Manual 3.0, као петогодишњи подухват који траје и кроз 2026.

[761] Joubert, *Five Years After Estonia's Cyber Attacks*, 1–2; Estonian Ministry of Defence, *Cyber Security Strategy 2008–2013* (Tallinn, 2008), 3–6.
[762] Michael N. Schmitt, gen. ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), xxiii–xxiv.
[763] Исто, xxiii–xxiv; Vincent Joubert, *Five Years After Estonia's Cyber Attacks: Lessons Learned for NATO?* (Rome: NATO Defense College, 2012), 3–5.
[764] Joubert, *Five Years After Estonia's Cyber Attacks*, 3–5.
[765] North Atlantic Treaty Organization, "Cyber Defence," 2024.
[766] North Atlantic Treaty Organization, "Cyber Defence," 2024.
[767] NATO Cooperative Cyber Defence Centre of Excellence, "About Us."
[768] Estonian Ministry of Defence, *Cyber Security Strategy 2008–2013* (Tallinn, 2008), 3–12.
[769] Joubert, *Five Years After Estonia's Cyber Attacks*, 5–7.
[770] Ибид. 5–7.
[771] Michael N. Schmitt, gen. ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), xxiii–xxiv.
[772] Ибид, xxiii–xxiv.

годину, потврђује да напади на Естонију и даље представљају једну од кључних референтних тачака за разумевање правних и стратешких дилема сајбер простора.[773] Зато се може закључити да је најдубља импликација естонског случаја у томе што је показао да сајбер напади могу имати озбиљне државне последице и онда када не производе физичко уништење, јер нарушавају поверење у институције, утичу на економију, откривају рањивост друштва и приморавају државе и савезе да мењају своје правне, стратешке и институционалне моделе безбедности.[774]

Из данашње перспективе, естонски напади из 2007. године имају и трајну методолошку и политичку вредност. Они су показали да дигитална зависност модерних друштава производи нову врсту рањивости у којој се паралисање комуникација, банкарских услуга, медија и рада институција може остварити без преласка државне границе у физичком смислу.[775] Истовремено, показали су да се отпорност не гради само техничким средствима, већ и јасним правилима командовања, координацијом између државе и привреде, брзом међународном сарадњом и развијеном правном свешћу о томе шта сајбер операције јесу, а шта нису у смислу међународног права.[776] Управо због тога Естонија је после 2007. године постала један од највидљивијих заговорника јачања међународне регулације, развоја сајбер одбрамбених политика у НАТО-у и Европи и подизања глобалне свести о томе да сајбер безбедност више није споредна техничка тема, већ једна од основних димензија савремене националне и међународне безбедности.[777] И до 2026. године, у стручним, политичким и правним расправама, случај Естоније остао је полазна тачка за разумевање односа између дигиталне зависности, сајбер отпорности, хибридних претњи, државне одговорности и колективне одбране у информационом добу.[778]

4.6 Вођење сајбер рата паралелно уз конвенционални сукоб – рат у Украјини

Руско-украјински сукоб у сајбер простору не може се разумети као низ изолованих инцидената, већ као дуготрајан и свеобухватан облик дигиталне конфронтације који се развија упоредо са ширим политичким и војним сукобом између две државе.[779]

Од 2014. године па надаље, украјински дигитални простор постао је једно од кључних „полигона“ за испробавање руских офанзивних сајбер капацитета, а од прединвазионе фазе 2021. и отворене инвазије 24. фебруара 2022. тај сукоб је ушао у нову, далеко интензивнију фазу.[780] Његова посебност огледа се у томе што су сајбер операције у украјинском случају тесно повезане са обавештајним радом, политичким притиском, информационим операцијама и кинетичким дејствима и не представљају споредну димензију рата, већ један од његових конститутивних

[773] NATO Cooperative Cyber Defence Centre of Excellence, “The Tallinn Manual”; NATO Cooperative Cyber Defence Centre of Excellence, “Tallinn Manual 3.0,” 2021.
[774] Joubert, *Five Years After Estonia’s Cyber Attacks*, 1–7; Schmitt, *Tallinn Manual 2.0*, xxiii–xxiv.
[775] Ottis, “Analysis of the 2007 Cyber Attacks Against Estonia,” 163–168.
[776] Estonian Ministry of Defence, *Cyber Security Strategy 2008–2013* (Tallinn, 2008), 3–12; Joubert, *Five Years After Estonia’s Cyber Attacks*, 5–7.
[777] North Atlantic Treaty Organization, “Cyber Defence,” updated July 30, 2024; NATO Cooperative Cyber Defence Centre of Excellence, “About Us.”
[778] NATO Cooperative Cyber Defence Centre of Excellence, “The Tallinn Manual”; NATO Cooperative Cyber Defence Centre of Excellence, “Tallinn Manual 3.0,” 2021.
[779] Google Threat Analysis Group, *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape* (2022), 4–6; Microsoft, *An Overview of Russia’s Cyberattack Activity in Ukraine: Special Report: Ukraine* (April 27, 2022), 1.
[780] Google Threat Analysis Group, *Fog of War*, 6; ESET, *ESET Threat Report T1 2022* (2022), 6.

елемената.[781] Украјински пример има посебан значај за теорију и праксу сајбер безбедности јер доказује да сајбер простор није само место техничких упада у мреже, већ поље у коме се истовремено води борба за команду, комуникације, инфраструктуру, морал становништва и институционалну отпорност државе.[782]

Историјски посматрано, ране фазе овог сукоба почињу већ након руске анексије Крима и избијања оружаног конфликта у Донбасу 2014. године, када су забележене кампање сајбер шпијунаже усмерене на украјинске државне (и са државом повезане) мете.[783] Истраживачи компаније ESET указали су да је злонамерни софтвер BlackEnergy још 2014. коришћен у серији сајбер-шпијунских операција против високопозиционираних, са владом повезаних циљева у Украјини.[784] Тиме је већ у раној фази сукоба успостављен образац који ће касније постати типичан за сукоб а то је дуготрајно убацивање у мреже, прикривено присуство шпијунског софтвера, прикупљање података и накнадна могућност преласка са шпијунаже на деструкцију.[785] Значај тог периода не лежи само у чињеници да су руске групе тестирале техничке алате, већ и у томе што је Украјина постала простор у коме се испробавао модел спајања државног интереса, обавештајних капацитета и дигиталног притиска.[786]

Први велики преломни тренутак наступио је крајем 2015. године, када је изведен напад на украјински електроенергетски систем, у стручној литератури широко препознат као први јавно познат успешан сајбер напад који је изазвао нестанак електричне енергије у реалном свету.[787] Према истраживањима ESET-а и америчким анализама индустријске безбедности, напад је укључивао злоупотребу BlackEnergy алата, постављање деструктивне компоненте KillDisk и циљање дистрибутивних електроенергетских компанија, што је довело до вишечасовних прекида у снабдевању електричном енергијом.[788] Већ следеће године уследио је још напреднији напад на електроенергетску мрежу у Кијеву, повезан са злонамерним софтвером Industroyer/CrashOverride, који је по својој природи представљао далеко софистицираније инструмент за нападе на индустријске контролне системе.[789] Напад из 2016. године имао је посебну тежину зато што је показао да руски актери не циљају само канцеларијске и административне системе, већ и сам оперативни слој критичне инфраструктуре.[790] Коначно, 2017. године уследио је напад NotPetya, који је започео као напад на Украјину, укључујући финансијске, енергетске и владине системе, али је убрзо прерастао у глобалну деструктивну кампању са огромним међународним економским

[781] Google Threat Analysis Group, *Fog of War,* 4–6; Microsoft, *Defending Ukraine: Early Lessons from the Cyber War* (June 2022), 8, 15.
[782] Microsoft, *An Overview of Russia's Cyberattack Activity in Ukraine*, 1; Google Threat Analysis Group, *Fog of War,* 4–6.
[783] ESET, *ESET Threat Report T1 2022*, 6.
[784] ESET, "ESET Finds Connection Between Cyber Espionage and Electricity Outage in Ukraine," 2016.
[785] ESET, "ESET Finds Connection Between Cyber Espionage and Electricity Outage in Ukraine," 2016; ESET, *ESET Threat Report T1 2022*, 6.
[786] ESET, *ESET Threat Report T1 2022*, 6.
[787] Cybersecurity and Infrastructure Security Agency, "Cyber-Attack Against Ukrainian Critical Infrastructure," IR-ALERT-H-16-056-01, updated July 20, 2021; ESET, *ESET Threat Report T1 2022*, 6.
[788] ESET, "ESET Finds Connection Between Cyber Espionage and Electricity Outage in Ukraine," 2016; Cybersecurity and Infrastructure Security Agency, "Cyber-Attack Against Ukrainian Critical Infrastructure," IR-ALERT-H-16-056-01, updated July 20, 2021.
[789] Cybersecurity and Infrastructure Security Agency, "CRASHOVERRIDE Malware," ICS-ALERT-17-206-01, updated July 20, 2021; ESET, "Industroyer: Biggest Malware Threat to Critical Infrastructure Since Stuxnet," 2017.
[790] Cybersecurity and Infrastructure Security Agency, "CRASHOVERRIDE Malware," ICS-ALERT-17-206-01, updated July 20, 2021; ESET, *ESET Threat Report T1 2022*, 6.

последицама.[791] Овим је постало јасно да руско деловање против Украјине није више ограничено на локални или регионални ниво, већ да сајбер операције усмерене против једне државе могу имати транснационалне ефекте и глобалне последице.[792]

Са аналитичког становишта, период 2014–2017. има двоструки значај. С једне стране, показао је да је Украјина била својеврсни полигон за испитивање руских метода напада на критичну инфраструктуру, укључујући електроенергетски сектор, медије, владине системе и финансијске токове.[793] С друге стране, тај период је открио да циљ руских операција није био само тренутни технички ефекат, већ и демонстрација способности, психолошки притисак, нарушавање поверења у институције и сигнализирање да је дигитална зависност државе истовремено и извор њене рањивости.[794] Управо због тога је еволуција од шпијунских кампања, преко напада на електромрежу, до глобално деструктивног NotPetya инцидента важна не само као хронологија, већ и као образац стратешког учења и постепене ескалације.[795]

Прединвазиона 2021. година и почетак 2022. представљају нову фазу у којој сајбер операције постају још повезаније са непосредним војним планирањем. Google Threat Analysis Group је утврдио да су руски државно подржани актери појачали сајбер операције уочи саме инвазије 2021. године, а да је 2022. забележено повећање од око 250% руског фишинг циљања корисника у Украјини у односу на 2020. годину.[796] Microsoft је, са друге стране, у свом извештају из априла 2022. указао да је сајбер компонента руског напада на Украјину била „деструктивна и непрекидна“, као и да су најмање шест руских APT актера истовремено спроводили деструктивне, шпијунске или комбиноване операције.[797] Дан уочи отворене инвазије, руски актери су покренули деструктивне сајбер нападе на стотине система у украјинским владиним, IT, енергетским и финансијским организацијама, чиме је јасно показано да дигитални напад треба да омогући, убрза или појача кинетички напад.[798] Управо у овом периоду постаје јасно да руска страна сајбер операције не третира као независан фронт, већ као инструмент за деградацију украјинских командних, безбедносних, административних и цивилних капацитета у условима непосредне инвазије.[799]

[791] The White House, “Statement from the Press Secretary,” February 15, 2018; U.S. Department of Justice, “Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace,” October 19, 2020; ESET, *ESET Threat Report T1 2022*, 6.
[792] The White House, “Statement from the Press Secretary,” February 15, 2018; U.S. Department of Justice, “Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace,” October 19, 2020.
[793] ESET, *ESET Threat Report T1 2022* (2022), 6; Cybersecurity and Infrastructure Security Agency, “Cyber-Attack Against Ukrainian Critical Infrastructure,” IR-ALERT-H-16-056-01, updated July 20, 2021; The White House, “Statement from the Press Secretary,” February 15, 2018.
[794] Microsoft, *An Overview of Russia’s Cyberattack Activity in Ukraine: Special Report: Ukraine* (April 27, 2022), 1, 8–11; Google Threat Analysis Group, *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape* (2022), 4–6.
[795] ESET, *ESET Threat Report T1 2022* (2022), 6; Microsoft, *Defending Ukraine: Early Lessons from the Cyber War* (June 2022), 2, 8; The White House, “Statement from the Press Secretary,” February 15, 2018.
[796] Google Threat Analysis Group, *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape* (2022), 4, 7.
[797] Microsoft, *An Overview of Russia’s Cyberattack Activity in Ukraine: Special Report: Ukraine* (April 27, 2022), 1, 8.
[798] Ибид, 1, 6.
[799] Ибид, 8–11; Google Threat Analysis Group, *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape* (2022), 4–6.

Један од најзначајнијих напада на критичну инфраструктуру на самом почетку инвазије био је напад на сателитску мрежу KA-SAT компаније Viasat, изведен непосредно пре уласка руских снага у Украјину.[800] Савет Европске уније је у мају 2022. званично саопштио да је напад, усмерен против сателитске мреже, изведен око сат времена пре руске инвазије и да је имао значајан ефекат, изазвавши прекиде комуникација у Украјини, али и у више држава чланица ЕУ.[801] Google је додатно указао да је овај напад представљао изузетак у односу на иначе ограничен домет руског сајбер деловања 2022. године, јер је његов ефекат био осетан и ван Украјине, укључујући поремећаје у раду хиљада ветроелектрана у Европи.[802] Значај напада на Viasat је у томе што је показао да критична инфраструктура у савременом рату више није ограничена на класичне домаће мреже, већ обухвата и комерцијалне сателитске комуникације на које се ослањају државни, војни и цивилни системи.[803] Овај случај је уједно показао колико су у савременом сукобу границе између војних и цивилних комуникационих система замагљене, а самим тим и колико напади на „комерцијалне“ платформе могу да имају стратешке последице.[804]

Током првих месеци 2022. напади на критичну инфраструктуру били су концентрисани на телекомуникације и енергетику. Крајем марта 2022. украјински званичници су саопштили да је Ukrtelecom био изложен снажном сајбер нападу који је пореметио услуге, мада је напад одбијен и услуге су постепено обновљене.[805] Још опаснији био је покушај саботаже украјинске електроенергетске мреже у априлу 2022. године, када су украјинске власти и истраживачи ESET-а саопштили да су осујетили напад малвером Industroyer2, модернизованом варијантом алата повезаног са нападом на Кијев 2016. године.[806] Према доступним подацима, нападачи су најпре компромитовали мрежу енергетске компаније, а затим планирали искључење подстаница и брисање података како би отежали обнову снабдевања.[807] Овај случај показује да је руска страна и током пуног рата задржала способност, а очигледно и намеру, да изведе оперативне нападе на индустријске системе и да изазове материјалне последице по снабдевање електричном енергијом.[808] Google је додатно оценио да је у прва четири месеца 2022.године у Украјини забележено више деструктивних сајбер напада него у претходних осам година заједно, што сведочи о драматичној ескалацији интензитета дигиталног фронта.[809]

Ипак, један од најзанимљивијих аналитичких закључака овог периода јесте да руски сајбер напади, иако интензивни, нису произвели ону врсту стратешког слома украјинске државе коју су

[800] Council of the European Union, “Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union,” May 10, 2022.
[801] Council of the European Union, “Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union,” May 10, 2022.
[802] Google Threat Analysis Group, *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape* (2022), 8; CyberPeace Institute, “Case Study: Viasat Attack.”
[803] Council of the European Union, “Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union,” May 10, 2022; CyberPeace Institute, “Case Study: Viasat Attack.”
[804] CyberPeace Institute, “Case Study: Viasat Attack”; Microsoft, *An Overview of Russia’s Cyberattack Activity in Ukraine: Special Report: Ukraine* (April 27, 2022), 6.
[805] Reuters, “Ukrainian telecom company’s internet service disrupted by ‘powerful’ cyberattack,” March 28, 2022.
[806] Reuters, “Ukraine says it thwarted Russian cyberattack on electricity grid,” April 12, 2022; ESET, “Industroyer2: Industroyer reloaded,” April 12, 2022.
[807] Reuters, “Ukraine says it thwarted Russian cyberattack on electricity grid,” April 12, 2022; ESET, “Industroyer2: Industroyer reloaded,” April 12, 2022.
[808] Reuters, “Ukraine says it thwarted Russian cyberattack on electricity grid,” April 12, 2022; ESET, *ESET Threat Report T1 2022* (2022), 6.
[809] Google Threat Analysis Group, *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape* (2022), 8.

многи очекивали уочи инвазије.[810] Разлози за то су вишеструки. Microsoft је указао да је брзо пребацивање државних података и операција у cloud окружења, у сарадњи са украјинским органима, значајно ограничило оперативни ефекат руских сајбер и кинетичких напада на државне центре података и локалне мреже.[811] Google је оценио и да је након почетног таласа 2022. године темпо деструктивних напада успорио и постао мање координисан, те да је руска страна често морала да балансира између потребе за дугорочним приступом мрежама, прикупљања обавештајних података и жеље да се постигне деструктиван ефекат.[812] То упућује на важан закључак: у украјинском случају сајбер операције нису биле пресудно средство за добијање рата, али су представљале значајан чинилац укупног притиска на државу, посебно када су биле временски координисане са ракетним и дронским нападима на исте или међусобно повезане секторе.[813]

Током 2023. године уочљива је тактичка адаптација руског деловања. Према Microsoft-у, руски актери су између марта и октобра 2023. показали већу флексибилност, уз јачи фокус на сајбер шпијунажу, логистичке линије снабдевања, пољопривредни сектор и цивилне инфраструктурне мете повезане са функционисањем државе и ратне економије.[814] Истовремено, CERT-UA је у септембру 2023. саопштио да је осујетио циљани напад групе APT28 на објекат критичне енергетске инфраструктуре у Украјини, при чему није дошло до продора и саботаже.[815] То је важан показатељ промене баланса: руски актери нису одустали од критичне инфраструктуре као мете, али је украјинска одбрана до те мере ојачала да су неке од најопаснијих операција биле пресретнуте пре изазивања материјалне штете.[816] У овој фази се зато руска тактика све мање ослања на спектакуларне, једнократне деструктивне догађаје, а све више на дубоко продирање, обавештајно позиционирање и припрему услова за каснију деструкцију или експлоатацију.[817]

Најупечатљивији пример напада на критичну инфраструктуру у другој половини 2023. био је напад на Kyivstar, највећег украјинског мобилног оператера. Reuters је тај догађај описао као највећи сајбер напад на Украјину од почетка рата, при чему су услуге оператера биле прекинуте, IT инфраструктура тешко оштећена, а милиони корисника привремено лишени комуникационих услуга.[818] Посебну тежину овом нападу даје чињеница да је он утицао и на системе за ваздушну узбуну у појединим деловима Кијева, као и на банкомате и друге услуге које су се ослањале на мобилну повезаност.[819] Накнадно је Reuters, позивајући се на шефа украјинске сајбер-шпијунаже, објавио да су руски хакери месецима били унутар система Kyivstar-a и да је највероватнији

[810] Microsoft, *Defending Ukraine: Early Lessons from the Cyber War* (June 2022), 2–5; Google Threat Analysis Group, *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape* (2022), 8–9.
[811] Microsoft, *Defending Ukraine: Early Lessons from the Cyber War* (June 2022), 12–14.
[812] Google Threat Analysis Group, *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape* (2022), 8–9.
[813] Microsoft, *An Overview of Russia's Cyberattack Activity in Ukraine: Special Report: Ukraine* (April 27, 2022), 1, 6, 8–11; Microsoft, *Defending Ukraine: Early Lessons from the Cyber War* (June 2022), 8, 15.
[814] Microsoft Threat Intelligence, "Russian threat actors dig in, prepare to seize on war fatigue," December 7, 2023.
[815] State Service of Special Communications and Information Protection of Ukraine, "Russian hackers attacked users in Ukraine and Poland…" December 28, 2023; State Service of Special Communications and Information Protection of Ukraine, *Russian Cyber Operations: APT Activity Report #3, H2 2023* (2024).
[816] Microsoft Threat Intelligence, "Russian threat actors dig in, prepare to seize on war fatigue," December 7, 2023; State Service of Special Communications and Information Protection of Ukraine, *Russian Cyber Operations: APT Activity Report #3, H2 2023* (2024).
[817] Microsoft Threat Intelligence, "Russian threat actors dig in, prepare to seize on war fatigue," December 7, 2023
[818] Reuters, "Ukraine's top mobile operator hit by biggest cyberattack of war," December 12, 2023
[819] Reuters, "Ukraine's top mobile operator hit by biggest cyberattack of war," December 12, 2023; Reuters, "Russian hackers were inside Ukraine telecoms giant for months, cyber spy chief says," January 4, 2024.

извршилац била група Sandworm, повезана са руском војном обавештајном службом.[820] Иако је оператор до 20. децембра 2023. обновио све услуге, овај случај је показао да телекомуникациона инфраструктура у ратним условима није само цивилна услуга, већ један од кључних елемената националне отпорности.[821] Напад на Kyivstar је зато имао снажан стратешки и симболички ефекат: он је показао да чак и без уништења електромреже или железнице напад на телекомуникациону кичму може озбиљно пореметити свакодневни живот, кретање информација и осећај безбедности становништва.[822]

Година 2024. потврдила је да руска стратегија напада на украјинску критичну инфраструктуру не слаби, већ се прилагођава. У јануару 2024. више државних и квазијавних система пријавило је сајбер инциденте, укључујући Naftogaz, чији је један дата центар погођен „великим сајбер нападом", затим Ukrposhta, Ukrtransbezpeka, као и железничке и друге сервисе.[823] Средином 2024. јавност је сазнала и за напад малвером FrostyGoop на комунално предузеће за даљинско грејање у Украјини, где је манипулација индустријским контролерима изазвала прекид испоруке грејања за стотине зграда током зимског периода.[824] Још значајније, у интервјуу објављеном у фебруару 2025. шеф украјинске службе за специјалне везе и заштиту информација изјавио је да су током марта 2024. откривене припреме групе UAC-0002/Sandworm за нападе на приближно двадесет енергетских, водоводних и топланских предузећа у десет украјинских региона, и то путем компромитованих ланаца снабдевања кроз фирме које развијају специјализовани индустријски софтвер.[825] Он је нагласио и да је временско поклапање ових припрема са руским ракетним нападима на инфраструктуру у пролеће 2024. снажна индиција да је сајбер компонента требало да појача ефекат физичких удара.[826] Крајем 2024. уследио је и масовни напад на државне регистре Министарства правде Украјине, који је привремено суспендовао низ услуга и који је украјинска влада јавно окарактерисала као руски напад на критично важну инфраструктуру државе.[827] Ови догађаји потврђују да руски приступ све више тежи комбинацији снабдевачких напада, оперативно-технолошких продора и удара на административно-правне системе без којих модерна држава не може несметано да функционише.[828]

Развој догађаја током 2025. године указује на даљу трансформацију руске тактике. Украјинска државна служба за специјалне везе саопштила је да је број руских сајбер операција у другој половини 2024. порастао за 48% у односу на прву половину године, а украјински и савезнички извори су почетком 2025. истицали да Русија све више делује прикривеније, са нагласком на

[820] Reuters, "Russian hackers were inside Ukraine telecoms giant for months, cyber spy chief says," January 4, 2024; Reuters, "Hackers linked to Russian spy agency claim cyberattack on Ukraine mobile operator," December 13, 2023.
[821] Reuters, "Ukraine's Kyivstar says it is fully operational after cyber attack," December 20, 2023.
[822] Reuters, "Ukraine's top mobile operator hit by biggest cyberattack of war," December 12, 2023; Reuters, "Russian hackers were inside Ukraine telecoms giant for months, cyber spy chief says," January 4, 2024.
[823] Reuters, "Several Ukrainian state-run bodies report cyber attacks," January 25, 2024.
[824] MITRE ATT&CK, "FrostyGoop Incident, Campaign C0041," March 5, 2025; Dragos, "How to Protect Against FrostyGoop: ICS Malware Targeting Operational Technology," July 23, 2024.
[825] Information System Authority of Estonia, "SSSCIP chief: Russia operates more covertly in cyberspace," February 17, 2025.
[826] Information System Authority of Estonia, "SSSCIP chief: Russia operates more covertly in cyberspace," February 17, 2025.
[827] Reuters, "Russia conducted mass cyberattack on Ukraine's state registries, deputy PM says," December 19, 2024; Reuters, "Ukraine says Russian cyberattack hits state registries, no data lost," December 20, 2024.
[828] Reuters, "Russia conducted mass cyberattack on Ukraine's state registries, deputy PM says," December 19, 2024; Information System Authority of Estonia, "SSSCIP chief: Russia operates more covertly in cyberspace," February 17, 2025.

сајбер обавештајне операције и мете повезане са ратом и политиком.[829] Ипак, то не значи да је деструктивна димензија нестала. У марту 2025. Ukrzaliznytsia, украјинска државна железница и највећи носилац теретног саобраћаја у земљи, била је изложена великом циљаном сајбер нападу који је оборио систем онлајн продаје карата и друге IT услуге, што је изазвало дуге редове на станицама и пореметило функционисање једног од кључних логистичких система у држави захваћеној ратом.[830] Reuters је потом известио да је и две недеље након напада обновљена тек око половина IT услуга, што показује да ефекат оваквих напада није само тренутни прекид, већ и продужена операционализациона штета.[831] Напад на железницу имао је посебну тежину јер украјински ваздушни саобраћај у ратним условима практично не функционише, па железница представља централну инфраструктуру за превоз цивила, војних материјала и робе.[832] Стога се може рећи да је у 2025. години руски сајбер притисак на критичну инфраструктуру ушао у фазу у којој су логистичка уска грла, комуникациона чворишта и системи дуготрајног функционисања државе постали подједнако важне мете као и енергетика.[833]

До марта 2026. године у јавно доступним изворима не појављује се нови, глобално препознатљив инцидент исте симболичке тежине као напади на електромрежу 2015/2016. или Kyivstar 2023. године, али то не значи да је претња ослабила. Напротив, украјински и савезнички извори указују да је руска страна све више прешла на тиши, упорнији и обавештајно усмеренији модел деловања, уз истовремено задржавање капацитета за деструктивне нападе на критичну инфраструктуру када се за то укаже погодан тренутак.[834] Због тога је најтачније оценити да је сајбер део руско-украјинског сукоба ушао у фазу перманентног притиска: мање спектакуларног него у првим месецима инвазије, али не мање опасног, јер се ослања на дубоко продирање, припрему терена, компромитовање ланаца снабдевања и синхронизацију са физичким нападима на инфраструктуру.[835] Управо ту лежи и главна поука украјинског случаја а то је да у савременом рату напад на критичну инфраструктуру не мора увек да изгледа као тренутно гашење електромреже или пад целе државне мреже; он може имати облик постепеног трошења отпорности, ремећења јавних услуга, нарушавања поверења грађана, исцрпљивања ресурса за одбрану и стварања сталне неизвесности.[836] Из научне перспективе, то значи да руско-украјински сукоб у сајбер простору треба посматрати не као споредни дигитални додатак конвенционалном

[829] State Service of Special Communications and Information Protection of Ukraine, "Russian Cyber Operations: Attack Automation, Espionage against Defense Sector and New Tactics Analysis for the Second Half of 2024," April 29, 2025; Information System Authority of Estonia, "SSSCIP chief: Russia operates more covertly in cyberspace," February 17, 2025.
[830] Reuters, "Ukraine sees Russian effort to sow chaos as cyberattack hits rail service," March 24, 2025; Reuters, "Ukraine railways say Sunday's cyber attack hit its online freight services," March 25, 2025.
[831] Reuters, "Ukraine's railways restore half of IT services hit by cyber attack so far," April 9, 2025.
[832] Reuters, "Ukraine sees Russian effort to sow chaos as cyberattack hits rail service," March 24, 2025; Reuters, "Ukraine railways say Sunday's cyber attack hit its online freight services," March 25, 2025.
[833] Reuters, "Ukraine's railways restore half of IT services hit by cyber attack so far," April 9, 2025; State Service of Special Communications and Information Protection of Ukraine, "Russian Cyber Operations: Attack Automation, Espionage against Defense Sector and New Tactics Analysis for the Second Half of 2024," April 29, 2025.
[834] Information System Authority of Estonia, "SSSCIP chief: Russia operates more covertly in cyberspace," February 17, 2025; State Service of Special Communications and Information Protection of Ukraine, "Russian Cyber Operations: Attack Automation, Espionage against Defense Sector and New Tactics Analysis for the Second Half of 2024," April 29, 2025.
[835] Исто.
[836] Reuters, "Ukraine's railways restore half of IT services hit by cyber attack so far," April 9, 2025; Reuters, "Ukraine says Russian cyberattack hits state registries, no data lost," December 20, 2024; Information System Authority of Estonia, "SSSCIP chief: Russia operates more covertly in cyberspace," February 17, 2025.

рату, већ као интегрисани облик стратегијског деловања усмереног на државне функције, критичну инфраструктуру и друштвену отпорност у целини.[837]

Иако је тежиште сајбер сукоба у руско-украјинском рату несумњиво било на руским операцијама усмереним против Украјине, јавно доступни подаци показују да сајбер деловање није било једносмерно. Постоје индиције да су украјинске, односно проукрајинске структуре, подстицале или изводиле операције у сајбер простору усмерене против руских циљева. Тако је Reuters у јануару 2024. известио да су хакери повезани са главном украјинском војном обавештајном службом продрли у системе једног московског интернет провајдера, при чему је ова операција у медијима представљена као одговор на напад на украјинског оператера Kyivstar.[838] Овај случај је важан не само зато што показује способност украјинске стране да таргетира руске циље, већ и зато што упућује на постојање логике реципрочног дигиталног одговора у условима ширег оружаног сукоба. У том смислу, сајбер простор се показује као арена у којој се, поред офанзиве и одбране, развија и образац симетричног или асиметричног узвраћања.

У јулу 2025. године забележен је и велики сајбер напад на руску авио-компанију Аерофлот, после кога су отказане десетине летова, а Reuters је пренео да су две проукрајинске групе јавно преузеле одговорност за напад, док је Кремљ ситуацију оценио као алармантну.[839] Напад на Аерофлот имао је посебну симболичку тежину, јер је био усмерен на једну од најпрепознатљивијих руских транспортних и државно значајних компанија, што упућује на настојање да се произведе не само оперативна, већ и политичко-психолошка штета. Овакви напади показују да циљ није искључиво војна инфраструктура у ужем смислу, већ и системи који носе економску, логистичку и симболичку функцију државе.

Током 2024. године забележени су и напади на поједина руска министарства, укључујући и сајбер инцидент усмерен против Министарства спољних послова Русије у октобру 2024. године, што додатно показује да је и руска држава била изложена дигиталном деловању противничке стране.[840] Ови случајеви су важни и зато што указују на ширење листе мета: од телекомуникационих и транспортних система до државних институција и органа спољнополитичког апарата. Украјинске и/или проукрајинске активности у сајбер простору, иако обимом и ресурсима неупоредиве са руским државним операцијама, представљале су реалну компоненту дигиталне конфронтације. Сајбер димензија рата не може се свести на једноставан модел једностраног руског деловања, већ мора да се посматра као динамичан простор међусобних удара, одговора, демонстрације способности и политичких реакција. Са становишта анализе савремених конфликата, ова околност је значајна јер показује да и страна која се налази у претежно одбрамбеном положају може да настоји да у дигиталном домену наметне сопствене циљеве, наруши осећај сигурности противника и покаже да поседује способности за узвратно деловање. Због тога ове операције треба разумети као део шире логике ратне комуникације и стратегијског утицаја, а не само као техничке инциденте ограниченог домета.

[837] State Service of Special Communications and Information Protection of Ukraine, "Russian Cyber Operations: Attack Automation, Espionage against Defense Sector and New Tactics Analysis for the Second Half of 2024," April 29, 2025; Information System Authority of Estonia, "SSSCIP chief: Russia operates more covertly in cyberspace," February 17, 2025.
[838] Reuters, "Hackers Hit Moscow Internet Provider in Response to Kyivstar Cyber Attack - Source," January 9, 2024
[839] Reuters, "Pro-Ukrainian Hackers Claim Massive Cyberattack on Russia's Aeroflot," July 28, 2025; Reuters, "Russia Opens Criminal Case over Aeroflot Cyberattack," July 28, 2025
[840] Reuters, "Russia Says 'Unprecedented' Cyber Attack Hits Foreign Ministry amid BRICS Summit," October 23, 2024.

Ипак, ове случајеве треба тумачити са великим опрезом. У сајбер простору јавно доступна атрибуција често остаје непотпуна, а разлика између техничке индиције, политичке процене и правно поузданог утврђивања одговорности није увек јасно успостављена.[841] То значи да чињеница да је одређена операција у медијима или обавештајним круговима повезана са неком државом или групом не представља аутоматски и довољан доказ у правном смислу. У пракси се често дешава да се технички трагови, инфраструктура напада, избор мете и временско поклапање са политичким догађајима тумаче као снажне индиције, али без потпуно јасног ланца доказивања. Додатни проблем представља то што актери у сајбер простору свесно користе посреднике, туђу инфраструктуру, компромитоване системе и групе са нејасним статусом како би замаглили порекло операције и отежали приписивање одговорности. Због тога у великом броју случајева остаје отворено питање да ли иза напада стоји држава, државно група спонзорисана и подржана од стране државе, парадржавни актер, идеолошки мотивисана хакерска заједница или комбинација више различитих субјеката. Управо је из тог разлога, у академској, безбедносној, политиколошкој и правној анализи неопходно је правити јасну разлику између медијски приписане одговорности, политички вероватне одговорности и правно доказане одговорности, јер тек такво разграничење омогућава прецизно и научно утемељено тумачење сајбер операција.

[841] Jakub Spáčil, "Attribution of Cyber Operations: Technical, Legal and Political Perspectives," *International and Comparative Law Review* 24, no. 2 (2024): 150–168.

5. Концепт сајбер ратовања у Сједињеним Америчким Државама

Стратешки приступ сајбер безбедности у Сједињеним Америчким Државама развијао се упоредо са трансформацијом сајбер простора из технолошке инфраструктуре у поље националне моћи, економске стабилности, војне пројекције и геополитичког надметања. Дуже од две деценије, америчка политика у овој области полази од становишта да сајбер простор не представља само комуникационо окружење, већ простор у коме се одлучује о безбедности критичне инфраструктуре, отпорности државе, заштити тржишта, очувању технолошке предности и способности одвраћања према државним и недржавним актерима. Управо зато се стратегија сајбер безбедности Сједињених Америчких Држава не може посматрати као изолован скуп техничких мера, већ као интегрални део шире националне безбедносне, одбрамбене, спољнополитичке и економске стратегије. У том смислу, САД се не појављују само као држава која реагује на сајбер претње, већ као држава која настоји да обликује међународне норме, да одреди стандарде понашања у сајбер простору и да сопствене технолошке, војне и институционалне капацитете претвори у инструмент глобалне предности.[842]

Кључна доктринарна полазишта савремене америчке сајбер политике јасно су формулисана још у Међународној стратегији за сајбер простор у периоду тадашњег председника Барака Обаме из маја 2011. године. У том документу Сједињене Државе су изричито потврдиле да државе имају инхерентно право на самоодбрану и у сајбер простору, те да одређени непријатељски акти извршени сајбер средствима могу да активирају право на самоодбрану, укључујући и обавезе према савезницима. Истовремено, Вашингтон је нагласио да ће, када то околности захтевају, на непријатељске акте у сајбер простору, одговарати као и на друге претње по државу, користећи дипломатска, информативна, војна и економска средства, у складу са важећим међународним правом. Ово је био изузетно важан корак у нормативном уобличавању америчке позиције, јер је сајбер напад престао да буде схваћен искључиво као технички инцидент, а почео да се третира као потенцијално стратешки догађај који може произвести последице упоредиве са последицама традиционалних облика угрожавања безбедности.[843]

Иако се у ранијој литератури често истицало да су САД прве међу великим силама систематски почеле да третирају сајбер простор као засебну сферу стратешког деловања, у последњих неколико година овај приступ је додатно институционално и доктринарно ојачан. Национална одбрамбена стратегија из 2022. године смешта сајбер и космички простор у само средиште савремених ризика ескалације, указујући да су управо у тим доменима границе између мира, кризе и оружаног сукоба најнејасније. Истовремено, Министарство одбране сајбер способности посматра као суштински елемент „интегрисаног одвраћања“, односно као саставни део способности САД да координисано делују кроз све ратне домене, уз употребу свих инструмената националне моћи и у блиској сарадњи са савезницима. То значи да у америчком стратешком мишљењу сајбер више није споредна или помоћна категорија, већ један од темељних механизама одбране државе, одвраћања стратешких напада и очувања слободе маневра оружаних снага.[844]

---

[842] The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011), 3–5; Vladimir Lović, „Sajber prostor kao novo bojno polje: međunarodni odnosi, geopolitika i bezbednost u digitalnom dobu,” *Megatrend revija* 22, br. 1 (2025): 215–230.

[843] The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011), 10, 14; Ljubomir Tintor, „Međunarodna odgovornost države u digitalnom (sajber) prostoru,” u *Srpski godišnjak za međunarodno pravo* (Beograd: Srpsko udruženje za međunarodno pravo, 2023).

[844] Department of Defense, *2022 National Defense Strategy of the United States of America, Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review* (Washington, DC: Department of Defense, 2022), 2, 8; Department of

5.1. Стратегија сајбер безбедности САД

Посматрано у периоду последњих пет година, односно од 2021. до маја 2026. године, развој америчке сајбер стратегије показује јасан континуитет у погледу основних циљева, али и видљиве промене у погледу инструмената, правне регулације и односа између државе и приватног сектора. Година 2021. представља важну преломницу јер је после инцидента *SolarWinds* федерална власт убрзала прелазак са реактивне на проактивну сајбер одбрану. Извршна наредба 14028 о унапређењу сајбер безбедности нације и каснија буџетска и управљачка документа поставили су темеље за свеобухватну модернизацију федералних система, увођење напредног откривања и реаговања на крајњим тачкама, као и прелазак ка моделу *zero trust* архитектуре.[845]

У том контексту, меморандум OMB *M-22-09* из јануара 2022. године имао је изузетан значај, јер је федералним агенцијама наметнуо конкретне стандарде и рокове за усвајање *zero trust* принципа до краја фискалне 2024. године. Овим документом америчка администрација није само технички ажурирала приступ заштити мрежи, већ је прихватила дубљу доктринарну промену а то је да се претња не може више посматрати као нешто што нужно долази споља, већ као могућност која може настати било где унутар дигиталног екосистема. Зато су идентитет, уређаји, мреже, апликације и подаци третирани као повезани стубови одбране, а федерална држава је настојала да сама постане модел отпорности за шири систем критичне инфраструктуре. Истовремено, Национална одбрамбена стратегија из 2022. године изричито повезује сајбер отпорност са модерном енкрипцијом и *zero trust* архитектуром, што показује да техничка заштита у америчком приступу није одвојена од стратегије одвраћања, већ представља њен саставни део.[846]

Најпотпуније уобличење америчке сајбер стратегије у новијем периоду представља Национална стратегија сајбер безбедности из марта 2023. године. Стратегија почива на пет стубова[847]:

1. одбрани критичне инфраструктуре,
2. ремећењу и разбијању актера претњи,
3. обликовању тржишних сила ради подстицања безбедности и отпорности,
4. улагању у отпорну будућност и
5. јачању међународних партнерстава.

Најзначајнији концептуални допринос Стратегије огледа се у идеји „пребацивања терета“ одговорности са појединачних корисника и мањих организација на актере који су најспособнији да смање ризик — пре свега на велике операторе критичне инфраструктуре, пружаоце услуга у

Defense, *2023 DoD Cyber Strategy Summary* (Washington, DC: Department of Defense, September 2023), 1–3; Veljko Blagojević, „Strategija nacionalne bezbednosti SAD iz 2025: kontinuitet i promene,” *Međunarodna politika* 77, br. 1196 (2026): 79–103.

[845] Joseph R. Biden Jr., Executive Order 14028, “Improving the Nation’s Cybersecurity,” May 12, 2021, *Federal Register* 86, no. 93 (May 17, 2021): 26633–26647; Office of Management and Budget, *M-21-31: Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (Washington, DC: Executive Office of the President, August 27, 2021); Office of Management and Budget, *M-22-01: Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (Washington, DC: Executive Office of the President, October 8, 2021).

[846] Office of Management and Budget, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Washington, DC: Executive Office of the President, January 26, 2022).

[847] The White House, *National Cybersecurity Strategy* (Washington, DC: The White House, March 2023), 1–2, 13–23.

облаку, произвођаче софтвера и друге системски значајне субјекте. Другим речима, Бајденова администрација је сајбер безбедност све отвореније посматрала као питање јавне политике, регулације и корекције тржишних неуспеха.[848]

Посебно је важно нагласити да се стратегија сајбер безбедности Сједињених Америчких Држава не исцрпљује у једном документу, већ функционише као вишеслојни систем стратешких, имплементационих, буџетских и институционалних аката. У том систему Национална стратегија сајбер безбедности из 2023. године представља кровни цивилни стратешки документ, јер формулише пет носећих стубова деловања и двадесет седам стратешких циљева који треба да усмере целокупну федералну политику у овој области. Њен значај није само у идентификовању претњи, већ у томе што уводи јасну логику државног деловања: одбрана критичне инфраструктуре, разбијање и ремећење актера претњи, обликовање тржишних подстицаја, изградња дугорочне отпорности и јачање међународне сарадње постају међусобно повезани елементи јединствене стратегије. Посебну нормативну тежину и значај имају два принципа на којима се ова стратегија заснива — први је да већи и способнији актери морају носити и већи терет одговорности за безбедност дигиталног екосистема, а други да држава мора да коригује тржишне подстицаје како би безбедност постала исплативија од небезбедности. Управо због тога ова стратегија представља више од политичке декларације већ је покушај да се сајбер безбедност претвори у трајну осу јавне политике, регулаторног деловања и буџетског планирања.[849]

Да амерички приступ остаје усмерен на спроводљивост, а не само на програмска начела, најбоље показује План имплементације Националне стратегије сајбер безбедности из 2023. године, а затим и његова друга верзија из 2024. године. Прва верзија плана предвидела је више од 65 иницијатива које захтевају извршну видљивост и међуагенцијску координацију, док је друга верзија проширила овај оквир на 100 високоприоритетних иницијатива, уз одређивање носећих агенција, рокова и доприносећих субјеката за сваку појединачну меру. Оваква структура показује да стратегија сајбер безбедности САД није конципирана као општа визија, већ као систем у коме се сваки стратешки циљ преводи у конкретне управљачке и извршне кораке. Посебну улогу има Канцеларија националног директора за сајбер простор, која координише спровођење плана, прати напредак и извештава председника и Конгрес, док Канцеларија за управљање и буџет обезбеђује да буџетски захтеви агенција буду усклађени са стратешким приоритетима. Ово је важан показатељ да је америчка стратегија сајбер безбедности снажно институционализована. Њено спровођење није препуштено појединачним органима без центра координације, већ се води кроз јасно постављену вертикалу стратешког управљања.[850] У истом правцу иду и буџетске смернице OMB-а и Канцеларије националног директора за сајбер простор из 2024. године, које од федералних агенција захтевају да инвестиције у сајбер безбедност вежу за мерљиве резултате, показатеље учинка и вишегодишње планирање, чиме се стратегија непосредно повезује са управљањем ресурсима.[851]

Један од најважнијих инструмената спровођења америчке стратегије јесте и *zero trust* приступ, који је федералној администрацији нормативно наметнут меморандумом OMB *M-22-09*. Тим документом федералним агенцијама су постављени конкретни стандарди и циљеви које су морале

[848] The White House, *National Cybersecurity Strategy* (Washington, DC: The White House, March 2023), 1–2, 13–23.
[849] The White House, *National Cybersecurity Strategy* (Washington, DC: The White House, March 2023), 2–6.
[850] The White House, *National Cybersecurity Strategy Implementation Plan, Version 2* (Washington, DC: The White House, May 2024).
[851] Office of Management and Budget and Office of the National Cyber Director, *M-24-14: Administration Cybersecurity Priorities for the FY 2026 Budget* (Washington, DC: Executive Office of the President, July 10, 2024).

