UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Peter Mikelj

Kibernetski prostor – novo področje geopolitičnega delovanja ZDA

Diplomsko delo

Ljubljana, 2016

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Peter Mikelj
Mentorica: doc. dr. Jelena Juvan
Somentor: izr. prof. dr. Uroš Svete

Kibernetski prostor – novo področje geopolitičnega delovanja ZDA

Diplomsko delo

Ljubljana, 2016

Zahvala

Zahvaljujem se svoji mentorici dr. Jeleni Juvan in somentorju dr. Urošu Svetetu za usmerjanje, strokovne nasvete in pomoč pri pisanju diplomske naloge.
Hvala moji družini za potrpežljivost in Anji, ker je verjela vame.

Kibernetski prostor – novo področje geopolitičnega delovanja ZDA

Medsebojno odvisna omrežja informacijsko komunikacijskih tehnologij, imenovana kibernetski prostor, so močno preobrazila svetovno politiko in spremenila načine poslovanja, delovanja vlade in vodenja nacionalne obrambe. Kibernetska varnost postaja predmet nacionalnih politik, saj lahko zlonamerna raba kibernetskega prostora ovira delovanje gospodarskih aktivnosti, aktivnosti javnega zdravja, varnosti in nacionalne varnosti. Nastajajoče spremembe predstavljajo pomemben izziv za države in ostale akterje na področju politike moči in pri zagotavljanju varnosti ter konkurenčne prednosti v svetovni politiki. S tem ko je kibernetski prostor postal novo področje za doseganje političnih ciljev postaja strateškega pomena za uresničevanje geopolitičnih interesov ZDA. Kibernetski terorizem, kibernetski kriminal, hekerski napadi na kritično informacijsko infrastrukturo ter povečevanje kibernetskih vojaških zmogljivosti nacionalnih držav predstavljajo nove tipe groženj in ranljivosti, na katere se ZDA odzivajo s sprejemanjem strateških dokumentov, s katerimi poskušajo zaščititi svoje geopolitične interese in opredeliti svojo vlogo in načine delovanja v tem novem prostoru. V diplomskem delu bom poskušal analizirati strateške dokumente ZDA v zvezi s kibernetskim prostorom in dokazati, da so začele ZDA kibernetski prostor obravnavati kot nov geostrateški prostor delovanja, ki je enakovreden ostalim prostorom kopnega, morja, zraka in vesolja.

Ključne besede: *kibernetski prostor, kibernetska varnost, geopolitika, ZDA.*

Cyberspace – a new area of geopolitical action of the United States

Cyberspace as an interdependent network of information and communication technologies has thoroughly changed world politics, business activities, government functioning and national defence management. With the abuses of cyberspace that hinder economic activities, and endanger public health, safety and national security, cyber-security has become an important part of national politics. These new changes represent a great challenge both on the national level and on the level of other actors within the power politics, and should be taken into consideration when providing security and ensuring competitive advantages in the world politics. As a new domain for reaching political goals, cyberspace has become a strategically important tool for the geopolitical interests of the USA. Cyberterrorism, cyber crime, hacker attacks on the critical information infrastructure and the expansion of military cyber command of nation states are new types of threats that can increase nation's vulnerability. In the USA, these have been countered with the adoption of strategic documents aimed at securing geopolitical interests, as well as defining the role and the operating principles of the USA in this new space. The aim of thesis is to analyse strategic documents issued by the USA concerning cyberspace and to prove that the USA have started to treat cyberspace as a new space for geostrategic action equal to all the other geostrategic domains, i.e. the land, the sea, the air and the space.