да достигну до краја фискалне 2024. године, што сведочи о високом степену оперативне разраде стратешких приоритета.[852]

Касније смернице о спровођењу FISMA обавеза из 2023. године додатно су повезале Националну стратегију сајбер безбедности са модернизацијом федералних система и изградњом колективне одбране федералног предузећа, чиме је створена веза између стратешког документа и свакодневног управљања сајбер ризицима у државној управи.[853]
Истовремено, Агенција за сајбер безбедност и безбедност инфраструктуре делује као кључни оперативни носилац у цивилном домену, нарочито у погледу заштите федералних цивилних мрежа, сарадње са операторима критичне инфраструктуре и промовисања модела *secure by design,* док Министарство правде и Федерални истражни биро имају централну улогу у истрагама, кривичном гоњењу и разбијању актера претњи.[8547]

У војно-безбедносној сфери, Министарство одбране своју сајбер стратегију из 2023. године отворено везује за Националну стратегију сајбер безбедности, чиме се потврђује да амерички систем не познаје потпуно одвојене цивилне и војне стратегије, већ међусобно усклађене документе различитог домашаја.[855]

Зато је за тему стратегије сајбер безбедности САД пресудно уочити да се њена суштина не налази само у реторичком истицању опасности, већ у повезивању стратешких циљева, институционалних носилаца, правних инструмената, буџетских механизама и мерљивих корака примене у један релативно кохерентан систем националног управљања сајбер ризицима.[856]

Да ова стратегија није остала на нивоу декларације показује *План имплементације* Националне стратегије сајбер безбедности из јула 2023. године, који је предвидео више од 65 иницијатива, расподелио носиоце послова међу федералним органима и нагласио да је реч о „живом документу“ који захтева континуирано ажурирање.[857]

Истовремено, Министарство одбране је 2023. године усвојило нову сајбер стратегију која операционализује приоритете одбране отаџбине, одбране унапређеним деловањем (*defend forward*), припреме за вођење и добијање ратова, као и заштите сајбер домена са савезницима и партнерима. Посебно је значајно што DoD у овој стратегији наглашава „упорно кампањско деловање“ испод прага оружаног сукоба. Ово потврђује да америчка доктрина не полази од идеје да се сајбер операције активирају само током оружаног сукоба, већ и да се у миру, кризама и тзв. сивој зони константно обликује оперативно окружење, прикупљају увиди, ремете противничке припреме и јача колективна отпорност са савезницима.[858]

---

[852] Office of Management and Budget, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Washington, DC: Executive Office of the President, January 26, 2022).
[853] Office of Management and Budget, *M-24-04: Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements* (Washington, DC: Executive Office of the President, December 4, 2023).
[854] Cybersecurity and Infrastructure Security Agency, “CISA Announces Secure by Design Commitments from Leading Technology Providers,” May 8, 2024.
[855] Department of Defense, *2023 DoD Cyber Strategy Summary* (Washington, DC: Department of Defense, September 2023), 1–3.
[856] The White House, *National Cybersecurity Strategy* (Washington, DC: The White House, March 2023), 2–6.
[857] The White House, *National Cybersecurity Strategy Implementation Plan* (Washington, DC: The White House, July 2023), 1–2.
[858] Department of Defense, *2023 DoD Cyber Strategy Summary* (Washington, DC: Department of Defense, September 2023), 1–4, 7–8.

Током 2024. године америчка сајбер политика добија додатну нормативну и оперативну дубину. Администрација је у буџетским смерницама поново потврдила пет стубова Националне стратегије сајбер безбедности, а тежиште је задржано на модернизацији федералне државе, јачању јавно-приватне сарадње, изградњи отпорности критичне инфраструктуре и улагањима у будућност и развој. У истом правцу иду и смернице OMB-а и Канцеларије националног директора за сајбер простор, које од федералних агенција захтевају да инвестиције у сајбер безбедност вежу за мерљиве резултате, показатеље учинка и вишегодишње планирање, чиме се стратегија непосредно повезује са управљањем ресурсима.[859]

Паралелно с тим, CISA је наставила да операционализује приступ *secure by design*, настојећи да одговорност за безбедност буде уграђена у сам дизајн производа, а не да се накнадно пребацује на кориснике. У мају 2024. године CISA је објавила да је 68 водећих технолошких компанија приступило добровољној *Secure by Design* обавези, док је у јануару 2025. наведено да се број компанија које су се обавезале на мерљив напредак повећао на преко 250. У истом раздобљу, CISA је наставила и регулаторно-институционално обликовање обавезног пријављивања инцидената кроз CIRCIA оквир, што показује да Сједињене Америчке Државе истовремено развијају и техничку и правно-управну архитектуру сајбер отпорности.[860]

Потреба за овако амбициозним приступом додатно је потврђена растом претњи усмерених ка америчкој критичној инфраструктури. Годишња процена претњи америчке обавештајне заједнице из марта 2025. године наводи да Народна Република Кина остаје најактивнија и најупорнија сајбер претња америчкој влади, приватном сектору и критичној инфраструктури, при чему се посебно истичу кампања *Volt Typhoon*, усмерена на пред-позиционирање приступа критичној инфраструктури, и компромитацију рада америчке телекомуникационе инфраструктуре позната као *Salt Typhoon*. FBI и CISA су у новембру 2024. године саопштили да је кинеска операција усмерена на комерцијалну телекомуникациону инфраструктуру представљала широку и значајну кампању сајбер шпијунаже, укључујући крађу метаподатака о позивима и компромитовање приватних комуникација одређеног броја лица, превасходно из државне и политичке сфере. Због тога се савремена америчка стратегија не гради више само око опште идеје дигиталне безбедности, већ око конкретне претпоставке да противници настоје да унапред успоставе позиције унутар критичних система, како би у кризи или сукобу могли да изазову поремећаје великог обима.[861]

Промена администрације 2025. године није значила потпуни раскид са претходном сајбер политиком, али јесте донела јасан стилски и концептуални заокрет. Још 16. јануара 2025. године, пред крај Бајденовог мандата, усвојена је Извршна наредба 14144 о јачању и подстицању иновација у сајбер безбедности нације, која је градила даље на темељима Извршне наредбе 14028 и Националне стратегије сајбер безбедности. Међутим, Трамп је 6. јуна 2025. године Извршном

[859] Office of Management and Budget and Office of the National Cyber Director, *M-24-14: Administration Cybersecurity Priorities for the FY 2026 Budget* (Washington, DC: Executive Office of the President, July 10, 2024).
[860] Cybersecurity and Infrastructure Security Agency, "CISA Announces Secure by Design Commitments from Leading Technology Providers," May 8, 2024; Cybersecurity and Infrastructure Security Agency, "Building a Secure by Design Ecosystem," January 13, 2025; Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)," accessed May 5, 2026.
[861] Office of the Director of National Intelligence, *2025 Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: ODNI, March 2025), 10; Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, "Joint Statement from FBI and CISA on the People's Republic of China (PRC) Targeting of Commercial Telecommunications Infrastructure," November 13, 2024

наредбом 14306 селективно изменио ту наредбу, задржавајући део техничких и институционалних решења, али одбацујући или сужавајући поједине елементе које је његова администрација оценила као претерано оптерећујуће. Ипак, овде није реч о напуштању политике сајбер безбедности, већ о њеном репозиционирању. Задржан је део решења у области безбедности софтвера, криптографске заштите и модернизације мрежа, али је акценат политике сајбер безбедности пребачен на одбрану од страних претњи, технолошку агилност и смањење регулаторних трошкова.[862]

Овај заокрет је нарочито јасан у новој Трамповој Стратегији за Америку у сајбер простору из марта 2026. године. За разлику од ранијих, обимнијих стратегијских докумената, ова стратегија је сажетија, али врло јасно артикулише шест стубова деловања:

1. обликовање понашања противника,
2. „здраворазумску“ регулацију,
3. модернизацију и заштиту федералних мрежа,
4. обезбеђивање критичне инфраструктуре,
5. очување надмоћи у критичним и новим технологијама,
6. изградњу кадрова и капацитета.

У Стратегији се изричито наглашава употреба офанзивних и дефанзивних сајбер операција, подстицање приватног сектора да идентификује и ремети противничке мреже, убрзано усвајање *zero trust* архитектуре, постквантне криптографије и AI-решења, као и тежња да се америчка технолошка доминација учврсти кроз безбедне ланце снабдевања, заштиту дата центара и супротстављање страним технологијама које носе елементе цензуре, надзора и политичког утицаја.[863]

Посебно је значајно што Трампова стратегија из 2026. године не ограничава амерички одговор на противничке активности искључиво на сајбер домен. Напротив, у њој се јасно најављује координисано и трајно деловање читаве државе, уз сарадњу са савезницима, индустријом и академском заједницом, као и коришћење различитих инструмената моћи ради наметања трошкова противницима. У том смислу, ова стратегија сајбер безбедност отворено поставља у шири оквир државне моћи, технолошке супериорности и политике *America First*.[864]

Овакво повезивање сајбер политике, технолошке предности и геополитичког позиционирања у складу је и са ширим правцем Трампове стратегијске политике након 2025. године, у којој се национална безбедност, економска конкурентност и технолошка доминација све јасније посматрају као међусобно повезане целине.[865]

Додатну димензију новој америчкој стратегији даје и Извршна наредба од 6. марта 2026. године, усмерена на борбу против сајбер криминала, превара и предаторских махинација усмерених

---

[862] Joseph R. Biden Jr., Executive Order 14144, “Strengthening and Promoting Innovation in the Nation’s Cybersecurity,” *Federal Register* 90, no. 11 (January 17, 2025): 6755–6771; Donald J. Trump, Executive Order 14306, “Sustaining Select Efforts To Strengthen the Nation’s Cybersecurity and Amending Executive Order 13694 and Executive Order 14144,” *Federal Register* 90, no. 111 (June 11, 2025): 24723–24726; Veljko Blagojević, „Strategija nacionalne bezbednosti SAD iz 2025: kontinuitet i promene,” *Međunarodna politika* 77, br. 1196 (2026): 79–103.

[863] The White House, *President Trump’s Cyber Strategy for America* (Washington, DC: The White House, March 2026), 4–6.

[864] The White House, *President Trump’s Cyber Strategy for America* (Washington, DC: The White House, March 2026), 4.

[865] Вељко Благојевић, „Стратегија националне безбедности САД из 2025: континуитет и промене,” *Међународна политика* 77, бр. 1196 (2026): 79–103.

против америчких грађана. Том наредбом сајбер безбедност је још чвршће повезана са заштитом становништва, борбом против транснационалних криминалних организација, изградњом отпорности државних и локалних капацитета и употребом дипломатских, регулаторних, истражних, па и оперативних мера против актера који организују преваре и друге различите облике сајбер криминала. Тако се амерички стратешки оквир данас не односи више само на конфликте држава у ужем смислу, већ обухвата и криминалне екосистеме који делују уз прећутну или непосредну подршку појединих страних режима.[866]

Континуитет у америчком приступу огледа се у томе што Сједињене Државе сајбер простор и даље третирају као домен од виталног значаја за националну безбедност, одбрану домовине и очување стратешке предности.[867]

Бајденов период је посебно нагласио институционално продубљивање *zero trust* логике и модернизацију федералних система кроз прецизно постављене стандарде и рокове за њихово спровођење.[868] Трампова стратегија из 2026. године, међутим, много отвореније ставља у први план офанзивно-дефанзивну државну моћ, технолошку доминацију, дерегулацију и повезивање сајбер безбедности са широм индустријском и геополитичком конкуренцијом.[869]
Управо зато се може закључити да стратегија сајбер безбедности Сједињених Америчких Држава данас представља један од најразвијенијих примера спајања безбедносне, технолошке, правне, регулаторне и геополитичке логике у јединствен стратешки оквир.[870]

5.2 Америчка концепција сајбер операција и сајбер ратовања

Крајем деведесетих година прошлог века, у америчкој војној доктрини сајбер деловање није се посматрало као потпуно самостално и заокружено подручје ратовања, већ као део ширег оквира информационих операција. Документ *Joint Doctrine for Information Operations* из 1998. године дефинисао је информационе операције као активности усмерене на утицај на информације и информационе системе противника, уз истовремену одбрану сопствених информација и информационих система[871]. У истом документу, рачунарски мрежни напад био је одређен као операција усмерена на ометање, ускраћивање, деградацију или уништење информација које се налазе у рачунарима и рачунарским мрежама, као и самих рачунара и мрежа. Због тога је научно прецизније овај период посматрати као доктринарну претходницу америчке концепције сајбер ратовања, а не као фазу у којој је тај концепт већ био у потпуности заокружен.[872]

Рани амерички приступ је тежиште стављао не на апстрактни „дигитални простор“, већ на конкретно деловање на информације, информационе токове, системе за обраду података и мреже

[866] Donald J. Trump, “Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens,” Executive Order, March 6, 2026.
[867] The White House, *President Trump’s Cyber Strategy for America* (Washington, DC: The White House, March 2026), 3–4.
[868] Office of Management and Budget, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Washington, DC: Executive Office of the President, January 26, 2022).
[869] The White House, *President Trump’s Cyber Strategy for America* (Washington, DC: The White House, March 2026), 4–6
[870] Ибид
[871] Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Pub 3-13 (Washington, DC: Joint Chiefs of Staff, October 9, 1998), I-1, I-10, GL-4.
[872] Ибид, I-1, I-10, GL-4.

које подржавају војно и друштвено функционисање. Сајбер способности су посматране као средство за постизање информационе надмоћи, за слабљење способности противника да прикупља, обрађује и користи податке, као и за заштиту сопствених система од упада, обмане, саботаже, и прекида рада. Истовремено, у тој раној доктрини сајбер домен је био дубоко испреплетен са психолошким операцијама, електронским ратовањем, обманом, физичким уништењем и другим елементима информационог деловања, што значи да тадашњи амерички приступ није правио оштру границу између сајбер операција у ужем смислу и ширег информационог окружења.[873]

Суштински доктринарни заокрет настаје у наредној деценији, када Сједињене Америчке Државе све јасније почињу да третирају сајбер простор као засебан оперативни домен. *Department of Defense Strategy for Operating in Cyberspace* из 2011. године изричито је истакла да ће Министарство одбране сајбер простор третирати као оперативни домен у коме је неопходно организовати, обучавати и опремати оружане снаге, на исти начин као што то чини у копненом, поморском, ваздушном и космичком домену. Значај овог корака био је много већи од саме терминолошке промене. Признавање сајбер простора као домена значило је да сајбер способности више нису посматране само као помоћне техничке функције, већ као способност од суштинске важности за извршавање националних безбедносних и војних мисија. У истом документу истакнуто је и да је успостављање Команде САД за сајбер простор одраз потребе да се обезбеди институционална структура способна да уједињено планира и спроводи операције у овом домену.[874]

Документ из 2011. године показао је и да америчка сајбер стратегија не почива искључиво на офанзивној логици, већ на комбинацији организационог, одбрамбеног, партнерског и иновационог приступа. Пет стратешких иницијатива тог документа обухватале су: третирање сајбер простора као оперативног домена, развој нових одбрамбених концепата за заштиту мрежа и система Министарства одбране, сарадњу са другим државним органима и приватним сектором, изградњу односа са савезницима и партнерима, као и ослањање на изузетан сајбер кадар и убрзану технолошку иновацију. Ово је важно јер показује да америчка концепција сајбер ратовања није ограничена на питање „напада“ и „одбране“ у уском војном смислу, већ укључује и питања кадровске политике, иновационог екосистема, сарадње са технолошким компанијама и припреме за деловање у деградираном дигиталном окружењу.[875]

Наредна важна фаза развоја америчког концепта огледа се у документу *The Department of Defense Cyber Strategy* из 2015. године. Ова стратегија је много прецизније дефинисала три примарне мисије америчких војних сајбер снага:

1. одбрану сопствених мрежа, система и информација;
2. припрему за одбрану територије САД и виталних интереса од сајбер напада са значајним последицама;
3. и обезбеђивање интегрисаних сајбер способности за подршку војним операцијама и плановима за кризе и сукобе.

[873] Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Pub 3-13 (Washington, DC: Joint Chiefs of Staff, October 9, 1998), vii, I-3, I-10–I-11.
[874] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011), 5–7.
[875] Ибид, 5, 8–10.

Поред тога, документ је поставио пет стратешких циљева, међу којима су изградња спремних снага и способности за сајбер операције, заштита информационих мрежа Министарства одбране, припрема за одбрану домовине, развој одрживих сајбер опција за контролу ескалације и обликовање окружења конфликта, као и јачање међународних савезништава и партнерстава.[876]

У оквиру исте стратегије посебно је истакнута изградња *Cyber Mission Force*, која је замишљена као структурисана сила састављена од 133 тима и око 6.200 припадника, што сведочи о томе да је сајбер домен у америчком систему прешао пут од помоћне функције до институционално оформљене борбене способности.

Још један битан елемент америчког концепта сајбер ратовања јесте и схватање принципа одвраћања. У стратегији из 2015. године Министарство одбране је нагласило да се одвраћање у сајбер простору не може постићи само декларативном политиком, већ укупношћу америчких мера коју чине јасна политика, способност упозоравања, дефанзивно држање, способност да се одговори, отпорност система и већом поузданошћу атрибуције. Амерички приступ не полази од претпоставке да је једини циљ кажњавање противника након напада, већ и да се потенцијалном противнику унапред смањи вероватноћа успеха, те да му се покаже да ће Сједињене Државе одговорити у време, на месту и на начин који саме изаберу, користећи одговарајуће инструменте националне моћи и у складу са правом. Ова логика одвраћања кроз комбинацију одмазде, отпорности, ускраћивања и атрибуције представља једну од кључних особености америчког модела.[877] Овакву еволуцију — од ранијег смештања сајбер деловања у шири оквир информационих операција до његовог постепеног обликовања као посебног стратешког и оперативног домена — препознаје и домаћа литература, која амерички приступ посматра као један од најважнијих примера милитаризације и геополитичке инструментализације сајбер простора у савременим међународним односима.[878]

Стратегија из 2018. године уноси нову фазу у развоју америчке сајбер безбедносне мисли, а то је да сајбер простор више није само домен који треба бранити, већ и простор сталног надметања у условима стратегијске конкуренције. У сажетку *Сајбер стратегије Министарства одбране* из 2018. године посебно је наглашено да Кина и Русија спроводе упорне кампање у и кроз сајбер простор, да је растућа зависност САД од сајбер домена ризик, као и да је потребно деловати превентивно, а не тек у тренутку оружаног сукоба. У том оквиру појављује се доктринарно изузетно важан концепт *defend forward,* односно деловања унапред ради нарушавања или заустављања злонамерне сајбер активности на самом извору, укључујући и деловање испод прага оружаног сукоба. Истовремено је истакнуто да ће америчке сајбер снаге у рату деловати заједно са копненим, ваздушним, поморским и космичким снагама и да ће бити способне да користе сајбер могућности у читавом спектру конфликта. Овим је америчка концепција сајбер ратовања добила изразито офанзивно-оперативну димензију, али без напуштања одбрамбене и партнерске логике.[879]

[876] Department of Defense, *The Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, April 2015), 5–9.
[877] Department of Defense, *The Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, April 2015), 6–9, 13.
[878] Vladimir Lović, „Sajber prostor kao novo bojno polje: međunarodni odnosi, geopolitika i bezbednost u digitalnom dobu," *Megatrend revija* 22, br. 1 (2025): 215–230.
[879] Department of Defense, *Cyber Strategy Summary* (Washington, DC: Department of Defense, 2018), 1–5.

Савремени амерички приступ додатно је учвршћен Националном одбрамбеном стратегијом из 2022. године. Та стратегија полази од интегрисаног одвраћања, односно од потребе да се делује координисано кроз све домене ратовања, кроз све инструменте националне моћи и у тесној сарадњи са савезницима и партнерима. Она јасно препознаје да противници користе сајбер и космички домен како би стекли оперативне, логистичке и информационе предности, као и да би угрозили домовину, критичну инфраструктуру и способност САД да пројектују силу.[880]

На то се надовезује Стратегија Министарства одбране за сајбер простор из 2023. године, која утврђује како ће Министарство одбране деловати „у и кроз“ сајбер простор ради заштите америчког становништва и остваривања одбрамбених приоритета САД, при чему изричито наглашава реално искуство стечено од 2018. године и досадашње операције спроведене у оквиру политике *defending forward*. За академску прецизност посебно је важно нагласити да овај документ изричито наводи да је његов обим ограничен на сајбер домен и да не успоставља политику за деловање Министарства у ширем информационом окружењу.[881]

Са друге стране, *Стратегија за операције у информационом окружењу* из 2023. године показује да САД информационе операције схватају као ширу категорију која обухвата војне информационе операције, цивилне послове, односе с јавношћу, здружене електромагнетне спектарске операције, сајбер операције, космичке операције, обману, оперативну безбедност и друге дисциплине. Зато је са научног становишта исправније говорити да амерички концепт сајбер ратовања потиче из оквира информационих операција, али да се данас развија као засебан домен који се координише са информационим окружењем, а не као његов синоним.[882]

Једна од трајних карактеристика америчког приступа јесте и повезивање сајбер безбедности, сајбер операција и међународног нормативног поретка. У Међународној стратегији за сајбер простор из 2011. године САД су нагласиле да ће радити на промовисању отворене, безбедне, интероперабилне и поуздане информационе и комуникационе инфраструктуре, која подржава међународну трговину, безбедност и слободу изражавања. У истом документу је наведено да Сједињене Државе настоје да изграде и одрже окружење у којем норме одговорног понашања усмеравају деловање држава, јачају партнерства и подржавају владавину права у сајбер простору. Посебно је значајно што је у овом документу наглашено да државе не морају да бирају између слободног протока информација и безбедности мрежа, као и да национални филтери и „фајерволи“ пружају само привид сигурности, док истовремено успоравају развој интернета као отвореног, интероперабилног, безбедног и поузданог медијума размене. Америчка међународна позиција у овој области није усмерена само на војну предност, већ и на креирање глобалних правила у складу са либералном визијом дигиталног поретка.[883] Истовремено, америчка концепција сајбер ратовања почива на снажној институционалној и извршној инфраструктури. Команда САД за сајбер простор је у мају 2018. године постала засебна здружена борбена команда,

[880] Department of Defense, *2022 National Defense Strategy of the United States of America, Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review* (Washington, DC: Department of Defense, 2022), 8.
[881] Department of Defense, *2023 DoD Cyber Strategy Summary* (Washington, DC: Department of Defense, September 2023), 1–3.
[882] Department of Defense, *Strategy for Operations in the Information Environment* (Washington, DC: Department of Defense, 2023), 5.
[883] The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011), 14, 17, 20.

што је сајбер домену дало додатну организациону тежину у самом систему националне одбране.[884]

Поред тога, савремени амерички приступ не ослања се само на офанзивне способности, већ и на дубоку унутрашњу трансформацију сопствених информационих система. *DoD Zero Trust Strategy* из 2022. године јасно полази од става да класична одбрана више није довољна. У оквиру истог документа успостављена је и Канцеларија за управљање портфолиом *Zero Trust* (*Zero Trust Portfolio Management Office*), са задатком да координише примену Стратегије на нивоу читавог Министарства одбране. Овде се види да америчко схватање сајбер ратовања не подразумева само пројекцију силе ка споља, већ и трајну унутрашњу институционалну адаптацију ради очувања отпорности, континуитета команде и способности деловања у условима угроженог или деградираног сајбер окружења.[885]

Посебно место у америчком концепту има и питање критичне инфраструктуре. *The Department of Defense Cyber Strategy* из 2015. године јасно наглашава да приватни сектор поседује и управља већином мрежа и инфраструктуре сајбер простора, те да је због тога прва линија одбране, док и држава мора бити спремна да се брани од најопаснијих напада са значајним последицама.[886]

Cyber Strategy Summary из 2018. године додатно наглашава да Министарство одбране настоји да одврати, предухитри или порази злонамерне активности усмерене на критичну инфраструктуру САД и да у том контексту делује превентивно и унапред, пре него што претње досегну своје циљеве.[887] Тако се америчка концепција сајбер ратовања све мање може разумети као питање изолованог „војног хаковања“, а све више као системско повезивање војне моћи, сарадње са приватним сектором, заштите критичне инфраструктуре, отпорности одбрамбено-индустријске базе, међународних партнерстава и управљања ескалацијом.[888]

Амерички концепт сајбер ратовања развијао се од почетног уклапања рачунарско-мрежних напада у шири оквир информационих операција ка данашњем схватању сајбер простора као самосталног оперативног домена од пресудног значаја за националну безбедност и војну моћ.[889] Централна одлика концепта јесте технолошко-оперативна усмереност на утицај на противничке информације, системе и процесе одлучивања, али је временом тај приступ проширен ка интегрисаном одвраћању, деловању испод прага оружаног сукоба, одбрани критичне инфраструктуре, развоју здружених сајбер снага, партнерству са приватним сектором и обликовању међународних норми понашања у сајбер простору.[890] Амерички концепцт сајбер ратовања данас представља спој војне доктрине, технолошке иновације, институционалне изградње, одбрамбене политике и међународног нормативног деловања.[891]

---

[884] Jim Garamone, “Cyber Command Becomes Unified Combatant Command,” U.S. Department of Defense News, May 4, 2018.
[885] Department of Defense, *DoD Zero Trust Strategy* (Washington, DC: Department of Defense, October 21, 2022), 1, 5, 28.
[886] Department of Defense, *The Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, April 2015), 5, 14.
[887] Department of Defense, *Cyber Strategy Summary* (Washington, DC: Department of Defense, 2018), 3–4.
[888] Department of Defense, *Cyber Strategy Summary* (Washington, DC: Department of Defense, 2018), 3–4.
[889] Vladimir Lović, „Sajber prostor kao novo bojno polje: međunarodni odnosi, geopolitika i bezbednost u digitalnom dobu,” *Megatrend revija* 22, br. 1 (2025): 227–229.
[890] Department of Defense, *2022 National Defense Strategy of the United States of America, Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review* (Washington, DC: Department of Defense, 2022), 8.
[891] Vladimir Lović, „Sajber prostor kao novo bojno polje: međunarodni odnosi, geopolitika i bezbednost u digitalnom dobu,” *Megatrend revija* 22, br. 1 (2025): 228–229.

5.3 Механизми заштите сајбер простора од сајбер напада – Сајбер команда САД

Сајбер команда Сједињених Америчких Држава, позната као *U.S. Cyber Command (USCYBERCOM)*, представља централну војну институцију америчке државе за планирање, координацију и извођење операција у сајбер простору. Њен значај не произилази само из чињенице да је реч о специјализованој војној команди, већ из тога што је сајбер простор у америчкој стратешкој мисли постепено израстао у засебан домен сукоба, упоредив по важности са копном, морем, ваздухом и космосом. У званичном одређењу саме Команде наглашава се да је њена мисија да „усмерава, синхронизује и координише планирање и операције у сајбер простору ради одбране и унапређења националних интереса, у сарадњи са домаћим и међународним партнерима“[892]. Сајбер команда брани информационе системе Министарства одбране, подржава здружене команданте операцијама у сајбер простору и брани државу од сајбер напада од значајних последица. Управо зато се Сајбер команда САД не сме посматрати као техничка служба за заштиту мрежа, већ као инструмент државне моћи који обједињује војну, обавештајну, технолошку и оперативну компоненту америчке националне безбедности.[893]

Формирање Сајбер команде био је резултат постепеног доктринарног и организационог сазревања америчког одбрамбеног система. Званична историја саме Команде прати овај развој још од седамдесетих година, када су у склопу војних и обавештајних структура започети први напори за смањење рањивости информационих система. Током деведесетих година, а нарочито након вежбе *Eligible Receiver 97*, постало је јасно да су америчке мреже подложне удаљеним нападима и да потенцијални противници могу угрозити виталне функције државе без класичне употребе оружане силе. Због тога је 1998. године формирана *Joint Task Force–Computer Network Defense*, која је већ 1999. еволуирала у *Joint Task Force–Computer Network Operations*, да би 2004. дошло до функционалног раздвајања одбрамбене и офанзивне компоненте кроз *Joint Task Force–Global Network Operations* и *Joint Functional Component Command–Network Warfare*. Ове институционалне промене показују да USCYBERCOM није настао изненада, већ као завршна фаза ширег процеса у коме је америчка војска постепено схватила да без централизоване команде над сајбер простором не може поуздано да штити сопствене системе нити да створи предност над противником.[894]

Сајбер команда је успостављена као потчињена команда у оквиру *U.S. Strategic Command*-а, на основу одлуке тадашњег секретара одбране Роберта Гејтса од 23. јуна 2009. године. Команда је почела са радом 21. маја 2010. године, а први командант био је генерал Кит Александер, који је истовремено био и директор Националне безбедносне агенције. Већ овај први институционални аранжман открива једну од трајних карактеристика USCYBERCOM-а а то је повезаност са обавештајном заједницом, нарочито са NSA, са којом је ко-лоциран у Форт Џорџ Г. Миду у Мериленду. После неколико година организационог развоја, председник Доналд Трамп је 2018. године наложио подизање Сајбер команде на ниво посебне јединствене борбене команде, а та промена је формално ступила на снагу 4. маја 2018. године. Подизањем статуса Сајбер команде потврђено је да сајбер безбедност више није споредна функција унутар стратешког командовања, већ захтева сопствену институционалну вертикалу, сопствене приоритете, засебно планирање и команду са већом оперативном тежином.[895]

---

[892] U.S. Cyber Command, “Mission and Vision,” , прегледано 5.маја 2026
[893] U.S. Cyber Command, “Mission and Vision,”, прегледано 5.маја 2026
[894] U.S. Cyber Command, “Command History,” прегледано 5.маја 2026
[895] U.S. Cyber Command, “Command History,” прегледано 5.маја, 2026; Jim Garamone, “Cyber Command Becomes Unified Combatant Command,” *U.S. Department of Defense News*, May 4, 2018.

Подизање на ниво јединствене борбене команде није било само симболичко. У *Command Vision* документу из 2018. године наглашено је да је сврха Команде постизање и одржавање супериорности у сајбер простору кроз преузимање и задржавање тактичке и оперативне иницијативе, отежавање деловања противника и поткопавање његовог уверења да су непријатељске активности у сајбер простору против Сједињених Америчких Држава исплативе. У истом документу истиче се да USCYBERCOM мора да делује заједно са здруженим командама, родовима војске, органима власти, савезницима и привредом, као и да своју снагу гради на јединственом сајбер предузећу, оснаженом људству, скалабилним решењима и дугорочној кампањској логици. Овај документ је важан јер показује да Сајбер команда није замишљена само као реактивни механизам за одбрану после напада, већ као активан инструмент који стално мора да обликује оперативно окружење, ограничава слободу маневра противника и ствара предуслове за америчко одвраћање.[896]

У институционалном погледу, USCYBERCOM је специфичан и по томе што његов командант традиционално истовремено обавља и функцију директора Националне безбедносне агенције и начелника *Central Security Service*-а. Ова двострука улога има далекосежан значај јер омогућава јединство напора између војних сајбер операција и сигнала обавештајних активности, бржи проток обавештајних сазнања ка оперативном нивоу и ефикасније повезивање одбране, атрибуције, праћења противника и активног супротстављања. Истовремено, управо овај аранжман годинама уназад изазива расправе у америчкој стручној и политичкој јавности о томе да ли је боље задржати јединство командовања или раздвојити функције ради јаснијег институционалног разграничења. Ипак, са становишта оперативне ефикасности, америчка држава до данас није одустала од логике да USCYBERCOM и NSA, када је реч о сајбер домену, остварују далеко већи ефекат заједно него одвојено.[897]

Организационо, Сајбер команда почива на више слојева компоненти и потчињених структура. На нивоу сервисних партнера, званична страница Команде наводи Army Cyber Command, Fleet Cyber Command/Tenth Fleet, Sixteenth Air Force (Air Forces Cyber) и Marine Corps Forces Cyberspace Command као главне сервисне носиоце сајбер способности по родовима војске. Поред њих, у структури Команде посебно место заузима *Cyber National Mission Force*, чији је задатак да планира, усмерава и синхронизује операције пуног спектра како би одвраћао, реметио и, ако је потребно, поразио непријатељске сајбер актере у функцији одбране САД. На званичној страници компоненти USCYBERCOM-а наводи се и *Department of Defense Cyber Defense Command*, са мисијом да надзире свакодневно функционисање DoD мрежа и да их активно брани, осигуравајући кључни сајбер терен и неутралишући противника који успе да пробије спољне одбране. Поред тога, Команда је 2016. додала и *Joint Task Force–Ares* ради борбе против терористичких претњи у сајбер простору. USCYBERCOM представља сложен систем који обједињује родовске компоненте, националне снаге, одбрану DoD информационих мрежа и специјализоване оперативне елементе.[898]

У ширем аналитичком смислу, институционални развој Сајбер команде може се посматрати као један од најизразитијих примера како је америчка држава сајбер простор постепено превела из техничко-обавештајне сфере у пуноправно поље стратешког и војног деловања. У том смислу,

[896] U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Fort George G. Meade, MD: U.S. Cyber Command, April 2018), 5–6.
[897] U.S. Cyber Command, "Command History," прегледано 5.маја 2026, 2026.
[898] U.S. Cyber Command, "U.S. Cyber Command" official homepage, прегледано 5.маја 2026, 2026.

домаћа литература с правом указује да управо институционализација сајбер капацитета представља један од најупадљивијих показатеља ширег процеса милитаризације сајбер простора у савременим међународним односима.[899]

Један од кључних инструмената Сајбер команде јесте *Cyber Mission Force (CMF)*, односно здружена сајбер сила формирана за извршавање основних мисија у сајбер простору. Званични подаци Команде показују да је изградња CMF започела 2013. године, да су свих 133 тима достигла пуну оперативну способност у мају 2018. године, након што су претходно прошли фазу изградње, обуке и сертификације.[900]1 Према званичним објашњењима Министарства одбране, та сила је организована у 13 *National Mission Teams,* 68 *Cyber Protection Teams,* 27 *Combat Mission Teams* и 25 *Support Teams*. Ова подела је концептуално веома важна: *National Mission Teams* су усмерени на одбрану државе од најзначајнијих претњи, *Cyber Protection Teams* на заштиту DoD мрежа и система, *Combat Mission Teams* на подршку здруженим командама кроз сајбер дејства, а *Support Teams* на аналитичку и планску потпору. Тиме је Сајбер команда добила не само бројчану масу, већ функционално диференцирану силу која може истовремено да брани, напада, подржава и анализира.[901]

Од стратешког значаја за разумевање улоге Сајбер команде јесте доктрина *persistent engagement* и политика *defend forward*. У званично објављеној визији USCYBERCOM-а из 2018. године већ се јасно види идеја да команда мора деловати континуирано, а не повремено, како би осујећивала противничке активности тамо где настају и одржавала супериорност у сајбер простору.[902] Ова логика је потврђена и у *2023 DoD Cyber Strategy Summary*, где се наглашава да је Министарство одбране од 2018. спровело значајан број операција у сајбер простору кроз политику *defending forward*, односно активног ремећења злонамерних сајбер активности пре него што оне досегну америчку домовину. Исти документ наводи четири комплементарне линије напора: одбрану нације, припрему за вођење и добијање ратова, заштиту сајбер домена са савезницима и партнерима и изградњу трајних предности у сајбер простору. Према тој логици, Сајбер команда није ограничена на реакцију после напада, већ делује кампањски, испод прага оружаног сукоба, ради стицања увида, нарушавања противничких способности, јачања одвраћања и стварања повољнијих безбедносних услова за САД и њихове савезнике.[903]

Практичан израз овакве филозофије представљају такозване *hunt forward operations*, које су постале један од најпрепознатљивијих облика деловања Сајбер команде последњих година. У сведочењу генерала Накосонеа из 2023. године наведено је да је од 2018. *Cyber National Mission Force* распоредио *hunt forward* тимове 40 пута у 21 земљи, радећи на 59 мрежа, при чему су те операције допринеле откривању активности Кине, Русије, Ирана и сајбер криминалних група, јачању безбедности партнерских мрежа и објављивању више од 90 узорака малвера ради шире анализе.[904] Годину дана касније, *2024 Report on the Cybersecurity Posture of the United States* наводи да је само у 2023. години *Cyber National Mission Force* распоредио тимове 22 пута у 17 земаља ради партнерски омогућених *hunt forward* операција које идентификују злонамерне активности у

[899] Vladimir Lović, „Sajber prostor kao novo bojno polje: međunarodni odnosi, geopolitika i bezbednost u digitalnom dobu," *Megatrend revija* 22, br. 1 (2025): 215–230.
[900] U.S. Cyber Command, "Cyber Mission Force Achieves Full Operational Capability," May 17, 2018.
[901] U.S. Department of Defense, *FY 2020 Defense Budget Overview* (Washington, DC: Department of Defense, 2019), 4-14.
[902] U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Fort George G. Meade, MD: U.S. Cyber Command, April 2018), 3–6.
[903] Department of Defense, *2023 DoD Cyber Strategy Summary* (Washington, DC: Department of Defense, September 2023), 1–4.
[904] Paul M. Nakasone, "2023 Posture Statement of General Paul M. Nakasone," U.S. Cyber Command, March 7, 2023.

иностранству и ограничавају слободу маневра противника.[905] Чланци о операцијама у Албанији и Летонији из 2023. године додатно показују да ове мисије имају двоструку сврху: помажу партнерима да ојачају сопствену одбрану и истовремено дају САД увид у злонамерне технике пре него што се оне окрену према америчким мрежама. Због тога *hunt forward* није само партнерска активност, већ један од централних механизама пројекције америчке сајбер безбедности у иностранству.[906]

Институционална логика Сајбер команде не значи да америчка војска има неограничена овлашћења у домену заштите свих дигиталних система на територији САД. *2023 DoD Cyber Strategy Summary* изричито наглашава да Министарство одбране има ограничена средства да директно утиче на сајбер безбедност приватних компанија ван одбрамбено-индустријске базе и да војне снаге не могу да бране приватне субјекте од сајбер напада осим ако то не наложи председник или ако надлежни орган одобри захтев за подршку цивилним властима. Управо зато Сајбер команда све више развија моделе сарадње уместо класичне субординације према приватном сектору.[907] Један од најзанимљивијих примера је програм *Under Advisement (UNAD),* који је *CNMF* представио као не-класификовани механизам двосмерне размене техничких информација о страним претњама са приватном индустријом. Према званичном опису, овај програм омогућава да се индикатори компромитације и сазнања прикупљена у страним мрежама брзо деле са индустријом и међуагенцијским партнерима, како би се америчке мреже ојачале пре него што претња стигне до њих. То показује да је Сајбер команда, иако војна институција, у савременом контексту постала и значајан чинилац у јавно-приватном екосистему сајбер одбране.[908]

Подједнако важно је и питање унутрашње спремности и обучавања кадрова. У сведочењу пред Конгресом из 2024. генерал Тимоти Д. Хо наглацио је да је један од главних изазова USCYBERCOM-а развој кадрова, попуна цивилних места, праћење спремности тимова и успостављање заједничких стандарда обуке на нивоу читавог Министарства одбране. Исто сведочење истиче да су побољшани механизми праћења спрмености тимова и да овлашћења Команде као *Joint Cyberspace Trainer* омогућавају успостављање заједничких стандарда обуке унутар целог ресора.[909] Практични израз ове еволуције види се и у вежби *CYBER FLAG 24-2,* одржаној 2024. године, која је по први пут укључила и офанзивне сајбер операције, не само дефанзивне. Званично саопштење USCYBERCOM-а о овој вежби нагласио је да је њен циљ био сертификација офанзивних тимова, јачање оперативне спремности и унапређење координације међу чланицама *Five Eyes* партнерства. То је важан показатељ институционалног сазревања: Сајбер команда више не развија само способност одбране мрежа, већ и стандарде за офанзивна дејства, интероперабилност са партнерима и здружено оперативно планирање у сајбер простору.[910]

---

[905] Office of the National Cyber Director, *2024 Report on the Cybersecurity Posture of the United States* (Washington, DC: Executive Office of the President, May 2024), 20–21.
[906] U.S. Cyber Command, "Committed Partners in Cyberspace: Following Cyberattack, U.S. Conducts First Defensive Hunt Operation in Albania," March 23, 2023; and U.S. Cyber Command, "Shared Threats, Shared Understanding: U.S., Canada and Latvia Conclude Defensive Hunt Operations," May 10, 2023.
[907] Department of Defense, *2023 DoD Cyber Strategy Summary* (Washington, DC: Department of Defense, September 2023), 7–8.
[908] U.S. Cyber Command, "CYBERCOM's 'Under Advisement' to Increase Private Sector Partnerships, Industry Data-Sharing in 2023," June 29, 2023.
[909] Timothy D. Haugh, "Posture Statement of General Timothy D. Haugh," U.S. Cyber Command, April 12, 2024.
[910] U.S. Cyber Command, "U.S. Cyber Command Hosts First Offensive Cyber Flag 2024 Exercise," September 3, 2024.