Keywords: *cyberspace, cyber-security, geopolitics, USA.*

KAZALO

SEZNAM KRATIC

ZDA	Združene države Amerike
BDP	bruto domači proizvod
NATO	North Atlantic Treaty Organisation – severno atlantska organizacija
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance – poveljevanje, upravljanje, računalništvo, obveščevalna dejavnost, nadzor in izvidovanje
IKT	informacijsko komunikacijska tehnologija
RMA	Revolution in Military Affairs – revolucija v vojaških zadevah
SIW	Strategic Information Warfare – strateško informacijsko vojskovanje
NII	National Information Infrastructure – nacionalna informacijska infrastruktura
DDoS	Distributed Denial of Service – distribuiran napad za zavrnitev storitve
SCADA	Supervisory Control and Data Acquisition − sistem za nadzor, vodenje in zbiranje podatkov
IEEE	Institute of Electrical and Electronics Engineers – Inštitut inženirjev za elektriko in elektroniko
ITU	The International Telecommunication Union – Mednarodna telekomunikacijska zveza
W3C	World Wide Web Consortium – Konzorcij za svetovni splet
IANA	Internet Assigned Numbers Authority − Organ za dodeljevanje internetnih naslovov
NIST	National Institute of Standards and Technology − Nacionalni institut za standarde in tehnologijo ZDA
NSA	National Security Agency – Nacionalna varnostna agencija
FBI	Federal Bureau of Investigation – Zvezni preiskovalni urad
MMORPG	Massive Multiplayer Online Role-Playing Game – množična mrežna igra za več igralcev
DOS	Denial of Service – zavrnitev storitve
DOD	Department of Defense – Ministrstvo za obrambo
CNCI	The Comprehensive National Cybersecurity Initiative – Vseobsegajoča nacionalna iniciativa glede kibernetske varnosti
CMF	Cyber Mission Force – Sile za izvajanje kibernetskih nalog

DHS	Department of Homeland Security – Ministrstvo za domovinsko varnost
C3	Cyber Crime Center - Center za kibernetski kriminal
NPPD	National Protection and Programs Directorate - Direktorat za nacionalno zaščito in programe
ISAO	Information Sharing and Analysis Organisation - Organizacija za izmenjavo podatkov in analize
NCCIC	The National Cybersecurity and Communications Integration Center - Nacionalni center za kibernetsko varnost in integracijo komunikacij
SECIR	Stakeholder Engagement and Cyber Infrastructure Resilience – Oddelek za udeležbo zainteresiranih strani in odpornost kibernetske infrastrukture
US-CERT	U.S. Computer Emergency Readiness Team - Računalniška skupina ZDA za nujno pripravljenost
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team - Skupina za nujen kibernetski odziv za industrijske nadzorne sisteme
NCC	National Coordination Center for Communications - Nacionalni koordinacijski center za komunikacije
HSI	Homeland Security Investigations - Preiskovalni oddelek domovinske varnosti
CDM	Continuous Diagnostics and Mitigation - Program za stalno diagnostiko in zmanjševanje tveganj
DoJ	Department of Justice - Ministrstvo za pravosodje
CAT	Cyber Action Team - Skupina za kibernetske akcije
NCIJTF	National Cyber Investigative Joint Task Force - Nacionalne združene sile za izvajanje preiskovalnih nalog
CIA	Central Intelligence Agency - Centralna obveščevalna agencija
CCIPS	Computer Crime and Intellectual Property Section - Sekcija za računalniški kriminal in intelektualno lastnino
DODIN	DOD Information Network - Informacijsko omrežje Ministrstva za obrambo
CCMD	Combatant Command - bojno poveljstvo
USCYBERCOM	U.S Cyberspace Command - Kibernetsko poveljstvo ZDA
DISA	Defense Information Systems Agency - Agencija za obrambne informacijske sisteme

USSTRATCOM	U.S. Strategic Command – Strateško poveljstvo ZDA

1 UVOD

> *Ogroženi smo. Amerika je vedno bolj odvisna od računalnikov. Nadzirajo distribucijo energije, komunikacije, letalstvo in finančne storitve. Uporabljajo se za hrambo vitalnih informacij, zdravstvenih datotek, poslovnih načrtov in kriminalnih datotek. Čeprav jim zaupamo, so ranljivi – na učinke slabega načrtovanja, nezadostnega ustreznega nadzora, nesreče, in kar je najbolj zaskrbljujoče, namerne napade. Sodobni ropar lahko z računalnikom ukrade več kot s pištolo. Terorist prihodnosti bo lahko napravil večjo škodo s tipkovnico kot z bombo* (National Research Council 1991, 7).