Савремени значај Сајбер команде додатно се види у њеној позицији унутар ширег америчког одбрамбеног система. У свом сведочењу из 2025. године Хартман је нагласио да USCYBERCOM има одговорности не само у погледу извођења операција, већ и у погледу опремања, одржавања и развоја здружене сајбер силе, док сваки ред војске обезбеђује људство за *Cyber Mission Force*. Истакао је и да сваки командант сервисне сајбер компоненте истовремено делује као командант *Joint Force Headquarters-Cyber*, чиме се обезбеђује веза између родовских способности и здружене команде. Ово је важно јер показује да је Сајбер команда временом добила одлике које превазилазе класичну улогу оперативне команде. Команда све више функционише као институција која истовремено командује, развија снаге, обликује стандарде спремности и утиче на буџетске и програмске процесе. Управо та институционална хибридност један је од разлога због којих се USCYBERCOM данас сматра једним од најважнијих примера како се једна модерна држава организационо прилагођава условима трајне сајбер конкуренције.[911]

Из академског угла, Сајбер команда САД може да се разумети као производ три паралелна процеса. Први је милитаризација сајбер простора, односно прихватање да се у дигиталном окружењу воде операције од непосредног значаја за рат, кризе и мирнодопску конкуренцију. Други је институционализација сајбер моћи, кроз стварање засебне команде, сопствених снага, потчињених организација и система обуке. Трећи је интеграција сајбер способности у шире државне инструменте моћи, укључујући обавештајну сарадњу, партнерство са савезницима, размену с индустријом, заштиту критичне инфраструктуре и подршку здруженим операцијама. USCYBERCOM данас није тек команда која реагује на инциденте, већ институција која настоји да континуирано обликује безбедносно окружење, да ојача америчку и савезничку отпорност и да обезбеди да Сједињене Америчке Државе не изгубе стратешку предност у домену који је постао једно од кључних поља савременог надметања.[912]

Управо зато се о Сајбер команди САД не може писати само као о једној уобичајној организационој јединици створеној у склопу Пентагона. Њена вредност је у томе што представља концентрисани израз америчког схватања да је у 21. веку надметање за информацију, приступ, отпорност, брзину реаговања и слободу маневра у мрежама постало неодвојиво од националне моћи у целини. Ако је крајем деведесетих сајбер деловање у америчком систему још било посматрано као део ширих информационих операција, данас је Сајбер команда институционални доказ да је сајбер простор постао стално, глобално и високо професионализовано подручје војног деловања. Њен даљи развој, посебно у области кадрова, вештачке интелигенције, аутоматизације, сарадње са савезницима и активне одбране критичне инфраструктуре, остаће један од најпоузданијих показатеља како САД виде будућност рата, одбране и међународне безбедности у дигиталном добу.[913]

Међутим, за потпуно разумевање америчког модела сајбер ратовања није довољно анализирати само улогу U.S. Cyber Command-a, већ и ширу институционалну, правну и савезничку архитектуру кроз коју се америчка сајбер моћ организује, усмерава и примењује.

---

[911] William J. Hartman, "Posture Statement of Lieutenant General William J. Hartman," U.S. Cyber Command, April 9, 2025.
[912] Владимир Ловић, „Сајбер простор као ново бојно поље: међународни односи, геополитика и безбедност у дигиталном добу," *Megatrend revija* 22, бр. 1 (2025): 227–229.
[913] William J. Hartman, "Posture Statement of Lieutenant General William J. Hartman," U.S. Cyber Command, April 9, 2025.

5.4 Институционална, правна и савезничка архитектура америчког модела сајбер ратовања

Као логичан наставак претходног разматрања америчких стратегијских докумената и Сајбер команде потребно је посебно осветлити институционалну, правну и савезничку архитектуру америчког модела сајбер ратовања. Без тог корака, амерички приступ би се могао погрешно свести или на низ техничких мера, или на изоловане офанзивне операције, иако је његова суштина управо у повезивању више институционалних нивоа, више домена сукоба и више инструмената државне моћи.[914]

У савременом америчком схватању сајбер ратовање није ни искључиво војна, ни искључиво цивилна, ни искључиво технолошка категорија. Оно је постало облик стратешког деловања који обједињује војну силу, обавештајни рад, заштиту федералних система, кривичноправну реакцију, регулаторно усмеравање тржишта, сарадња са савезницима и обликовање међународних правила понашања.[915] Управо зато амерички модел данас делује и као најразвијенији и као најспорнији: најразвијенији јер је институционално најразрађенији, а најспорнији јер најотвореније нормализује трајно деловање у страним мрежама испод прага рата.[916]

У институционалном смислу, средиште америчког војног приступа остаје *U.S. Cyber Command*, који усмерава, синхронизује и координише планирање и операције у сајбер простору ради одбране и унапређења националних интереса.[917] Међутим, Сајбер команда не делује као усамљен војни орган, већ као оперативно језгро ширег система. Њена посебна вредност лежи у томе што повезује здружене војне потребе, националне мисије одбране, обавештајне увиде и сталну кампањску логику деловања у сајбер простору.[918] Управо зато је за разумевање америчког модела пресудно уочити да USCYBERCOM није једноставно „сајбер верзија“ класичне команде, већ институција која делује на заустављању конкуренције, кризе и оружаног сукоба, при чему истовремено подржава здружене команданте, брани DoD информационе системе и учествује у широј одбрани САД.[919]

Војна улога Сајбер команде не може да се одвоји од односа са Националном безбедносном агенцијом. Званична историја Команде и каснија сведочења њених команданата показују да је такозвани *dual-hat* аранжман — у коме исти појединац истовремено обавља дужност команданта USCYBERCOM-а и директора NSA — остао једна од темељних карактеристика америчког модела.[920] Америчка страна је овај аранжман бранила тврдњом да се војне сајбер операције и сигнално-обавештајни рад међусобно појачавају: обавештајни увид омогућава ефикасније и брже операције, док операције проширују увид у противничке технике, инфраструктуру и намере.[921] Генерал Пол Накасоне је 2023. године изричито нагласио да су највећи успеси USCYBERCOM-а и NSA у одбрани избора, супротстављању актерима и ширем ометању непријатељског деловања

[914] Department of Defense, *2022 National Defense Strategy of the United States of America, Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review* (Washington, DC: Department of Defense, 2022), 6–8.
[915] Ibid., 8.
[916] Veljko Blagojević, „Strategija nacionalne bezbednosti SAD iz 2025: kontinuitet i promene,” *Međunarodna politika* 77, br. 1196 (2026): 79–103.
[917] U.S. Cyber Command, “Mission and Vision,”, прегледано 8.мај 2026
[918] U.S. Cyber Command, “Command History,”, прегледано 8.мај 2026
[919] Department of Defense, *2023 DoD Cyber Strategy Summary* (Washington, DC: Department of Defense, September 2023), 1–3.
[920] U.S. Cyber Command, “Command History,”, прегледано 8.мај 2026
[921] Paul M. Nakasone, “2023 Posture Statement of General Paul M. Nakasone,” U.S. Cyber Command, March 7, 2023.

почивали управо на овој повезаности.[922] Генерал Тимоти Хо је 2024. године додао да и конкретни оперативни механизми, попут *China Outcomes Group*, показују колико је вредна ова институционална синергија.[923] Зато у америчком систему сајбер ратовање није само питање примене кода или операционализације алата, већ и питање јединства између прикупљања увида, атрибуције, планирања и дејства.[924]

Али америчка архитектура не завршава се на односу USCYBERCOM–NSA. У цивилно-извршној сфери једнако важну улогу имају *Office of the National Cyber Director (ONCD), Office of Management and Budget (OMB), Cybersecurity and Infrastructure Security Agency* (CISA) и *Federal Bureau of Investigation (*FBI).[925] ONCD делује као главни координатор националне сајбер политике у оквиру Извршне канцеларије председника и као главни саветодавни центар за интегрисање сајбер стратегије на нивоу читаве владе.[926] OMB, с друге стране, не води операције, али претвара стратегију у управљачке и буџетске обавезе и његов спектар дужности обухвата од меморандума о *zero trust* архитектури до смерница које агенцијама налажу да инвестиције у сајбер безбедност вежу за мерљиве резултате и стратешке приоритете.[927] CISA има оперативно-цивилну улогу: она поставља заједничку безбедносну основу за *Federal Civilian Executive Branch*, делује као национална агенција за смањење ризика над критичном инфраструктуром и последњих година агресивно развија концепт *secure by design*.[928] FBI је, пак, водећа федерална институција за истраге сајбер напада, атрибуцију, кривичноправни одговор и разбијање криминалних и државно спонзорисаних мрежа.[929] Из тога произилази да амерички модел није организован по линији једног центра који командује свима, већ као функционално распоређен систем: USCYBERCOM и NSA обезбеђују војно-обавештајни ударни капацитет, CISA цивилну и инфраструктурну отпорност, FBI истрагу и санкционисање, OMB и ONCD управљачко, буџетско и стратешко усклађивање.[930]

Оваква институционална расподела надлежности важна је и зато што показује да се америчко схватање сајбер ратовања не може поистоветити са ширим појмом информационих операција, али ни потпуно одвојити од њега. Ранија америчка доктрина крајем деведесетих је сајбер деловање посматрала као део ширег оквира информационих операција, али новији документи праве далеко јаснију концептуалну разлику.[931] *2023 DoD Cyber Strategy Summary* наглашава да је његов предмет сам сајбер домен и деловање „у и кроз“ њега.[932] Насупрот томе, *Strategy for Operations in the Information Environment* из 2023. године много шире уређује институционалну и оперативну синергију између војних информационих операција, сајбер операција, цивилних послова, односа с јавношћу, електромагнетног спектра, космичких операција, обмане и оперативне

[922] Ibid
[923]Timothy D. Haugh, “Posture Statement of General Timothy D. Haugh 2024,” U.S. Cyber Command, April 12, 2024.
[924] Vladimir Lović, „Sajber prostor kao novo bojno polje: međunarodni odnosi, geopolitika i bezbednost u digitalnom dobu,” *Megatrend revija* 22, br. 1 (2025): 215–230.
[925] The White House, “Office of the National Cyber Director,” прегледано 7. мај 2026.
[926] Ibid.
[927] Office of Management and Budget, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Washington, DC: Executive Office of the President, January 26, 2022).
[928] Cybersecurity and Infrastructure Security Agency, “Federal Government,” accessed May 8, 2026.
[929] Federal Bureau of Investigation, “The Cyber Threat,” accessed May 8, 2026.
[930] Office of Management and Budget and Office of the National Cyber Director, *M-24-14: Administration Cybersecurity Priorities for the FY 2026 Budget* (Washington, DC: Executive Office of the President, July 10, 2024).
[931] Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Pub 3-13 (Washington, DC: Joint Chiefs of Staff, October 9, 1998).
[932] Department of Defense, *2023 DoD Cyber Strategy Summary* (Washington, DC: Department of Defense, September 2023), 1–3.

безбедности.[933] То значи да у савременом америчком моделу сајбер ратовање више није просто синоним за информационо деловање, али ни самостална затворена сфера. Напротив, сајбер је засебан домен, док су информационе операције шири оквир у коме се различити инструменти укључујући сајбер компоненту, координишу ради утицаја на одлучивање, перцепцију, вољу и способност противника.[934] Управо је то показатељ да је амерички модел еволуирао од утапања сајбера у информационо поље ка јаснијем раздвајању домена, али је истовремено задржао логичку потребу да их у пракси поново повеже.[935]

Савезничка димензија америчког модела једнако је важна као и институционална. *2023 DoD Cyber Strategy Summary* једну од четири кључне линије напора изричито формулише као заштиту сајбер домена заједно са савезницима и партнерима.[936] У том светлу, америчка сајбер моћ није само национална, већ и мрежна. *Hunt forward* операције у Албанији и Летонији показале су да се део америчке одбране остварује на туђим мрежама, али уз сагласност и у корист државе домаћина, чиме се истовремено јача отпорност партнера и проширује увид у непријатељске технике пре него што буду употребљене против САД.[937] *Cyber Flag 24-2* је 2024. године по први пут укључио и офанзивне сајбер операције и тиме послужио као механизам сертификације и координације међу *Five Eyes* партнерима.[938] На ширем стратешком нивоу, НАТО је на Самиту у Вашингтону 2024. године одлучио да успостави *NATO Integrated Cyber Defence Centre*, како би ојачао заштиту мрежа, ситуациону свест и даљу имплементацију сајбер простора као оперативног домена у миру, кризи и сукобу.[939] То показује да амерички модел сајбер ратовања није више питање само националне одбране, већ и савезничке способности, интероперабилности и колективног одвраћања.[940] У том смислу, америчка сајбер моћ делује не само кроз сопствене капацитете, већ и кроз способност да обликује стандарде, праксе, вежбе и одбрамбене обрасце читаве савезничке мреже.[941]

Правне и политичке контроверзе почињу управо тамо где амерички модел постаје најефикаснији. На домаћем правном плану, 10 U.S.C. § 394 даје секретару одбране основ за развијање, координацију, припрему и извођење војних активности у сајбер простору, укључујући и тајне војне активности, при чему закон такве активности третира као *traditional military activities*, а не као *covert action* у ужем смислу.[942] Последица тога није само убрзано одобравање, већ и већи маневарски простор за извођење операција испод прага отворених непријатељстава.[943] Пол Неј је 2020. године дао правну артикулацију овом приступу тврдњом да не постоји опште правило по коме би свака не-консензуална сајбер операција на туђој територији аутоматски представљала

[933] Department of Defense, *Strategy for Operations in the Information Environment* (Washington, DC: Department of Defense, 2023), 5–7.
[934] Ibid.
[935] Lović, „Sajber prostor kao novo bojno polje," 215–230.
[936] Department of Defense, *2023 DoD Cyber Strategy Summary* (Washington, DC: Department of Defense, September 2023), 8–9.
[937] U.S. Cyber Command, "Committed Partners in Cyberspace: Following Cyberattack, U.S. Conducts First Defensive Hunt Operation in Albania," March 23, 2023.
[938] U.S. Cyber Command, "U.S. Cyber Command Hosts First Offensive Cyber Flag 2024 Exercise," September 3, 2024.
[939] NATO, "Washington Summit Declaration," July 10, 2024.
[940] Ibid.
[941] U.S. Cyber Command, "Shared Threats, Shared Understanding: U.S., Canada and Latvia Conclude Defensive Hunt Operations," May 10, 2023.
[942] United States Code, "10 U.S.C. § 394. Authorities Concerning Military Cyber Operations."
[943] Ibid.

повреду међународног права.[944] Док америчка страна настоји да задржи широку слободу за позиционирање, деградацију противничких способности и ремећење текућих злонамерних активности испод прага употребе силе, док многе друге државе и део литературе упозоравају да такво тумачење подрива строже схватање суверенитета, чиме се ствара тачка неслагања.[945] Посматрано из те перспективе, амерички модел је иновативан јер покушава да прилагоди право новој технолошкој стварности, али и дестабилишући јер проширује простор у коме државе могу тврдити да је прекогранично деловање допуштено све док не достигне јасно препознат праг силе или принуде.[946]

Савремени развој америчког модела показује и још једну важну промену а то је да је сајбер безбедност је све мање само питање операција, а све више и питање тржишне корекције, технолошке политике и индустријске отпорности. *National Cybersecurity Strategy* из 2023. године отворено је преусмерила тежиште са индивидуалне „сајбер хигијене“ на одговорност системски способнијих актера и на државно обликовање тржишних подстицаја.[947] CISA је 2024. године ту логику конкретизовала кроз *Secure by Design* обавезе које је прихватило 68 водећих технолошких компанија.[948] OMB и ONCD су у буџетским смерницама за FY 2026 инсистирали на томе да се стратешки приоритети преводе у улагања, мерљиве резултате и дугорочну институционалну модернизацију.[949] У том погледу, амерички модел више не третира сајбер искључиво као војно питање, већ као простор у коме се укрштају национална безбедност, стандарди развоја софтвера, облак, идентитет, *zero trust* архитектура и критична инфраструктура.[950] Континуитет те логике види се и у раније поменутој Трамповој *Cyber Strategy for America* из марта 2026. године, која, иако стилски одступа од Бајденове стратегије, ипак задржава снажан нагласак на AI решењима, отпорности националних система, сигурним ланцима снабдевања, постквантној криптографији и сталном тестирању и лову на противничке актере на федералним мрежама.[951] Зато је погрешно амерички модел свести на једноставну поделу између „Бајденове регулације“ и „Трампове дерегулације“ јер је суштина у томе да обе администрације, свака својим језиком, сајбер везују за националну моћ, технолошку предност и способност државе да обликује и дигитално окружење и понашање приватног сектора.[952]

Амерички концепт сајбер безбедности и његов приступ данас делује као парадигматичан пример спајања безбедносне, технолошке, правне и политичке логике.[953] Али он је истовремено и пример дубоке противречности савременог дигиталног поретка који показује што је модел развијенији, то снажније нормализује трајно прекогранично деловање испод прага оружаног сукоба и шири

[944] Paul C. Ney, Jr., “DOD General Counsel Remarks at U.S. Cyber Command Legal Conference,” U.S. Department of Defense, March 2, 2020.
[945] Ljubomir Tintor, „Međunarodna odgovornost države u digitalnom (sajber) prostoru,” u *Srpski godišnjak za međunarodno pravo* (Beograd: Srpsko udruženje za međunarodno pravo, 2023).
[946] Ney, “DOD General Counsel Remarks.”
[947] The White House, *National Cybersecurity Strategy* (Washington, DC: The White House, March 2023).
[948] Cybersecurity and Infrastructure Security Agency, “CISA Announces Secure by Design Commitments from Leading Technology Providers,” May 8, 2024.
[949] Office of Management and Budget and Office of the National Cyber Director, *M-24-14: Administration Cybersecurity Priorities for the FY 2026 Budget* (Washington, DC: Executive Office of the President, July 10, 2024).
[950] Office of Management and Budget, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Washington, DC: Executive Office of the President, January 26, 2022).
[951] The White House, *President Trump’s Cyber Strategy for America* (Washington, DC: The White House, March 2026).
[952] Donald J. Trump, “Sustaining Select Efforts to Strengthen the Nation’s Cybersecurity and Amending Executive Order 13694 and Executive Order 14144,” Executive Order, June 6, 2025.
[953] Department of Defense, *2023 DoD Cyber Strategy Summary* (Washington, DC: Department of Defense, September 2023), 1–9.

простор у коме се стратешка конкуренција води без јасне границе између мира и сукоба.[954] У томе лежи и његова највећа аналитичка вредност за ово поглавље дисертације: амерички модел није значајан само зато што је моћан, већ зато што најјасније показује како изгледа сајбер ратовање када прерасте из техничког питања у централни инструмент националне стратегије.[955]

5.5 Извођење сајбер напада САД на територијама других држава

Анализа извођења сајбер напада Сједињених Америчких Држава на територијама других држава захтева нарочиту методолошку опрезност, јер је реч о области у којој се готово увек преплићу тајност, обавештајна природа операција и ограничена јавна транспарентност.

За разлику од класичних војних операција, које су често видљиве, временски и просторно одредиве и праћене формалним саопштењима, офанзивне сајбер операције се по правилу спроводе тако да се њихово извођење дуго не признаје, а неретко се никада ни не потврди. Зато је у научној обради ове теме неопходно разликовати три категорије случајева: прво, операције које су амерички званичници директно признали или суштински потврдили; друго, операције које нису формално признате, али су потврђене кроз поуздане изворе, истраживачко новинарство и накнадно доступне документе; и треће, операције које се широко приписују САД, али код којих коначна атрибуција остаје у домену високо уверљиве, али ипак посредне процене. Питање америчких сајбер напада у иностранству није само питање оперативне праксе, већ и питање стандарда доказивања, атрибуције, политичког тумачења и правне квалификације.[956]

У доктринарном смислу, амерички приступ офанзивним сајбер операцијама у иностранству развијао се од ранијег схватања сајбер деловања као дела ширих информационих операција ка јаснијем прихватању сајбер простора као посебног домена у којем се могу предузимати и одбрамбена и офанзивна војна дејства. Од посебног значаја је *Сажетак Сајбер стратегије Министарства одбране* из 2018. године, који је изричит да ће Сједињене Државе „бранити унапред“ ради заустављања или деградације злонамерних активности на самом извору и пре него што оне погоде своје циљеве. Документ такође наглашава да Министарство одбране настоји да предухитри, порази или одврати злонамерне сајбер активности усмерене ка америчкој критичној инфраструктури и да ће, када је то потребно, деловати у и кроз сајбер простор ради ширих циљева националне одбране.[957]
Оваква логика је додатно потврђена у *2023 DoD Cyber Strategy Summary*, где се наглашава да је Министарство одбране од 2018. године спровело значајан број операција у сајбер простору кроз политику *defending forward*, односно активног ремећења злонамерне активности пре него што она досегне америчку домовину.[958]

На домаћем правном плану, америчка пракса офанзивних сајбер операција у иностранству добила је снажнији нормативни ослонац кроз 10 U.S.C. § 394, који овлашћује секретара одбране да, када је то прописно одобрено, развија, припрема и спроводи војне активности и операције у сајбер простору, укључујући и тајне војне активности у сајбер простору, ради одбране Сједињених

[954] Ney, “DOD General Counsel Remarks.”
[955] Blagojević, „Strategija nacionalne bezbednosti SAD iz 2025,” 79–103.
[956] International Institute for Strategic Studies, *Great-Power Offensive Cyber Campaigns: Experiments in Strategy – 2. US Cyber Campaigns* (London: IISS, 2022), 15–16.
[957] Department of Defense, *Cyber Strategy Summary* (Washington, DC: Department of Defense, 2018), 1–4.
[958] Department of Defense, *2023 DoD Cyber Strategy Summary* (Washington, DC: Department of Defense, September 2023), 1–4.

Држава и њихових савезника. Посебно је значајно што закон предвиђа да се такве активности у сајбер простору сматрају „традиционалним војним активностима“, што има важне последице по институционалну процедуру одобравања и конгресни надзор.[959] Додатну правну артикулацију овој пракси дао је и тадашњи генерални правни саветник Министарства одбране Пол Неј, који је 2020. године нагласио да DoD у правној анализи војних сајбер операција полази од постојећих правила међународног права, укључујући забрану употребе силе, забрану принудне интервенције и могућност самоодбране, али и од става да не постоји довољно уједначена пракса држава да би се закључило да су све не-консензуалне сајбер операције на туђој територији саме по себи забрањене међународним правом. Овај став је од изузетног значаја јер показује да амерички правни приступ офанзивним операцијама у иностранству није случајан, већ почива на свесно артикулисаном тумачењу међународног права које оставља релативно широк оперативни простор за деловање испод прага употребе силе.[960]

Најпознатији и историјски најзначајнији пример америчког сајбер напада на територији друге државе представља операција против иранског постројења за обогаћивање уранијума у Натанцу, у јавности позната преко злонамерног кода *Stuxnet*. Иако Сједињене Америчке Државе никада нису формално признале ову операцију, *Reuters* је још 2012. године, позивајући се на америчке изворе, известио да су сајбер напади на Иран „купили време“ и да је *Stuxnet* употребљен против главних иранских капацитета за обогаћивање уранијума.[961] У исто време, и стручна литература и каснији аналитички радови третирају *Stuxnet* као парадигматичан пример високо циљаног државног сајбер оружја које је изазвало физичке последице унутар критичне инфраструктуре друге државе.[962] Значај овог случаја превазилази питање саме атрибуције. Он је показао да сајбер напад може да буде употребљен као алтернатива класичном војном удару, као средство успоравања стратешки осетљивог програма, као инструмент принуде без отвореног преласка у оружани сукоб и као средство за производњу физичке штете без класичне војне инвазије. Управо је зато *Stuxnet* ушао у теоријску и правну литературу као прекретница у милитаризацији сајбер простора.[963]

Други важан пример, овога пута много јасније документован, јесу америчке сајбер операције против тзв. Исламске државе на територијама Ирака и Сирије. Секретар одбране Ештон Картер је у марту 2016. отворено изјавио да САД „иду у офанзиву против ISIL-а у Ираку и Сирији“ и да нема разлога да та организација слободно користи интернет за командовање, контролу, пропаганду и терор над становништвом на чијој територији делује.[964] Неколико месеци касније, у јавним наступима је додатно нагласио да је кампања против ISIL-а проширена на све домене, укључујући и сајбер, чиме је сајбер простор јасно постављен као саставни део савремених војних дејстава против недржавних актера.[965] Национални безбедносни архив је касније, на основу докумената прибављених путем FOIA поступка, објавио материјал који показује да је операција

[959] United States Code, “10 U.S.C. § 394. Authorities Concerning Military Cyber Operations.”
[960] Paul C. Ney, Jr., “DOD General Counsel Remarks at U.S. Cyber Command Legal Conference,” U.S. Department of Defense, March 2, 2020.
[961] *Reuters*, “Cyber-attacks ‘Bought Us Time’ on Iran: U.S. Sources,” June 1, 2012
[962] International Institute for Strategic Studies, *Great-Power Offensive Cyber Campaigns: Experiments in Strategy – 2. US Cyber Campaigns* (London: IISS, 2022), 33–34.
[963] International Institute for Strategic Studies, *Great-Power Offensive Cyber Campaigns: Experiments in Strategy – 2. US Cyber Campaigns* (London: IISS, 2022), 33–34.
[964] Ashton B. Carter, “Remarks by Secretary Carter at a Troop Event at Joint Base Lewis-McChord, Washington,” U.S. Department of Defense, March 4, 2016.
[965] Ashton B. Carter, “Remarks by Secretary Carter at the University of Oxford’s Blavatnik School of Government,” U.S. Department of Defense, September 7, 2016.

Glowing Symphony била изузетно сложена офанзивна сајбер кампања усмерена на ремећење пропаганде, логистике, ауторитета и контроле ISIS-а у сајбер простору. Документи које је Архив објавио показују и нешто још важније а то је да је сама операција унутар USCYBERCOM-а схваћена као преломни тренутак који је убрзао сазревање командних процедура, валидације циљева и међуагенцијске координације. Другим речима, *Glowing Symphony* није била само напад на противничку инфраструктуру, већ и институционални тест зрелости и оперативности саме Сајбер команде.[966] Посебан значај овог примера лежи у томе што је операција против ISIS-а показала да америчке сајбер операције у иностранству нису ограничене на физичко оштећење инфраструктуре. Напротив, циљеви су обухватали онемогућавање командовања, прекид комуникације, ремећење логистике, слабљење пропаганде и ограничавање способности организације да у дигиталном окружењу одржава контролу, шири утицај и привлачи нове следбенике[967]. На тај начин америчка пракса је показала да „сајбер напад" у савременом смислу не мора нужно значити уништење техничке опреме, већ може подразумевати и системско деградирање способности противника да користи дигиталну инфраструктуру као функционални продужетак војне и политичке моћи[968]. Ово је посебно важно у контексту овог истраживања, јер показује да је америчка пракса шире схватила офанзивно сајбер деловање: као ремећење екосистема противника, а не само као напад на конкретну машину или мрежу.[969]

Трећи значајан случај представља операција против *Internet Research Agency* у Санкт Петербургу током избора за Конгрес САД 2018. године. *Washington Post* је 2019. објавио да је америчка војска блокирала интернет приступ овој организацији на дан избора, а касније је исти лист известио и да је Доналд Трамп потврдио операцију против руских „тролова". Иако технички детаљи нису званично откривени, политичка порука ове акције била је јасна а то је да су САД употребиле офанзивне сајбер способности ради ремећења страног информационог мешања које је долазило са територије друге државе. Ово је нарочито важан пример зато што се не уклапа у класичан образац сајбер саботаже усмерене на критичну инфраструктуру. Уместо тога, реч је о офанзивном деловању усмереном на информационо-политички апарат страног актера, и то у контексту заштите изборног процеса и одбране демократских институција. Овде сајбер напад делује као средство против мешања, ограниченог одвраћања и политичког сигнала да страни утицај преко дигиталних платформи неће остати без одговора.[970]

Операције против Ирана 2019. године представљају још један важан пример америчке праксе. *Washington Post* је у јуну 2019. објавио да је председник Трамп одобрио офанзивни сајбер удар на иранске компјутерске системе коришћене за планирање напада на нафтне танкере у Персијском заливу. *Reuters* је у октобру исте године известио о још једној тајној операцији усмереној на иранске способности за ширење пропаганде после напада на саудијска нафтна постројења. Према тим извештајима, америчка страна је у оба случаја сајбер инструмент користила као ограничен,

[966] Michael Martelle, ed., "USCYBERCOM After Action Assessments of Operation *GLOWING SYMPHONY*," National Security Archive, January 21, 2020.
[967] Katarina Jonev, „Sajber terorizam i upotreba sajber prostora u terorističke svrhe," *Bezbednost* 58, br. 2 (2016): 206–222
[968] Ибид, 206-222
[969] International Institute for Strategic Studies, *Great-Power Offensive Cyber Campaigns: Experiments in Strategy – 2. US Cyber Campaigns* (London: IISS, 2022), 28–31.
[970] Ellen Nakashima, "Trump Confirms Cyberattack on Russian Trolls to Deter Them During 2018 Midterms," *Washington Post*, July 11, 2020.

пропорционалан и оперативно значајан одговор који треба да наметне цену противнику, а да избегне ширу кинетичку ескалацију.[971]

5.6. Правне и политичке контроверзе америчког приступа сајбер ратовању

Из претодно наведених примера може да се изведе неколико важних закључака о карактеру америчке праксе. Најпре, САД не прибегавају искључиво једном моделу офанзивног деловања. У појединим случајевима, као код *Stuxnet*-а, реч је о високо прецизном дејству против критичне инфраструктуре. У другим случајевима, као код операције против ISIS-а, циљ је деградација дигиталног екосистема једног недржавног противника. Код руске *Internet Research Agency* фокус је на ремећењу страних операција утицаја, док је код Ирана 2019. нагласак био на пропорционалном и ограниченом одговору у условима кризе. Према томе, амерички сајбер напади у иностранству нису униформна категорија, већ скуп различитих инструмената који се користе у зависности од циља, противника, правног оквира и процене ризика од ескалације. Управо та адаптабилност представља једну од најупадљивијих одлика америчке сајбер моћи.[972]

Међутим, оваква пракса производи озбиљне међународноправне дилеме. Основно питање тиче се односа између сајбер операција и државног суверенитета. Пол Неј је 2020. године нагласио да DoD узима у обзир принцип државног суверенитета над информационо-комуникационом инфраструктуром на њеној територији, али и да, по америчком ставу, не постоји правило по којем би сваки упад у туђу инфраструктуру у сајбер простору аутоматски представљао повреду међународног права. Он је истовремено указао да операција може, у зависности од околности, представљати употребу силе, забрањену интервенцију или, пак, меру која остаје испод тих прагова. Управо је у томе суштина америчке позиције: САД настоје да задрже релативно широк простор за не-консензуално деловање на туђој територији онда када таква дејства не достижу ниво употребе силе или принудне интервенције, а посебно када су усмерена на спречавање или ремећење текућих злонамерних активности.[973]

Овај став је значајан и зато што продубљује неслагања међу државама и у стручној литератури о томе где се тачно налази граница законитог деловања у сајбер простору. У домаћој литератури се с правом указује да специфичности сајбер простора нарочито отежавају приписивост, утврђивање одговорности државе и јасно разграничење између противправне интервенције, шпијунаже и других облика прикривеног деловања.[974]

Друга велика дилема односи се на однос између сајбер напада и других облика америчког деловања у страним мрежама, нарочито *hunt forward* операција. *Сажетак DoD сајбер стратегије из 2023. године* изричито наводи да САД од 2018. редовно раде са савезницима и партнерима на идентификовању рањивости у њиховим државним мрежама и да су те операције допринеле припремљености САД, јачању сајбер отпорности партнера и разобличавању непријатељских техника, укључујући и у Украјини. Такве активности, међутим, не треба поистоветити са

[971] Ellen Nakashima, "Trump Approved Cyber-Strikes Against Iranian Computer Database Used to Plan Attacks on Oil Tankers," *Washington Post*, June 22, 2019, Idrees Ali and Phil Stewart, "Exclusive: U.S. Carried Out Secret Cyber Strike on Iran in Wake of Saudi Oil Attack: Officials," Reuters, October 16, 2019.
[972] International Institute for Strategic Studies, *Great-Power Offensive Cyber Campaigns: Experiments in Strategy – 2. US Cyber Campaigns* (London: IISS, 2022), 15–16, 99–100.
[973] Paul C. Ney, Jr., "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference," U.S. Department of Defense, March 2, 2020.
[974] Љубомир Тинтор, „Међународна одговорност државе у дигиталном (сајбер) простору," у *Српски годишњак за међународно право* (Београд: Српско удружење за међународно право, 2023).

офанзивним нападом у ужем смислу речи, јер се оне најчешће спроводе уз сагласност државе домаћина. Ово разграничење је важно за научну тачност јер није свако америчко војно деловање у страним мрежама напад, баш као што није свака офанзивна сајбер активност исте правне природе. Управо зато је у анализи америчке праксе потребно разликовати консензуалне, партнерски засноване операције од не-консензуалних, тајних или полу-тајних операција усмерених на деградацију противничких способности на територији друге државе.[975]

Са критичког становишта, америчка пракса офанзивних сајбер операција у иностранству може се посматрати двојако. Са једне стране, она показује висок степен адаптације савремене војне силе условима дигиталног доба. Сједињене Државе су развиле инструмент који омогућава селективност, брзину, ограничену видљивост, прецизност и могућност управљања ескалацијом. Тај инструмент им омогућава да ометају нуклеарне програме, деградирају терористичке капацитете, штите изборне процесе и кажњавају државне или парадржавне актере, а да не прибегну класичном бомбардовању. Са друге стране, ова пракса објективно доприноси нормализацији прекограничног, не-консензуалног деловања у туђој дигиталној инфраструктури и тиме слабљењу класичног схватања територијалног суверенитета једне државе. Другим речима, америчка пракса је ефикасна са становишта државне моћи, али истовремено доприноси формирању нестабилнијег и правно нејаснијег међународног окружења, у коме све већи број држава може да покуша да позивањем на сличну логику оправда сопствене прекограничне сајбер операције.[976]

Сумирано посматрано, извођење сајбер напада САД на територијама других држава представља важну, али и правно најосетљивију димензију америчке националне моћи. Од *Stuxnet*-а, као широко приписане операције против иранске критичне инфраструктуре, преко јавно потврђених офанзивних кампања против ISIS-а у Ираку и Сирији, до ограничених дејстава усмерених против руских и иранских циљева, приметно је да Сједињене Државе сајбер простор третирају као инструмент прекограничне принуде, ремећења и стратешког обликовања окружења. У том смислу, америчка пракса не своди се само на „сајбер одбрану“, већ на пројекцију силе у дигиталном облику, често испод прага рата, али са последицама које су за међународне односе и право далеко од безначајних. Управо зато ово питање заузима централно место у расправама о савременој природи силе, суверенитета и ескалације у сајбер простору.[977]

5.7. Да ли је сајбер простор једини домен где САД морају да се бране?

У оквиру савременог америчког стратешког мишљења, питање да ли је сајбер простор једини домен одбране Сједињених Америчких Држава не може се разматрати изоловано, већ искључиво унутар ширег концепта вишедоменске одбране домовине, интегрисаног одвраћања и националне отпорности. Кратак и научно најпрецизнији одговор зато гласи: не, сајбер простор није једини домен у коме се Сједињене Америчке Државе морају бранити, али јесте домен у коме се одбрана најчешће одвија непрекидно, испод прага отвореног сукоба и у непосредном додиру са цивилним друштвом, критичном инфраструктуром и приватним сектором. Управо у томе лежи и разлог због кога се у савременој литератури и стратешким документима често стиче утисак да је сајбер постао

[975] Department of Defense, *2023 DoD Cyber Strategy Summary* (Washington, DC: Department of Defense, September 2023), 8–9.
[976] Paul C. Ney, Jr., “DOD General Counsel Remarks at U.S. Cyber Command Legal Conference,” U.S. Department of Defense, March 2, 2020.
[977] Владимир Ловић, „Сајбер простор као ново бојно поље: међународни односи, геополитика и безбедност у дигиталном добу,” *Megatrend revija* 22, бр. 1 (2025): 227–229.

„главни“ или чак „унутрашњи“ фронт америчке одбране. Међутим, ако се питање постави строго у стратешком и доктринарном смислу, амерички званични документи јасно показују да је реч о вишедоменском проблему. Сједињене Америчке Државе морају да се бране истовремено у сајбер домену, ваздушном, космичком, поморском, подморском, информационом и ракетном простору, а у ширем смислу и у сфери критичне инфраструктуре, ланаца снабдевања и опште националне отпорности.[978]

Основ за овакав закључак налази се већ у *Националној одбрамбеној стратегији САД из 2022. године*. Тај документ поставља као први приоритет „одбрану домовине“, а не одбрану искључиво сајбер простора. Истовремено, иста стратегија наглашава да су претње по домовину вишедоменске, те да их производе и нуклеарне претње, и крстареће ракете великог домета, и сајбер и информационе операције, и противсвемирске способности, и подморничко ратовање, као и сивозонске кампање. Другим речима, у америчком стратешком мишљењу држава је изложена комбинованом притиску различитих домена који све чешће делују истовремено и међусобно повезано. Отуда произилази да је нетачно сајбер простор посматрати као једини фронт америчке одбране, он јесте централни, али није усамљен.[979]

Постоји разлог због кога се сајбер често издваја. *2023 DoD Cyber Strategy Summary* изричито наводи да је први одбрамбени приоритет утврђен у NDS-у одбрана државе, „темпирана“ растућом вишедоменском претњом коју представља Народна Република Кина, а да ће се у сајбер домену Министарство одбране ослањати на спољa усмерене способности како би омогућило унутрашњу одбрану, односно откривало и ублажавало претње пре него што оне нашкоде америчком становништву. Овде се види оно што сајбер чини посебним: америчка одбрана у том домену не почиње на географској граници, нити тек у тренутку удара, већ у сталном откривању, ремећењу и умањивању претњи пре него што оне произведу последице унутар САД. Сајбер је, дакле, домен у коме се унутрашња и спољна одбрана највише преплићу. Али управо та формулација „растуће вишедоменске претње“ потврђује да ни сам Пентагон сајбер не третира као једино место одбране, већ као кључну компоненту много ширег одбрамбеног проблема.[980]

Ако се питање сагледа из перспективе ваздухопловно-ракетне одбране, постаје још јасније да сајбер није једини домен. *Missile Defense Review*, који је саставни део *NDS/NPR/MDR* пакета из 2022. године, наглашава да садашње и нове балистичке, крстареће и хиперсоничне ракете, као и мале беспилотне летелице, представљају растући и убрзани ризик за територију САД, америчке снаге у иностранству и савезнике. Документ говори о „интегрисаној одбрани домовине“ и захтева развој интегрисаних, интероперабилних и покретљивих система ваздушне и ракетне одбране, као и сензора, радара и система упозоравања способних да штите домовину од пуног спектра ваздушних и ракетних претњи. Посебно је важно што се у истом документу истиче да се граница између регионалне и *homeland defense* све више замагљује, управо због развоја домета, брзине и профила лета савремених оружја. То значи да америчка одбрана данас не може бити сведена на дигиталну одбрану мрежа; она мора бити и радарска, противракетна, ваздушна и сензорска, јер државу могу погодити и кинетичке претње великог домета.[981]

---

[978] Department of Defense, *2022 National Defense Strategy of the United States of America, Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review* (Washington, DC: Department of Defense, 2022), 8.
[979] Ибид, 8.
[980] Department of Defense, *2023 DoD Cyber Strategy Summary* (Washington, DC: Department of Defense, September 2023), 6–8.
[981] Department of Defense, *2022 National Defense Strategy of the United States of America, Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review* (Washington, DC: Department of Defense, 2022), 67–74.

Подједнако је важан и космички домен. *Space Force Doctrine Document–1* из 2025. године формулише тврдњу да су свемирске способности критичне и за здружене снаге и за амерички начин живота, као и да најмање половина критичне инфраструктуре САД зависи од свемира. У истом документу се наглашава да без свемира ланци уништења не могу да се затворе, операције постају мање синхронизоване, индикације и упозорења се сужавају, а слобода маневра здружених снага опада. У јануару 2026. године активирана је и компонента *SPACEFOR-NORTH* за потребе *USNORTHCOM-a*, са задатком да развија и обезбеђује свемирске способности за одбрану земље . То, заједно са мисијом NORAD-а и USNORTHCOM-а да бране државу „кроз све домене“, јасно показује да се америчка одбрана више не замишља без свемирских функција и њиховог непосредног повезивања са ваздушном, ракетном, сајбер и општом командно-информационом архитектуром. Према томе, чак и када би сајбер био савршено заштићен, америчка рањивост би и даље постојала у космосу, јер губитак свемирских способности може да непосредно ослаби и војну и цивилну отпорност државе.[982]

Осим тога, амерички стратешки документи упорно указују и на поморски и подморски правац угрожавања. *NDS* из 2022. године међу ризицима које Русија представља САД и њиховим савезницима изричито наводи подморничко ратовање, дугометне крстареће ракете и противсвемирске способности. Ово је важно јер показује да америчка одбрана не зависи само од заштите мрежа и сервера, већ и од надзора прилаза, подводне ситуационе свести, откривања лансирних платформи и заштите поморских линија комуникације. У стратешком смислу, САД су и даље океанска сила, што значи да је њихова одбрана неминовно и поморска. Сајбер може појачати поморску рањивост, рецимо компромитовањем навигације, логистике, лука или командно-комуникационих система, али не може да замени потребу за одбраном у морском и подморском домену.[983]

Када се питање анализира из шире перспективе информационог и друштвеног простора, види се још један разлог зашто сајбер није једини домен, иако је највидљивији. *NDS* из 2022. године не помиње само сајбер, већ и информационе операције као средство којим противници настоје да обликују кризу, друштвене поделе и политичко окружење без отвореног рата. То значи да америчка територија може да буде угрожена не само техничким продором у системе, већ и дезинформацијом, психолошким утицајем, подривањем поверења у институције и операцијама у сивој зони усмереним на демократију и друштвену кохезију. У том смислу, сајбер простор често служи као инфраструктура за информационе операције, али није исто што и информациона димензија сукоба. Напад на друштво не мора увек да се манифестује као хакерски инцидент већ може да се одвија и кроз алгоритамски појачану пропаганду, манипулацију публиком и ерозију јавног поверења. Зато је научно прецизније говорити о међусобно повезаним доменима и слојевима рањивости пре него о једном једином домену одбране.[984]

Још шира и, за савремено схватање безбедности, веома важна димензија односи се на критичну инфраструктуру, технологију и ланце снабдевања. *Национална безбедносна стратегија САД из 2022. године* наглашава да су критична инфраструктура — од електроенергетских система до цевовода — и друштва која на њој почивају све више дигитализовани и тиме рањиви на сајбер нападе. Али исти документ истовремено повезује безбедност са јачањем производних ланаца, 5G

[982] United States Space Force, *Space Force Doctrine Document–1: The Space Force* (Peterson Space Force Base, CO: STARCOM, April 3, 2025), 2–3.
[983] U.S. Northern Command, “Homeland Defense”
[984] Department of Defense, *2022 National Defense Strategy of the United States of America, Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review* (Washington, DC: Department of Defense, 2022), 6–8.