Informacijska revolucija, globalizacija in internacionalizacija so preobrazile sodobne mednarodne odnose. Ti se sedaj odvijajo v globalnem informacijskem okolju, kjer veljajo nova načela političnega sodelovanja, tekmovanja in konflikta med subjekti mednarodnega sistema. V tem okolju se politični procesi odvijajo v realnem času, geografske ovire izgubljajo svojo prejšnjo pomembnost in celoten koncept geopolitike se spreminja. Največjo spremembo v primerjavi s prejšnjim obdobjem predstavlja svetovna povezanost zaradi razvojnih dosežkov, kot so satelitska televizija, mobilni telefoni oz. internet. Tehnične zmogljivosti procesiranja, prenašanja in hrambe informacij v t. i. kibernetskem prostoru so revolucionalizirale moderno družbo. Nove interaktivne elektronske komunikacije v prvih desetletjih 21. stoletja bodo močno zaznamovale posameznike in skupine, mogoče celo v takšnem obsegu, kot je radijski in televizijski prenos zaznamoval 20. stoletje. Učinkovita povezava med računalniki, računalniškimi omrežji in ljudmi je že postala največji tehnološki dosežek na Zemlji (Krenn 2003; Maliukevičius 2007; Geers 2014).

Trenutna informacijska revolucija, včasih imenovana "tretja industrijska revolucija", temelji na hitrem tehnološkem napredku na področju računalništva, komunikacij in programske opreme, kar je vodilo k dramatičnim zmanjševanjem stroškov ustvarjanja, procesiranja in prenašanja informacij. Računalniška moč se je v zadnjih tridesetih letih podvojila vsakih 18 mesecev in v začetku 21. stoletja stane tisočkrat manj, kot je v 70. letih. Leta 1993 je bilo na svetu okrog 50 spletnih strani. Do konca 2016 bo število strani preseglo milijardo. Število internetnih uporabnikov je že preseglo 3 milijarde. Danes ima približno 40 % svetovne populacije dostop do interneta, leta 1995 je bilo teh manj kot 1 %. Komunikacijske širokopasovne povezave naraščajo še hitreje, saj stroški komunikacije padajo še močneje kot stroški računalniške moči. Če je bila v letu 1980 telefonska povezava preko bakrene žice

zmožna prenosa ene strani informacij na sekundo, lahko danes optično vlakno prenese 90.000 strani v sekundi. Hramba enega gigabajta podatkov je takrat zasedala površino sobe, danes dvesto gigabajtov podatkov shranimo v žep na srajci. Količina digitalnih informacij naraste desetkratno vsakih pet let (Nye 2010; Internet Live Stats − Internet Usage & Social Media Statistics 2016).

Načini poslovanja, delovanja vlade in vodenja nacionalne obrambe so se spremenili. Te aktivnosti so sedaj odvisne od medsebojno odvisnih infrastruktur omrežij informacijske tehnologije, imenovane kibernetski prostor. Internet je v izjemno kratkem času postal temeljnega pomena za globalno gospodarstvo. Milijarde ljudi po svetu ga uporabljajo tako pri opravljanju dela kot v svojem zasebnem življenju. Danes podpira številne nove gospodarske aktivnosti, kot tudi aktivnosti in infrastrukture, ki podpirajo naše gospodarstvo, od finančnih trgov in zdravstvenih storitev do energetike in transporta. Zaradi interneta je gospodarska aktivnost učinkovitejša, hitrejša, cenejša. Največji presežki produktivnosti podjetij vse bolj izhajajo iz uporabe spletnih omrežij v kakršnikoli obliki. Multinacionalna prehrambena veriga Nestle prejema vsa naročila supermarketov neposredno preko interneta. Dostavna služba UPS uporablja spletna omrežja za optimizacijo svojih dostavnih poti, pri čemer so v letu 2006 prihranili 12 milijonov litrov goriva. V ZDA se preko spleta izvede za več kot 3 bilijone denarnih transakcij v tujino. Preko omrežja 300.000 kilometrov žic prenaša 4 milijarde gigavatov moči na leto. Napredni sistemi nadzora zračnega prometa in planiranja omogočajo letalskim družbam prevoz več kot 700 milijonov potnikov letno po celem svetu. Ekonomski vpliv interneta je ogromen, saj vsako leto prispeva kar 6500 dolarjev na prebivalca k ameriškemu BDP (Organisation for Economic Co-operation and Development 2008; Booz Allen Hamilton 2011; Lord in Sharp 2011).