и напредних комуникација, стандардима, полупроводницима и отпорношћу мрежне инфраструктуре. Другим речима, америчка одбрана се данас не води само у оперативним доменима у ужем војном смислу, већ и у индустријској, технолошкој и инфраструктурној основи националне моћи. Управо зато је погрешно мислити да би заштита сајбер домена сама по себи решила проблем: ако су ланци снабдевања крхки, ако је производна база зависна, ако су телекомуникације и енергетика недовољно отпорне, онда је и одбрана домовине недовољна, чак и без класичног „сајбер напада“.[985]

Ову логику данас додатно потврђује чињеница да америчка држава све мање одваја „одбрану“ од „отпорности“. Изворно је зато сигурније ослонити се на извршни акт од 18. марта 2025. године, којим је наложено да се припремљеност државе и локалних заједница унапреди кроз инфраструктурно приоритизовање, стратешка улагања и већу отпорност на динамичне претње и опасности, укључујући и сајбер инциденте. То показује да се америчка одбрана више не подразумева само као функција оружаних снага, већ и као способност друштва и институција да издрже поремећај, ублаже последице и обнове функционисање. У том смислу, сајбер простор јесте централна оса отпорности, али није једина јер одбрана укључује и физичку инфраструктуру, јавне институције, снабдевање, цивилно управљање и социјалну кохезију.[986]

Ипак, и после свега наведеног, остаје суштинско питање: зашто онда управо сајбер толико доминира расправом? Одговор је у његовој специфичној природи. За разлику од већине других домена, сајбер омогућава да противник већ у мирнодопском периоду допре до унутрашњости америчког система, да циља војне и цивилне мреже истовремено, да се креће испод прага јасне употребе силе, да отежа атрибуцију, да производи последице у другим доменима, укључујући свемир, логистику, финансије, енергетику и командовање. Стратегија националне безбедности из 2022. године управо зато истиче да је ризик ненамерне ескалације нарочито висок у сајбер и космичком домену, због нејасних норми, сложених међудоменских интеракција и нових способности. То значи да сајбер није једини домен одбране, али јесте домен који има највећи капацитет да продре у све остале и да их учини истовремено рањивим.[987]

Из тога следи и закључак. Сједињене Америчке Државе се не бране само у сајбер простору, бране се у више међусобно зависних домена, при чему је сајбер истовремено посебан домен и попречни слој који прожима остале. Ваздухопловно-ракетна одбрана штити од кинетичких удара великог домета; свемирска одбрана чува кичму командовања, упозоравања и навигације; поморска и подморска одбрана штити прилазе и линије комуникације; информациона и друштвена одбрана штити политичку кохезију и демократску стабилност; технолошка и инфраструктурна отпорност штите способност државе да уопште функционише. Сајбер је, међутим, јединствен по томе што спаја унутрашње и спољно, мир и сукоб, државне и приватне актере, војно и цивилно. Управо зато би најтачнија формулација била следећа: сајбер простор није једини домен у коме САД морају да се бране, али је данас најсвеобухватнији домен, јер кроз њега постају рањиви и сви остали домени америчке моћи.[988]

Из наведеног произилази да савремена одбрана Сједињених Америчких Држава више не може да се разуме кроз традиционалну поделу на одвојене ратне просторе, нити кроз претпоставку да је

[985] Ibid., 6–8, 12–13.
[986] The White House, *National Security Strategy* (Washington, DC: The White House, October 2022), 13, 33.
[987]Donald J. Trump, “Achieving Efficiency Through State and Local Preparedness,” Executive Order, March 18, 2025.
[988] Department of Defense, *2022 National Defense Strategy of the United States of America, Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review* (Washington, DC: Department of Defense, 2022), 12–13.

територија државе сама по себи заштићена географским положајем. Напротив, америчка држава је данас изложена истовременом деловању претњи које долазе из више међусобно повезаних домена, при чему се граница између спољне и унутрашње безбедности све више брише. У таквим околностима, одбрана више није само и искључиво задатак војске, већ подразумева сарадњу државних институција, приватног сектора, технолошке индустрије, оператора критичне инфраструктуре и савезника. Управо зато је сајбер простор од посебног значаја, не јер је то једино место на коме Сједињене Америчке Државе морају да се бране, већ зато што представља домен кроз који рањивост једног система може брзо постати рањивост читаве државе.

Најпрецизније речено, сајбер простор у савременом америчком стратешком мишљењу није једини домен одбране, али јесте домен који најнепосредније повезује све остале облике угрожавања националне безбедности у јединствену, вишеслојну и трајну одбрамбену проблематику.[989]

[989] Veljko Blagojević, „Strategija nacionalne bezbednosti SAD iz 2025: kontinuitet i promene," *Međunarodna politika* 77, br. 1196 (2026): 96–99.

6. Сајбер ратовање у доктрини Народне Републике Кине

Разматрање и тумачење кинеске војне доктрине представља сложен задатак, пре свега зато што Народна Република Кина не излаже своје стратегијске ставове кроз јединствен и потпуно кодификован систем докумената какав је уобичајен у већини западних држава.[990] Уместо тога, кинеска стратегијска и доктринарна мисао обликује се кроз Беле књиге одбране, ставове војног и партијског и руководства, реформе Народноослободилачке војске Кине, као и кроз шири политички наратив о националном препороду и технолошкој модернизацији.[991] То је разлог зашто кинеска доктрина не може да се посматра као статичан скуп норми, већ као развојни оквир који се постепено прилагођава променама у међународном безбедносном окружењу.

Кинеско разумевање савременог рата треба тумачити као спој политичког усмерења, војне трансформације и технолошке амбиције. Посебно место у том оквиру заузима сајбер простор, који се у кинеском приступу не третира само као техничко окружење комуникације, већ као један од кључних домена будућег међудржавног сукоба.[992]

Савремена кинеска доктринарна мисао полази од становишта да се природа рата темељно мења под утицајем информационих технологија и да се тежиште оружаног сукоба постепено помера ка борби за информациону надмоћ.[993] У кинеском војном размишљању рат више није ограничен само на бојиште у физичком простору, већ се све више одвија у умреженом простору података, комуникација, алгоритама и система командовања. У кинеским анализама будућег оружаног сукоба наглашава се значај онога што западни аутори описују као сукоб „информационо заснованих система система“.[994] У Белој књизи одбране из 2019. године ова промена је формулисана посебно јасно, јер се наводи да „рат еволуира у правцу информатизованог ратовања, а паметни рат је на хоризонту“.[995] Та формулација показује да Кина информатизацију не посматра као завршен процес, већ као прелазну фазу ка новом облику ратовања у коме ће напредне технологије имати пресудну улогу. Овде је важно уочити да се сајбер операције у таквом концепту не јављају као споредна подршка, већ су једно од главних средстава за стицање предности на самом почетку и током самог конфликта. Нарушавање противникових комуникација, система командовања, прикупљања података и дигиталне координације у том оквиру постаје централни предуслов успеха у другим доменима рата.[996]

---

[990] Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, *People's Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), 1–2.
[991] Joel Wuthnow and M. Taylor Fravel, "China's Military Strategy for a 'New Era': Some Change, More Continuity, and Tantalizing Hints," *Journal of Strategic Studies* 46, no. 6–7 (2023): 1149–1150.
[992] Burke et al., *People's Liberation Army Operational Concepts*, 1–2, 9–10.
[993] Burke et al., *People's Liberation Army Operational Concepts*, 1.
[994] Ibid., 1, 9–10.
[995] State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing: Foreign Languages Press, 2019), 8; Masaaki Yatsuzuka, "China's 2019 National Defense White Paper and Intelligent Warfare," *NIDS Commentary* no. 105 (October 10, 2019): 2.
[996] Burke et al., *People's Liberation Army Operational Concepts*, 21–24.

Концепт „паметног рата“, односно интелигентизованог ратовања, представља следећу фазу у еволуцији кинеске војне мисли после информатизованог рата.[997] Иако овај концепт још увек није у потпуности доктринарно завршен, његово присуство у званичним и аналитичким текстовима указује на јасан правац кинеске војне трансформације. Према тумачењима релевантних аутора, под овим појмом подразумева се све интензивнија употреба вештачке интелигенције, квантних информација, big data, cloud computing-а и интернета ствари у војној сфери.[998] То значи да ће будући сукоби, према кинеском виђењу, зависити не само од традиционалне моћи, већ и од способности да се огромне количине података брзо прикупе, обраде и претворе у оперативну предност. На тај начин, брзина одлучивања и квалитет алгоритамске подршке добијају стратешки значај. Истовремено, то појачава важност сајбер домена, јер без стабилне, заштићене и офанзивно употребљиве мрежне инфраструктуре није могуће изградити систем интелигентизованог ратовања. Зато се може закључити да у кинеској доктрини сајбер ратовање постаје једна од основа будућег ратовања, а не само инструмент техничке заштите војних мрежа.[999]

Посебно је значајно то што кинески извори сајбер домен не третирају изоловано, већ у тесној вези са свемирским, електромагнетним и ширим информационим простором.[1000] У Белој књизи *China's Military Strategy* из 2015. године наглашава се да су „свемир и сајбер простор постали нови стратешки висови у конкуренцији свих страна“.[1001] Касније анализе показују да Кина будући рат све више посматра као вишедимензионално надметање у коме информациона контрола постаје услов за деловање у свим осталим доменима. Такво одређење има крупне доктринарне последице. Оно показује да Кина будући рат не посматра више као сукоб ограничен на копно, море и ваздух, већ као вишедимензионално надметање у коме информациона контрола постаје услов за деловање у свим осталим доменима. У том контексту, сајбер простор добија двоструку функцију. Он је истовремено подручје одбране националне инфраструктуре али и простор за активно обликовање услова под којима ће се сукоб одвијати. Управо због тога сајбер дејства у кинеском приступу треба разумети као интегрални део здружених операција. Њихова улога није само да заштите сопствени систем већ и да успоре, ослепе или дезорганизују противнички. Такав приступ је посебно важан у контексту међудржавног сукоба, јер упућује на припрему за рано постизање информационе доминације.[1002]

Бела књига одбране из 2019. године јасно истиче да су свемир и сајбер простор од кључног значаја за националну безбедност, економски развој и друштвени напредак Кине.[1003] Отуд није случајно што се у кинеском стратешком језику сајбер безбедност често повезује са ширим појмом државног суверенитета. Из угла кинеског политичког система, контрола над информацијама и мрежама не односи се само на војну заштиту, већ и на очување унутрашње стабилности и политичке безбедности режима.[1004] Управо ту се кинеско разумевање сајбер моћи разликује од уже западне техничке концепције сајбер безбедности. У кинеском случају, сајбер простор је

[997] Yatsuzuka, "China's 2019 National Defense White Paper and Intelligent Warfare," 2.
[998] Ибид., 2–3.
[999] Ибид, 2–3; Burke et al., *People's Liberation Army Operational Concepts*, 21–24.
[1000] State Council Information Office of the People's Republic of China, *China's Military Strategy* (Beijing: State Council Information Office, 2015), 8–9; Burke et al., *People's Liberation Army Operational Concepts*, 21–24.
[1001] State Council Information Office of the People's Republic of China, *China's Military Strategy*, 8–9.
[1002] Burke et al., *People's Liberation Army Operational Concepts*, 21–24; Joel Wuthnow and M. Taylor Fravel, "China's Military Strategy for a 'New Era'," 1151–1153.
[1003] State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing: Foreign Languages Press, 2019), 14–15.
[1004] International Institute for Strategic Studies, *Cyber Capabilities and National Power: China* (London: IISS, 2021), 95–97.

истовремено безбедносно, политичко, економско и идеолошко питање. То додатно објашњава зашто Кина последњих деценија улаже у развој сајбер способности улаже не само ради заштите мрежа, већ и због изградње шире националне моћи. За потребе анализе међудржавног сајбер ратовања то је веома важно, јер показује да кинеске сајбер способности треба посматрати као део опште државне стратегије, а не само као ужи војни инструмент.[1005]

У организационом смислу, најупечатљивији израз оваквог приступа представља формирање Стратешке помоћне снаге крајем 2015. године.[1006] Ова формација настала је у оквиру ширих војних реформи са циљем да интегрише способности у области свемира, сајбер операција, електронског ратовања и информационе подршке.[1007] Према релевантним анализама, њено стварање показује да је кинеско руководство настојало да створи структуру способну за деловање у условима високо интегрисаног, технолошки напредног сукоба.[1008] То значи да се сајбер способности више не развијају као изоловани сегмент, већ као део јединствене архитектуре информационог ратовања. Оваква институционална интеграција омогућава ефикаснију подршку здруженим операцијама, али и боље повезивање сајбер дејстава са свемирским и електромагнетним активностима. Са становишта доктрине, то представља важан корак ка моделу ратовања у коме се противнички оперативни систем настоји паралисати пре него што дође до одлучујуће кинетичке фазе. Зато се Стратешка помоћна снага може тумачити као институционални носилац кинеске тежње ка информационој надмоћи.[1009]

С тим је тесно повезан и шири циљ модернизације НОАК, који се у кинеским документима формулише као изградња војске „светске класе“ до средине XXI века.[1010] Ова формулација, која припада самом службеном кинеском стратешком наративу, није само политичка парола, већ израз амбиције да Кина изгради снаге способне за вођење рата у условима високе технолошке конкуренције. У том оквиру, модернизација не обухвата само наоружање, већ и организацију, командовање, обуку, логистику и примену нових технологија. Посебно место у том процесу заузимају дигитализација, умрежавање и аутоматизација војног система. Сајбер способности су зато двоструко важне: с једне стране, оне омогућавају унутрашњу информатизацију и повезивање снага, а с друге, представљају средство за стицање стратегијске предности у односу на спољног противника.[1011] У том смислу, сајбер ратовање у кинеској доктрини има и унутрашњу модернизацијску и спољну оперативну функцију. Управо та двострука улога чини га једним од централних елемената кинеске визије будућег рата.

Сајбер ратовање у кинеској доктрини не своди на заштиту информационих система, већ представља важан стуб шире стратегије ратовања међу државама. Кинески приступ полази од претпоставке да ће исход будућих конфликата све више зависити од способности да се контролишу токови информација, заштите сопствени системи и истовремено наруши

[1005] Ибид, 95–99.
[1006] Kevin L. Pollpeter, Michael S. Chase, and Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations* (Santa Monica, CA: RAND Corporation, 2017), 1, 13–14.
[1007] Ibid., 14, 27–29.
[1008] Elsa B. Kania and John K. Costello, “The Strategic Support Force and the Future of Chinese Information Operations,” *Cyber Defense Review* 3, no. 1 (2018): 109–112.
[1009] Pollpeter, Chase, and Heginbotham, *The Creation of the PLA Strategic Support Force*, 27–29; Kania and Costello, “The Strategic Support Force and the Future of Chinese Information Operations,” 115–117.
[1010] State Council Information Office of the People’s Republic of China, *China’s National Defense in the New Era*, 7–9; Joel Wuthnow and M. Taylor Fravel, “China’s Military Strategy for a ‘New Era’: Some Change, More Continuity, and Tantalizing Hints,” *Journal of Strategic Studies* 46, no. 6–7 (2023): 1150–1153.
[1011] Wuthnow and Fravel, “China’s Military Strategy for a ‘New Era’,” 1151–1153.

функционалност противничких мрежа и командних структура.[1012] Због тога се сајбер простор у кинеској војној мисли јавља као домен у коме се истовремено брани суверенитет, пројектује моћ и припремају услови за успех здружених операција. То значи да сајбер дејства имају и одбрамбену и потенцијално офанзивну функцију. У условима савременог међудржавног надметања, такав приступ Кини омогућава да сајбер способности користи као средство одвраћања, принуде и оперативне подршке. Кинеска доктрина показује да је сајбер ратовање прерасло ниво помоћне војне активности и постало један од носећих елемената савременог начина вођења рата.[1013]

6.1 Савремена кинеска војна доктрина: између одбрамбеног наратива и ширења оперативних способности

Важно је истаћи да кинеско руководство сопствени војни развој доследно представља као средство одвраћања и заштите суверенитета, уз тврдњу да је кинеска политика одбране по својој природи дефанзивна.[1014] Ипак, такво самоописивање не исцрпљује стварни садржај кинеске војне мисли. Савремена кинеска доктрина заснива се на концепту „активне одбране“, који, иако полази од стратегијског одбрамбеног оквира, истовремено наглашава јединство стратегијске одбране и офанзиве на оперативном и тактичком нивоу.[1015] Зато је прецизније закључити да кинеска војна стратегија није искључиво пасивно-одбрамбена, већ да садржи елементе проактивног деловања онда када руководство процени да су угрожени суверенитет, безбедност или развојни интереси државе. Међутим, формулацију о „превентивним ударима“ треба заменити прецизнијим тумачењем јер кинеска доктрина не легитимише отворено превентивни рат као опште начело, али оставља простор за рано, интензивно и офанзивно деловање у оквиру концепта активне одбране.[1016]

Истовремено, пораст кинеских војних способности доприноси неповерењу у стварне намере Пекинга. То се не односи само на убрзану модернизацију ракетних снага и далекометних прецизних система, већ и на развој хиперсоничних технологија, примену вештачке интелигенције у војној сфери и јачање интегрисаних способности противваздухопловне и противракетне одбране.[1017] Ови капацитети, посматрани у ширем стратешком контексту, превазилазе оквир уске територијалне одбране државе и повећавају способност Кине да врши одвраћање, принуду и пројекцију моћи у регионалном окружењу. Уз то, кинески документи изричито повезују војну модернизацију са заштитом интереса у „новим доменима“, безбедношћу прекоморских интереса и постепеним померањем тежишта са искључиво приобалне одбране ка комбинацији „одбране приобалних вода“ и „заштите отвореног мора“.[1018] Савремена кинеска доктрина, иако задржава снажан одбрамбени дискурс, истовремено развија инструменте који омогућавају деловање и изван непосредног територијалног оквира.

[1012] Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, *People's Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), 21–24.
[1013] State Council Information Office of the People's Republic of China, *China's Military Strategy* (Beijing: State Council Information Office, 2015), 8–9; Burke et al., *People's Liberation Army Operational Concepts*, 21–24.
[1014] State Council Information Office of the People's Republic of China, *China's Military Strategy* (Beijing: State Council Information Office, 2015), 1, 6.
[1015] Ибид., 6.
[1016] Joel Wuthnow and M. Taylor Fravel, "China's Military Strategy for a 'New Era': Some Change, More Continuity, and Tantalizing Hints," *Journal of Strategic Studies* 46, no. 6–7 (2023): 1149–1152.
[1017] State Council Information Office of the People's Republic of China, *China's Military Strategy*, 1–3; Joel Wuthnow and M. Taylor Fravel, "China's Military Strategy for a 'New Era'," 1150–1153.
[1018] State Council Information Office of the People's Republic of China, *China's Military Strategy*, 5–6.

Историјски посматрано, кинеска војна мисао прошла је пут од концепта народног, односно тоталног рата, ка доктрини локалних ратова у условима савремене технологије, затим локалних ратова у условима информатизације, а потом ка идеји „информатизованих локалних ратова“.[1019] Ова еволуција није била само терминолошка, већ је одражавала промену у схватању карактера будућег оружаног сукоба: од масовне, дуготрајне и територијално усмерене одбране ка бржим, технолошки интензивнијим и географски ограниченијим операцијама. Суштина њене војне стратегије налази у концепту „војних стратешких смерница“, које усмеравају оперативну доктрину, структуру снага и припреме за рат, али нису увек јавно и систематски објављене у облику засебних докумената.[1020] Та околност чини анализу кинеске доктрине сложенијом, али истовремено показује да је реч о кохерентном, мада мање транспарентном стратегијском моделу.

У том оквиру, посебно место заузима и сајбер димензија вођења сукоба. Кинески званични документи сајбер простор одређују као нови домен националне безбедности, док релевантне анализе показују да се он у све већој мери интегрише у шири концепт информатизованог и интелигентизованог ратовања. Сајбер способности за Кину немају само дефанзивну функцију заштите мрежа и инфраструктуре, већ имају и оперативну вредност у постизању информационе надмоћи, нарушавању противничких командно-информационих система и подршци здруженим операцијама у свемирском, електромагнетном и физичком домену. Управо због тога сајбер димензија у савременој кинеској доктрини није споредни елемент, већ један од кључних инструмената будућег међудржавног сукоба.[1021]

Савремену кинеску војну доктрину треба тумачити као динамичан и вишеслојан инструмент државне моћи. Њена званична реторика несумњиво наглашава дефанзивност, мирољубиви успон и одвраћање, али детаљнија анализа показује да Кина истовремено развија капацитете за офанзивно, брзо и технолошки интензивно деловање у конфликтима. Због тога је најпрецизније рећи да је реч о доктрини која је стратегијски представљена као одбрамбена, али оперативно и технолошки конципирана тако да омогући иницијативу, ескалациону контролу и заштиту кинеских интереса у све ширем географском и доменском простору.[1022]

6.2 Војне стратешке смернице као кључ за разумевање кинеске војне доктрине

Као што је већ истакнуто, разумевање савремене кинеске војне доктрине није могуће засновати на једном јавно доступном и систематизованом документу, већ захтева анализу више међусобно повезаних извора. Суштински елементи кинеске војне стратегије и доктрине морају да се траже у различитим врстама материјала, пре свега у белим књигама одбране, војним стратешким смерницама, извештајима Националног народног конгреса, документима партијских конгреса, као и у говорима и ауторитативним текстовима највиших кинеских званичника.[1023] Оваква структура извора представља један од главних разлога због којих се кинеска стратегија често оцењује као мање транспарентна у поређењу са стратегијским праксама западних држава.

[1019] State Council Information Office of the People's Republic of China, *China's Military Strategy*, 6; Joel Wuthnow and M. Taylor Fravel, "China's Military Strategy for a 'New Era'," 1149–1152.
[1020] Joel Wuthnow and M. Taylor Fravel, "China's Military Strategy for a 'New Era'," 1149–1150.
[1021] State Council Information Office of the People's Republic of China, *China's Military Strategy*, 8–9; International Institute for Strategic Studies, *Cyber Capabilities and National Power: China* (London: IISS, 2021), 90–92, 95–97.
[1022] Joel Wuthnow and M. Taylor Fravel, "China's Military Strategy for a 'New Era'," 1150–1153; State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing: Foreign Languages Press, 2019), 7–9.
[1023] Prashant Kumar Singh, *Changing Contexts of Chinese Military Strategy and Doctrine* (New Delhi: Institute for Defence Studies and Analyses, 2015), 15–16.

Међутим, та мања транспарентност не значи одсуство стратешке кохерентности, већ пре указује на другачији модел формулисања и саопштавања стратешких приоритета.

Посебан значај имају војне стратешке смернице, јер се у релевантној литератури управо оне сматрају најмеродавнијим показатељем кинеске војне стратегије.[1024] У кинеском војном појмовном систему, војна стратешка смерница садржи суштину стратегије, односно „принципе и планове за припремање и вођење целокупне ситуације рата".[1025] Због тога је научно оправдано посматрати ове смернице као кључни посредни оквир између политичког врха, процене безбедносног окружења и конкретног усмеравања организације, обуке, модернизације и употребе Народноослободилачке армије Кине. Оне не представљају само декларативна начела, већ полазну основу за развој оперативне доктрине, структуре снага и приоритета у припремама за рат. Управо зато западни аутори највећу пажњу посвећују тренуцима у којима долази до измене или прилагођавања ових смерница, јер се у таквим променама најјасније огледају дубљи заокрети у кинеском разумевању рата.[1026]

Суштина војних стратешких смерница најбоље се разуме ако се има у виду да оне одговарају на неколико основних питања: с ким ће Кина ратовати, где ће се рат водити, какав ће бити карактер тог рата и на који начин га треба водити.[1027] У том смислу, смернице обухватају процену стратешког окружења, идентификацију главних праваца претње, дефинисање највероватнијег облика оружаног сукоба, као и одређивање способности неопходних за деловање у таквим условима. Када се ови елементи сагледају као целина, постаје јасно да војне стратешке смернице имају функцију много ширу од политичког усмеравања. Оне, заправо, обликују визију будућег рата и представљају основу за планирање војне изградње. Зато није случајно што део литературе указује да кинески концепти „припреме за војну борбу" и његове „основне тачке" у великој мери одговарају ономе што се у западној литератури најчешће означава као војна доктрина.[1028]

Еволуција кинеске војне стратегије може да се пратити кроз развој ових стратешких смерница. Од оснивања Народне Републике Кине усвојено је девет војних стратешких смерница, али све нису имале подједнак значај.[1029] Највеће доктринарне промене везују се за смернице из 1956, 1980. и 1993. године, јер су означиле прелазак на нови начин разумевања будућег рата и, сходно томе, захтевале реорганизацију организације, обуке и оперативних концепата НОАК-а.[1030] Ове промене су подразумевале суштинску ревизију начина на који Кина замишља простор, карактер и темпо оружаног сукоба. Управо зато су оне у литератури препознате као прекретнице у развоју кинеске војне мисли. Кинеска доктрина није настала линеарно, већ кроз фазе у којима су се дубље промене јављале као одговор на нове претње, технолошке промене и померања у укупном међународном окружењу.[1031]

[1024] Joel Wuthnow and M. Taylor Fravel, "China's Military Strategy for a 'New Era': Some Change, More Continuity, and Tantalizing Hints," *Journal of Strategic Studies* 46, no. 6–7 (2023): 1148–1150; Prashant Kumar Singh, *Changing Contexts of Chinese Military Strategy and Doctrine*, 15–16.
[1025] Joel Wuthnow and M. Taylor Fravel, "China's Military Strategy for a 'New Era'," 1148.
[1026] Ibid., 1148–1150.
[1027] Ibid., 1148–1149; M. Taylor Fravel, "Shifts in Warfare and Party Unity: Explaining China's Changes in Military Strategy," *International Security* 42, no. 3 (2018): 37–38, 40.
[1028] Prashant Kumar Singh, *Changing Contexts of Chinese Military Strategy and Doctrine*, 15–16; Joel Wuthnow and M. Taylor Fravel, "China's Military Strategy for a 'New Era'," 1148–1149.
[1029] M. Taylor Fravel, "Shifts in Warfare and Party Unity: Explaining China's Changes in Military Strategy," *International Security* 42, no. 3 (2018): 37, 49.
[1030] Ibid., 37, 49; Joel Wuthnow and M. Taylor Fravel, "China's Military Strategy for a 'New Era': Some Change, More Continuity, and Tantalizing Hints," *Journal of Strategic Studies* 46, no. 6–7 (2023): 1154.
[1031] Fravel, "Shifts in Warfare and Party Unity," 37–38, 49.

Посебно место у овом процесу има концепт „припреме за војну борбу“, у оквиру којег значајну улогу има такозвана „основна тачка“. У појединим анализама управо се овај појам тумачи као најближи функционални еквивалент западном разумевању војне доктрине, јер означава основни, највероватнији и најрелевантнији облик оружаног сукоба за који се оружане снаге припремају.[1032] Другим речима, „основна тачка“ представља доктринарно језгро кинеске стратегије, пошто усмерава не само размишљање о природи будућег сукоба већ и читав процес организационог и технолошког прилагођавања оружаних снага. Она има и далеко ширу улогу од појединачне оперативне идеје: она служи као оријентир за развој способности, обуку, наоружање и структуру команде. Управо због тога промена „основне тачке“ у кинеском стратешком мишљењу најчешће указује на дубљу промену у самом разумевању рата.[1033]

Последња деценија XX века представљала је преломан тренутак у том процесу. Заливски рат из 1991. године снажно је утицао на кинеске војне теоретичаре и највише војно руководство, јер је указао на трансформацију вођења оружаних сукоба под утицајем високе технологије, прецизног наоружања, надмоћних система командовања, комуникација и управљања информацијама.[1034] Кинеска процена није била ограничена само на техничко дивљење војним способностима Сједињених Америчких Држава и њихових савезника, већ је водила ка закључку да се карактер будућег рата суштински мења. У том смислу, кинеско војно руководство је оценило да ратови будућности више неће бити искључиво дуготрајни и масовни копнени сукоби, већ ограничени, брзи и технолошки високо интензивни ратови на периферији државних интереса.[1035] Тај увид је имао далекосежне последице и покренуо је преиспитивање дотадашњих концепата и убрзао напуштање старијих образаца који су били дубоко везани за маоистичко наслеђе.[1036]

Из тог искуства проистекла је једна од најзначајнијих промена у кинеској војној доктрини. Војне стратешке смернице из 1993. године утврдиле су да „основна тачка“ припреме за војну борбу треба да буде усмерена на добијање локалних ратова у условима модерне, нарочито високе технологије.[1037] Ова формулација означила је дубок дисконтинуитет у односу на раније концепте засноване на дуготрајној одбрани унутрашњости и на наслеђу „Народног рата“. За разлику од претходних стратегија, нови приступ више није полазио од сценарија опште инвазије, већ од ограничених, регионално усмерених и технолошки захтевних сукоба.[1038] Ова промена је подстакла јачање заједничких операција, брже одлучивање, интеграцију различитих видова оружаних снага и наглашенију улогу информационе подршке у планирању и извођењу операција.[1039]

Усвајање смерница из 1993. године представљало је више од доктринарне ревизије: оно је означило почетак дугорочне трансформације НОАК-а у правцу технолошки модерније,

[1032] Prashant Kumar Singh, *Changing Contexts of Chinese Military Strategy and Doctrine* (New Delhi: Institute for Defence Studies and Analyses, 2015), 19–20, 35.
[1033] Ибид, 19–20, 35.
[1034] Fravel, “Shifts in Warfare and Party Unity,” 74–75.
[1035] Ибид, 74–75.
[1036] Ибид, 72–75.
[1037] Ибид 72–73.
[1038] Wuthnow and Fravel, “China’s Military Strategy for a ‘New Era’,” 1154–1155; Fravel, “Shifts in Warfare and Party Unity,” 72–73.
[1039] Wuthnow and Fravel, “China’s Military Strategy for a ‘New Era’,” 1154–1155; Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, *People’s Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), 3–4.

флексибилније и оперативно интегрисаније војне силе.[1040] Тај заокрет поставио је темеље за каснији прелазак ка информатизованом ратовању.

Народна Република Кина је постепено јачала и улогу нових домена, посебно космичког и сајбер простора, који су у наредним фазама кинеске војне мисли постали саставни део припреме за будуће сукобе.[1041] Анализа војних стратешких смерница не открива само еволуцију формалне стратегије, већ и дубљу трансформацију кинеског разумевања рата — од народног и масовног ка локалном, високотехнолошком, информатизованом и све израженије вишедоменском сукобу.[1042]

Доктрина „локалних ратова у високотехнолошким условима“ представљала је једну од првих великих прекретница у постхладноратовској еволуцији кинеске војне мисли. Њеним прихватањем тежиште је померено са маоистичког концепта дуготрајног „Народног рата“ ка схватању да ће будући сукоби бити ограничени по обиму, брзи по темпу и у великој мери одређени технолошком надмоћи, прецизношћу удара и способношћу координације различитих видова оружаних снага.[1043] Ова промена није била само оперативна већ и концептуална, јер је указала на напуштање старог модела ослањања на масовност, дубину територије и дуготрајно исцрпљивање противника. Уместо тога, кинеска војна мисао почела је да предност даје покретљивости, здруженим операцијама и употреби напредних система наоружања као главним условима успеха у савременом рату.[1044]

Даљи развој ове доктрине снажно је подстакнут кинеским анализама Заливског рата, а потом и сукоба на простору СР Југославије, Авганистана и Ирака. У тим оружаним сукобима кинески стратези препознали су растући значај информационе технологије, високопрецизних удара, умреженог командовања и способности да се противник паралише нарушавањем његових кључних система.[1045] Зато је током прве деценије XXI века дошло до постепеног преласка ка доктрини „локалних ратова у информатизованим условима“, у којој информација постаје кључни ресурс, а електронско ратовање, оперативна обмана и интегрисане здружене операције добијају централно место.[1046]

Беле књиге одбране из 2006, 2008. и 2010. године показују да је кинеско војно руководство информатизацију почело да посматра као покретач целокупне модернизације оружаних снага. Документ из 2006. године наглашава да механизација мора да се повеже са информатизацијом и да је циљ НОАК победа у локалним ратовима у условима информатизације.[1047] Бела књига из 2008. године додатно истиче стварање научног система обуке у условима информатизације и посебно наглашава обуку у сложеном електромагнетном окружењу, што показује да се информационо и електронско ратовање више није схватало као споредна способност, већ као

[1040] Burke et al., *People's Liberation Army Operational Concepts*, 3–4; Wuthnow and Fravel, "China's Military Strategy for a 'New Era'," 1154–1155.
[1041] State Council Information Office of the People's Republic of China, *China's Military Strategy* (Beijing: State Council Information Office, 2015), 8–9; Burke et al., *People's Liberation Army Operational Concepts*, 3–4, 21–24.
[1042] Burke et al., *People's Liberation Army Operational Concepts*, 3–4, 21–24; Wuthnow and Fravel, "China's Military Strategy for a 'New Era'," 1154–1155.
[1043] M. Taylor Fravel, "Shifts in Warfare and Party Unity: Explaining China's Changes in Military Strategy," *International Security* 42, no. 3 (2018): 72–75.
[1044] Ibid., 72–75.
[1045] Ibid., 74–78.
[1046] Information Office of the State Council of the People's Republic of China, *China's National Defense in 2006* (Beijing: Information Office of the State Council, 2006), 4–5; Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, *People's Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), 3–4.
[1047] Information Office of the State Council of the People's Republic of China, *China's National Defense in 2006*, 4–5.

саставни део будућег конфликта.[1048] У Белој књизи из 2010. године овај правац је јасније формулисан кроз став да је потребно окончати механизацију и остварити крупан напредак у информатизацији до 2020. године, уз развој здружених операција у условима информатизованог рата.[1049]

У том процесу постепено је сазревала и сајбер димензија вођења сукоба, која у кинеском приступу није третирана као изолована техничка област, већ као део ширег информационог ратовања. Развој информатизованих локалних ратова подразумевао је не само прикупљање и заштиту података већ и способност нарушавања противничких командно-информационих система, ометања комуникација, слабљења извиђачко-обавештајних капацитета и стицања информационе надмоћи.[1050] Због тога је нагласак на мрежној инфраструктури, електронском надметању и каснијем издвајању свемира и сајбер простора као нових стратешких висова представљао логичан наставак већ започете доктринарне трансформације.[1051] У том смислу, сајбер простор у кинеској војној мисли постепено прераста из помоћне техничке сфере у један од носећих домена будућег међудржавног сукоба.[1052]

Бела књига *China's Military Strategy* из 2015. године није означила потпуни раскид са ранијом доктрином, већ њену јаснију артикулацију и даљу надоградњу. У њој се истиче да рат убрзано еволуира ка информатизацији, да су интегрисане борбене снаге намењене операцијама „систем против система" које карактеришу информациона доминација, прецизни удари и здружене операције, као и да су свемир и сајбер простор постали нови стратешки висови надметања.[1053] На тај начин је кинеска доктрина коначно повезала технолошку модернизацију, информациону доминацију, прецизне ударе и вишедоменске операције у јединствен стратешки оквир. Због тога је најпрецизније закључити да је развој од „локалних ратова у високотехнолошким условима" ка „информатизованим локалним ратовима" представљао постепен, али суштински дубок процес у коме су информациона и сајбер компонента постале кључне за разумевање савремене кинеске војне доктрине.[1054]

6.3 Бела књига одбране из 2019. године и сајбер димензија кинеске војне доктрине

Бела књига одбране из 2019. године, *China's National Defense in the New Era*, представља значајан документ за разумевање савремене кинеске војне мисли, јер систематизује претходни ток војне модернизације и јасније дефинише улогу нових домена у будућем ратовању.[1055] Иако овај

[1048] Information Office of the State Council of the People's Republic of China, *China's National Defense in 2008* (Beijing: Information Office of the State Council, 2009), 14–15.
[1049] Information Office of the State Council of the People's Republic of China, *China's National Defense in 2010* (Beijing: Information Office of the State Council, 2011), 6, 11–12.
[1050] Burke et al., *People's Liberation Army Operational Concepts*, 21–24.
[1051] State Council Information Office of the People's Republic of China, *China's Military Strategy* (Beijing: State Council Information Office, 2015), 8–9; Burke et al., *People's Liberation Army Operational Concepts*, 21–24.
[1052] State Council Information Office of the People's Republic of China, *China's Military Strategy*, 8–9; Burke et al., *People's Liberation Army Operational Concepts*, 21–24.
[1053] State Council Information Office of the People's Republic of China, *China's Military Strategy* (Beijing: State Council Information Office, 2015), 5, 11.
[1054] Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, *People's Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), 3–4, 21–24; Joel Wuthnow and M. Taylor Fravel, "China's Military Strategy for a 'New Era': Some Change, More Continuity, and Tantalizing Hints," *Journal of Strategic Studies* 46, no. 6–7 (2023): 1154–1155.
[1055] State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing: Foreign Languages Press, 2019), 1–3.

документ не доноси потпуни раскид са концептуалним основама изложеним у Белој књизи из 2015. године, он их даље развија и смешта у шири оквир „нове ере“, у којој је модернизација НОАК-а непосредно повезана са дугорочним државним циљем изградње оружаних снага „светске класе“.[1056] У том смислу, Бела књига из 2019. године нема значај само као политичка декларација, већ и као показатељ начина на који кинеско руководство тумачи промене у савременом безбедносном и технолошком окружењу.[1057]

Посебна вредност овог документа за анализу сајбер аспекта ратовања лежи у чињеници што недвосмислено потврђује да се карактер рата мења под утицајем информационих технологија. У Белој књизи се истиче да „рат еволуира у правцу информатизованог ратовања, а паметни рат је на хоризонту“.[1058] Ова формулација представља један од најзначајнијих доктринарних елемената у савременој кинеској војној литератури, јер показује да информатизација више није схваћена као крајњи циљ, већ као прелазна фаза ка сложенијем облику ратовања заснованом на вештачкој интелигенцији, квантним информацијама, cloud инфраструктури и интензивној обради података.[1059] У таквом оквиру, сајбер простор добија суштински значај, пошто постаје један од кључних домена у којем се обезбеђује информациона надмоћ, штите сопствени системи и ремете противнички командно-информациони капацитети.[1060]

Бела књига из 2019. године истовремено потврђује да Кина сајбер простор не посматра као издвојену техничку област, већ као питање националне безбедности, економског развоја и друштвене стабилности. Документ наглашава да су свемир и сајбер простор међу кључним областима од стратешког значаја, што упућује на шире схватање ратовања као вишедоменског процеса.[1061] Треба истаћи да сајбер домен у кинеској доктрини има двоструку улогу. С једне стране, он је простор заштите критичне инфраструктуре, војних комуникација и информационе безбедности, док са друге стране, он представља оперативно поље у којем се могу нарушавати противнички системи командовања, комуникације, извиђања и обавештајне подршке.[1062] Управо зато је убрзање изградње сајбер капацитета представљено као један од приоритета у јачању укупне борбене ефикасности НОАК-а.[1063]

Овакво одређење сајбер простора треба посматрати и у контексту шире трансформације кинеске војне доктрине ка интегрисаним здруженим операцијама. Бела књига не говори о сајбер способностима изоловано, већ их доводи у везу са потребом развоја прецизних, мултидимензионалних и мултифункционалних интегрисаних операција.[1064] Сајбер капацитети се развијају као саставни део вишедоменске борбене архитектуре, у којој су повезани са

[1056] Ibid., 7–9; Joel Wuthnow and M. Taylor Fravel, “China’s Military Strategy for a ‘New Era’: Some Change, More Continuity, and Tantalizing Hints,” *Journal of Strategic Studies* 46, no. 6–7 (2023): 1150–1153.
[1057] Wuthnow and Fravel, “China’s Military Strategy for a ‘New Era’,” 1149–1153.
[1058] State Council Information Office of the People’s Republic of China, *China’s National Defense in the New Era*, 5; Masaaki Yatsuzuka, “China’s 2019 National Defense White Paper and Intelligent Warfare,” *NIDS Commentary* no. 105 (October 10, 2019): 2.
[1059] Yatsuzuka, “China’s 2019 National Defense White Paper and Intelligent Warfare,” 2–3.
[1060] Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, *People’s Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), 21–24; International Institute for Strategic Studies, *Cyber Capabilities and National Power: China* (London: IISS, 2021), 89–91.
[1061] State Council Information Office of the People’s Republic of China, *China’s National Defense in the New Era*, 12–13.
[1062] International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 89–91, 95–97; Burke et al., *People’s Liberation Army Operational Concepts*, 21–24.
[1063] State Council Information Office of the People’s Republic of China, *China’s National Defense in the New Era*, 12–13.
[1064] State Council Information Office of the People’s Republic of China, *China’s National Defense in the New Era*, 15–16; Burke et al., *People’s Liberation Army Operational Concepts*, 21–24.

електромагнетним, свемирским и класичним војним способностима. У том моделу, сајбер дејства немају само заштитну функцију, већ и шири значај за постизање иницијативе, брзине одлучивања и координације у условима савременог сукоба.[1065] Из тог разлога, сајбер димензија у кинеској војној мисли мора да се тумачи као један од кључних елемената будућег међудржавног ратовања, а не као споредна техничка подршка.[1066]

Бела књига одбране из 2019. године потврђује континуитет кинеске стратегије „активне одбране", али у исто време показује да се та стратегија све више ослања на нове технолошке домене и дигитализоване облике сукоба. Документ представља важну етапу у даљем доктринарном учвршћивању сајбер простора као једног од носећих стубова кинеске војне модернизације у ком се сајбер димензија више не појављује само као питање безбедности мрежа, већ као саставни део борбе за информациону надмоћ, оперативну предност и дугорочну трансформацију НОАК-а у војску способну за деловање у условима информатизованог и све израженије интелигентизованог рата.[1067]

Бела књига China's Law-Based Cyberspace Governance in the New Era, објављена у марту 2023. године, представља важан документ за разумевање начина на који Народна Република Кина нормативно уређује сајбер простор. Реч је о првој белој књизи која је у целини посвећена управо правно заснованом управљању сајбер простором, што показује да је Пекинг питање дигиталног окружења подигао на ниво посебно значајне државне политике.[1068] У документу се наглашава да је Кина током претходне деценије изградила релативно заокружен систем сајбер законодавства, који се ослања на интегрисани развој законодавства, спровођења права, правосуђа и правне едукације у дигиталној сфери.[1069] На тај начин, сајбер простор се више не третира само као техничка или економска област, већ као нормативно уређен простор у којем држава настоји да истовремено обезбеди безбедност, развој и поредак.

Посебан значај овог документа је и томе што јасно показује да Кина сајбер управљање заснива на широј логици суверенитета, контроле и институционалне стабилности. Званично тумачење наглашава да је до 2023. године у великој мери формиран нормативни оквир који обухвата, између осталог, закон о сајбер безбедности, закон о електронској трговини, закон о безбедности података, закон о заштити личних података и закон о борби против телекомуникационих и онлајн превара.[1070] Иако ова бела књига није војни документ, она је веома значајна за анализу сајбер конфликта, јер показује да Кина сајбер домен не посматра одвојено од државне безбедности, управљања подацима, контроле платформи и технолошког развоја. Правно уређење сајбер простора у кинеском случају делује као ослонац за јачање државне контроле над информационим токовима, дигиталном инфраструктуром и кључним технолошким ресурсима.[1071]

[1065] Burke et al., *People's Liberation Army Operational Concepts*, 21–24.
[1066] Burke et al., *People's Liberation Army Operational Concepts*, 21–24; Wuthnow and Fravel, "China's Military Strategy for a 'New Era'," 1151–1153.
[1067] State Council Information Office of the People's Republic of China, *China's National Defense in the New Era*, 12–13; Yatsuzuka, "China's 2019 National Defense White Paper and Intelligent Warfare," 2–3; Wuthnow and Fravel, "China's Military Strategy for a 'New Era'," 1150–1153.
[1068] State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era* (Beijing: State Council Information Office, 2023).
[1069] Ibid.
[1070] "China Sees Historical Achievements in Law-Based Cyberspace Governance: Official," *The State Council of the People's Republic of China*, March 17, 2023.
[1071] State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era* (Beijing: State Council Information Office, 2023).

Из перспективе проучавања сајбер ратовања, ова бела књига је значајна пре свега јер показује да Кина после 2019. године наставља да јача сајбер домен превасходно кроз правне, регулаторне и институционалне механизме, а не кроз јавно објављивање нове засебне војне доктрине. Документ из 2023. године потврђује да се сајбер простор у кинеском приступу схвата као јединствено поље у коме се преплићу безбедносна, правна, економска и политичка димензија. China's Law-Based Cyberspace Governance in the New Era није документ о сајбер ратовању у ужем смислу, али јесте важан извор за разумевање ширег институционалног оквира у коме Кина развија своје сајбер способности. Документ допуњује војно-стратешке документе тако што показује да се кинеска моћ у сајбер простору не гради само кроз војну модернизацију, већ и кроз правно уређење, контролу података и институционално учвршћивање државног ауторитета у дигиталној сфери.[1072]

После 2019. године Кина није јавно објавила нову самосталну војну стратегију посвећену искључиво сајбер ратовању. Уместо тога, њен приступ сајбер домену после Беле књиге China's National Defense in the New Era из 2019. године све више је артикулисан кроз документе усмерене на управљање сајбер простором, безбедност података и правно уређење дигиталног окружења, међу којима посебно место заузимају беле књиге Jointly Build a Community with a Shared Future in Cyberspace из 2022. и China's Law-Based Cyberspace Governance in the New Era из 2023. године. Пекинг сајбер питања све израженије третира као спој војне, безбедносне, правне и управљачке димензије, при чему се јавно формулисање сајбер политике после 2019. више помера ка нормативном и институционалном регистру него ка експлицитној војној доктрини.[1073]

6.4 Значај заштите од сајбер напада и утицаја са интернета у НР Кини

У кинеском стратегијском и безбедносном размишљању, заштита од сајбер напада не посматра се као уско техничко питање, већ као саставни део очувања државне безбедности, економског развоја и друштвене стабилности. Још у Белој књизи *China's Military Strategy* из 2015. године истакнуто је да је сајбер простор постао нови домен националне безбедности, док је у Белој књизи *China's National Defense in the New Era* из 2019. године тај став додатно учвршћен оценом да сајбер безбедност представља озбиљну претњу за Кину.[1074] То показује да Пекинг сајбер нападе не доживљава само као опасност по информационе системе, већ и као ризик за функционисање државе у целини. У таквом приступу, угрожавање мрежа, података, командних система и критичне инфраструктуре може имати последице које превазилазе технички ниво и задиру у сферу политичке стабилности, јавног поретка и укупне националне моћи.[1075]

[1072] State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era* (Beijing: State Council Information Office, 2023); State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing: Foreign Languages Press, 2019).
[1073] State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing: Foreign Languages Press, 2019); State Council Information Office of the People's Republic of China, *Jointly Build a Community with a Shared Future in Cyberspace* (Beijing: State Council Information Office, 2022); State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era* (Beijing: State Council Information Office, 2023).
[1074] State Council Information Office of the People's Republic of China, *China's Military Strategy* (Beijing: State Council Information Office, 2015), 8; State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing: Foreign Languages Press, 2019), 13.
[1075] State Council Information Office of the People's Republic of China, *China's National Defense in the New Era*, 13; International Institute for Strategic Studies, *Cyber Capabilities and National Power: China* (London: IISS, 2021), 95–97.

Због тога заштита од сајбер напада у кинеском моделу обухвата много више од класичне мрежне одбране једне државе. Она подразумева развој способности за рано откривање и сузбијање мрежних упада, јачање сајбер одбране, заштиту информационе и комуникационе инфраструктуре, али и очување такозваног сајбер суверенитета.[1076] У војном контексту, ова логика је непосредно повезана са способношћу државе да одржи командовање, комуникације и координацију у условима кризе или сукоба. Кина зато сајбер заштиту посматра као предуслов за ефикасност здружених операција и отпорност државе у ширем вишедоменском надметању. Овакво схватање нарочито добија на значају у ери информатизованог ратовања, у којој рањивост дигиталних система може директно утицати на исход међудржавног сукоба.[1077]

Међутим, у кинеском случају питање заштите не односи се само на сајбер нападе у ужем смислу, већ и на утицаје који се путем интернета испољавају у информационој, идеолошкој и политичкој сфери. Релевантне анализе указују да је кинеско руководство дуго придавало посебан значај такозваној „content security", односно контроли политички осетљивих, субверзивних или дестабилизујућих садржаја у дигиталном простору.[1078] То произлази из ширег схватања државне безбедности, у коме интернет није само комуникациона инфраструктура, већ и простор обликовања јавног мњења, друштвене мобилизације и потенцијалног спољног утицаја. Управо зато Кина правно и институционално повезује борбу против сајбер криминала, заштиту података, регулисање платформи, алгоритама и онлајн садржаја са очувањем укупног друштвеног поретка. Бела књига China's Law-Based Cyberspace Governance in the New Era из 2023. године јасно показује да Пекинг настоји да истовремено развија интернет и јача механизме контроле, полазећи од начела да се развој и безбедност у сајбер простору морају остваривати упоредо.[1079]

Сагледано у целини, значај заштите од сајбер напада и утицаја са интернета у Кини лежи у чињеници да се оба феномена третирају као повезане димензије истог безбедносног изазова. Са једне стране, неопходно је заштитити мреже, податке, инфраструктуру и војне системе од спољних упада и техничке дестабилизације док са друге, држава настоји да контролише проток информација и ограничи оне утицаје из сајбер простора које доживљава као претњу политичкој, идеолошкој и социјалној стабилности.[1080] Овај спој техничке, правне, политичке и безбедносне димензије представља једно од обележја кинеског приступа сајбер простору. Управо зато се у кинеској стратегијској култури заштита од сајбер напада и утицаја са интернета не може разумети одвојено од концепата државног суверенитета, информационе контроле и отпорности у условима савременог међудржавног надметања.[1081]

[1076] State Council Information Office of the People's Republic of China, *China's National Defense in the New Era*, 13; International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 89–91.
[1077] Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, *People's Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), 21–24; State Council Information Office of the People's Republic of China, *China's National Defense in the New Era*, 5, 13.
[1078] International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 95–97.
[1079] State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era* (Beijing: State Council Information Office, 2023), 2–3, 6, 10–11; "China Sees Historical Achievements in Law-Based Cyberspace Governance: Official," *The State Council of the People's Republic of China*, March 17, 2023.
[1080] International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 95–97; State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era*, 2–3, 10–11.
[1081] State Council Information Office of the People's Republic of China, *China's Military Strategy*, 8; State Council Information Office of the People's Republic of China, *China's National Defense in the New Era*, 13; State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era*, 2–3, 10–11; International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 89–97.

Кроз дужи историјски развој кинеске државности, безбедност је често схватана не само као одбрана граница, већ и као способност државе да благовремено уочи, прати и неутралише унутрашње и спољне ризике.

Савремени кинески систем надзора зато не треба тумачити као потпуно нов феномен, већ као технолошки модернизован израз старије политичке логике у којој су контрола информација, рано упозоравање и управљање друштвеним ризицима чврсто повезани са националном безбедношћу.[1082] Овакво разумевање безбедности нарочито је добило на значају са дигитализацијом друштва, јер је интернет отворио нове могућности не само за економски развој, већ и за ширење утицаја, идеја и облика комуникације које држава није желела да препусти неконтролисаном развоју.[1083]

После смрти Мао Це Тунга и почетка политике реформи и отварања, кинеска држава није напустила механизме контроле, већ их је постепено прилагодила новим друштвеним и технолошким околностима. Модернизација привреде и јачање веза са иностранством довели су до шире употребе телекомуникационе и рачунарске технологије, што је истовремено отворило нови простор за модернизацију државних безбедносних капацитета. У том процесу је безбедносни апарат постајао све више ослоњен на информационе системе, базе података и технике обраде података, а касније и на дигиталне механизме надзора. Посебно је важно исправно уочити да је 1983. године основано Министарство државне безбедности, док је Министарство јавне безбедности наставило да постоји као кључни полицијски орган а каснији развој њихових капацитета допринео је јачању институционалне основе за савремени надзорни систем.[1084] Тиме је створен амбијент у коме је контрола све мање зависила искључиво од класичних полицијских метода, а све више од интеграције обавештајних, административних и технолошких инструмената. Овај процес је временом довео до тога да надзор у Кини постане не само средство репресије, већ и механизам управљања сложеним, брзо умреженим и технолошки трансформисаним друштвом.[1085]

Интернет је у Кини формално добио пуну функционалну повезаност са глобалном мрежом 20. априла 1994. године, а држава је од самог почетка настојала да његов развој усмерава тако да истовремено служи модернизацији и очувању политичког поретка. Кинеска званична документа касније су то и експлицитно формулисала, наглашавајући да питање изградње, коришћења и управљања интернетом непосредно утиче на економски развој, државну безбедност, друштвену хармонију и суверенитет.[1086] У том двоструком приступу налази се суштина кинеске интернет политике. Интернет је прихваћен као средство развоја државе, али истовремено и као простор који мора да буде подложан политичкој и правној контроли. Како се број корисника повећавао, кинеске власти су све јасније уочавале да дигитални простор може да постане канал за неконтролисан проток информација, идеја и утицаја из иностранства. Због тога је крајем

[1082] Lokman Tsui, "The Panopticon as the Antithesis of a Space of Freedom: Control and Regulation of the Internet in China," *China Information* 17, no. 2 (2003): 65–67; Rebecca MacKinnon, "China's Networked Authoritarianism," *Journal of Democracy* 22, no. 2 (2011): 32–35.
[1083] MacKinnon, "China's Networked Authoritarianism," 35–38.
[1084] Alex Joske, "State Security Departments: The Birth of China's Nationwide State Security System," *Deserepi: Studies in Chinese Communist Party External Work* 0 (2023): 3–5; John Costello, "China's Intelligence Agencies," written testimony before the U.S.-China Economic and Security Review Commission, June 9, 2016, 1–2.
[1085] Edward Schwarck, "Intelligence and Informatization: The Rise of the Ministry of Public Security in Intelligence Work in China," *The China Journal* 80 (2018): 1–7.
[1086] Information Office of the State Council of the People's Republic of China, *The Internet in China* (Beijing: Information Office of the State Council, 2010), 1–2.

деведесетих година покренут пројекат *Golden Shield* под окриљем Министарства јавне безбедности, са циљем изградње ширег информационог и безбедносног система за потребе полицијског рада, праћења и управљања информацијама.[1087] У западној и академској литератури појам *Great Firewall* касније се усталио као назив за ужи скуп техничких и регулаторних механизама филтрирања, блокирања и контроле прекограничног интернет саобраћаја, који се најчешће посматра као део ширег система надзора и цензуре.[1088] Отуда је прецизније говорити о Golden Shield-у као општем оквиру полицијско-информационе контроле, а о Great Firewall-у као о његовој највидљивијој интернетској и цензорској компоненти.[1089]

Из те перспективе, „Велики заштитни интернет зид“ не треба посматрати искључиво као инструмент политичке цензуре, већ и као део шире националне архитектуре сајбер безбедности и контроле информационог простора. Његова функција није ограничена на блокирање појединих садржаја, већ обухвата и филтрирање, надзор, усмеравање интернет саобраћаја, подршку идентификацији ризичних активности и јачање капацитета државе да управља дигиталним окружењем. Кинески модел повезује заштиту од спољних сајбер претњи са заштитом од онлајн политичких и идеолошких утицаја, па се техничка безбедност мрежа и контрола садржаја појављују као међусобно испреплетене димензије истог државног пројекта. Управо зато је у литератури кинески приступ често описиван као облик „умреженог ауторитаризма“, у коме интернет није одбачен, већ укључен у систем контролисаног развоја, надгледања и селективне отворености. За анализу сајбер аспекта ово је од посебне важности, јер показује да Кина не раздваја оштро питања сајбер одбране, контроле информација и политичке безбедности. Напротив, она их посматра као јединствену целину у којој су заштита од сајбер напада, отпорност државне инфраструктуре и ограничавање спољних утицаја део исте стратегије очувања суверенитета и унутрашње стабилности.

У литератури се пројекат *Golden Shield* често означава и као *National Public Security Work Informational Project*, односно као широки државни програм информатизације и умрежавања структура јавне безбедности у Народној Републици Кини.[1090] Његов значај не треба сводити искључиво на интернет цензуру, јер је од самог почетка био замишљен као много шири безбедносно-информациони оквир. У тај оквир спадају и системи за управљање безбедносним информацијама, криминалистичке базе података, системи за контролу уласка и изласка из земље, платформе за надзор, као и информациони системи намењени управљању саобраћајем и полицијском координацијом.[1091] Прецизније је говорити о *Golden Shield*-у као о државном пројекту дигиталне интеграције у области јавне безбедности, а не само као о механизму блокирања интернет садржаја. Његова суштина лежала је у повезивању прикупљања података, надзора, анализе и бржег одлучивања унутар безбедносног апарата. На тај начин је технолошка

[1087] Greg Walton, *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China* (Montreal: International Centre for Human Rights and Democratic Development, 2001), 5–7; Garden Networks, *Breaking Through the "Golden Shield"* (New York: Open Society Institute, 2005), 1–2.
[1088] Garden Networks, *Breaking Through the "Golden Shield"*, 1–2.
[1089] Garden Networks, *Breaking Through the "Golden Shield"*, 1–2; Sonali Chandel et al., "The Golden Shield Project of China: A Decade Later—An In-Depth Study of the Great Firewall," *Asia-Pacific Journal of Information Technology and Multimedia* 8, no. 2 (2019): 1–3.
[1090] Sonali Chandel, Zang Jingji, Yu Yunnan, Sun Jingyao, and Zhang Zhipeng, "The Golden Shield Project of China: A Decade Later—An In-Depth Study of the Great Firewall," *Asia-Pacific Journal of Information Technology and Multimedia* 8, no. 2 (2019): 2–3.
[1091] Greg Walton, *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China* (Montreal: International Centre for Human Rights and Democratic Development, 2001), 13–17; Sonali Chandel et al., "The Golden Shield Project of China," 2–3.

инфраструктура постала један од носећих елемената модернизације кинеске државне контроле.[1092]

Према званичном образложењу и каснијим тумачењима у литератури, пројекат је требало да допринесе ефикаснијем одржавању јавног поретка, сузбијању криминала и јачању способности државе да управља безбедносним ризицима. Међутим, у пракси је његов развој био тесно повезан и са филтрирањем, надзором и ограничавањем протока информација које су власти сматрале политички осетљивим или друштвено штетним.[1093] Управо због тога је у западној и академској литератури посебну пажњу привукао његов највидљивији сегмент — систем техничких и регулаторних механизама који је постао познат под називом *Great Firewall*. Важно је, међутим, нагласити да *Great Firewall* није исто што и *Golden Shield* у целини, већ његова најпознатија интернетска компонента, усмерена на филтрирање, блокирање и контролу прекограничног интернет саобраћаја.[1094] Ова разлика је од значаја за научну анализу, јер показује да је кинески модел дигиталне контроле истовремено и полицијски, и административни, и технички. У том смислу, цензура онлајн садржаја представља само један део ширег система безбедносног управљања информационим простором.[1095]

Један од кључних разлога за настанак и развој овог система било је уверење кинеског државног врха да интернет, поред развојних могућности, носи и озбиљне ризике по идеолошку контролу, политичку стабилност и државни суверенитет. После догађаја из 1989. године и у условима постхладноратовских геополитичких промена, кинеско руководство је посебно осетљиво приступало питању контроле јавног наратива и спречавања ширења садржаја који би могли да подстакну организовано незадовољство или спољни утицај.[1096] Са ширењем интернета та брига је добила нову димензију, јер је дигитални простор отворио могућност брже циркулације информација, алтернативних тумачења политичких догађаја и транснационалне комуникације ван непосредне контроле државе. Отуда је Golden Shield развијан не само као реакција на техничке безбедносне изазове, већ и као средство очувања унутрашње стабилности у условима дигиталне повезаности. Поред идеолошке и политичке димензије, пројекат је имао и економско-стратешку улогу, јер је омогућио Кини да интернет развија под условима који су били компатибилни са јачањем домаћих платформи, регулаторном контролом и заштитом технолошког суверенитета.[1097]

Имплементација овог пројекта одвијала се постепено, кроз фазно јачање мрежне инфраструктуре, база података, стандарда и процедура унутар система јавне безбедности. Прва фаза обухватала је изградњу основне комуникационе мреже, развој апликативних база и успостављање платформи за размену података, док је каснији период био обележен унапређењем терминалне

[1092] Rebecca MacKinnon, "China's Networked Authoritarianism," *Journal of Democracy* 22, no. 2 (2011): 32–40.
[1093] Richard Clayton, Steven J. Murdoch, and Robert N. M. Watson, "Ignoring the Great Firewall of China," in *Privacy Enhancing Technologies*, ed. George Danezis and Philippe Golle (Berlin: Springer, 2006), 20–23.
[1094] Ngoc Phong Hoang, Arian Akhavan Niaki, Jakub Dalek, Michalis Polychronakis, Phillipa Gill, and Nick Feamster, "How Great Is the Great Firewall? Measuring China's DNS Censorship," in *30th USENIX Security Symposium (USENIX Security 21)* (Berkeley, CA: USENIX Association, 2021), 3381–3385.
[1095] Raymond Rambert, Zachary Weinberg, Diogo Barradas, and Nicolas Christin, "Chinese Wall or Swiss Cheese? Keyword Filtering in the Great Firewall of China," in *Proceedings of the Web Conference 2021* (New York: ACM, 2021), 472–475.
[1096] Clayton, Murdoch, and Watson, "Ignoring the Great Firewall of China," 20–23.
[1097] Hoang et al., "How Great Is the Great Firewall?," 3381–3387; Rambert et al., "Chinese Wall or Swiss Cheese?," 472–478.

инфраструктуре, стандардизацијом рада и даљом интеграцијом надзорних способности.[1098] Тиме је *Golden Shield* временом прерастао оквир класичног полицијског информатичког пројекта и постао симбол кинеског поимања дигиталног суверенитета. Његов значај лежи управо у томе што спаја техничку заштиту, институционални надзор и политичко управљање интернет простором у јединствен механизам државне контроле. Кина заштиту од сајбер претњи и управљање информационим утицајима не посматра одвојено, већ као део исте безбедносне логике.[1099]

Надовезујући се на претходно разматрање пројекта *Golden Shield* и ширег кинеског модела дигиталне контроле, потребно је ближе објаснити на који начин функционише његова најпознатија интернетска компонента, односно *Great Firewall*. Његова суштина не исцрпљује се у једноставном „блокирању сајтова“, већ у споју правних, административних и техничких механизама који заједно омогућавају усмеравање и ограничење протока информација у кинеском дигиталном простору.[1100] Прецизније је *Great Firewall* посматрати као вишеслојни социотехнички систем, а не само као низ изолованих техничких баријера. У његовом функционисању подједнако су важни закони и подзаконски акти, обавезе интернет посредника и телекомуникационих оператера, механизми саморегулације платформи, али и мрежни алати за филтрирање и преусмеравање саобраћаја.[1101] Такав модел омогућава држави да цензуру не спроводи искључиво централизовано, већ и кроз сарадњу са приватним актерима, што знатно повећава његову ефикасност и отпорност. Због тога је „Велики заштитни интернет зид“ истовремено и техничка инфраструктура и институционални механизам управљања дигиталним простором који представља један од најважнијих инструмената преко којих Кина повезује сајбер безбедност, контролу информација и очување политичке стабилности.

На техничком плану, издваја се неколико основних механизама на којима почива рад овог система. Први је блокирање IP адреса, којим се корисницима унутар Кине онемогућава приступ одређеним серверима или интернет сервисима.[1102] Други је DNS филтрирање, односно активирање лажних или нетачних DNS одговора, чиме се корисник преусмерава ка неисправној адреси или добија привид да тражени домен не постоји.[1103] Трећи механизам обухвата филтрирање URL захтева и кључних речи, нарочито у нешифрованом HTTP саобраћају, где систем може да детектује осетљиве термине и реагује прекидањем везе.[1104] У ранијим фазама развоја Great Firewall-a то је често чињено убацивањем лажних TCP reset пакета, који обе стране у комуникацији наводе да прекину везу.[1105] Четврти механизам односи се на инспекцију пакета и саобраћајних образаца, што омогућава прецизније откривање садржаја, типова протокола и понашања која систем препознаје као непожељна или осетљива.[1106] Важно је нагласити да ови механизми не делују одвојено, већ се међусобно допуњују, тако да се филтрирање у пракси често

[1098] Clayton, Murdoch, and Watson, “Ignoring the Great Firewall of China,” 20–23; Hoang et al., “How Great Is the Great Firewall?,” 3381–3387; Rambert et al., “Chinese Wall or Swiss Cheese?,” 472–478.
[1099] MacKinnon, “China’s Networked Authoritarianism,” 32–46; Walton, *China’s Golden Shield*, 13–17.
[1100] Rebecca MacKinnon, “China’s Networked Authoritarianism,” *Journal of Democracy* 22, no. 2 (2011): 32–40.
[1101] Ibid., 35–40.
[1102] Richard Clayton, Steven J. Murdoch, and Robert N. M. Watson, “Ignoring the Great Firewall of China,” in *Privacy Enhancing Technologies*, ed. George Danezis and Philippe Golle (Berlin: Springer, 2006), 20–23.
[1103] Ngoc Phong Hoang, Arian Akhavan Niaki, Jakub Dalek, Michalis Polychronakis, Phillipa Gill, and Nick Feamster, “How Great Is the Great Firewall? Measuring China’s DNS Censorship,” in *30th USENIX Security Symposium (USENIX Security 21)* (Berkeley, CA: USENIX Association, 2021), 3381–3385.
[1104] Zachary Weinberg, Diogo Barradas, and Nicolas Christin, “Chinese Wall or Swiss Cheese? Keyword Filtering in the Great Firewall of China,” in *Proceedings of the Web Conference 2021* (New York: ACM, 2021), 472–475.
[1105] Clayton, Murdoch, and Watson, “Ignoring the Great Firewall of China,” 20–23.
[1106] Hoang et al., “How Great Is the Great Firewall?,” 3381–3387; Weinberg, Barradas, and Christin, “Chinese Wall or Swiss Cheese?,” 472–478.

заснива на њиховој комбинованој примени. Та слојевитост чини систем технички флексибилним и прилагодљивим различитим врстама интернет садржаја и комуникације.

Истовремено, развој интернета и ширење шифрованог саобраћаја натерали су кинески систем цензуре да се прилагоди новим условима. Савремена истраживања показују да класични модели филтрирања нешифрованог HTTP саобраћаја и даље постоје, али да су временом добили нове допуне. Тако је уочено да Great Firewall не врши масовну декрипцију HTTPS саобраћаја, али да користи друге начине контроле, као што су цензура заснована на SNI пољу у TLS комуникацији, блокирање одређених домена и анализа саобраћајних образаца.[1107] Поред тога, новија истраживања показала су да је од новембра 2021. године систем развио и способност пасивног препознавања појединих потпуно шифрованих протокола на основу њихових саобраћајних обележја, чак и онда када не може да се непосредно прочита садржај порука.[1108] То значи да Great Firewall више не зависи искључиво од класичне садржинске цензуре, већ све више користи технике препознавања образаца и протоколског понашања. На тај начин је кинески модел филтрирања прешао са једноставнијег блокирања садржаја на напреднији режим детекције, класификације и селективног прекида сумњивих комуникација. Ова технолошка адаптација показује да је реч о систему који се континуирано унапређује у складу са променама у дигиталном окружењу.

Сама ефикасност овог система предмет је бројних расправа у академској и стручној литератури. Несумњиво је да је Great Firewall био и остао веома успешан у ограничавању приступа великом броју страних сервиса, у обликовању домаћег информационог окружења и у наметању високог степена контроле над прекограничним интернет саобраћајем.[1109] Његова стварна снага, међутим, не почива само на техничкој способности да блокира или прекине појединачне везе, већ и на чињеници да је уграђен у шири институционални и тржишни оквир у коме домаће платформе делују под регулаторним надзором државе. Корисници у Кини не наилазе само на спољну мрежну баријеру, већ функционишу у окружењу у коме су домаће алтернативе страним сервисима већ интегрисане у систем националне регулације. Са тог становишта, ефикасност зида није само питање да ли нешто може да се отвори, већ и питање да ли држава успева да обликује навике коришћења интернета, оквир јавно дозвољеног говора и доступност дигиталних алтернатива. Истовремено, емпиријска истраживања показују да овај систем није технички савршен јер долази до пропуста у филтрирању, случајева преобимног блокирања, као и до тога да неки захтеви буду пропуштени, а неки легитимни захтеви погрешно означени као спорни. Зато Great Firewall треба разумети пре као систем високе, али не и апсолутне ефикасности. Његова снага лежи управо у комбинацији техничке селективности, правне подршке и психолошког ефекта неизвесности код корисника.

Систем није без слабости и дуго је био предмет различитих покушаја заобилажења. У литератури се често описује динамика „мачке и миша“ између цензора и корисника, у којој нове технике филтрирања подстичу развој нових начина прикривања или заобилажења ограничења, а затим

[1107] Kevin Bock, George Hughey, Xiao Qiang, and Dave Levin, “China’s Censors Have a Back Up Plan: Examining China’s Double HTTPS Censorship Middleboxes,” in *Proceedings of the 11th USENIX Workshop on Free and Open Communications on the Internet (FOCI 21)* (Berkeley, CA: USENIX Association, 2021), 1–3.
[1108] Mingshi Wu, Roya Ensafi, and Jedidiah R. Crandall, “How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic,” in *32nd USENIX Security Symposium (USENIX Security 23)* (Berkeley, CA: USENIX Association, 2023), 2653–2658.
[1109] MacKinnon, “China’s Networked Authoritarianism,” 32–46; Clayton, Murdoch, and Watson, “Ignoring the Great Firewall of China,” 20–23; Hoang et al., “How Great Is the Great Firewall?,” 3392–3398.

држава на то одговара новим техничким прилагођавањем.[1110] Због тога се ефикасност Great Firewall-а не може мерити искључиво бројем блокираних домена или сервиса, већ и његовом способношћу да се временом адаптира, да уграђује нове методе препознавања и да се интегрише у шири државни концепт сајбер суверенитета. Ту се види његова највећа важност за разумевање кинеског приступа сајбер безбедности. Он није само инструмент цензуре, већ средство којим се истовремено штите информациона инфраструктура, политички поредак и контролисани модел дигиталне модернизације. Great Firewall има знатно шири значај од саме интернет контроле: он је један од носећих инструмената преко којих Кина повезује техничку заштиту, правну регулацију, идеолошку контролу и отпорност државе у дигиталној ери.[1111] Његово функционисање треба тумачити као део шире стратегије националне безбедности, а не као издвојену меру интернет политике.[1112]

У кинеском приступу, заштита дигиталног простора не своди се само на техничко спречавање злонамерних упада, већ обухвата и контролу прекограничног информационог тока, управљање дигиталном инфраструктуром, смањење изложености спољним ризицима и очување друштвене и политичке стабилности.[1113] Зато Great Firewall у кинеском моделу треба разумети као гранични безбедносни механизам који истовремено има филтрациону, надзорну, регулаторну и превентивну функцију. Он није еквивалент класичном заштитном зиду у уском информатичком смислу, али делује као један од кључних елемената ширег система државне одбране дигиталног простора. Кинеске беле књиге из 2015. и 2019. године изричито третирају сајбер простор као нови, односно један од кључних домена националне безбедности, док Бела књига из 2023. године показује да је тај став додатно учвршћен кроз концепт правно заснованог управљања сајбер простором.[1114] У том оквиру, интернет зид не представља само техничко средство блокаде, већ и материјализовани израз кинеске идеје да дигиталне границе морају бити подједнако заштићене као и територијалне.[1115]

Из перспективе превенције сајбер напада, улога овог система је вишеструка. Најпре, он омогућава држави да селективно ограничи или надзире прекограничне комуникационе токове, што умањује број директних канала кроз које злонамерни садржај, поједини сервиси или политички осетљиве платформе могу деловати на домаће кориснике и институције.[1116] Поред тога, инфраструктура филтрирања, DNS интервенција, блокирања домена, контроле саобраћаја и препознавања образаца понашања омогућава раније уочавање одређених аномалија и брже реаговање на неке

[1110] Rebecca MacKinnon, "China's Networked Authoritarianism," *Journal of Democracy* 22, no. 2 (2011): 32–46; Mingshi Wu, Roya Ensafi, and Jedidiah R. Crandall, "How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic," in *32nd USENIX Security Symposium (USENIX Security 23)* (Berkeley, CA: USENIX Association, 2023), 2653–2658.
[1111] MacKinnon, "China's Networked Authoritarianism," 35–40; International Institute for Strategic Studies, *Cyber Capabilities and National Power: China* (London: IISS, 2021), 89–97.
[1112] International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 89–97; State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era* (Beijing: State Council Information Office, 2023), 2–3, 10–11
[1113] MacKinnon, "China's Networked Authoritarianism," 35–40; International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 95–97.
[1114] State Council Information Office of the People's Republic of China, *China's Military Strategy* (Beijing: State Council Information Office, 2015), 8; State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing: Foreign Languages Press, 2019), 13; State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era*, 2–3, 10–11.
[1115] State Council Information Office of the People's Republic of China, *China's Military Strategy*, 8; International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 89–97.
[1116] MacKinnon, "China's Networked Authoritarianism," 35–40; International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 95–97.

облике ризичне комуникације.[1117] То, наравно, не значи да *Great Firewall* сам по себи спречава све сложене сајбер нападе, нарочито оне који се ослањају на експлоатацију рањивости, компромитацију ланца снабдевања или унутрашњих система. Ипак, систем смањује површину изложености, олакшава централизовано управљање ризиком и јача државну способност да надгледа и обликује улазно-излазне дигиталне токове. У томе се види његова превентивна вредност: не као самодовољног одбрамбеног алата, већ као прве, спољне линије дигиталног разграничења.[1118]

Овај приступ добија још већи значај када се посматра у контексту кинеског разумевања сајбер ратовања. У кинеској војној мисли, нарочито од преласка ка информатизованом ратовању, исход будућег сукоба све више зависи од способности да се штите сопствени информациони системи, обезбеди непрекинутост командовања и истовремено наруше противнички капацитети за комуникацију, извиђање, обраду података и доношење одлука.[1119] Управо зато одбрана националног дигиталног простора у кинеском случају има и јасну војно-стратегијску димензију. Ако се прихвати да је сајбер простор поприште у коме се води борба за информациону надмоћ, онда механизми који омогућавају држави да филтрира, успорава, блокира, прати и преусмерава токове дигиталне комуникације постају релевантни и за припрему за потенцијални међудржавни сукоб. У том смислу, интернет зид није само средство контроле цивилног интернета, већ и део шире инфраструктуре отпорности која треба да умањи рањивост државе на спољне притиске, дестабилизацију, инфилтрацију злонамерних садржаја и онлајн операције утицаја.

Посебну улогу у том систему има идеја сајбер суверенитета. За Пекинг, заштита од сајбер напада не почиње тек у тренутку када дође до конкретног техничког инцидента, већ много раније — у самом праву државе да одреди ко, како и под којим условима може да делује унутар њеног дигиталног простора.[1120] Из тог разлога, механизми попут Great Firewall-a, законских ограничења за операторе, правила о критичној инфраструктури и норми о подацима функционишу као део истог концепта а то је да се дигитални простор посматра као зона суверене регулације. Та логика омогућава Кини да превенцију сајбер претњи повеже са контролом платформске архитектуре, домаћим технолошким екосистемом и политиком развоја националних алтернатива страним сервисима. Такво институционално затварање и селективно отварање интернета има и безбедносну последицу јер што је држава мање зависна од спољних платформи, стандарда и

[1117] Richard Clayton, Steven J. Murdoch, and Robert N. M. Watson, "Ignoring the Great Firewall of China," in *Privacy Enhancing Technologies*, ed. George Danezis and Philippe Golle (Berlin: Springer, 2006), 20–23; Ngoc Phong Hoang, Arian Akhavan Niaki, Jakub Dalek, Michalis Polychronakis, Phillipa Gill, and Nick Feamster, "How Great Is the Great Firewall? Measuring China's DNS Censorship," in *30th USENIX Security Symposium (USENIX Security 21)* (Berkeley, CA: USENIX Association, 2021), 3381–3387; Mingshi Wu, Roya Ensafi, and Jedidiah R. Crandall, "How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic," 2653–2658.

[1118] International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 89–97; State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era*, 2–3, 10–11.

[1119] Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, *People's Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), 21–24; State Council Information Office of the People's Republic of China, *China's National Defense in the New Era*, 5, 13.

[1120] International Institute for Strategic Studies, *Cyber Capabilities and National Power: China* (London: IISS, 2021), 89–97; U.S.-China Economic and Security Review Commission, *China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States* (Washington, DC: U.S. Government Publishing Office, 2022), 31–33.

канала комуникације, то је, из њене перспективе, отпорнија на спољни притисак, технолошку принуду и одређене облике сајбер угрожавања.[1121]

У практичном смислу, веза између интернет зида и превенције сајбер напада видљива је и у начину на који Кина организује заштиту критичне информационе инфраструктуре. Кинески нормативни оквир полази од претпоставке да угрожавање кључних мрежа, информационих система и података може да има озбиљне последице по националну безбедност, друштвени поредак и јавни интерес.[1122] Зато се од оператора критичне инфраструктуре захтевају посебне мере заштите, процене ризика, безбедносне провере и тснија сарадња са државним органима. У таквом окружењу *Great Firewall* не делује самостално, већ као спољни заштитни појас који допуњује унутрашњу регулативу, контролу приступа, инспекцијске механизме и надзор над подацима. Ово је од посебног значаја за разумевање кинеске логике превенције јер се напад не посматра само као технички догађај који треба одбити када почне, већ као ризик који треба унапред сузити ограничавањем комуникационих канала, повећањем видљивости саобраћаја и јачањем државне способности координације.[1123] Одатле произлази да је интернет зид у тесној вези са концептом „отпорности система", односно са настојањем да дигитални простор остане управљив и под стратешком контролом чак и у условима кризе.[1124]

Истовремено, било би аналитички погрешно тврдити да интернет зид сам по себи представља довољну одбрану од сајбер напада и сајбер ратовања. Савремени сајбер напади често се ослањају на компромитацију унутрашњих система, људски фактор, ланац снабдевања, прикривене злонамерне кодове и друге методе које не зависе искључиво од јавног приступа интернету. Због тога се у стручној литератури наглашава да је кинески модел јачи у домену контроле садржаја, надзора и граничне регулације дигиталног простора него као потпуно затворен штит против свих сложених техничких претњи.[1125] Сама његова стварна вредност није у апсолутној заштити, већ у томе што отежава бројне канале спољног деловања, повећава трошкове заобилажења, омогућава ранију детекцију појединих образаца и држави даје већу контролу над дигиталним окружењем. У том смислу, *Great Firewall* делује као један од услова шире сајбер отпорности, а не као њен једини носилац.[1126] Ово је посебно видљиво у новијим истраживањима, која показују да је систем временом постао технички софистицираније и способан да детектује чак и одређене облике потпуно шифрованог саобраћаја на основу његових образаца.[1127] Управо зато Кинески интернет

[1121] International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 89–97; State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era* (Beijing: State Council Information Office, 2023), 2–3, 10–11.
[1122] State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era* (Beijing: State Council Information Office, 2023), 6, 10–11; State Council Information Office of the People's Republic of China, *Jointly Build a Community with a Shared Future in Cyberspace* (Beijing: State Council Information Office, 2022).
[1123] State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era*, 2–3, 6, 10–11; International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 89–97.
[1124] International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 89–97; State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era*, 2–3, 10–11.
[1125] Rebecca MacKinnon, "China's Networked Authoritarianism," *Journal of Democracy* 22, no. 2 (2011): 35–40; International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 89–97.
[1126] International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 89–97; Rebecca MacKinnon, "China's Networked Authoritarianism," 35–40.
[1127] Mingshi Wu, Jackson Sippe, Danesh Sivakumar, Jack Burg, Peter Anderson, Xiaokang Wang, Kevin Bock, Amir Houmansadr, Dave Levin, and Eric Wustrow, "How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic," in *32nd USENIX Security Symposium (USENIX Security 23)* (Berkeley, CA: USENIX Association, 2023), 2653–2658.

зид треба схватити као динамичан безбедносни инструмент који се стално прилагођава, а не као статичну баријеру једном за свагда подигнуту између Кине и остатка света.

Са становишта сајбер ратовања, Кина Кинески интернет зид не користи само ради унутрашње цензуре, већ као део ширег безбедносног екосистема који повезује заштиту од сајбер напада, контролу информационих утицаја, управљање критичном инфраструктуром и припрему за вишедоменски сукоб.[1128] У том екосистему, технички механизми филтрирања и блокирања добијају стратешки смисао тек када се доведу у везу са правним нормама, сајбер суверенитетом, институционалним надзором и војним схватањем информационе надмоћи. Зато је интернет зид у кинеском случају истовремено и инструмент државне контроле и средство превентивне сајбер одбране. Он не замењује војне капацитете, специјализоване сајбер јединице ни заштиту критичне инфраструктуре, али им обезбеђује повољнији унутрашњи амбијент деловања и смањује простор за спољну дигиталну пенетрацију. Управо у тој повезаности унутрашње контроле и спољне отпорности лежи његов посебан значај за разумевање кинеског модела сајбер безбедности. Стога се може закључити да је Great Firewall један од носећих елемената кинеске стратегије дигиталне самозаштите: не као потпуно затворен систем, већ као адаптивна, вишеслојна и политички усмерена инфраструктура која треба да смањи рањивост државе у условима све интензивнијег сајбер и информационог надметања.[1129]

6.5 Војна модернизација Кине и развој капацитета за сајбер ратовање

Као логичан наставак претходног разматрања Кинеског интернет зида, потребно је указати да кинески приступ сајбер безбедности није ограничен само на унутрашњу контролу дигиталног простора, већ је тесно повезан са широм војном модернизацијом државе.

Током последњих деценија Народна Република Кина систематски јача своје оружане снаге, посебно морнаричке, ракетне, свемирске и информационе компоненте, настојећи да класичну модернизацију наоружања повеже са изградњом способности за деловање у новим доменима ратовања.[1130] У том процесу сајбер простор добија посебно место, јер се у кинеским стратешким документима и анализама све јасније третира као кључан простор за очување националне безбедности, заштиту суверенитета и стицање информационе надмоћи.[1131] Управо зато развој кинеских сајбер капацитета треба разумети као део опште трансформације НОАК-а, а не као издвојену техничку специјалност. Тиме се надовезује логика већ уочена код Кинеског интернет зида а то је да заштита дигиталног простора и способност деловања у њему посматрају се као два међусобно условљена аспекта исте стратегије. Из те перспективе, контрола интернета унутар

[1128] Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, *People's Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), 21–24; State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing: Foreign Languages Press, 2019), 5, 13.
[1129] State Council Information Office of the People's Republic of China, *China's Military Strategy* (Beijing: State Council Information Office, 2015), 8; State Council Information Office of the People's Republic of China, *China's National Defense in the New Era*, 13; State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era*, 2–3, 10–11; International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 89–97; Burke et al., *People's Liberation Army Operational Concepts*, 21–24.
[1130] Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era," report delivered at the 19th National Congress of the Communist Party of China, October 18, 2017.
[1131] State Council Information Office of the People's Republic of China, *China's Military Strategy* (Beijing: State Council Information Office, 2015), 8; State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing: Foreign Languages Press, 2019), 13.