Žal je odprtost, ki je omogočila razširitev na skoraj vsako področje človeške aktivnosti, proizvedla neštete ranljivosti. Ameriški predsednik Barack Obama je razglasil, da "je sedaj jasno, da je kibernetska grožnja ena izmed najresnejših gospodarskih in nacionalno-varnostnih izzivov, s katerimi se soočamo kot narod" (The White House 2009b,). Z njegovim pogledom se strinjajo številni avtorji. Že leta ameriška vlada v zvezi z nacionalno varnostno strategijo ustvarja dokumente, ki poudarjajo velikansko tveganje, ki ga predstavljajo kibernetske grožnje in njihova medsebojna povezanost s kriminalom, vohunstvom in bojevanjem. Kibernetske grožnje brišejo tradicionalne meje med mirom in vojno, vladnim in zasebnim sektorjem, strategijo in taktiko. Kot take predstavljajo zastrašujoče ovire, ki so po svoji naravi zakonske, institucionalne, tehnične in kulturne. Njihovo premagovanje bo odvisno od novih načinov razmišljanja in novih načinov vladanja, vključujoč nove akterje in raven

prilagodljivosti, na katero vlada ZDA še ni pripravljena (Lord in Sharp 2011).

Sodobno življenje je odvisno od pravočasnega, ustreznega in zaupnega delovanja kibernetskega prostora. Koordinacija aktivnosti v kibernetskem prostoru je postala ključni izziv. Kibernetska varnost ni več zgolj področje računalniške varnosti. Kibernetska varnost postaja predmet nacionalnih politik, saj lahko zlonamerna raba kibernetskega prostora ovira delovanje gospodarskih aktivnosti, aktivnosti javnega zdravja, varnosti in nacionalne varnosti. Ker je funkcija vlade predvsem zagotavljanje družbenega reda, zaščita življenj in lastnine njenih državljanov ter spodbujanje trgovine, potem so nacionalni voditelji odgovorni za kibernetsko varnost, saj podpira vse zgoraj naštete storitve. Zato je potrebno, da vlade uporabijo vse instrumente nacionalne moči za ustrezno zmanjšanje kibernetskih tveganj. Pojem kibernetske varnosti je presegel golo tehnično zaznavo računalniške varnosti, ko se je začelo širiti prepričanje, da imajo grožnje, izhajajoče iz digitalnih tehnologij, lahko uničujoče družbene učinke. Ta opozorila so kasneje vedno bolj potrjevali pomembni ameriški politiki in zasebne korporacije, ki so govorili o "elektronskem Pearl Harborju" in "orožjih za množično prekinitev" in s tem naslikali skrb vzbujajoče grožnje ostalemu Zahodnemu svetu. Dogodki 11. septembra so dodatno vzpodbudili pozornost glede računalnikov, informacijske tehnologije in varnosti, predvsem pri vprašanjih zaščite digitalne infrastrukture, elektronskega nadzora in uporabe računalniškega znanja v teroristične namene. Zunaj ZDA so nedemokratični režimi svojim državljanom večkrat poskusili preprečiti dostop do tistih delov interneta, za katere so menili, da ogrožajo politično in družbeno stabilnost.

Še več, medsebojna povezljivost se je izkazala za neprecenljivo orodje družbene mobilizacije v primeru "arabske pomladi". Glede tako imenovanih "twitter revolucij" so mnenja deljena: družbeni entuziasti jih vidijo kot neločljivo povezane s procesi liberalizacije, medtem ko skeptiki opazujejo njihovo močno sposobnost avtoritarne uporabnosti. V letu 2007 so digitalne napade na javne in zasebne institucije Estonije označili kot prvo kibernetsko vojno, ki se je odvijala v kibernetskem prostoru in NATO se je odzval tako, da je zaščito informacijskih sistemov razglasil kot ključni sestavni del transformacije svojih sil. Kibernetski prostor je postal zadeva visoke politike. Nove prakse izklapljanja interneta v času vstaj v številnih državah, učinkovito uhajanje zaupnih vladnih dokumentov na Wikileaksu, uporaba kibernetskih napadov za zmanjšanje iranskih jedrskih zmogljivosti prikazujejo, da državni akterji ne morejo prezreti pomembnosti kibernetskega prostora in njegovih zmogljivosti (Hansen in Nissenbaum 2009; Choucri in Clark 2011; Wamala 2011).