државе и развој војних способности за сајбер простор припадају истом пројекту јачања националне моћи.[1132]

Појава интернета и убрзана глобална повезаност омогућиле су бржу размену података, лакши приступ информацијама и нове облике економске и технолошке сарадње, али су истовремено створиле и нове рањивости. У том контексту Кина је развијала двоструки приступ: са једне стране, јачала је механизме контроле унутар сопственог дигиталног простора, а са друге стране, улагала је у развој способности за одбрану и деловање у сајбер домену.[1133] Међутим, у академском смислу важно је избећи сувише поједностављену тврдњу да све сајбер операције које се у иностранству приписују кинеским актерима потичу непосредно од НОАК-а. Релевантни западни извештаји наглашавају да је неопходно разликовати војни, обавештајни и парадржавни сегмент кинеског сајбер екосистема, јер се значајан део глобалне сајбер шпијунаже у литератури чешће доводи у везу са Министарством државне безбедности и са њим повезаним актерима, док је улога НОАК-а израженија у припреми за војни сукоб, информационо ратовање и интеграцију сајбер дејстава у здружене операције.[1134] Ова разлика је од суштинског значаја за научну прецизност, јер спречава мешање цивилно-обавештајне са војно-оперативном димензијом кинеског сајбер деловања. Истовремено, она не умањује значај чињенице да Кина у целини улаже велика средства у развој софистицираних сајбер способности, образовање кадрова, истраживачке институте и војно-цивилну фузију у дигиталној сфери. Управо тај спој државе, војске, индустрије и технолошке политике представља једну од кључних одлика кинеског приступа сајбер ратовању.[1135]

Стратешки значај сајбер простора у кинеском систему посебно је наглашен у политичким смерницама које је формулисао Си Ђинпинг. На првом састанку Централне водеће групе за сајбер безбедност и информатизацију 2014. године он је истакао да „без сајбер безбедности нема националне безбедности, а без информатизације нема модернизације“, чиме је сајбер сферу поставио у само средиште државне стратегије развоја и безбедности.[1136] Овај став касније је потврђен и у извештају на 19. конгресу Комунистичке партије Кине 18. октобра 2017. године, у коме је утврђен тростепени оквир војне модернизације: до 2020. механизација је требало да буде у основи постигнута, информатизација знатно унапређена, а стратешке способности јасно ојачане; до 2035. модернизација националне одбране и оружаних снага требало је у основи да буде завршена; до средине XXI века кинеске оружане снаге требало би да буду потпуно трансформисане у војску „светске класе“.[1137] По овом оквиру сајбер домен није био споредна област, већ део ширег пројекта изградње стратешких способности у новим доменима. Посебно је значајно то што се у истом извештају наглашава да је „технологија срж борбене способности“, као и да је потребно развијати нове борбене и подржавајуће снаге и унапређивати способност за

[1132] Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, *People's Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), 1–4, 21–24.
[1133] International Institute for Strategic Studies, *Cyber Capabilities and National Power: China* (London: IISS, 2021), 89–97; State Council Information Office of the People's Republic of China, *China's Law-Based Cyberspace Governance in the New Era* (Beijing: State Council Information Office, 2023), 2–3, 10–11.
[1134] U.S.-China Economic and Security Review Commission, *China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States* (Washington, DC: U.S. Government Publishing Office, 2022), 31–40; International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 98–99.
[1135] International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 96–99; Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects."
[1136] "Elevating China's Internet Sector to New Heights," *The State Council of the People's Republic of China*, July 15, 2023.
[1137] Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects"; "Highlights of Report to 19th CPC National Congress," *SCIO*, October 18, 2017.

здружене операције засноване на мрежно-информационом систему.[1138] Кинеско руководство сајбер безбедност не схвата само као питање заштите мрежа, већ и као предуслов за целокупну војну трансформацију.[1139]

Ови политички и доктринарни ставови добили су јаснији институционални израз формирањем Стратешке помоћне снаге (ССФ) НОАК-а 31. децембра 2015. године. У литератури се овај корак препознаје као једна од најважнијих последица кинеских војних реформи, јер је по први пут у оквиру једне структуре настојано да се интегришу свемирске, сајбер, електронске и одређене информационе способности.[1140] RAND је 2017. године проценио да је ова снага задужена за развој и употребу великог дела кинеских војних способности у области свемира, сајбер простора и електронског ратовања, док су Елса Канија и Џон Костело указали да је њен Мрежни системски департман интегрисао значајан део стратегијских сајбер, електронских и психолошких капацитета НОАК-а.[1141] Стратешке помоћне снаге представљају институционални покушај да се обезбеди јединственија подршка здруженим операцијама. Департман је требало да делује као оквир за стратегијску информациону подршку целој НОАК, али и као средство стицања надмоћи у доменима који се у савременој кинеској војној мисли сматрају пресудним за исход будућег сукоба.[1142] Управо зато се у анализама често појављује као институционални мост између информатизованог ратовања, сајбер операција и шире доктрине „система против система“.[1143]

Када је реч о сајбер домену у ужем смислу, значај ССФ-а лежао је у томе што је омогућила да се сајбер операције више не третирају као споредна или искључиво дефанзивна активност, већ као део интегрисаних информационих операција. У том оквиру, сајбер шпијунажа, техничко извиђање, електронско ратовање, мрежна одбрана и потенцијалне офанзивне способности добијају место у ширем циклусу припреме и вођења сукоба.[1144] Ово је у складу и са широм кинеском представом о ратовању у којој су границе између мира и рата, цивилне и војне сфере, као и физичког и информационог бојишта све нејасније. Зато је ССФ имала значај не само за непосредне војне мисије, већ и за изградњу дугорочне инфраструктуре информационог ратовања, у којој се сајбер простор, електромагнетни спектар и свемир посматрају као међусобно повезана подручја. У том смислу, кинеско инвестирање у дигиталну инфраструктуру, обуку стручњака и интеграцију научноистраживачких капацитета није било усмерено само на заштиту од сајбер претњи, већ и на стварање способности за активно обликовање оперативног окружења.[1145] То је од посебне важности за разумевање кинеског модела сајбер ратовања, јер показује да превенција,

[1138] Xi Jinping, “Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects”; “Highlights of Report to 19th CPC National Congress,” *SCIO*, October 18, 2017.
[1139] Joel Wuthnow and M. Taylor Fravel, “China’s Military Strategy for a ‘New Era’: Some Change, More Continuity, and Tantalizing Hints,” *Journal of Strategic Studies* 46, no. 6–7 (2023): 1150–1155; Burke et al., *People’s Liberation Army Operational Concepts*, 21–24.
[1140] Kevin L. Pollpeter, Michael S. Chase, and Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations* (Santa Monica, CA: RAND Corporation, 2017), 1, 13–14.
[1141] Pollpeter, Chase, and Heginbotham, *The Creation of the PLA Strategic Support Force*, 27–29; Elsa B. Kania and John K. Costello, “The Strategic Support Force and the Future of Chinese Information Operations,” *Cyber Defense Review* 3, no. 1 (2018): 109–112.
[1142] Kania and Costello, “The Strategic Support Force and the Future of Chinese Information Operations,” 109–117.
[1143] Burke et al., *People’s Liberation Army Operational Concepts*, 21–24; Kania and Costello, “The Strategic Support Force and the Future of Chinese Information Operations,” 109–117.
[1144] Kania and Costello, “The Strategic Support Force and the Future of Chinese Information Operations,” 109–117.
[1145] International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 96–99; Kania and Costello, “The Strategic Support Force and the Future of Chinese Information Operations,” 115–117.

одбрана и потенцијално офанзивно деловање у овом домену чине јединствен стратегијски континуум.[1146]

Ипак, ради потпуне чињеничне прецизности, неопходно је напоменути да ССФ данас више не постоји у облику у ком је била формирана 2015. године. У априлу 2024. Кина је спровела нову реформу, којом је Стратешка помоћна снага укинута, а њене функције распоређене између новоформираних Снага за сајбер простор, Ваздухокосмичких снага и Информационе потпорне снаге, непосредно потчињених Централној војној комисији.[1147] Ова чињеница је важна јер се о ССФ-у говори пре свега као о историјски значајној фази у развоју кинеских способности за сајбер и информационо ратовање, а не као о трајно важећој организационој форми. Ипак, и после њеног формалног укидања, основна логика коју је ССФ оличавала — интеграција сајбер, свемирских, електронских и информационих способности ради стицања предности у савременом сукобу — остала је присутна у кинеском војном развоју. Управо зато је за разумевање кинеских капацитета за сајбер ратовање и даље неопходно проучавати ССФ, али увек уз јасну временску одредницу да је реч о структури која је била кључна у периоду од 2015. до 2024. године.[1148] То уједно показује и ширу тенденцију кинеских војних реформи: организациони облици се мењају, али стратешки циљ остаје исти — изградња оружаних снага способних за деловање у условима информатизованог, интелигентизованог и вишедоменског рата.[1149]

Важно је нагласити и да је Стратешка помоћна снага НОАК-а, до њене реорганизације 2024. године, имала улогу кључног инструмента за повезивање сајбер, свемирских, електронских и ширих информационих способности у јединствен оквир савременог ратовања.[1150] Њен значај није произлазио из бројности или класичне ватрене моћи, већ из способности да подржи и омогући деловање других родова оружаних снага у условима информатизованог и вишедоменског сукоба. У том смислу, ССФ је била замишљена као носилац онога што су кинески и западни аналитичари често описивали као „стратешку информациону подршку“ и „информационо ратовање“ на националном нивоу.[1151] То је значило да њена функција није била сведена само на одбрану мрежа, већ и на обезбеђивање надзора, извиђања, комуникација, информационе подршке, раног упозорења и других капацитета који су омогућавали да здружене снаге делују у јединственом информационом окружењу. Управо ту се јасно видела веза са претходно анализираним механизмима унутрашње контроле дигиталног простора: на нивоу државе Кина је тежила контроли и заштити информационог окружења, а на нивоу војске изградњи способности да то исто окружење користи као средство за стицање оперативне предности.[1152]

[1146] Burke et al., *People's Liberation Army Operational Concepts*, 21–24; Wuthnow and Fravel, "China's Military Strategy for a 'New Era'," 1151–1155.
[1147] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2024* (Washington, DC: Department of Defense, 2024), 8, 80–82.
[1148] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2024*, 80–82; Kania and Costello, "The Strategic Support Force and the Future of Chinese Information Operations," 109–117.
[1149] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2024*, 8, 80–82; Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects."
[1150] Kevin L. Pollpeter, Michael S. Chase, and Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations* (Santa Monica, CA: RAND Corporation, 2017), 1, 13–14.
[1151] Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *Cyber Defense Review* 3, no. 1 (2018): 106–109; Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, *People's Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), 21–24.
[1152] Burke et al., *People's Liberation Army Operational Concepts*, 21–24; International Institute for Strategic Studies, *Cyber Capabilities and National Power: China* (London: IISS, 2021), 89–97.

У ратним условима, ССФ је била замишљена као снага која се интегрисала у дејства копнене војске, морнарице, ваздухопловства и ракетних снага, тако што је подржавала њихове операције у доменима који су били од пресудне важности за савремено командовање и управљање бојиштем. Кинеска Бела књига одбране из 2019. године показала је да је после реформи успостављен систем у коме је Централна војна комисија остваривала свеукупно руководство, командне области водиле операције, а родови и службе развијали капацитете.[1153] У таквом моделу, ССФ није функционисала као класичан борбени род у истом смислу као копнена војска, морнарица или ваздухопловство, већ као посебна снага под директним ауторитетом војне команде, чија је основна вредност лежала у томе што је подржавала читаву НОАК преко способности релевантних за све правце и нивое операција.[1154] Због тога је њен положај у командној архитектури био функционално прилагодљив јер је у великој мери обезбеђивала информациону инфраструктуру и оперативне ефекте без којих би здружено ратовање било знатно мање ефикасно. Из тог разлога се у литератури с правом истицало да се значај ССФ-а није могао мерити искључиво формалним местом у хијерархији, већ пре свега улогом коју је имала у повезивању различитих родова и домена ратовања у једну оперативну целину.[1155]

На први поглед, ова снага могла је да се тумачи као структура чија је улога била превасходно подршка и заштита. Међутим, детаљније анализе показивале су да је њена оперативна функција била много шира. Kania и Costello су указали да је управо ССФ требало да постане примарна борбена снага за информационе операције и „информациону подршку“, укључујући извиђање, надзор и прибављање података у свемиру, сајбер простору и електромагнетном спектру.[1156] То је значило да су њени задаци обухватали не само одбрану сопствених мрежа, већ и стратешко техничко извиђање, електронско ратовање, психолошке и когнитивне елементе информационог надметања, као и способност да се противнички „систем система“ доведе у стање дезорганизације или парализе. У том смислу, ССФ је имала знатно активнију и потенцијално офанзивну улогу него што се могло закључити на основу формалне реторике о „подршци“. Управо зато је у литератури често описивана као институционални израз кинеске тежње да у будућем рату обезбеди предност у простору информација, комуникација и одлучивања.[1157] Истовремено, важно је нагласити да ССФ није била једини кинески актер у сајбер домену: државни сајбер екосистем Кине био је шири од саме НОАК и укључивао је и друге безбедносне и обавештајне структуре.[1158] Овај моменат је важан, јер указује да кинеске сајбер способности не смеју да се редукују искључиво на једну војну организацију, иако је ССФ несумњиво представљала кључну војну компоненту тог система.[1159]

Када је реч о унутрашњој организацији, неопходно је задржати одређену меру опреза, јер су доступни подаци дуго били фрагментарни, а сама структура ССФ-а само делимично видљива у отвореним изворима. Најпоузданије анализе, међутим, указивале су да су јавно најјасније

[1153] State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing: Foreign Languages Press, 2019), 26–27.
[1154] Pollpeter, Chase, and Heginbotham, *The Creation of the PLA Strategic Support Force*, 13–14; Kania and Costello, "The Strategic Support Force and the Future of Chinese Information Operations," 109–112.
[1155] Kania and Costello, "The Strategic Support Force and the Future of Chinese Information Operations," 109–117; Burke et al., *People's Liberation Army Operational Concepts*, 21–24.
[1156] Kania and Costello, "The Strategic Support Force and the Future of Chinese Information Operations," 109–112.
[1157] Ибид. 112–117.
[1158] International Institute for Strategic Studies, *Cyber Capabilities and National Power: China*, 96–99; U.S.-China Economic and Security Review Commission, *China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States* (Washington, DC: U.S. Government Publishing Office, 2022), 31–40.
[1159] Ибид.

потврђене две главне организационе целине: Одељење за аеро-космичке системе и Одељење за мрежне системе.[1160] У литератури су се понекад појављивала и шира тумачења која су помињала додатне функционалне подсекторе у области електронског и обавештајног деловања, али је у академском тексту прецизније разликовати оно што је било релативно чврсто потврђено од онога што је остајало аналитичка реконструкција.[1161] Посебно је важно то што је Одељење за мрежне системе, према Kania и Costello, интегрисало критичну масу стратегијских сајбер, електронских и психолошких способности НОАК-а, а као његово језгро били су препознати делови некадашњег Трећег одељења Генералштаба, задуженог за техничко извиђање и сајбер шпијунажу, као и најмање део капацитета бившег Четвртог одељења за електронска противдејства.[1162] Овај налаз је од великог значаја, јер показује да је кинеска реформа тежила не само административном премештању надлежности, већ и суштинској интеграцији дотад раздвојених функција у један ефикаснији систем. На тај начин, ССФ је постала институционални оквир у коме су се спојили сајбер, електронски и психолошки инструменти информационог ратовања.[1163]

Значај овако конципиране структуре најбоље се видео у начину на који је Кина замишљала њену улогу у времену оружаног сукоба. Kania и Costello су, анализирајући кинеску концепцију „информационе оперативне групе“, указали да би у условима сукоба различити елементи одговорни за сајбер, електронско и психолошко ратовање били окупљени у оперативни командни оквир на стратегијском, кампањском и тактичком нивоу.[1164] У том моделу ССФ се појављивала као централна борбена сила за информационе операције и „информациону подршку“, што је обухватало надзор, извиђање, рано упозоравање, комуникације, команду, контролу и навигацију.[1165] То је значило да њена улога није била ограничена на помоћне техничке функције, већ је имала непосредан утицај на способност целокупне НОАК да води здружене операције у условима савременог ратовања. Из перспективе сајбер ратовања, овај аспект је посебно важан, јер показује да се у кинеској војној мисли сајбер простор није третирао као издвојено бојиште, већ као део интегрисаног система којим су се обликовали услови за успех у свим другим доменима. Сходно томе, ССФ је била кључни инструмент за повезивање сајбер и електронског ратовања са ширим стратешким наступом НОАК-а.[1166]

ССФ, иако организационо укинута 2024. године, оставила трајан институционални и доктринарни траг у развоју кинеских способности за сајбер и информационо ратовање. У априлу 2024. њене функције су распоређене између новоформираних Снага за сајбер простор, Ваздухокосмичких снага и Информационе потпорне снаге, непосредно потчињених Централној војној комисији.[1167]. ССФ је представља једну од најважнијих фаза у еволуцији кинеске војне мисли од заштите и контроле дигиталног простора ка изградњи способности за активно и вишедоменско деловање у њему.

[1160] Pollpeter, Chase, and Heginbotham, *The Creation of the PLA Strategic Support Force*, 13–14, 27–29.
[1161] Ибид, 27–29; Kania and Costello, "The Strategic Support Force and the Future of Chinese Information Operations," 109–117.
[1162] Kania and Costello, "The Strategic Support Force and the Future of Chinese Information Operations," 109–117.
[1163] Burke et al., *People's Liberation Army Operational Concepts*, 21–24; Kania and Costello, "The Strategic Support Force and the Future of Chinese Information Operations," 112–117.
[1164] Kania and Costello, "The Strategic Support Force and the Future of Chinese Information Operations," 115–117.
[1165] Ибид.., 115–117; Burke et al., *People's Liberation Army Operational Concepts*, 21–24
[1166] Burke et al., *People's Liberation Army Operational Concepts*, 21–24; Joel Wuthnow and M. Taylor Fravel, "China's Military Strategy for a 'New Era': Some Change, More Continuity, and Tantalizing Hints," *Journal of Strategic Studies* 46, no. 6–7 (2023): 1151–1155.
[1167] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2024* (Washington, DC: Department of Defense, 2024), 8, 80–82.

Надовезујући се на претходно разматрање улоге Стратешке помоћне снаге у кинеској војној модернизацији, потребно је прецизније одредити њено место у оперативном извођењу сајбер и информационих дејстава. Уместо да се посматрала као класична помоћна структура, ССФ је у литератури много уверљивије описивана као носилац интеграције способности у сајбер простору, електромагнетном спектру и психолошком ратовању.[1168] Управо зато њена вредност у условима оружаних сукоба није била ограничена на техничку подршку другим родовима војске, већ је произлазила из способности да створи услове у којима копнене, поморске, ваздухопловне и ракетне снаге могу да делују у координисаном, мрежно повезаном и информационо заштићеном окружењу.[1169] То је значило да су задаци ССФ-а обухватали много шири спектар функција него што је на први поглед сугерисала сама формулација о „стратешкој информационој подршци“: у питању су били извиђање, техничко прикупљање података, рано упозоравање, комуникациона подршка, електронско супротстављање и различити облици сајбер деловања.[1170] ССФ је представљала институционални оквир преко кога је кинеска војна доктрина настојала да информациони простор претвори у активно средство за стицање предности у оружаном сукобу.

Под вођством Си Ђинпинга, процес укључивања сајбер простора у сам центар кинеског безбедносног и војног размишљања добио је знатно јаснију и концептуално зрелију форму. У том смислу, Бела књига *China's Military Strategy* из 2015. године представља важну прекретницу, јер је први пут у оквиру једног званичног документа под тим насловом сајбер простор јасно одредила као један од „нових стратешких висова“ у међудржавном надметању.[1171]Тиме је потврђено да информације и способност управљања њиховим токовима више не припадају искључиво помоћној сфери војног деловања, већ постају кључни елементи будућег сукоба. У кинеском схватању, то је значило да се војна моћ више не може мерити само бројношћу снага, ватреном моћи или територијалном дубином, већ и способношћу да се успостави информациона предност, заштите сопствени системи и наруше противничке мреже, комуникације и токови одлучивања. На тај начин, дигитална супериорност постепено је добила статус једне од носећих компоненти националне моћи и војне ефикасности.[1172] Овај заокрет је уједно представљао и доктринарну основу за касније институционалне реформе, укључујући и интеграцију сајбер, свемирских и електронских способности у оквиру Стратешке помоћне снаге.[1173] Овако схваћен сајбер простор постао је не само питање техничке безбедности, већ и питање стратешке иницијативе.

[1168] Kevin L. Pollpeter, Michael S. Chase, and Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations* (Santa Monica, CA: RAND Corporation, 2017), 1, 13–14.
[1169] Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *Cyber Defense Review* 3, no. 1 (2018): 106–109; Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, *People's Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), 21–24.
[1170] Burke et al., *People's Liberation Army Operational Concepts*, 21–24; International Institute for Strategic Studies, *Cyber Capabilities and National Power: China* (London: IISS, 2021), 89–97.
[1171] State Council Information Office of the People's Republic of China, *China's Military Strategy* (Beijing: State Council Information Office, 2015), 2.
[1172] Joel Wuthnow and M. Taylor Fravel, "China's Military Strategy for a 'New Era': Some Change, More Continuity, and Tantalizing Hints," *Journal of Strategic Studies* 46, no. 6–7 (2023): 1149–1155; Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, *People's Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), 21–24.
[1173] Kevin L. Pollpeter, Michael S. Chase, and Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations* (Santa Monica, CA: RAND Corporation, 2017), 14–16; Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *Cyber Defense Review* 3, no. 1 (2018): 106–109.

До краја друге деценије XXI века овај процес је додатно продубљен. Бела књига China's National Defense in the New Era из 2019. године не само да је потврдила централно место сајбер простора у националној безбедности, већ је и нагласила да „рат еволуира у правцу информатизованог ратовања, а интелигентизовано ратовање је на хоризонту".[1174] Ова формулација указује на важну промену у кинеском војном размишљању: информатизација више није била довољна сама по себи, већ се све јасније отварао простор за нову фазу у којој би вештачка интелигенција, аутоматизована обрада података, умрежени системи и алгоритамска подршка одлучивању постали пресудни за вођење операција. Због тога дигитална трансформација кинеског војног апарата није била само питање технолошке модернизације, већ и дубоког доктринарног преусмеравања. У том контексту, сајбер простор добија двоструки значај: он је истовремено и поприште борбе за информациону надмоћ и инфраструктурна основа без које не би било могуће спровести шире процесе интелигентизације оружаних снага.[1175] Управо зато се и у анализама војних стратегијских смерница за „нову еру" наглашава да је после 2019. године кинеска војна стратегија остала континуитетом везана за раније смернице, али је истовремено била постављена у нови политички и технолошки оквир који је захтевао брже прилагођавање новим облицима ратовања.[1176] Одатле произлази да је сајбер домен у кинеској доктрини од периферне теме прерастао у један од њених основних носећих стубова.

Овај доктринарни развој био је тесно повезан са ширим политичким оквиром војне модернизације који је Си Ђинпинг формулисао на 19. конгресу Комунистичке партије Кине 2017. године. У том извештају јасно је постављен временски оквир према коме је до 2020. требало у основи остварити механизацију, знатно унапредити информатизацију и ојачати стратешке способности, до 2035. завршити модернизацију националне одбране и оружаних снага, а до средине XXI века кинеску војску трансформисати у војску „светске класе".[1177] Ови циљеви показују да сајбер способности нису схваћене као споредан додатак, већ као део дугорочног пројекта трансформације читавог војног система. Нарочито је важно то што се у истом тексту наглашава да је технологија „срж борбене способности", што значи да су технолошка иновација, дигитална интеграција и изградња нових домена ратовања директно повезани са питањем способности НОАК-а да „се бори и победи".[1178] Из тога се може закључити да је тежња ка сајбер супериорности у кинеском случају императив који проистиче из опште стратегије војне трансформације, а не само из реакције на спољне претње или на туђе технолошке предности. У томе се види и суштинска веза са претходно анализираном ССФ: она је била институционални инструмент кроз који су ови доктринарни и политички циљеви добили оперативни облик.[1179]

У том смислу, формирање Стратешке помоћне снаге 2015. године не треба посматрати као изолован административни потез, већ као непосредну институционалну последицу нове парадигме кинеског безбедносног размишљања. Раније раздвојени капацитети за техничко

[1174] State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing: Foreign Languages Press, 2019), 5; Masaaki Yatsuzuka, "China's 2019 National Defense White Paper and Intelligent Warfare," *NIDS Commentary* no. 105 (October 10, 2019): 1–3.
[1175] Yatsuzuka, "China's 2019 National Defense White Paper and Intelligent Warfare," 2–3; Burke et al., *People's Liberation Army Operational Concepts*, 21–24.
[1176] Wuthnow and Fravel, "China's Military Strategy for a 'New Era'," 1149–1155.
[1177] Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era," report delivered at the 19th National Congress of the Communist Party of China, October 18, 2017, 48.
[1178] Xi Jinping, "Secure a Decisive Victory," 48; Burke et al., *People's Liberation Army Operational Concepts*, 1–4.
[1179] Pollpeter, Chase, and Heginbotham, *The Creation of the PLA Strategic Support Force*, 14–16; Kania and Costello, "The Strategic Support Force and the Future of Chinese Information Operations," 106–109.

извиђање, сајбер шпијунажу, електронске противмере, психолошке операције и заштиту војних информационих система били су интегрисани у шири оквир који је требало да омогући деловање у свим кључним доменима информационог ратовања.[1180] На тај начин је и организационо потврђено оно што је већ било видљиво на доктринарном плану: сајбер, свемирске и електромагнетне операције више нису схватане као подређене класичним видовима ратовања, већ као самостална и стратешки одлучујућа подручја савременог оружаног сукоба.[1181] Под Сијем кинеска војна мисао јасно је артикулисала прелаз са схватања сајбер простора као техничког домена на разумевање сајбер простора као једног од пресудних поља стратешке конкуренције и будућег ратовања.[1182]

Као наставак претходног разматрања доктринарног учвршћивања сајбер простора и институционалне улоге Стратешке помоћне снаге, потребно је указати да кинески приступ сајбер домену почива на тесном преплитању цивилних и војних механизама управљања. На цивилном плану, Кинеска управа за сајбер простор (CAC) под Си Ђинпингом постепено се профилисала као кључни партијско-државни координатор политике у области „сајбер безбедности и информатизације“, при чему је њена улога била да смањи ранију институционалну расцепканост и успостави снажнији модел и вертикалне координације.[1183] Ипак, ова централизација није значила нестанак других утицајних актера. Министарство јавне безбедности, Министарство државне безбедности и Министарство индустрије и информационих технологија задржали су важне надлежности у области мрежне безбедности, обавештајног рада, техничке регулације и индустријске политике.[1184] Управо зато кинеску сајбер архитектуру није могуће тумачити као једноставан хијерархијски систем, већ као политички координисан и институционално сложен механизам у коме су партијско руководство, цивилна регулатива и безбедносни апарат повезани у јединствену стратегијску целину. У том смислу, сајбер политика у Кини не представља само техничко питање регулације дигиталног простора, већ и средство за повезивање безбедности, развоја и политичке контроле.[1185]

Последице формирања Стратешке помоћне снаге за војне сајбер капацитете Кине могу се сагледати пре свега у њеној способности да интегрише различите облике информационог деловања у јединствен оперативни оквир. Уместо ранијег институционалног раздвајања техничког извиђања, електронског ратовања, сајбер деловања и психолошких операција, реформе су омогућиле да се ти инструменти посматрају као међусобно повезани елементи будућих конфликата.[1186] То је кинеској војсци отворило могућност за сложеније и мултидимензионалне информационе операције, у којима се психолошка, електронска, сајбер и, по потреби, кинетичка

[1180] Kania and Costello, “The Strategic Support Force and the Future of Chinese Information Operations,” 109–117; Pollpeter, Chase, and Heginbotham, *The Creation of the PLA Strategic Support Force*, 14–16.
[1181] Burke et al., *People’s Liberation Army Operational Concepts*, 21–24; Kania and Costello, “The Strategic Support Force and the Future of Chinese Information Operations,” 106–117.
[1182] Wuthnow and Fravel, “China’s Military Strategy for a ‘New Era’,” 1150–1155; Burke et al., *People’s Liberation Army Operational Concepts*, 21–24.
[1183] Jamie P. Horsley, “Behind the Facade of China’s Cyber Super-Regulator,” *DigiChina*, August 8, 2022; State Council Information Office of the People’s Republic of China, *China’s Law-Based Cyberspace Governance in the New Era* (Beijing: State Council Information Office, 2023).
[1184] Horsley, “Behind the Facade of China’s Cyber Super-Regulator”; International Institute for Strategic Studies, *Cyber Capabilities and National Power: China* (London: IISS, 2021), 89–97.
[1185] State Council Information Office of the People’s Republic of China, *China’s Law-Based Cyberspace Governance in the New Era* (Beijing: State Council Information Office, 2023).
[1186] Elsa B. Kania and John K. Costello, “The Strategic Support Force and the Future of Chinese Information Operations,” *Cyber Defense Review* 3, no. 1 (2018): 109–117; Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, *People’s Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), 21–24.

средства могу комбиновати у различитим фазама кризе или сукоба.[1187] На тај начин изграђен је образац који тежи већој оперативној еластичности, брзини реаговања и надмоћности у дигиталном окружењу. Посматрано у ширем контексту кинеске војне доктрине, овакав модел одговара тежњи ка „системској деструкцији“ противника, односно нарушавању његових комуникационих и логистичких капацитета у раној фази сукоба.[1188] Управо зато је у претходним одељцима било важно показати да ССФ није била тек помоћна служба, већ институционални израз шире кинеске амбиције да се постигне информациона надмоћ као предуслов успеха у савременом рату.[1189]

Овај процес добија додатну тежину када се посматра у светлу новијих података о кинеској војној модернизацији. Кина је и у 2025. години наставила раст званично објављеног војног буџета, при чему је најављено повећање од 7,2 процента..[1190] Истовремено, америчке процене наглашавају да стварни трошкови одбране значајно премашују јавно приказане бројке. Према процени Министарства одбране САД, стварна кинеска војна потрошња у 2024. години вероватно је износила приближно између 330 и 450 милијарди долара.[1191] Таква процена је важна не само због питања транспарентности, већ и зато што указује на ширину ресурса које Кина може усмеравати у развој истраживања и развоја, војно-цивилне фузије, дигиталне инфраструктуре и нових способности у сајбер, свемирском и информационом домену. У том смислу, савремена кинеска модернизација све мање зависи од једноставног увећања класичних платформи, а све више од интеграције напредних способности које могу да произведу асиметричне ефекте у кризним и ратним условима. Због тога сајбер капацитети у кинеској војној политици не треба да се посматрају као допуна конвенционалним снагама, већ као један од њених централних носећих ослонаца.[1192]

Посебно је значајно то што је Кина у априлу 2024. године спровела нову организациону реформу, којом је распуштена Стратешка помоћна снага, а њене кључне функције распоређене између Ваздухокосмичких снага, Сајбер снага, Информационе потпорне снаге и већ постојеће Јединствене логистичке потпорне снаге, све директно подређене Централној војној комисији.[1193] Ова промена показује да кинеско руководство и даље придаје изузетан значај свемирском, сајбер и информационом домену, али да настоји да њихову организацију учини функционалнијом и прилагођенијом потребама здруженог ратовања. Распуштање ССФ-а не значи слабљење значаја сајбер простора, већ пре његово даље институционално учвршћивање у новој форми. Америчке процене уједно наглашавају да кинески сајбер актери настављају да представљају значајну претњу војним, државним и критичним инфраструктурним системима, при чему су посебно истицане операције усмерене на дуготрајно прикривено присуство у мрежама и припрему

[1187] Burke et al., *People's Liberation Army Operational Concepts,* 21–24; Kania and Costello, "The Strategic Support Force and the Future of Chinese Information Operations," 115–117.
[1188] Burke et al., *People's Liberation Army Operational Concepts*, 21–24; Joel Wuthnow and M. Taylor Fravel, "China's Military Strategy for a 'New Era': Some Change, More Continuity, and Tantalizing Hints," *Journal of Strategic Studies* 46, no. 6–7 (2023): 1151–1155.
[1189] Kania and Costello, "The Strategic Support Force and the Future of Chinese Information Operations," 109–117.
[1190] "China to Increase Defense Budget by 7.2 Percent in 2025, Marking Single-Digit Growth for 10th Year," *The State Council of the People's Republic of China*, March 5, 2025.
[1191] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2024* (Washington, DC: Department of Defense, 2024), 160–161.
[1192] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2024*, 160–161; Edmund J. Burke et al., *People's Liberation Army Operational Concepts*, 21–24.
[1193] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2024*, 8, 80–82.

приступа за евентуалне кризне сценарије.[1194] Према америчким званичним проценама из 2024. године, група позната као *Volt Typhoon* компромитовала је више критичних инфраструктурних мрежа у Сједињеним Државама и унапред се позиционирала ради могућег ометања или уништавања услуга у случају већих геополитичких тензија или војног сукоба.[1195] Овакав образац деловања показује да је сајбер домен за Кину важан не само у обавештајном и политичком, већ и у оперативно-стратешком смислу.[1196]

Сходно томе, све је теже одржати јасну разлику између мира и конфликта у сајбер простору. Савремени облици дигиталног надметања омогућавају државама да остварују притисак, врше инфилтрацију, припремају приступе и обликују оперативно окружење дуго пре него што дође до отвореног оружаног сукоба.[1197] Управо ту лежи шири значај кинеских улагања у вештачку интелигенцију, квантне технологије, алгоритамску подршку обавештајној обради, извиђању и одлучивању, као и интеграцију цивилних и војних дигиталних капацитета. Циљ Кине није само реаговање на претње, већ и дугорочно позиционирање државе у дигиталној сфери као силе способне да делује превентивно, адаптивно и вишедоменски.[1198] У том смислу, сајбер простор више се не посматра као споредно ратно поље, већ као један од главних стубова савременог војног деловања и геополитичког надметања. Зато се и у ширем међународном контексту поставља питање норми, ограничења и механизама контроле у дигиталном простору. За Кину, међутим, суштинско питање није само правно регулисање сајбер домена, већ изградња способности да се у том домену обезбеди стратешка предност. Управо зато овај део логично следи након претходног: ако је било неопходно показати како су сајбер, свемирске и информационе способности институционализоване, сада је једнако важно показати како се те способности преливају у шири модел цивилно-војне координације и савремене стратегијске примене.[1199]

6.6 Кинеске војне јединице и извођење напада у сајбер простору

Народноослободилачка армија Кине представља главну оружану силу Народне Републике Кине и у савременој кинеској доктрини има кључну улогу у припреми и извођењу рата у условима информатизованог и све израженије интелигентизованог сукоба. У том оквиру, сајбер простор није схваћен као споредна техничка област, већ као један од „нових стратешких висова“ међудржавног надметања и једно од поља у коме се стиче информациона предност, штите сопствени системи и обликују услови за успех здружених операција.[1200]

[1194] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2024*, 99

[1195] Cybersecurity and Infrastructure Security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," Advisory AA24-038A, February 7, 2024; U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2024*, 99.

[1196] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2024*, 99.

[1197] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2024*, 99; Cybersecurity and Infrastructure Security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," Advisory AA24-038A, February 7, 2024.

[1198] Graham Webster, "China as a 'Cyber Great Power': Beijing's Two Voices in Telecommunications," *Brookings Institution*, April 5, 2021, 5–8; Elsa B. Kania, "AI Weapons in China's Military Innovation," *Brookings Institution*, April 2020, 2–3.

[1199] Joel Wuthnow and M. Taylor Fravel, "China's Military Strategy for a 'New Era': Some Change, More Continuity, and Tantalizing Hints," 1150–1155; Burke et al., *People's Liberation Army Operational Concepts*, 21–24.

[1200] State Council Information Office of the People's Republic of China, *China's Military Strategy* (Beijing: State Council Information Office, 2015); State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing: Foreign Languages Press, 2019), 5, 13; U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2024* (Washington, DC: Department of Defense, 2024), 80–82.

Када се говори о кинеским сајбер војним јединицама, не говори се само о посебним техничким структурама, већ о делу ширег војног система који сајбер, електромагнетни, свемирски и информациони домен третира као међусобно повезане компоненте савременог ратовања. Са становишта ове дисертације, то је од посебне важности, јер показује да се улога НОАК-а у сајбер ратовању мора разумети унутар шире кинеске доктрине рата између држава, а не само кроз призму изолованих техничких упада.

За ову тему је, међутим, неопходно поставити једну методолошку напомену. Није могуће сачинити потпуно исцрпан списак свих кинеских сајбер напада и свих случајева у којима су кинески системи били мета, јер велики број операција остаје поверљив, атрибуција је често спорна, а у отвореним изворима се после 2015. године много чешће појављују ознаке за кинеске државно спонзорисане актере у ширем смислу него јасне и јавне идентификације конкретних војних јединица.[1201] Због тога је научно прецизније говорити о најважнијим јавно документованим и релативно поуздано атрибутованим примерима. Посебно је важно не мешати операције које се приписују НОАК/ПЛА са операцијама које западни извори чешће везују за Министарство државне безбедности и његове сараднике. Таква дистинкција није само формална, већ је суштинска за разумевање кинеског сајбер екосистема, у коме војни, обавештајни и шири државни актери делују у истом стратешком правцу, али не увек у истом институционалном оквиру.

Најчвршће документован и у академској литератури најчешће навођен пример јесте случај APT1, који је компанија Mandiant 2013. године повезала са ПЛА јединицом 61398, односно са Другим бироом Трећег одељења Генералштаба.[1202] Према том извештају, APT1 је од најмање 2006. године компромитовала 141 организацију у 20 главних индустријских сектора, систематски крадући велике количине података и задржавајући приступ жртвама у просеку скоро годину дана. Мета су били сектори као што су ваздухопловство, енергетика, информационе технологије, телекомуникације, металургија, јавна управа, научна истраживања и транспорт. Овај случај је и данас кључан, јер представља најпознатији отворено документован пример повезивања једне кинеске војне јединице са дуготрајном сајбер шпијунажом великог обима. Управо због детаљности техничке документације, обима компромитованих жртава и јасне везе са конкретном војном формацијом, APT1 остаје полазна тачка готово сваке озбиљније анализе кинеских војних сајбер операција.

Још конкретнији и правно најјаснији пример представља америчка оптужница из 2014. године против петорице официра НОАК повезаних са јединицом 61398.[1203] У оптужници и пратећем саопштењу Министарства правде САД именоване су и конкретне жртве: Westinghouse, U.S. Steel, Allegheny Technologies, Alcoa, SolarWorld и синдикат United Steelworkers. Према тим документима, напади су укључивали spear-phishing, крађу акредитива, успостављање backdoor приступа и ексфилтрацију интерних стратешких информација, укључујући податке значајне за трговинске спорове, пословне преговоре и индустријску конкуренцију. Посебно је важно што овај случај показује како су, бар у једном периоду, поједине кинеске војне сајбер операције биле

[1201] U.S.-China Economic and Security Review Commission, *China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States* (Washington, DC: U.S. Government Publishing Office, 2022), 1, 31, 34–35; International Institute for Strategic Studies, *Cyber Capabilities and National Power: China* (London: IISS, 2021), 96–99.
[1202] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: Mandiant, 2013), 3–4.
[1203] U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage," press release, May 19, 2014; *United States v. Wang Dong et al.*, Indictment, No. 14-118 (W.D. Pa. May 1, 2014).

усмерене не само на класичну војну обавештајну делатност, већ и на економску и индустријску предност. Овај пример уједно показује и ширу природу кинеског приступа сајбер моћи а то је да граница између државне безбедности, индустријског развоја и сајбер операција у пракси је знатно флуиднија него што би се могло закључити из формално одвојених категорија.

Други важан пример у отвореним изворима представља група Putter Panda, коју је CrowdStrike 2014. године повезао са НОАК јединицом 61486, односно са Дванаестим бироом Трећег одељења Генералштаба.[1204] Према том извештају, ова група је деловала од 2007. године и била је усмерена на владин, одбрамбени, истраживачки и технолошки сектор, са нарочитим фокусом на свемирску, сателитску, ваздухопловну и комуникациону индустрију у Сједињеним Државама и Европи. Овај извештај је важан зато што указује на могућу специјализацију појединих кинеских војних сајбер структура за циљеве непосредно повезане са космичким системима, даљинским осматрањем и војно релевантним технологијама. Ипак, овде је неопходно задржати и методолошку резерву јер за разлику од оптужнице против јединице 61398, реч је о приватној атрибуцији, а не о судски потврђеном случају. Упркос томе, Putter Panda и даље остаје један од најважнијих јавно описаних примера активности војно повезане кинеске сајбер јединице и стога заслужује место у овој анализи.

После формирања Стратешке помоћне снаге 2015. године, а нарочито после тога што су западне процене све чешће поједине глобалне сајбер шпијунажне кампање доводиле у везу са Министарством државне безбедности и његовим сарадницима, у отвореним изворима постало је много теже поуздано приписивати појединачне кампање конкретним кинеским војним јединицама.[1205] То, међутим, не значи да је војна димензија нестала, већ да је јавна атрибуција постала сложенија и институционално мање јасна.

Један од ретких новијих примера у коме се војна компонента експлицитно истиче јесте извештај тајванског National Security Bureau о кинеским нападним техникама током 2024. године. У том извештају се наводи да је „PRC cyber force“ деловала против тајванских државних органа и приватног сектора, да су посебно порасли напади на телекомуникације, транспорт и одбрамбени ланац снабдевања, као и да су напади на критичну инфраструктуру обухватали ауто-путеве, луке и друге системе. Извештај такође наглашава да су сајбер напади коришћени паралелно са војним вежбама НОАК укључујући DDoS дејства ради појачавања ефекта притиска и војног застрашивања. Иако је реч о тајванској, а не неутралној атрибуцији, овај случај је важан јер показује како у непосредном безбедносном окружењу Кине сајбер деловање све отвореније прати војно надметање.

Када је реч о примерима у којима су кинески системи били мета, потребно је правити јасну разлику између независно потврђених инцидената и случајева које су јавно изнеле кинеске власти, али који нису у истој мери независно верификовани. Најпознатији такав пример је напад на Northwestern Polytechnical University из 2022. године. Кинеске власти и домаће безбедносне компаније, пре свега Qihoo 360, јавно су тај напад приписале америчкој NSA. За академску анализу је значајно то што је SIPRI овај случај издвојио као редак пример у коме је кинеска јавна атрибуција била поткрепљена техничким форензичким детаљима које су објавили и домаћи

[1204] CrowdStrike, *Putter Panda* (Irvine, CA: CrowdStrike, 2014), 1–2.
[1205] U.S.-China Economic and Security Review Commission, *China's Cyber Capabilities*, 31, 34–35; National Security Bureau, Republic of China (Taiwan), *Analysis on China's Cyberattack Techniques in 2024* (Taipei: NSB, 2025), 1–4.