Bivši načelnik obrambnega štaba Velike Britanije Sir David Richards je opisal prihodnost vojne v podobnih besedah, ko je govoril, da se bodo konflikti sodobnega časa odvijali znotraj

medija "komunikacijske revolucije". Vpliv kibernetskega prostora na vojaške operacije je preobrazil koncepte delovanja, kot so nevojaške operacije in informacijske operacije z dodajanjem novih orodij in postopkov. Skupaj s kibernetsko močjo predstavljata velikanski vpliv na vse vzvode moči (diplomatsko/politične, informacijske, vojaške in gospodarske), kot tudi na krepitev posameznikov skupin in držav. Internet je omogočil virtualno zatočišče za nekonvencionalne vojaške grožnje vključno z nedržavnimi akterji, teroristi in kriminalnimi skupinami. V industrijski dobi po drugi svetovni vojni je vojaška superiornost ZDA temeljila na industrijski moči, superiorni tehnologiji in platformah, orožju in C4ISR sistemih ter robustni vojaški infrastrukturi. Zdaj, ko smo se premaknili iz industrijske v informacijsko dobo, je razširjenost informacijske tehnologije spremenila določene dejavnike bojevanja, ki niso več prednost ZDA. Natančna orožja in nevojaške operacije, ki so ZDA dajale prednost na bojišču, so pri asimetričnem bojevanju pokazale svoje slabosti. Čeprav so ZDA ustvarjalke kibernetske infrastrukture, je ta sedaj na voljo vsakomur, ki poseduje sredstva za vstopanje. Zato ni presenečenje, da so se tudi ZDA kot velesila znašle na strani prejemnice kibernetskih napadov. V zgolj prvi polovici leta 2009 je ministrstvo za obrambo identificiralo 43785 zlonamernih napadov. Vdrli so v e-poštni račun obrambnega sekretarja, uradniki ministrstva pa vsak dan poročajo o več tisoč poskusih vdora. ZDA so preprosto gledano že več let udeležene v konflikt znotraj kibernetskega prostora (Wentz in drugi 2009; Sterner 2011; Betz 2012).

2 METODOLOŠKI OKVIR

2.1 Opredelitev predmeta in ciljev preučevanja

Osrednji predmet preučevanja v diplomski nalogi predstavlja kibernetski prostor in njegova umestitev v sodobni geopolitični kontekst ZDA. Kibernetski prostor postaja pomembno področje človekovega delovanja in s tem pomembno sredstvo za doseganje državnih interesov. Preko analize pomembnih strateških dokumentov ZDA, ki zadevajo kibernetski prostor, bomo poskušali preučiti, ali kibernetski prostor postaja strateškega pomena za uresničevanje geopolitičnih interesov ZDA.

Pri raziskovanju sem si zastavil naslednje cilje naloge:

- opredelitev temeljnih pojmov kibernetskega prostora in geopolitike
- umestitev kibernetskega prostora v sodobni strateški kontekst

- opredelitev značilnosti kibernetskega prostora
- predstavitev in analiza akterjev ter njihovih sredstev moči v kibernetskem prostoru
- predstavitev in analiza kibernetskih groženj
- opredelitev kibernetske moči
- analiza in pregled strateških dokumentov ZDA glede kibernetske varnosti

2.2 Hipoteze

V diplomskem delu sem oblikoval naslednje hipoteze:

H1: Nadzor nad kibernetskim prostorom postaja strateškega pomena za uresničevanje geopolitičnih interesov ZDA.

H2: V zadnjih desetih letih smo priča porastu smernic, strategij in politik, s katerimi si ZDA želijo zagotoviti oz. ohraniti nadzor nad vodenjem in upravljanjem kibernetskega prostora.

2.3 Uporabljena metodologija

Pri pisanju diplomske naloge sem uporabljal različne raziskovalne metode. Z analizo in interpretacijo sekundarnih virov, kot so knjige, članki, enciklopedije in raziskovalna dela, ter deskriptivno metodo sem opredelil temeljne pojme svoje naloge, opisal akterje in grožnje v kibernetskem prostoru. Za analizo strateških dokumentov sem uporabil metodo analize primarnih virov.