приватни актери, а не само државни органи.[1206] И у овом случају треба задржати напомену да се изван кинеског оквира ове тврдње не сматрају у целини независно потврђеним на нивоу општеприхваћеног међународног консензуса.Следећи важан пример јесте Wuhan Earthquake Monitoring Center из 2023. године. Кинеске власти су тада саопштиле да је центар био изложен сајбер нападу из иностранства и да је напад, према њиховом тумачењу, био државно подржан и повезан са Сједињеним Државама.[1207] Тај случај је забележен и у аналитичком прегледу CERT-EU, што му је дало нешто већу видљивост у међународном аналитичком простору, мада ни овде не постоји пуна независна верификација свих елемената кинеске атрибуције. Ипак, за ово поглавље је овај пример важан јер показује да Кина све чешће јавно наступа не само као оптужени актер већ и као држава која тврди да су њени сопствени критични и научно-технички системи предмет државно спонзорисаних упада.

У исту групу спадају и случајеви које је CNCERT/CC јавно објавио у јануару 2025. године, наводећи да су од маја 2023. откривена и „обрађена“ два упада из Сједињених Држава усмерена на велике кинеске технолошке фирме ради крађе трговинских тајни.[1208] За академску употребу важно је да се овде јасно нагласи да је реч о кинеској службеној тврдњи, али да сам пример ипак има аналитичку вредност, јер показује да Пекинг сајбер претње сопственим технолошким компанијама све отвореније повезује са широм стратешком конкуренцијом у области напредних технологија, извозних ограничења и индустријске политике. У том смислу, ово није само безбедносно већ и геоекономско питање.

Поред тога, у отвореним изворима постоје и примери који нису везани искључиво за америчко-кинеско узајамно оптуживање, али показују да су кинески системи били предмет страних операција. Reuters је у априлу 2020. известио, позивајући се на компанију FireEye, да су хакери повезани са Вијетнамом покушавали да продру у кинеске државне организације у самом средишту одговора на почетак пандемије ковида-19. CSIS је у својој хронологији значајних сајбер инцидената забележио да су у том периоду сумњиви вијетнамски хакери циљали владине органе у Вухану и кинеско Министарство за ванредне ситуације, док је иста база бележила и нападе на кинеске државне институције и дипломатске мисије у иностранству злоупотребом *zero-day* рањивости у VPN инфраструктури.[1209] Ови случајеви су важни јер показују да Кина није само извор сајбер претњи, већ и мета операција других држава и државно повезаних актера, нарочито у периодима кризе и геополитичке неизвесности.

Најновији примери, које треба користити са јасно означеним степеном резерве, јесу кинеске оптужбе из 2025. године. У априлу 2025. кинеске власти у Харбину оптужиле су америчку NSA за „напредне“ сајбер нападе током Азијских зимских игара, наводећи да су мета били системи везани за сам догађај, али и критична инфраструктура у Хејлунгђангу и поједине кинеске компаније. У октобру 2025. кинеско Министарство државне безбедности оптужило је NSA и за вишегодишње нападе на National Time Service Center, уз тврдњу да су од 2022. до 2024. покушаване инфилтрације у системе релевантне за комуникације, финансије и електроенергетску

[1206] Lora Saalman, Fei Su, and Larisa Saveleva Dovgal, *Cyber Crossover and its Escalatory Risks for Europe* (Stockholm: SIPRI, 2023), 8–10.
[1207] CERT-EU, “Cyber Security Brief 23-08 – July 2023,” July 2023; “China says Wuhan earthquake centre attacked by overseas hackers,” *Reuters*, July 26, 2023.
[1208] CNCERT/CC, “CNCERT/CC Found and Handled Two U.S. Cyber Attacks on China’s Large-Scale Tech Firms,” January 17, 2025.
[1209] “Vietnam-linked hackers targeted Chinese government over coronavirus response, FireEye says,” *Reuters*, April 22, 2020; Center for Strategic and International Studies, *Significant Cyber Incidents*, timeline entry for April 2020.

мрежу.[1210] И у једном и у другом случају потребно је изричито нагласити да су то кинеске службене оптужбе и да нису у истој мери независно потврђене као, на пример, случај оптужнице против јединице 61398. Али управо због тога су корисне за научну анализу: оне показују како Пекинг постепено гради и сопствени наратив о томе да је Кина истовремено и сајбер сила и жртва туђих сајбер операција.

Ако се сви ови примери посматрају као целина, добија се прилично јасна слика. Најчвршће документовани примери кинеских војних сајбер напада и даље су они који се везују за ПЛА јединицу 61398 и, уз нешто већу резерву, за јединицу 61486. После 2015. године јавна атрибуција конкретних војних јединица постаје ређа и тежа, док у први план излазе шири појмови попут „кинески државно спонзорисани актери“, „сајбер снаге НР Кине“ или групе које се чешће везују за Министарство државне безбедности него за НОАК. Са друге стране, примери у којима су кинески системи били мета постоје, али су мање уједначени по степену доказаности: неки су забележени у независним базама и аналитичким прегледима, док су други пре свега део кинеских службених тврдњи и државног наратива.

6.7 Улога НР Кине у обликовању глобалних трендова сајбер безбедности

Значај Кине у обликовању глобалних трендова сајбер безбедности. не произлази само из њене технолошке величине, обима дигиталне економије и војне модернизације, већ и из чињенице да је Пекинг развио препознатљив и утицајан модел разумевања сајбер простора. У том моделу, сајбер безбедност се не третира као уско техничко питање заштите мрежа, већ као спој државног суверенитета, политичке стабилности, технолошке самосталности, економског развоја и националне одбране. Кина је постала један од кључних актера који утичу на то како се глобално разумеју појмови сајбер управљања, дигиталне отпорности, критичне инфраструктуре, технолошке зависности и државног понашања у сајбер простору.[1211]

Први и вероватно најзначајнији утицај НР Кине на глобалне трендове сајбер безбедности огледа се у томе што је она снажно афирмисала државоцентричан приступ сајбер простору, заснован на идеји сајбер суверенитета. У кинеским званичним документима, нарочито у белим књигама Jointly Build a Community with a Shared Future in Cyberspace из 2022. године и China’s Law-Based Cyberspace Governance in the New Era из 2023. године, јасно се наглашава да међународно управљање интернетом и сајбер простором мора почивати на уважавању суверенитета сваке државе, њеног права да уређује сопствени дигитални простор и да самостално одлучује о правилима која важе унутар њених мрежа и платформи.[1212] На глобалном плану, овај приступ је имао двоструки ефекат. С једне стране, Кина је постала водећи заговорник норме према којој државе не треба да буду пасивни посматрачи дигиталне глобализације, већ активни регулатори сопственог кибернетичког простора. С друге стране, овај кинески приступ допринео је ширем јачању тренда који се данас често описује као дигитални суверенитет, односно тежња држава да

[1210] “China accuses U.S. of launching ‘advanced’ cyberattacks, names alleged NSA agents,” *Reuters,* April 15, 2025; “China accuses U.S. of cyber breaches at national time centre,” *Reuters*, October 19, 2025.
[1211] State Council Information Office of the People’s Republic of China, *Jointly Build a Community with a Shared Future in Cyberspace* (Beijing, November 2022); Ministry of Foreign Affairs of the People’s Republic of China, *International Strategy of Cooperation on Cyberspace*, March 1, 2017.
[1212] State Council Information Office of the People’s Republic of China, *Jointly Build a Community with a Shared Future in Cyberspace*; State Council Information Office of the People’s Republic of China, *China’s Law-Based Cyberspace Governance in the New Era* (Beijing, March 2023).

смање зависност од страних платформи, инфраструктуре, стандарда и технолошких ланаца вредности.[1213]

Други важан правац кинеског утицаја односи се на повезивање сајбер безбедности са правним и институционалним уређењем дигиталног окружења. Кина не настоји да своју сајбер стратегију обликује само кроз војне документе и безбедносне наративе, већ истовремено гради свеобухватан правни оквир за податке, критичну информациону инфраструктуру, платформе, алгоритме, сајбер безбедност и јавну власт у дигиталном простору. Бела књига из 2023. године због тога има велику међународну тежину јер показује да је Пекинг сајбер безбедност уклопио у шири модел управљања, у коме се законодавство, регулаторни надзор, технички стандарди и институционална контрола посматрају као јединствен систем.[1214] Овај модел је утицао на глобалне трендове јер је многим државама, нарочито оним које су склоније снажнијој улози државе у дигиталном простору, показао да је могуће сајбер политику засновати не само на тржишној саморегулацији и либералној интероперабилности, већ и на снажној правној и административној координацији. На тај начин, Кина је постала један од главних симбола глобалног померања са идеје „отвореног интернета без граница“ ка идеји „управљивог, регулисаног и суверено организованог дигиталног простора“.

Кинеског утицај се види и у области међународних норми и дипломатских расправа о сајбер безбедности. Пекинг инсистира на томе да Уједињене нације имају централну улогу у обликовању правила понашања држава у сајбер простору, да безбедност не може да се гради кроз једностране интерпретације и да појам суверенитета мора да има примену и у сајбер домену. Кина је у разним мултилатералним форматима — укључујући расправе у УН и рад Отворене радне групе о безбедности и употреби информационо-комуникационих технологија — подржавала приступ који наглашава мирно решавање спорова, одбацивање логике отворене сајбер ескалације и већу тежину државне сагласности у обликовању норми.[1215] Кинески утицај није нужно значио да је њена визија постала доминантна, али је несумњиво допринео томе да глобална расправа о сајбер безбедности више не буде вођена искључиво из перспективе западних либералних демократија. Самим тим, Кина је помогла да се међународна дебата трајно помери ка питањима суверенитета, неинтервенције, контроле ескалације и институционалне централности УН.

Посебно је значајна сарадња НР Кине са Уједињеним нацијама у области сајбер безбедности, јер управо кроз тај оквир Пекинг настоји да своју визију сајбер суверенитета преведе у шири међународни нормативни језик. Кина је, према сопственим званичним документима, подржавала водећу улогу УН у глобалном управљању сајбер простором и учествовала у раду Групе владиних експерата и Отворене радне групе за безбедност и употребу информационо-комуникационих технологија у контексту међународне безбедности.[1216] Поред тога, заједно са државама Шангајске организације за сарадњу, Кина је подржала предлог *Међународног кодекса понашања за*

[1213] Adam Segal, “When China Rules the Web: Technology in Service of the State,” *Foreign Affairs* 97, no. 5 (September/October 2018); Adam Segal, *China’s Vision for Cyber Sovereignty and the Global Governance of Cyberspace*, NBR Special Report no. 87 (Seattle: National Bureau of Asian Research, 2020).
[1214] State Council Information Office of the People’s Republic of China, *China’s Law-Based Cyberspace Governance in the New Era*.
[1215] United Nations Office for Disarmament Affairs, “Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025”; Ministry of Foreign Affairs of the People’s Republic of China, *China’s Positions on International Rules-making in Cyberspace*, October 20, 2021.
[1216] Ministry of Foreign Affairs of the People’s Republic of China, *China’s Positions on International Rules-making in Cyberspace*; United Nations Office for Disarmament Affairs, “Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025.”

информациону безбедност, који је био усмерен на формулисање права и одговорности држава у информационом простору.[1217] У оквиру УН процеса, Кина је настојала да нагласи неколико принципа а то су примена Повеље УН у сајбер простору, поштовање суверене једнакости држава, спречавање употребе информационо-комуникационих технологија за мешање у унутрашње послове других држава, заштиту критичне информационе инфраструктуре и развој механизма у којем би све државе, а не само технолошки најмоћнији актери, учествовале у креирању правила.[1218] Управо због тога сарадња Кине са УН није само техничко или дипломатско питање, већ један од главних канала кроз који Пекинг настоји да обликује будући међународни поредак у сајбер простору.

Утицај НР Кине на глобалне трендове сајбер безбедности везан је за технолошку и индустријску димензију. У кинеској стратегијској мисли, сајбер безбедност није одвојена од питања технологије, технолошке аутономије и контроле над кључним стандардима, мрежама и платформама. Анализе кинеске амбиције да постане „сајбер велесила“ показују да Пекинг сајбер политику повезује са производњом стандарда, развојем телекомуникационих инфраструктура, дигиталним ланцима вредности и концептом „независних и контролисаних“ система.[1219] Ово питање има глобалне последице јер је подстакло и друге државе да безбедност све више повезују са питањем технолошке зависности. У том смислу, кинески успон није утицао само кроз сопствене прописе и безбедносне доктрине, већ и кроз чињеницу да је натерао друге велике актере да озбиљније размишљају о безбедности телекомуникационих мрежа, софтверских екосистема, стандарда, добављачких ланаца и дигиталне инфраструктуре.

Кинески утицај се огледа у томе што је војно и обавештајно деловање актера повезаних са Кином снажно обликовало глобалне приоритете у заштити критичне инфраструктуре. Последњих година западне владе, а посебно Сједињене Државе, све чешће упозоравају да кинески државно спонзорисани актери не делују само ради класичне шпијунаже, већ и ради дуготрајног прикривеног позиционирања у мрежама, како би у условима кризе могли да угрозе или ометају кључне услуге. Случај Volt Typhoon постао је глобално значајан јер је у званичним америчким упозорењима представљен као пример дуготрајног приступа критичној инфраструктури, уз употребу техника које се ослањају на легитимне системске алате и тешко се уочавају класичним безбедносним механизмима.[1220] Последица тога није само јачање антикинеских безбедносних политика, већ и шири помак у глобалном разумевању сајбер безбедности: критична инфраструктура, отпорност, видљивост мрежа, сарадња државе и приватног сектора и припрема за сајбер претње постале су централне теме међународне безбедносне расправе. На тај начин је Кина, било као активни стратегијски актер било као перципирани извор високоризичних сајбер

[1217] United Nations General Assembly, *Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General*, A/69/723, January 13, 2015; Ministry of Foreign Affairs of the People's Republic of China, *International Code of Conduct for Information Security*, September 12, 2011.
[1218] Ministry of Foreign Affairs of the People's Republic of China, *China's Positions on International Rules-making in Cyberspace*; United Nations Office for Disarmament Affairs, "Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025."
[1219] Segal, "When China Rules the Web"; Segal, *China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace*.
[1220] Cybersecurity and Infrastructure Security Agency, *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, Joint Cybersecurity Advisory AA24-038A, February 7, 2024; Microsoft Threat Intelligence, "Volt Typhoon Targets US Critical Infrastructure with Living-off-the-Land Techniques," May 24, 2023.

активности, утицала на то да глобални дискурс сајбер безбедности све више тежиште ставља на отпорност, континуитет услуга и заштиту друштвено критичних система.[1221]

Важан аспект је и чињеница да је Кина сајбер безбедност све отвореније повезивала са војно-цивилном фузијом, вештачком интелигенцијом, великим количинама података и дигиталном инфраструктуром двоструке намене. У кинеском приступу, безбедност мрежа, технолошки развој, индустријска политика и војна модернизација не стоје као одвојене области, већ као узајамно повезани елементи једног ширег пројекта националне моћи.[1222] То има глобалне последице јер утиче на промену саме дефиниције сајбер безбедности. Ако је раније у многим државама сајбер безбедност била углавном везивана за заштиту информационих система од техничких упада, кинески модел и реакције на њега допринели су томе да се она све више схвата као питање државне стратегије, индустријске базе, стандарда, алгоритамске моћи, обраде података и војне примене нових технологија. Другим речима, Кина није само утицала на то како се бране мреже, већ и на то шта се уопште сматра пољем сајбер безбедности.

Уз све побројано, потребно је нагласити да кинески утицај на глобалне трендове сајбер безбедности није једносмеран нити искључиво нормативан. Кина је истовремено и нормативни актер, јер нуди визију сајбер суверенитета, правно заснованог управљања и државне координације, и стратешки катализатор, јер њене способности, праксе и амбиције приморавају друге државе да убрзано унапређују сопствене моделе одбране, отпорности и регулаторног надзора. Управо у томе је њена специфична глобална улога: Пекинг не обликује глобалне трендове само зато што активно промовише сопствене идеје, већ и зато што његов успон мења понашање других актера. Растућа забринутост за критичну инфраструктуру, дигитални суверенитет, сигурност телекомуникационих мрежа и технолошку самосталност у многим деловима света делимично је производ управо кинеске тежине у савременом дигиталном поретку. Стога је НР Кина постала један од главних полова око којих се обликује савремена глобална расправа о сајбер безбедности.[1223]

За разумевање савремених међудржавних односа неопходно је посматрати Кину не само као једног од учесника у глобалној сајбер безбедности, већ као једног од њених кључних обликовалаца.

[1221] Cybersecurity and Infrastructure Security Agency, *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*; Microsoft Threat Intelligence, "Volt Typhoon Targets US Critical Infrastructure with Living-off-the-Land Techniques."
[1222] State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing, July 2019); Alex Stone and Peter Wood, *China's Military-Civil Fusion Strategy: A View from Chinese Strategists* (Montgomery, AL: China Aerospace Studies Institute, 2020).
[1223] Segal, *China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace*; Ministry of Foreign Affairs of the People's Republic of China, *China's Positions on International Rules-making in Cyberspace*.

7. Закључак

Савремени развој међународних односа јасно показује да сајбер простор више не може да се посматра као искључиво технолошко окружење које само прати политичке, безбедносне и војне процесе, већ као једно од кључних поља у коме се ти процеси обликују, продубљују, убрзавају, и, у све већој мери, одлучују.

Основна полазна теза ове дисертације била је да сајбер ратовање између држава није периферна, пролазна или искључиво техничка појава, већ структурни део савремене моћи, безбедности и сукоба. Анализа је показала да је таква теза оправдана. Сајбер простор се током последњих деценија развио у домен у коме државе не само да бране сопствене информационе системе и критичну инфраструктуру, већ у њему трајно делују ради остваривања геополитичких, војних, економских и обавештајних предности. Сајбер ратовање данас, и у будуће, треба разумети и прихватити као трајни облик стратегијског надметања, а не као појаву која настаје тек у моменту отвореног оружаног сукоба.

Полазећи од опште хипотезе дисертације, према којој сајбер ратовање представља специфичан облик стратешког деловања држава у савременим међународним односима, може се закључити да је спроведено истраживање у целини потврдило њену основну научну претпоставку. Анализа је показала да сајбер ратовање није само „ново“ средство у арсеналу држава, већ посебан облик деловања који мења начин на који се моћ производи, употребљава, прикрива и пројектује у међународном систему. За разлику од традиционалне примене силе, која се најчешће повезује са физичким простором, видљивом употребом војних средстава, јаснијим актерима и непосредним материјалним последицама, сајбер ратовање делује у простору који је нематеријалан, мрежно повезан, технолошки посредован и правно недовољно прецизно регулисан. Сајбер ратовање не представља само техничку иновацију у области безбедности, већ дубоку трансформацију саме природе стратегијског надметања.

Истраживање је потврдило да се специфичност сајбер ратовања огледа најпре у средствима и методама деловања држава. Док се традиционална војна сила заснива на употреби оружја, војних јединица, контроле територије и физичког уништења, сајбер деловање користи дигиталне алате, злонамерни код, мрежне инфраструктуре, експлоатацију рањивости, манипулацију подацима, електронско позиционирање и операције утицаја. Оно може да буде усмерено не само на војне и стратешке циљеве, већ и на цивилну инфраструктуру, енергетске мреже, финансијске системе, комуникационе платформе, изборне процесе, медијски простор, државну управу и приватни сектор. На овај начин, сајбер ратовање проширује поље стратегијског деловања далеко изван класичног бојишта и показује да савремена државна моћ више не зависи само од способности физичке принуде, већ и од способности контроле, заштите, нарушавања и обликовања дигиталних система.

Посебно је значајно то што је истраживање потврдило да се простор извођења сајбер ратовања битно разликује од простора традиционалног сукоба. Сајбер простор није ограничен класичним границама државне територије, али није ни потпуно одвојен од ње. Сајбер простор истовремено почива на физичкој инфраструктури, глобалним мрежама, приватним платформама, националним регулативама и транснационалним токовима података. Управо због те хибридне природе, сајбер операције могу да производу ефекте унутар једне државе, могу да буду покренуте са територије друге, да пролазе кроз инфраструктуру трећих држава и да укључе актере чија веза са државом не може увек лако да се докаже. Просторна димензија сајбер ратовања чини овај феномен посебно

сложеним, јер доводи у питање класичне категорије границе, надлежности, одговорности и суверенитета.

Потврђен је и део хипотезе који се односи на актере сајбер ратовања. Иако су државе остале централни носиоци стратегијског деловања, сајбер простор је омогућио значајну улогу и другим актерима попут обавештајних служби, војним сајбер командама, приватним технолошким компанијама, хакерским групама, прокси актерима, криминалним мрежама, истраживачким заједницама и платформама које управљају енормном количином података. Ова чињеница не умањује улогу државе, већ је чини сложенијом. Савремена држава у сајбер простору не делује само кроз класичне органе власти, већ и кроз мреже сарадње, прикривене канале, партнерства са приватним сектором, нормативне инструменте и технолошке капацитете који су неретко изван директне војне структуре. Због тога је сајбер ратовање истовремено државно, мрежно, институционално и делимично прикривено деловање.

Један од најјасније потврђених елемената опште хипотезе јесте проблем атрибуције. У традиционалним облицима употребе силе, иако ни они нису увек потпуно јасни, једноставније је утврдити ко је извршилац напада, одакле напад долази и које су његове непосредне последице. У сајбер простору, међутим, атрибуција је технички, политички и правно сложен процес. Напад може да буде прикривен, усмерен преко туђе инфраструктуре, изведен употребом алата који могу да се копирају или лажно припишу другом актеру, а његови трагови могу да буду намерно постављени како би довели до погрешног закључка. Истовремено, чак и када постоје техничке индиције, политичка одлука да се одговорност за напад јавно припише одређеној држави зависи од ширег дипломатског, безбедносног и стратешког контекста. Због тога атрибуција у сајбер ратовању није само техничко питање, већ и питање моћи, кредибилитета, савезништва и политичке процене.

Истраживање је показало и да се последице сајбер ратовања разликују од последица традиционалне примене силе. Оне не морају увек да буду видљиве у облику физичког уништења, људских жртава или заузимања територије, али могу да оставе дубоко дестабилизујуће последице. Сајбер операције могу да наруше поверење у институције, да доведи до прекида јавних услуга, угрозе критичну инфраструктуру, компромитују поверљиве податке, ослабе економску стабилност, утичу на политичке процесе, смање способност државе да управља кризом и створе дугорочан осећај несигурности у друштву. Важно је истаћи да последице сајбер ратовања не треба мерити само степеном физичке штете, већ и степеном нарушавања функционалности, поверења, отпорности и способности државе да одржи контролу над сопственим системима.

Други део опште хипотезе, који полази од претпоставке да ће у условима растућих геополитичких тензија велике силе наставити да развијају сајбер капацитете и да ће сајбер простор све изразитије укључивати у своје доктрине, стратешке документе и безбедносне политике, такође је потврђен. Упоредна анализа војних стратегија Сједињених Америчких Држава, Народне Републике Кине и Руске Федерације показала је да сајбер простор више није споредна област националне безбедности, већ један од њених централних стубова. Свака од ових сила, на различит начин и у складу са сопственом стратешком културом, настоји да институционализује сајбер деловање, развије доктринарне основе, ојача технолошку независност, заштити критичну инфраструктуру и обезбеди способност деловања у дигиталном окружењу. То показује да сајбер капацитети постају трајни део државне моћи, а не привремени одговор на појединачне претње.

У том смислу, Сједињене Америчке Државе, Кина и Русија потврђују различите, али међусобно упоредиве путање развоја сајбер моћи. Амерички модел показује како се сајбер простор интегрише у војне, обавештајне, институционалне, савезничке и регулаторне механизме глобалне силе. Руски модел показује како се сајбер деловање уклапа у шири концепт информационог сукоба, политичког утицаја, стратешке нејасноће и хибридног надметања. Кинески модел показује како се сајбер простор може разумети као продужетак државног суверенитета, партијскодржавне контроле, технолошке модернизације и дугорочног националног развоја. Иако се ови модели разликују, они потврђују исту основну тенденцију а то је да велике силе више не могу да замисле националну безбедност, војну стратегију, економску моћ и политички утицај без систематског развоја сајбер капацитета.

На основу тога може се закључити да је општа хипотеза дисертације потврђена не само на теоријском, већ и на емпиријском нивоу. Теоријски, рад је показао да сајбер ратовање поседује довољно специфичности да не може да се сведе на традиционалну употребу силе нити на класичну информациону безбедност. Емпиријски, анализа стратешких докумената, институционалних решења и праксе великих сила показала је да државе сајбер простор све изразитије третирају као домен трајног стратегијског надметања. Зато се може рећи да сајбер ратовање представља један од најзначајнијих показатеља трансформације савремених међународних односа јер мења средства сукоба, проширује простор деловања, усложњава актере, отежава утврђивање одговорности и производи последице које могу да буду подједнако озбиљне као и последице традиционалних облика притиска и принуде.

Због свега наведеног, потврда опште хипотезе има и шири научни значај. Она показује да се сајбер ратовање не може да се анализира искључиво у оквирима техничке сајбер безбедности, већ мора да буде предмет интердисциплинарног проучавања које обухвата међународне односе, студије безбедности, војну стратегију, међународно право, политичку теорију, технологију и јавне политике. Такав приступ омогућава разумевање чињенице да сајбер простор није неутралан технички амбијент, већ политички и стратегијски простор у коме се обликују односи моћи између држава. Стога је једна од теза ове дисертација становиште да сајбер ратовање треба разумети као један од кључних феномена савремених међународних односа, јер оно истовремено одражава и убрзава промене у начину на који државе штите своје интересе, пројектују моћ и воде сукобе у дигиталном добу.

Један од најважнијих закључака до којих је истраживање дошло јесте да су државе и даље кључни актери сајбер сукоба. Иако је ранија литература, нарочито у првим фазама развоја интернета, често наглашавала децентрализовану природу дигиталног простора и претпостављала да ће државе у њему изгубити део свог традиционалног значаја, развој праксе је показао супротно. Најмоћније државе нису нестале из сајбер простора већ су га институционално преобликовале, правно регулисале, војно интегрисале и технолошки структурисале. Данас државе креирају националне сајбер стратегије, оснивају специјализоване команде у војним организационим јединицама, развијају офанзивне и дефанзивне капацитете, доносе законе о критичној инфраструктури, регулишу податке, дефинишу сајбер суверенитет и све чешће сајбер средство повезују са економском, индустријском и спољнополитичком стратегијом. Сајбер простор је постао нова позорница старог процеса борбе за моћ, утицај и безбедност, али сада у технолошки изузетно динамичном облику.

Упоредна анализа Сједињених Америчких Држава, Народне Републике Кине и Руске Федерације показала је да не постоји један универзалан модел сајбер ратовања, већ да свака од ових сила

развија сопствени концепт у складу са сопственом политичком традицијом, стратешком културом, институционалном архитектуром и перцепцијом претњи. Истовремено је утврђено да између њих постоји и важна заједничка основа а то је да све три државе сајбер простор посматрају као кључну сферу националне безбедности, као домен у коме могу да се остваре асиметричне предности и као простор у коме се границе између мира, кризе и сукоба замагљују. Сајбер више није додатак класичном ратовању, он је постао саставни део стратегије у целини.

У случају Сједињених Америчких Држава, истраживање је показало да је реч о најразвијенијем и институционално најкомплекснијем моделу сајбер ратовања. Амерички приступ је током времена еволуирао од ранијег уклапања сајбер деловања у шири оквир информационих операција ка јасном признавању сајбер простора као засебног оперативног домена. Та еволуција није била само доктринарна, већ дубоко организациона и политичка. Развој USCYBERCOM-а, изградња Cyber Mission Force, концепти persistent engagement и defend forward, као и деловање ширег федералног екосистема који обухвата NSA, CISA, FBI, OMB и ONCD, показују да САД сајбер простор не третирају као техничку функцију, већ као централни инструмент интегрисаног одвраћања, одбране домовине и глобалне пројекције моћи. Посебан значај америчког модела је у томе што повезује војни систем, обавештајну праксу, јавну политику, буџетску координацију, приватни сектор и савезничке мреже. Амерички приступ представља парадигму развијеног државног сајбер модела али истовремено, тај модел отвара и највећи број правних и политичких спорова, јер најотвореније легитимише трајно деловање испод прага рата, прекограничне операције и релативно флексибилно тумачење међународноправних ограничења.

Руски модел је, с друге стране, показао другачију унутрашњу логику. За разлику од америчког нагласка на „сајбер безбедности“ и оперативном домену, руски приступ је укорењен у шири концепт „информационе безбедности“, који обухвата и техничку и когнитивну, и инфраструктурну и друштвено-политичку димензију. Управо зато руска сајбер стратегија не прави тако оштру линију између напада на системе и утицаја на друштво, између мрежног деловања и психолошко-информационог ефекта. Анализа руских доктринарних докумената показала је континуитет у појму заштите информационог простора државе, очувања суверенитета, контроле над информативном сфером и одбране политичке стабилности. У практичном смислу, руски модел се показује као модел који високо вреднује вишеслојност деловања и повезивање сајбер операција са ширим инструментима хибридног надметања. Руска пракса игра важну улогу у обликовању сиве зоне између мира и рата. Напади на критичну инфраструктуру, операције утицаја, обавештајно позиционирање и дигитално подривање поверења у институције не појављују се као одвојене активности, већ као делови исте стратегијске логике. Из тог угла, руски модел показује да сајбер ратовање може да буде схваћено мање као издвојени технички напад, а више као средство за системско разарање противничке отпорности, дезоријентацију, притисак и политичко обликовање кризе.

Кинески модел се издваја по снажној вези између сајбер суверенитета, партијскодржавне контроле, правно-нормативног уређивања интернета и дугорочне технолошке стратегије. За Кину сајбер простор није само арена претњи и операција, већ и простор управљања, развоја и очувања државног ауторитета. Беле књиге, закони и институционална решења показали су да кинеско схватање сајбер ратовања не може да буде одвојено од ширег концепта сајбер суверенитета, контроле токова података, филтрирања информација, управљања платформама и развоја технолошке самосталности. Истовремено, војни аспект тог модела, нарочито у контексту PLA, некадашње Стратешке потпорне снаге и њене реорганизације 2024. године кроз јачање информационих, сајбер и космичких капацитета под непосреднијом контролом Централне војне

комисије, показује да Кина сајбер посматра као домен који мора да буде интегрисан са космичким, обавештајним и информационим капацитетима. Кинески приступ можда наизглед делује мање „спектакуларно“ од америчког у погледу отворених доктринарних формула о офанзивном деловању, али је стратешки дубоко интегрисан, јер повезује безбедност, индустрију, право, контролу интернета, национални развој и војну модернизацију у јединствену државну логику. Из те перспективе, кинески модел показује да сајбер ратовање није нужно само питање употребе дигиталне силе у ужем смислу, већ и питање трајног обликовања дигиталног окружења тако да оно постане подложно политичким и безбедносним циљевима државе.

Упоредна анализа ове три силе доводи до важног закључка а то је да, иако се њихови модели разликују, све три државе потврђују да сајбер ратовање више није могуће разумети искључиво као низ изолованих хакерских напада. Сајбер ративање данас обухвата читав спектар деловања као што су шпијунажа, позиционирање у противничким мрежама, припрема бојишта, ремећење критичне инфраструктуре, утицај на јавност, дестабилизација одлучивања, заштита сопствених мрежа, изградња правног оквира, технолошка политика, индустријска стратегија и савезничка координација. То је и суштински резултат овог истраживања: сајбер ратовање није више ужа подкатегорија војне технике, већ свеобухватни облик стратегијског деловања који захвата више нивоа државне моћи.

Посебно важан допринос овог рада јесте уочавање да сајбер простор не сме да буде изолован од осталих домена безбедности. Анализа је показала да Сједињене Америчке Државе, Кина и Русија сајбер простор све чешће посматрају као домен који је нераздвојив од информационог окружења, економије, технологије, енергетике, логистике и укупне отпорности државе. То не значи да сајбер ратовање замена за традиционални оружани сукоб, али јесте средство које мења начин на који се класично ратовање припрема, подржава, одлаже, убрзава или замењује деловањем испод прага. Другим речима, сајбер није једини домен савременог сукоба, али је домен који продире у све остале. Његов значај у савременој стратегији превазилази оквир уске „сајбер безбедности“.

Питање суверенитета једно је од централних теоријских и практичних питања сајбер ратовања. У класичном међународноправном оквиру територија и граница представљају темељ државне безбедности и међусобног разграничења надлежности. У сајбер простору, међутим, држава може да буде угрожена без физичког преласка границе, а може и сама да делује унутар туђе инфраструктуре без конвенционалне инвазије. Та чињеница не укида суверенитет, али га чини суштински сложенијим. Амерички приступ настоји да задржи широк простор за деловање испод прага силе; руски приступ наглашава заштиту сопствене информационе сфере и истовремено користи нејасноћу као средство деловања; кинески приступ суверенитет проширује дубоко унутар дигиталног простора, укључујући контролу података, платформи и садржаја. Ови различити приступи показују да се суверенитет у дигиталном добу не напушта, већ реинтерпретира постајући истовремено техничко, правно, политичко и инфраструктурно питање. С тим је тесно повезано и питање међународног права. Међународноправни оквир, иако важан, и даље заостаје за стварношћу државне праксе. Нема сумње да су кључна начела међународнох права (забрана употребе силе, суверена једнакост, немешање, самоодбрана, државна одговорност) и даље релевантна. Међутим, у сајбер простору њихова примена постаје далеко сложенија. Тешкоће атрибуције, нејасноћа око прага употребе силе, проблем разликовања шпијунаже, саботаже, сајбер тероризма, позиционирања и напада, као и растућа пракса деловања испод прага оружаног сукоба, показују да постојећа правила нису довољно прецизна да би сама по себи обезбедила висок ниво правне извесности. Из тога произилази да је сајбер ратовање истовремено

и практичан и нормативан изазов мењајући начин на који се државе сукобљавају и услове под којима право покушава да ту стварност уреди.

Још један важан резултат истраживања односи се на однос између офанзиве и одбране. У класичној војној теорији та два појма се релативно јасно разликују, али у сајбер простору граница између њих постаје нестабилна. Многе операције које државе представљају као „одбрану“ у стварности подразумевају деловање у туђим мрежама, тражење и ремећење претњи далеко од сопствене територије, па чак и припрему будућих опција деловања. САД су ову логику најотвореније формулисале кроз defend forward, Русија је практикује кроз дуготрајно позиционирање и операције утицаја, Кина је спроводи унутар много ширег оквира управљања дигиталним простором и технолошке безбедности. Сајбер одбрана не може да се разуме искључиво као пасивна заштита сопствених система, већ и као активно, често прекогранично деловање ради спречавања, ублажавања и обликовања претње пре него што она произведе ефекат. У овом сегменту се открива једна од најдубљих трансформација савремене безбедности која доводи до тога да одбрана постаје проактивна, трајна и делимично офанзивна.

Иако је предмет ове дисертације био усмерен на анализу великих сила и њихових модела сајбер ратовања, резултати истраживања имају значај и за мање државе, укључујући и Републику Србију. Србија је у претходном периоду развијала стратешки и нормативни оквир у области информационог друштва и информационе безбедности, али савремена динамика сајбер претњи показује да ће у наредном периоду бити неопходно да тај оквир буде додатно унапређен, конкретизован и прилагођен реалности у којој сајбер простор постаје један од кључних домена међународног надметања. Ауторка ове дисертације изражава наду да ће Република Србија у будућности наставити да развија свеобухватну, модерну и јасно операционализовану стратегију сајбер безбедности, која ће обухватити заштиту критичне инфраструктуре, јачање институционалних капацитета, сарадњу јавног и приватног сектора, развој стручних кадрова, међународну сарадњу, образовање грађана и изградњу националне сајбер отпорности. Такав приступ био би од посебног значаја јер државе које на време препознају стратешку вредност сајбер простора не штите само своје информационе системе, већ и сопствени суверенитет, демократске институције, економску стабилност и дугорочну безбедност друштва.

У светлу свега наведеног, може да се закључи да су државе у сајбер сукобима ушле у фазу трајне конкуренције која више не зависи искључиво од постојања формално проглашеног рата. Сајбер простор је постао подручје у коме се константно испитују рањивости, постављају капацитети, тестирају границе толерисаног понашања, шаљу сигнали, намећу трошкови и обликује понашање противника.

На крају, најопштији и најважнији закључак ове дисертације гласи да сајбер ратовање није пролазна епизода у историји међународних односа, већ трајна последица дигиталне трансформације државе, друштва и безбедности. Сједињене Америчке Државе, Кина и Русија показују три различите, али подједнако значајне путање тог развоја. Упркос разликама у њиховим доктринама, све три силе потврђују исту историјску чињеницу: ко данас контролише способност деловања у сајбер простору, не контролише само мреже, већ у великој мери и услове под којима ће се у будућности одвијати политичко надметање, војна принуда, економска безбедност и сам опстанак државне моћи. Због тога је сајбер ратовање једно од централних питања савремене политике, стратегије, безбедности и међународнх односа.

Литература:

1. Albright, David, Paul Brannan, and Christina Walrond. “Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?” Institute for Science and International Security, December 22, 2010.
2. Ali, Idrees, and Phil Stewart. “Exclusive: U.S. Carried Out Secret Cyber Strike on Iran in Wake of Saudi Oil Attack: Officials.” Reuters, October 16, 2019.
3. Arquilla, John, and David Ronfeldt. “Cyberwar Is Coming!” Comparative Strategy 12, no. 2 (1993): 141–165.
4. Australian Signals Directorate, Australian Cyber Security Centre. Supporting Australian Organisations through a Cyber Security Incident. Canberra: ASD/ACSC, 2024.
5. Biden, Joseph R., Jr. Executive Order 14028. “Improving the Nation’s Cybersecurity.” Federal Register 86, no. 93 (May 17, 2021): 26633–47.
6. Biden, Joseph R., Jr. Executive Order 14144. “Strengthening and Promoting Innovation in the Nation’s Cybersecurity.” Federal Register 90, no. 11 (January 17, 2025): 6755–71.
7. Blagojević, Veljko. „Strategija nacionalne bezbednosti SAD iz 2025: kontinuitet i promene.” Međunarodna politika 77, br. 1196 (2026): 79–103.
8. Blasco, Jaime, and Juan Andres Guerrero-Saade. “Reviewing the 2022 KA-SAT Incident and Implications for Distributed Communication Environments.” Virus Bulletin Conference Proceedings, 2024.
9. Boyson, Sandor, et al. NotPetya: A Columbia University Case Study. New York: Columbia University, 2022.
10. Bradford, Anu. The Brussels Effect: How the European Union Rules the World. New York: Oxford University Press, 2020.
11. Brenner, Susan W. “U.S. Cybercrime Law: Defining Offenses.” Information & Communications Technology Law 13, no. 3 (2004): 231–243.
12. Buchanan, Ben. The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Cambridge, MA: Harvard University Press, 2020.
13. Buchan, Russell. “The International Legal Regulation of Cyber Espionage.” In Cyber Espionage and International Law, 2016.
14. Canadian Centre for Cyber Security. Cyber Threat Activity Related to the Russian Invasion of Ukraine. Ottawa: Canadian Centre for Cyber Security, 2022.
15. Carter, Ashton B. “Remarks by Secretary Carter at a Troop Event at Joint Base Lewis-McChord, Washington.” U.S. Department of Defense, March 4, 2016.
16. Carter, Ashton B. “Remarks by Secretary Carter at the University of Oxford’s Blavatnik School of Government.” U.S. Department of Defense, September 7, 2016.
17. Case Study: The NotPetya Campaign. Budapest: Ludovika University of Public Service, 2024.
18. Citizen Lab. “Submission to the UN Working Group on the Use of Mercenaries.” March 25, 2026.
19. Clarke, Richard A., and Robert K. Knake. Cyber War: The Next Threat to National Security and What to Do About It. New York: Ecco/HarperCollins, 2010.
20. Clausewitz, Carl von. On War. Translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.
21. Conway, Maura. “Cyberterrorism: Hype and Reality.” 2007.
22. Costello, John, and Joe McReynolds. China’s Strategic Support Force: A Force for a New Era. China Strategic Perspectives 13. Washington, DC: Institute for National Strategic Studies, National Defense University Press, 2018.

23. Council of Europe. Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems. Strasbourg: Council of Europe, 2003.
24. Council of Europe. Convention on Cybercrime. ETS No. 185. Budapest: Council of Europe, November 23, 2001.
25. Council of Europe. Explanatory Report to the Convention on Cybercrime. ETS No. 185. Budapest: Council of Europe, November 23, 2001.
26. Council of the European Union. "Malicious Cyber-Attacks: EU Sanctions Two Individuals and One Body over 2015 Bundestag Hack." October 22, 2020.
27. Council of the European Union. "Russian Cyber Operations against Ukraine: Declaration by the High Representative on Behalf of the European Union." Brussels: Council of the European Union, May 10, 2022.
28. Council on Foreign Relations. "APT10." Cyber Operations Tracker. Приступљено 17. маја 2026.
29. Council on Foreign Relations. "Compromise of Saudi Aramco and RasGas." Cyber Operations Tracker. Приступљено 17. маја 2026.
30. Council on Foreign Relations. "Compromise of TV5 Monde." Cyber Operations Tracker. Приступљено 17. маја 2026.
31. Council on Foreign Relations. "Cyber Proxies in the Ukraine Conflict: Implications for International Norms." March 21, 2022.
32. Cyber Law Toolkit. "Cyber Attacks against Estonia (2007)." NATO Cooperative Cyber Defence Centre of Excellence, 2021.
33. Cyber Law Toolkit. "Georgia-Russia Conflict (2008)." NATO Cooperative Cyber Defence Centre of Excellence.
34. Cybercrime Convention Committee (T-CY). T-CY Guidance Note #3: Transborder Access to Data (Article 32). Strasbourg: Council of Europe, 2014.
35. CyberPeace Institute. "Case Study: Viasat Attack."
36. Cybersecurity and Infrastructure Security Agency. "Building a Secure by Design Ecosystem." January 13, 2025.
37. Cybersecurity and Infrastructure Security Agency. "CISA Announces Secure by Design Commitments from Leading Technology Providers." May 8, 2024.
38. Cybersecurity and Infrastructure Security Agency. "CRASHOVERRIDE Malware." ICS-ALERT-17-206-01. Updated July 20, 2021.
39. Cybersecurity and Infrastructure Security Agency. "Cyber-Attack against Ukrainian Critical Infrastructure." IR-ALERT-H-16-056-01. Updated July 20, 2021.
40. Cybersecurity and Infrastructure Security Agency. "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)." Accessed May 8, 2026.
41. Cybersecurity and Infrastructure Security Agency. PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. Joint Cybersecurity Advisory AA24-038A, February 7, 2024.
42. Damnjanović, Ivana S. Odnos politike i tehnologije u savremenoj političkoj teoriji. Докторска дисертација. Универзитет у Београду, Факултет политичких наука, 2013.
43. Danish Centre for Cyber Security. State-Sponsored Global Software Supply Chain Attack. Copenhagen: CFCS, 2021.
44. Defense Advanced Research Projects Agency. "ARPANET." DARPA.
45. Deibert, Ronald J., Rafal Rohozinski, and Masashi Crete-Nishihata. "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War." Security Dialogue 43, no. 1 (2012): 3–24.

46. Denning, Dorothy E. “Statement of Dorothy E. Denning.” Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, May 23, 2000.
47. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union L333 (2022): 80–152.
48. Dragos. “Impact of FrostyGoop ICS Malware on Connected OT Systems.” 2024.
49. Dragos. “How to Protect against FrostyGoop: ICS Malware Targeting Operational Technology.” July 23, 2024.
50. Dragos, Inc. CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations. Hanover, MD: Dragos, 2017.
51. Durojaye, Henry, and Oluwaukola Raji. “Impact of State and State-Sponsored Actors on the Cyber Environment and the Future of Critical Infrastructure.” arXiv, 2022.
52. Ensafi, Roya, Philipp Winter, Abdullah Mueen, and Jedidiah R. Crandall. “Analyzing the Great Firewall of China over Space and Time.” Proceedings on Privacy Enhancing Technologies 2015, no. 1 (2015): 61–76.
53. Estonian Ministry of Defence. Cyber Security Strategy 2008–2013. Tallinn, 2008.
54. ESET. “ESET Finds Connection between Cyber Espionage and Electricity Outage in Ukraine.” 2016.
55. ESET. “Industroyer: Biggest Malware Threat to Critical Infrastructure Since Stuxnet.” 2017.
56. ESET. “Industroyer2: Industroyer Reloaded.” April 12, 2022.
57. ESET. ESET Threat Report T1 2022. 2022.
58. European Parliamentary Research Service. Understanding Cybercrime. Brussels: European Parliament, 2024.
59. European Union Agency for Cybersecurity (ENISA). Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches. Heraklion: ENISA, 2015.
60. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2025. Athens: ENISA, 2025.
61. European Union Agency for Cybersecurity (ENISA). How to Set up CSIRT and SOC. Athens: ENISA, 2020.
62. European Union Agency for Cybersecurity (ENISA). National Cyber Security Strategies in Europe. Athens: ENISA, 2021.
63. European Union Agency for Network and Information Security (ENISA). National Cyber Security Strategies: Practical Guide on Development and Execution. Heraklion: ENISA, 2012.
64. European Union Agency for Network and Information Security (ENISA). Updated Good Practice Guide on National Cyber Security Strategies. Heraklion: ENISA, 2016.
65. Europol. Cyber-Attacks: The Apex of Crime-as-a-Service. The Hague: Europol, 2023.
66. Europol. Internet Organised Crime Threat Assessment 2024. The Hague: Europol, 2024.
67. Europol. Online Jihadist Propaganda: 2023 in Review. The Hague: Europol, 2024.
68. Falco, Edoardo. Stuxnet Facts Report: A Technical and Strategic Analysis. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012.
69. Falliere, Nicolas, Liam O Murchu, and Eric Chien. W32.Stuxnet Dossier. Version 1.4. Symantec Security Response, February 2011.
70. Federal Bureau of Investigation. “The Cyber Threat.” Accessed May 8, 2026.
71. Federal Bureau of Investigation, and Cybersecurity and Infrastructure Security Agency. “Joint Statement from FBI and CISA on the People’s Republic of China (PRC) Targeting of Commercial Telecommunications Infrastructure.” November 13, 2024.

72. Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, National Security Agency, and Department of Energy. TRITON Malware Remains Threat to Global Critical Infrastructure. Washington, DC, 2022.
73. Federal Ministry of the Interior and Community. Cyber Security Strategy for Germany 2021. Berlin: Federal Ministry of the Interior and Community, 2021.
74. Federal Office for Information Security. "Federal Office for Information Security." Приступљено 17. маја 2026.
75. Finnish Transport and Communications Agency (Traficom). "Aviation Cyber Security." Приступљено 17. маја 2026.
76. Finnish Transport and Communications Agency (Traficom). "Glossary of Central Cyber Security Terms." Приступљено 17. маја 2026.
77. Floridi, Luciano. "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU." Philosophy & Technology 33, no. 3 (2020): 369–378.
78. Floridi, Luciano. The Fourth Revolution: How the Infosphere Is Reshaping Human Reality. Oxford: Oxford University Press, 2014.
79. French Ministry for the Armed Forces. Droit international appliqué aux opérations dans le cyberespace. Paris: Ministry for the Armed Forces, 2019.
80. French Ministry for the Armed Forces. "Le Commandement de la cyberdéfense (COMCYBER)." Приступљено 17. маја 2026.
81. Garamone, Jim. "Cyber Command Becomes Unified Combatant Command." U.S. Department of Defense News, May 4, 2018.
82. Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." International Security 38, no. 2 (Fall 2013): 41–73.
83. Geers, Kenneth. Strategic Cyber Security. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publications, 2011.
84. German Federal Armed Forces (Bundeswehr). "The Cyber and Information Domain Service." December 8, 2020.
85. Giles, Keir. "'Information Troops' — A Russian Cyber Command?" NATO Cooperative Cyber Defence Centre of Excellence, 2011.
86. Giles, Keir. "Russia's Public Stance on Cyberspace Issues." In 2012 4th International Conference on Cyber Conflict, edited by Christian Czosseck, Rain Ottis, and Katharina Ziolkowski, 63–75. Tallinn: NATO CCD COE Publications, 2012.
87. Google Threat Analysis Group. Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape. 2022.
88. Government of Israel. National Cybersecurity Strategy 2025. Jerusalem: Israel National Cyber Directorate, 2025.
89. Government Office of Estonia. Cyber Security Strategy 2014–2017. Tallinn: Government Office of Estonia, 2014.
90. Government of the Russian Federation and Government of the People's Republic of China. Agreement on Cooperation in Ensuring International Information Security. April 30, 2015.
91. Grisé, Michelle, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn, and Khrystyna Holynska. Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation. Santa Monica, CA: RAND Corporation, 2022.
92. Gutterman, Steve. "Putin Orders Russian Computers to Be Protected after Spy Attacks." Reuters, January 21, 2013.
93. Hartman, William J. "Posture Statement of Lieutenant General William J. Hartman." U.S. Cyber Command, April 9, 2025.

94. Haugh, Timothy D. “Posture Statement of General Timothy D. Haugh 2024.” U.S. Cyber Command, April 12, 2024.
95. Hodgson, Quentin E., Nathan Beauchamp-Mustafaga, Jeffrey W. Hornung, and others. Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace. Santa Monica, CA: RAND Corporation, 2019.
96. Human Rights Watch. “Russia: ‘Big Brother’ Law Harms Security, Rights.” July 12, 2016.
97. Information System Authority of Estonia. “SSSCIP Chief: Russia Operates More Covertly in Cyberspace.” February 17, 2025.
98. International Institute for Strategic Studies. Great-Power Offensive Cyber Campaigns: Experiments in Strategy – 2. US Cyber Campaigns. London: IISS, 2022.
99. Joint Chiefs of Staff. Joint Doctrine for Information Operations. Joint Pub 3-13. Washington, DC: Joint Chiefs of Staff, October 9, 1998.
100. Joint Chiefs of Staff. Joint Publication 3-12: Cyberspace Operations. Washington, DC: Joint Chiefs of Staff, 2018.
101. Jonev, Katarina. „Sajber terorizam i upotreba sajber prostora u terorističke svrhe.” Bezbednost 58, br. 2 (2016): 206–222.
102. Jonev, Katarina, Hatidža Beriša, and Aleksandar Ćiraković. „Informaciona bezbednost Ruske Federacije.” Vojno delo 2 (2018): 100–112. DOI: 10.5937/vojdelo1802100J.
103. Joubert, Vincent. Five Years after Estonia’s Cyber Attacks: Lessons Learned for NATO? Rome: NATO Defense College, 2012.
104. Kania, Elsa B., and John K. Costello. “The Strategic Support Force and the Future of Chinese Information Operations.” Cyber Defense Review 3, no. 1 (2018): 105–122.
105. Kaplan, Fred. Dark Territory: The Secret History of Cyber War. New York: Simon & Schuster, 2016.
106. Kari, Martti J. “An Analytical Framework for Russian Cyber Threat Perception and Strategic Culture.” Journal of Information Warfare 18, no. 3 (2019): 1–21.
107. Kello, Lucas. “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft.” International Security 38, no. 2 (2013): 7–40.
108. Kello, Lucas. The Virtual Weapon and International Order. New Haven: Yale University Press, 2017.
109. Korać, Vanja, Dragan Prlja, and Andrej Diligenski. Digitalna forenzika. Beograd: Centar za nove tehnologije Viminacijum, Arheološki institut i Institut za uporedno pravo, 2016.
110. Korzak, Elaine. “Have Russia and China Signed a Cyber Nonaggression Pact?” The Diplomat, August 21, 2015.
111. Korzak, Elaine. Russia’s Cyber Policy Efforts in the United Nations. Tallinn Paper No. 11. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2021.
112. Krasner, Stephen D. Sovereignty: Organized Hypocrisy. Princeton, NJ: Princeton University Press, 1999.
113. Lee, Robert M., Michael J. Assante, and Tim Conway. Analysis of the Cyber Attack on the Ukrainian Power Grid. Washington, DC: SANS Industrial Control Systems and Electricity Information Sharing and Analysis Center, March 18, 2016.
114. Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. “A Brief History of the Internet.” Internet Society, 1997.
115. Lewis, James A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Washington, DC: Center for Strategic and International Studies, December 2002.
116. Libicki, Martin C. What Is Information Warfare? Washington, DC: National Defense University Press, 1995.

117. Libicki, Martin C. Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND Corporation, 2009.
118. Lović, Vladimir. „Sajber prostor kao novo bojno polje: međunarodni odnosi, geopolitika i bezbednost u digitalnom dobu.” Megatrend revija 22, br. 1 (2025): 215–230.
119. Marczak, Bill, John Scott-Railton, Kate Robertson, Astrid Perry, Rebekah Brown, Bahr Abdul Razzak, Siena Anstis, and Ron Deibert. “Virtue or Vice? A First Look at Paragon’s Proliferating Spyware Operations.” Citizen Lab Report No. 183. Toronto: University of Toronto, 2025.
120. Martelle, Michael, ed. “USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY.” National Security Archive, January 21, 2020.
121. McKune, Sarah. “An Analysis of the International Code of Conduct for Information Security.” Citizen Lab Research Report No. 63. University of Toronto, September 2015.
122. Microsoft. “An Overview of Russia’s Cyberattack Activity in Ukraine: Special Report: Ukraine.” April 27, 2022.
123. Microsoft. Defending Ukraine: Early Lessons from the Cyber War. June 2022.
124. Microsoft. Microsoft Digital Defense Report 2025: Safeguarding Trust in the AI Era. Redmond, WA: Microsoft, 2025.
125. Microsoft Security Response Center. “Cyber Threat Activity in Ukraine: Analysis and Resources.” February 28, 2022.
126. Microsoft Threat Intelligence. “Russian Threat Actors Dig In, Prepare to Seize on War Fatigue.” December 7, 2023.
127. Microsoft Threat Intelligence. “Volt Typhoon Targets US Critical Infrastructure with Living-off-the-Land Techniques.” May 24, 2023.
128. Ministry of Foreign Affairs of the People’s Republic of China. China’s Positions on International Rules-making in Cyberspace. October 20, 2021.
129. Ministry of Foreign Affairs of the People’s Republic of China. International Code of Conduct for Information Security. September 12, 2011.
130. Ministry of Foreign Affairs of the People’s Republic of China. International Strategy of Cooperation on Cyberspace. Beijing: Ministry of Foreign Affairs of the People’s Republic of China, March 1, 2017.
131. Ministry of Foreign Affairs of the Russian Federation. “Briefing by Foreign Ministry Spokeswoman Maria Zakharova.” January 30, 2026.
132. Ministry of Foreign Affairs of the Russian Federation. “Cyber Stability: Approaches, Prospects, Challenges.” December 12, 2024.
133. Ministry of Foreign Affairs of the Russian Federation. “On the Completion of the Activities of the UN Open-Ended Working Group on Security of and in the Use of ICTs 2021–2025.” July 14, 2025.
134. Ministry of Foreign Affairs of the Russian Federation. “Signing of the UN Convention against Cybercrime.” October 24, 2025.
135. Ministry of Foreign Affairs of the Russian Federation. “Statement on the UN Convention against Cybercrime.” October 26, 2025.
136. MITRE ATT&CK. “FrostyGoop Incident, Campaign C0041.” March 5, 2025.
137. Mladenović, Dragan D., Danko M. Jovanović, and Mirjana S. Drakulić. “Definisanje sajber ratovanja.” Vojnotehnički glasnik / Military Technical Courier 60, no. 2 (2012): 84–117.
138. Nakasone, Paul M. “Posture Statement of General Paul M. Nakasone.” U.S. Cyber Command, March 7, 2023.
139. Nakashima, Ellen. “Trump Approved Cyber-Strikes Against Iranian Computer Database Used to Plan Attacks on Oil Tankers.” Washington Post, June 22, 2019.

140. Nakashima, Ellen. “Trump Confirms Cyberattack on Russian Trolls to Deter Them During 2018 Midterms.” Washington Post, July 11, 2020.
141. National Counterintelligence and Security Center. SolarWinds Orion Software Supply Chain Attack. Washington, DC: ODNI/NCSC, 2021.
142. National Cyber Security Centre. The Launch of the National Cyber Security Centre. London: NCSC, 2016.
143. National Cyber Security Centre. “The National Cyber Security Centre.” Приступљено 17. маја 2026.
144. National Cyber Security Centre. TRITON Malware Targeting Safety Controllers. London: NCSC, 2017.
145. National Institute of Standards and Technology. “Advanced Persistent Threat.” Computer Security Resource Center Glossary. Gaithersburg, MD: NIST.
146. National People’s Congress of the People’s Republic of China. Cybersecurity Law of the People’s Republic of China. Adopted November 7, 2016. Effective June 1, 2017.
147. National People’s Congress of the People’s Republic of China. Data Security Law of the People’s Republic of China. Adopted June 10, 2021. Effective September 1, 2021.
148. National People’s Congress of the People’s Republic of China. Personal Information Protection Law of the People’s Republic of China. Adopted August 20, 2021. Effective November 1, 2021.
149. NATO. “Cyber Defence.” Приступљено 17. маја 2026.
150. NATO. “Warsaw Summit Communiqué.” July 9, 2016.
151. NATO. “Washington Summit Declaration.” July 10, 2024.
152. NATO Cooperative Cyber Defence Centre of Excellence. “About Us.” Приступљено 17. маја 2026.
153. NATO Cooperative Cyber Defence Centre of Excellence. “Peacetime Cyber Espionage.” International Cyber Law. Tallinn: NATO CCDCOE, 2025.
154. NATO Cooperative Cyber Defence Centre of Excellence. “Tallinn Manual.”
155. NATO Cooperative Cyber Defence Centre of Excellence. “Tallinn Manual 3.0.” 2021.
156. NATO Strategic Communications Centre of Excellence. 2007 Cyber Attacks on Estonia. Riga: NATO StratCom COE, 2018.
157. Ney, Paul C., Jr. “DOD General Counsel Remarks at U.S. Cyber Command Legal Conference.” U.S. Department of Defense, March 2, 2020.
158. Nuclear Threat Initiative. “Natanz Enrichment Complex.”
159. Nye, Joseph S., Jr. “Cyber Power.” Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010.
160. Nye, Joseph S., Jr. The Future of Power. New York: PublicAffairs, 2011.
161. Nye, Joseph S., Jr. “Deterrence and Dissuasion in Cyberspace.” International Security 41, no. 3 (2017): 44–71.
162. Office of Management and Budget. M-21-31: Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents. Washington, DC: Executive Office of the President, August 27, 2021.
163. Office of Management and Budget. M-22-01: Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response. Washington, DC: Executive Office of the President, October 8, 2021.
164. Office of Management and Budget. M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. Washington, DC: Executive Office of the President, January 26, 2022.

165. Office of Management and Budget. M-24-04: Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements. Washington, DC: Executive Office of the President, December 4, 2023.
166. Office of Management and Budget, and Office of the National Cyber Director. M-24-14: Administration Cybersecurity Priorities for the FY 2026 Budget. Washington, DC: Executive Office of the President, July 10, 2024.
167. Office of the Director of National Intelligence. 2025 Annual Threat Assessment of the U.S. Intelligence Community. Washington, DC: ODNI, March 2025.
168. Office of the Director of National Intelligence, National Counterintelligence and Security Center. Cyber Aware Case Study: OPM Data Breach. Washington, DC: ODNI/NCSC, n.d.
169. Office of the National Cyber Director. 2024 Report on the Cybersecurity Posture of the United States. Washington, DC: Executive Office of the President, May 2024.
170. Office of the Secretary of Defense. Military and Security Developments Involving the People's Republic of China. Washington, DC: Department of Defense, 2023.
171. Office of the Secretary of Defense. Military and Security Developments Involving the People's Republic of China. Washington, DC: Department of Defense, 2024.
172. Ottis, Rain. "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective." NATO Cooperative Cyber Defence Centre of Excellence, 2008.
173. Parliamentary Assembly of the Council of Europe. Opinion on the Draft Second Additional Protocol to the Convention on Cybercrime (ETS No. 185). Doc. 15379. Strasbourg, 2021.
174. Pavlović, Marija. Borba protiv visokotehnološkog kriminala u Srbiji: dostignuća i izazovi. Beograd: prEUgovor, 2022.
175. Peterson and Schriever Space Force Base. "Space Force Activates Component Command to NORTHCOM." January 30, 2026.
176. PIR Center. "International Information Security and Russia's National Interests." 2025.
177. Predsednik Rossiiskoi Federatsii. Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii. Utv. 09.09.2000, No. Pr-1895.
178. Prezident Rossiiskoi Federatsii. Ukaz ot 05.12.2016 No. 646. "Ob utverzhdenii Doktriny informatsionnoi bezopasnosti Rossiiskoi Federatsii."
179. Prezident Rossiiskoi Federatsii. Ukaz ot 12.04.2021 No. 213. "Ob utverzhdenii Osnov gosudarstvennoi politiki Rossiiskoi Federatsii v oblasti mezhdunarodnoi informatsionnoi bezopasnosti."
180. Prezident Rossiiskoi Federatsii. Ukaz ot 02.07.2021 No. 400. "O Strategii natsional'noi bezopasnosti Rossiiskoi Federatsii."
181. Prezident Rossiiskoi Federatsii. Ukaz ot 31.03.2023 No. 229. "Ob utverzhdenii Kontseptsii vneshnei politiki Rossiiskoi Federatsii."
182. Prezident Rossiiskoi Federatsii. Ukaz ot 07.05.2024 No. 309. "O natsional'nykh tseliakh razvitiia Rossiiskoi Federatsii na period do 2030 goda i na perspektivu do 2036 goda."
183. Putnik, Nenad R. Kiber ratovanje – novi oblik savremenih društvenih konflikata. Докторска дисертација. Универзитет у Београду, Факултет безбедности, 2012.
184. PwC UK, and BAE Systems. Operation Cloud Hopper. London: PwC and BAE Systems, 2017.
185. Pynnöniemi, Katri, and Martti J. Kari. "Russia's New Information Security Doctrine: Guarding a Besieged Cyber Fortress." FIIA Comment 26/2016. Helsinki: Finnish Institute of International Affairs, 2016.
186. Raska, Michael. Israel's Evolving Cyber Defense Strategy. Singapore: S. Rajaratnam School of International Studies, 2015.

187. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation). Official Journal of the European Union L119 (2016): 1–88.
188. Republic of Estonia. Cybersecurity Strategy 2019–2022. Tallinn: Ministry of Economic Affairs and Communications, 2019.
189. Reuters. “Cyber-Attacks ‘Bought Us Time’ on Iran: U.S. Sources.” June 1, 2012.
190. Reuters. “Exclusive: Russian Hackers Were Inside Ukraine Telecoms Giant for Months, Cyber Spy Chief Says.” January 4, 2024.
191. Reuters. “Hackers Linked to Russian Spy Agency Claim Cyberattack on Ukraine Mobile Operator.” December 13, 2023.
192. Reuters. “Russia Conducted Mass Cyberattack on Ukraine’s State Registries, Deputy PM Says.” December 19, 2024.
193. Reuters. “Several Ukrainian State-Run Bodies Report Cyber Attacks.” January 25, 2024.
194. Reuters. “Ukraine Railways Say Sunday’s Cyber Attack Hit Its Online Freight Services.” March 25, 2025.
195. Reuters. “Ukraine Says 2,000 Computers of State Firm Were Impacted in Cyber Attack.” February 1, 2024.
196. Reuters. “Ukraine Says It Thwarted Russian Cyberattack on Electricity Grid.” April 12, 2022.
197. Reuters. “Ukraine Says Russian Cyberattack Hits State Registries, No Data Lost.” December 20, 2024.
198. Reuters. “Ukraine Sees Russian Effort to Sow Chaos as Cyberattack Hits Rail Service.” March 24, 2025.
199. Reuters. “Ukraine’s Kyivstar Says It Is Fully Operational after Cyber Attack.” December 20, 2023.
200. Reuters. “Ukraine’s Railways Restore Half of IT Services Hit by Cyber Attack So Far.” April 9, 2025.
201. Reuters. “Ukraine’s Top Mobile Operator Hit by Biggest Cyberattack of War.” December 12, 2023.
202. Reuters. “Ukrainian Telecom Company’s Internet Service Disrupted by ‘Powerful’ Cyberattack.” March 28, 2022.
203. Rid, Thomas. “Cyber War Will Not Take Place.” Journal of Strategic Studies 35, no. 1 (2012): 5–32.
204. Rid, Thomas. Cyber War Will Not Take Place. London: Hurst & Company, 2013.
205. Rid, Thomas, and Ben Buchanan. “Attributing Cyber Attacks.” Journal of Strategic Studies 38, no. 1–2 (2015): 4–37.
206. Scarfone, Karen, Paul Cichonski, Tom Millar, Tim Grance, and Karen Kent. Computer Security Incident Handling Guide. NIST Special Publication 800-61 Revision 2. Gaithersburg, MD: National Institute of Standards and Technology, 2012.
207. Schmitt, Michael N., ed. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017.
208. Security Delta (HSD). “The Dutch Security Cluster.” Приступљено 17. маја 2026.
209. Segal, Adam. China’s Vision for Cyber Sovereignty and the Global Governance of Cyberspace. NBR Special Report No. 87. Seattle: National Bureau of Asian Research, 2020.
210. Segal, Adam. “When China Rules the Web: Technology in Service of the State.” Foreign Affairs 97, no. 5 (September/October 2018).

211. Singer, P. W., and Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press, 2014.
212. Slijepčević, Ljuba. „Visokotehnološki kriminal u domaćim i međunarodnim propisima, s posebnim osvrtom na odredbe Krivičnog zakonika koje su stupile na snagu od 1. juna 2017. i Konvenciju Saveta Evrope o visokotehnološkom kriminalu." Advokatska kancelarija, april 2018.
213. Smeets, Max. No Shortcuts: Why States Struggle to Develop a Military Cyber-Force. London: Hurst, 2022.
214. Soldatov, Andrei, and Irina Borogan. The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries. New York: PublicAffairs, 2015.
215. Stamenković, Branko, Saša Živanović, Bojana Paunović, and Ivana Stevanović. Vodič za sudije i tužioce na temu visokotehnološkog kriminala i zaštite maloletnih lica u Republici Srbiji. Sarajevo/Beograd: Save the Children / Pravosudna akademija, 2017.
216. State Council Information Office of the People's Republic of China. China's Law-Based Cyberspace Governance in the New Era. Beijing: State Council Information Office of the People's Republic of China, March 2023.
217. State Council Information Office of the People's Republic of China. China's National Defense in the New Era. Beijing: State Council Information Office of the People's Republic of China, July 2019.
218. State Council Information Office of the People's Republic of China. Jointly Build a Community with a Shared Future in Cyberspace. Beijing: State Council Information Office of the People's Republic of China, November 2022.
219. State Council of the People's Republic of China. Regulations on the Security Protection of Critical Information Infrastructure. Decree No. 745. Beijing: State Council of the People's Republic of China, 2021.
220. State Service of Special Communications and Information Protection of Ukraine. "Russian Cyber Operations: APT Activity Report #3, H2 2023." 2024.
221. State Service of Special Communications and Information Protection of Ukraine. "Russian Cyber Operations: Attack Automation, Espionage against Defense Sector and New Tactics Analysis for the Second Half of 2024." April 29, 2025.
222. State Service of Special Communications and Information Protection of Ukraine. "Russian Hackers Attacked Users in Ukraine and Poland." December 28, 2023.
223. Stone, Alex, and Peter Wood. China's Military-Civil Fusion Strategy: A View from Chinese Strategists. Montgomery, AL: China Aerospace Studies Institute, 2020.
224. Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Revision 3. Gaithersburg, MD: National Institute of Standards and Technology, 2023.
225. The White House. "Office of the National Cyber Director." Accessed May 8, 2026.
226. The White House. "Statement from the Press Secretary." February 15, 2018.
227. The White House. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Washington, DC: The White House, May 2011.
228. The White House. National Cybersecurity Strategy. Washington, DC: The White House, March 2023.
229. The White House. National Cybersecurity Strategy Implementation Plan. Washington, DC: The White House, July 2023.
230. The White House. National Cybersecurity Strategy Implementation Plan, Version 2. Washington, DC: The White House, May 2024.
231. The White House. National Security Strategy. Washington, DC: The White House, October 2022.

232. The White House. President Trump's Cyber Strategy for America. Washington, DC: The White House, March 2026.
233. Tikk, Eneken, Kadri Kaska, and Liis Vihul. International Cyber Incidents: Legal Considerations. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010.
234. Tintor, Ljubomir. „Međunarodna odgovornost države u digitalnom (sajber) prostoru." U Srpski godišnjak za međunarodno pravo, 270–294. Beograd: Srpsko udruženje za međunarodno pravo, 2023.
235. Todorovic, Branislav, and Darko Trifunovic. "Prevention of (Ab-)Use of the Internet for Terrorist Plotting and Related Purposes." In Handbook of Terrorism Prevention and Preparedness. The Hague: ICCT, 2020.
236. Trump, Donald J. "Achieving Efficiency Through State and Local Preparedness." Executive Order. March 18, 2025.
237. Trump, Donald J. "Combating Cybercrime, Fraud, and Predatory Schemes against American Citizens." Executive Order. March 6, 2026.
238. Trump, Donald J. Executive Order 14306. "Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144." Federal Register 90, no. 111 (June 11, 2025): 24723–26.
239. U.S. Cyber Command. Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command. Fort George G. Meade, MD: U.S. Cyber Command, April 2018.
240. U.S. Cyber Command. "Command History." Accessed May 8, 2026.
241. U.S. Cyber Command. "Committed Partners in Cyberspace: Following Cyberattack, U.S. Conducts First Defensive Hunt Operation in Albania." March 23, 2023.
242. U.S. Cyber Command. "Cyber Mission Force Achieves Full Operational Capability." May 17, 2018.
243. U.S. Cyber Command. "CYBERCOM's 'Under Advisement' to Increase Private Sector Partnerships, Industry Data-Sharing in 2023." June 29, 2023.
244. U.S. Cyber Command. "Mission and Vision." Accessed May 8, 2026.
245. U.S. Cyber Command. "Shared Threats, Shared Understanding: U.S., Canada and Latvia Conclude Defensive Hunt Operations." May 10, 2023.
246. U.S. Cyber Command. "U.S. Cyber Command Hosts First Offensive Cyber Flag 2024 Exercise." September 3, 2024.
247. U.S. Department of Defense. Department of Defense Strategy for Operating in Cyberspace. Washington, DC: Department of Defense, July 2011.
248. U.S. Department of Defense. The Department of Defense Cyber Strategy. Washington, DC: Department of Defense, April 2015.
249. U.S. Department of Defense. Cyber Strategy Summary. Washington, DC: Department of Defense, 2018.
250. U.S. Department of Defense. FY 2020 Defense Budget Overview. Washington, DC: Department of Defense, 2019.
251. U.S. Department of Defense. 2022 National Defense Strategy of the United States of America, Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review. Washington, DC: Department of Defense, 2022.
252. U.S. Department of Defense. DoD Zero Trust Strategy. Washington, DC: Department of Defense, October 2022.
253. U.S. Department of Defense. Strategy for Operations in the Information Environment. Washington, DC: Department of Defense, 2023.
254. U.S. Department of Defense. 2023 Department of Defense Cyber Strategy: Summary. Washington, DC: Department of Defense, 2023.

255. U.S. Department of Justice. “Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election.” July 13, 2018.
256. U.S. Department of Justice. “Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace.” October 19, 2020.
257. U.S. Northern Command. “Homeland Defense.” Accessed May 8, 2026.
258. Ukrinform. “Ukraine’s Naftogaz under Cyberattack – Statement.” January 25, 2024.
259. United Nations. Charter of the United Nations. San Francisco, 1945.
260. United Nations. Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. Final Report. New York: United Nations, 2021.
261. United Nations Economic and Social Council. Commission on Crime Prevention and Criminal Justice: Provisional Agenda for the Thirty-Fifth Session. E/CN.15/2026/1. January 30, 2026.
262. United Nations General Assembly. Countering the Use of Information and Communications Technologies for Criminal Purposes. A/RES/74/247. December 27, 2019.
263. United Nations General Assembly. Developments in the Field of Information and Telecommunications in the Context of International Security. A/RES/53/70. December 4, 1998.
264. United Nations General Assembly. Developments in the Field of Information and Telecommunications in the Context of International Security. A/RES/54/49. December 1, 1999.
265. United Nations General Assembly. Developments in the Field of Information and Telecommunications in the Context of International Security. A/RES/59/61. December 3, 2004.
266. United Nations General Assembly. Developments in the Field of Information and Telecommunications in the Context of International Security. A/RES/63/37. December 2, 2008.
267. United Nations General Assembly. Developments in the Field of Information and Telecommunications in the Context of International Security. A/80/257. July 24, 2025.
268. United Nations General Assembly. Developments in the Field of Information and Telecommunications in the Context of International Security: Russian Federation Draft Resolution. A/C.1/53/3. September 30, 1998.
269. United Nations General Assembly. Final Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. July 1, 2025.
270. United Nations General Assembly. Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. UN Doc. A/76/135. July 14, 2021.
271. United Nations General Assembly. Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General. A/66/359. September 14, 2011.
272. United Nations General Assembly. Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General. UN Doc. A/69/723. January 13, 2015.
273. United Nations General Assembly. Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. A/RES/75/240. December 31, 2020.
274. United Nations General Assembly. Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. A/77/275. August 8, 2022.

275. United Nations General Assembly. Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. A/78/265. August 1, 2023.
276. United Nations General Assembly. Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. A/79/214. July 18, 2024.
277. United Nations General Assembly. Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, Draft Final Report. July 11, 2025.
278. United Nations General Assembly. United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes. A/RES/79/243. December 24, 2024.
279. United Nations Human Rights Special Procedures. OL RUS 7/2016. July 28, 2016.
280. United Nations Office for Disarmament Affairs. "Developments in the Field of Information and Telecommunications in the Context of International Security."
281. United Nations Office for Disarmament Affairs. "Global Mechanism on ICTs in the Context of International Security: Plenary 2026."
282. United Nations Office for Disarmament Affairs. "Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025."
283. United Nations Office on Drugs and Crime. "Cybercrime in Brief." In Cybercrime Module 1: Introduction to Cybercrime.
284. United Nations Office on Drugs and Crime. "Offences against the Confidentiality, Integrity and Availability of Computer Data and Systems." In Cybercrime Module 2.
285. United Nations Secretary-General. "Secretary-General Welcomes Adoption of Final Report of Open-ended Working Group on Security of and in the Use of Information and Communications Technologies." SG/SM/22726. July 14, 2025.
286. United States Code. "10 U.S.C. § 394. Authorities Concerning Military Cyber Operations."
287. United States Space Force. Space Force Doctrine Document–1: The Space Force. Peterson Space Force Base, CO: STARCOM, April 3, 2025.
288. Viasat. "KA-SAT Network Cyber Attack Overview." March 30, 2022.
289. Vuletić, Dejan V. "Upotreba sajber prostora u kontekstu hibridnog ratovanja." Vojno delo 69, no. 7 (2017): 308–325.
290. Vukelić, Miloš. "Sukobi u sajber prostoru 'ispod praga rata': sajber oružje u obaveštajnom nadmetanju država." Međunarodni odnosi 74, no. 1183 (2023): 52–71.
291. Winter, Philipp, and Stefan Lindskog. "How the Great Firewall of China Is Blocking Tor." In Proceedings of the 2nd USENIX Workshop on Free and Open Communications on the Internet. Berkeley, CA: USENIX Association, 2012.
292. Zetter, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown, 2014.
293. Закон о информационој безбедности. „Службени гласник Републике Србије," бр. 91/2025.
294. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала. „Службени гласник РС," бр. 61/2005, 104/2009, 10/2023, 10/2023 — др. закон и 9/2026.
295. Канцеларија за информационе технологије и електронску управу. „CERT." Приступљено 17. маја 2026.
296. Канцеларија за информационе технологије и електронску управу. „О Канцеларији за информационе технологије и електронску управу." Приступљено 17. маја 2026.

297. Правительство Российской Федерации. Постановление от 17 ноября 2008 г. № 1662-р. „О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года.”
298. Правительство Российской Федерации. Постановление от 17 декабря 2024 г. № 1805. „О внесении изменений в некоторые акты Правительства Российской Федерации.”
299. Правительство Российской Федерации. Постановление от 19 декабря 2025 г. № 2068. „О внесении изменений в некоторые акты Правительства Российской Федерации.”
300. Република Србија. Стратегија националне безбедности Републике Србије. Београд: Министарство одбране, 2019.
301. Република Србија. Стратегија одбране Републике Србије. Београд: Министарство одбране, 2019.
302. Руска Федерација. Военная доктрина Российской Федерации. Approved by the President of the Russian Federation on December 25, 2014, No. Пр-2976.
303. Руска Федерација. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Approved by the President of the Russian Federation on July 24, 2013, No. Пр-1753.
304. Руска Федерација. Федеральный закон от 6 июля 2016 г. № 374-ФЗ. „О внесении изменений в Федеральный закон ‘О противодействии терроризму’ и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности.”
305. Руска Федерација. Федеральный закон от 6 июля 2016 г. № 375-ФЗ. „О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности.”
306. Руска Федерација. Федеральный закон от 26 июля 2017 г. № 187-ФЗ. „О безопасности критической информационной инфраструктуры Российской Федерации.”
307. Руска Федерација. Федеральный закон от 1 мая 2019 г. № 90-ФЗ. „О внесении изменений в Федеральный закон ‘О связи’ и Федеральный закон ‘Об информации, информационных технологиях и о защите информации.’”
308. Руска Федерација. Приказ Федеральной службы безопасности Российской Федерации от 23 декабря 2025 г. № 539. „Об утверждении Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения.”
309. Руска Федерација. Приказ Федеральной службы безопасности Российской Федерации от 25 декабря 2025 г. № 548. „Об утверждении Порядка осуществления непрерывного взаимодействия субъектов критической информационной инфраструктуры Российской Федерации.”
310. Руска Федерација. Приказ Федеральной службы безопасности Российской Федерации от 26 декабря 2025 г. № 553. „Об утверждении Порядка и Технических условий установки и эксплуатации средств.”
311. Руска Федерација. Приказ Федеральной службы безопасности Российской Федерации от 26 декабря 2025 г. № 554. „Об установлении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.”
312. Руска Федерација. Указ Президента Российской Федерации от 10 января 2000 г. № 24. „О Концепции национальной безопасности Российской Федерации.”

313. Руска Федерација. Указ Президента Российской Федерации от 12 мая 2009 г. № 537. „О Стратегии национальной безопасности Российской Федерации до 2020 года."
314. Руска Федерација. Указ Президента Российской Федерации от 15 января 2013 г. № 31. „О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации."
315. Руска Федерација. Указ Президента Российской Федерации от 31 декабря 2015 г. № 683. „О Стратегии национальной безопасности Российской Федерации."
316. Руска Федерација. Указ Президента Российской Федерации от 30 марта 2022 г. № 166. „О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации."
317. Руска Федерација. Указ Президента Российской Федерации от 13 июня 2024 г. № 500. „О внесении изменений в Указ Президента Российской Федерации от 1 мая 2022 г. № 250."
318. Руска Федерација. Указ Президента Российской Федерации от 7 апреля 2025 г. № 214. „О внесении изменения в Указ Президента Российской Федерации от 30 марта 2022 г. № 166."
319. Руска Федерација. Указ Президента Российской Федерации от 7 апреля 2025 г. № 219. „О внесении изменений в состав Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям, утвержденный Указом Президента Российской Федерации от 10 ноября 2018 г. № 648."
320. Руска Федерација. Указ Президента Российской Федерации от 5 ноября 2025 г. № 815. „О внесении изменений в состав Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям, утвержденный Указом Президента Российской Федерации от 10 ноября 2018 г. № 648."
321. Руска Федерација. Указ Президента Российской Федерации от 16 февраля 2026 г. № 88. „О внесении изменений в состав Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям, утвержденный Указом Президента Российской Федерации от 10 ноября 2018 г. № 648."
322. Руска Федерација. Указ Президента Российской Федерации от 4 марта 2026 г. № 136. „О внесении изменений в некоторые акты Президента Российской Федерации."

Биографија кандидаткиње

Катарина Јонев Ћираковић рођена је 1987. године у Београду, где је завршила основну школу и гимназију. Дипломирала је међународне односе на Факултету политичких наука Универзитета у Београду 2011. године, са 23 године, а две године касније завршила је мастер студије из области међународног јавног права на Правном факултету Универзитета у Београду. Њен мастер рад „Сајбер безбедност и међународни односи“ био је први академски рад на том факултету који је обрадио тему сајбер безбедности кроз призму међународних односа и оцењен је највишом оценом.

Професионално искуство стицала је као асистенткиња на Факултету за дипломатију и безбедност, на предмету Међународно јавно право. Ангажована је и као предавач на здравственим мастер струковним студијама на предметима „Заштита података у здравству“ и „Медицинско право“.

Од 2015. године интензивно се бави политикама сајбер безбедности, са посебним фокусом на међународну регулативу, сајбер простор и њихов утицај на децу и младе. Објавила је више од 50 научних радова, а њена истраживања обухватају области сајбер тероризма, дигиталног насиља, сајбер ратовања и безбедности рањивих група у дигиталном окружењу. Припада малобројном кругу аутора у региону који се системски баве утицајем сајбер претњи на децу и младе.

Као едукатор за безбедност деце на интернету, од 2016. године реализовала је више од 500 предавања за децу, родитеље и наставнике широм Републике Србије, али и у Црној Гори, Босни и Херцеговини, Северној Македонији и Хрватској. Године 2017. покренула је ауторски пројекат „Сајбер Атис“, са циљем развоја дигиталне писмености и превенције дигиталног насиља међу младима. Учествовала је у реализацији великог броја пројеката на локалном нивоу, као и у сарадњи са различитим министарствима и институцијама. Учествовала је и у имплементацији великог броја пројеката на европском нивоу. За свој рад у области развоја информационог друштва, дигиталне писмености и безбедности деце на интернету добила је више признања.

Ауторка је две референтне публикације намењене родитељима и професионалцима: „Безбедност деце на интернету и друштвеним мрежама – водич за родитеље“ (2019) и „Утицај мобилних телефона на развој деце“ (2024). Године 2025. објавила је књигу намењену деци, „Дигиталне авантуре“, која на едукативан и деци прилагођен начин обрађује тему безбедности на интернету и препознавања потенцијалних ризика дигиталног света. Такође је ауторка уџбеника за високо образовање здравствених радника „Мониторинг и заштита података у здравству“ и „Медицинско право“.

Удата је за супруга Александра Ћираковића, мама Владимира и Теодора.

Изјава о ауторству

Име и презиме аутора: Катарина Јонев Ћираковић
Број индекса: 8/2018

Изјављујем

да је докторска дисертација под насловом

„Концептуализација сајбер ратовања у доктринама и стратешким документима Руске Федерације, Сједињених Америчких Држава и Народне Републике Кине"

• резултат сопственог истраживачког рада;

• да дисертација у целини ни у деловима није била предложена за стицање друге дипломе према студијским програмима других високошколских установа;

• да су резултати коректно наведени и

• да нисам кршио/ла ауторска права и користио/ла интелектуалну својину других лица.

Потпис аутора

У Београду, _____ _____

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора Катарина Јонев Ћираковић

Број индекса 8/2018

Студијски програм: ДАС Међународне и европске студије

Наслов рада

„Концептуализација сајбер ратовања у доктринама и стратешким документима Руске Федерације, Сједињених Америчких Држава и Народне Републике Кине"

Ментор Ивана Дамњановић

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла ради похрањивања у Дигиталном репозиторијуму Универзитета у Београду.

Дозвољавам да се објаве моји лични подаци везани за добијање академског назива доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис аутора

У Београду, _____ _____

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

„Концептуализација сајбер ратовања у доктринама и стратешким документима Руске Федерације, Сједињених Америчких Држава и Народне Републике Кине" која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигиталном репозиторијуму Универзитета у Београду и доступну у отвореном приступу могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство (CC BY)

2. Ауторство – некомерцијално (CC BY-NC)

3. Ауторство – некомерцијално – без прерада (CC BY-NC-ND)

4. Ауторство – некомерцијално – делити под истим условима (CC BY-NC-SA)

5. Ауторство – без прерада (CC BY-ND)

6. Ауторство – делити под истим условима (CC BY-SA)
(Молимо да заокружите само једну од шест понуђених лиценци. Кратак опис лиценци је саставни део ове изјаве).

Потпис аутора

У Београду, _____ _____

Ауторство - Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и

прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце, чак и у комерцијалне сврхе. Ово је најслободнија од свих лиценци.

1. Ауторство – некомерцијално. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела.

2. Ауторство - некомерцијално – без прераде. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела. У односу на све остале лиценце, овом лиценцом се ограничава највећи обим права коришћења дела.

3. Ауторство - некомерцијално – делити под истим условима. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца не дозвољава комерцијалну употребу дела и прерада.

4. Ауторство – без прераде. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца дозвољава комерцијалну употребу дела.

5. Ауторство - делити под истим условима. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца дозвољава комерцијалну употребу дела и прерада. Слична је софтверским лиценцама, односно лиценцама отвореног кода.