3 OPREDELITEV TEMELJNIH POJMOV

3.1 Kibernetski prostor

> *Kiberprostor. Skupna halucinacija, ki jo vsak dan doživijo milijarde povsem legitimnih operaterjev, povsod na svetu, celo otroci, ki se učijo matematičnih pojmov /.../ Grafična predstavitev podatkov, abstrahiranih iz bank vseh računalnikov človeškega sistema. Nepredstavljiva kompleksnost. Svetlobni žarki, razporejeni v neprostoru uma, gruče in ozvezdja podatkov. Odmikajo se, kakor mestne luči ...* (Gibson 1997, 61).

To so besede, s katerimi je bil prvič opisan kibernetski prostor. Termin se je v literaturi pojavil pred več kot tridesetimi leti. Avtor besedne skovanke je kanadski pisatelj znanstvene fantastike William Gibson, ki je besedo prvič uporabil v romanu *Burning Chrome* iz leta 1982, bolj podrobno pa je pojem opredelil dve leti kasneje v svojem romanu *Nevromant*. Gibsonova vizija kibernetskega prostora se je razvila kot posledica tehničnih in družbenih inovacij osemdesetih let prejšnjega stoletja, ki so spremenile pogled na svet. Z navedenim pojmovanjem kibernetskega prostora je želel predstaviti svojo vizijo o globalnem računalniškem omrežju, ki povezuje vse ljudi, naprave in vire informacij na svetu in s pomočjo katerega se lahko gibljemo skozi virtualni prostor. Kibernetski prostor zanj predstavlja nek nov mejnik, kjer se pomembnost bolj pripisuje digitalnim informacijam kot geografskemu prostoru. Definicija je ustrezna še danes, saj je Gibsonu uspelo ustvariti vizijo "matrice", ki predstavlja več kot le golo tehnično ogrodje, ki ga danes simbolizira internet. Osredotoča se tudi na človeško percepcijo novega okolja, interakcijo med uporabniki in ponazarja resnično poglobljeno prostorsko izkušnjo kibernetskega prostora. Beseda, ki je bila prvotno ustvarjena za opis izmišljenega okolja v romanu, je nato postala širše uporabljana v strokovnih in akademskih krogih (Whittaker 2004).

Tekom let se je razvilo mnogo različnih definicij, pri čemer gre pri različnih avtorjih in organizacijah pravzaprav za poudarjanje različnih razsežnosti kibernetskega prostora. Kibernetski prostor se namreč lahko konceptualizira v smislu mnogih ravni delovanja, toda preprosta prva ocena ga prikazuje kot unikatni hibridni režim fizičnih in virtualnih lastnosti. Prva skupina definicij se zato bolj osredotoča na njegove metaforične značilnosti. Benedikt ga opredeljuje kot "globalno omreženje, računalniško vzdrževana, dostopna in generirana večdimenzionalna, umetelna ali "virtualna" resničnost. V tej resničnosti, za katero je vsak računalnik okno, videni in slišani predmeti niso fizični objekti niti niso nujno predstavitve fizičnih predmetov, temveč so pravzaprav po obliki, značaju in akciji produkti podatkov, čistih informacij" (Benedikt 1991, 122). Tudi ostali avtorji podarjajo njegovo virtualno komponento. Tako Strehovec pravi, da je kibernetski prostor "a-geografski in fizično nedoločljiv prostor" (Strehovec 1997, 300). Dutton pravi, da gre za "elektronsko simulirani prostor ali z omrežnim pretokom kreirani virtualni teritorij" (Dutton v Trček 1999, 346), Luke ga opisuje kot "pokrajino digitaliziranih informacij" (Luke 1998, 286), medtem ko Heim govori o prostoru, ki je realen po svojih učinkih in ne kot "fizično-geografska entiteta" (Heim v Trček 1993, 109). Tudi Mitchell opisuje kibernetski prostor kot "nadvse antiprostorski /…/ Ne moreš povedati, kje se nahaja, opisati njegove oblike ali razsežnosti oz. povedati tujcu,

kako priti do tja. Vendar lahko v njem najdeš stvari, brez da bi vedel, kje so" (Mitchell 1995, 8−9).

Druge definicije spet bolj poudarjajo strateško razsežnost kibernetskega prostora. Poudarjanje tehnološke komponente je opazno v opredelitvi, kot je zapisana v Nacionalni strategiji za zaščito kibernetskega prostora *(National Strategy to Secure Cyberspace*). V tem dokumentu je kibernetski prostor definiran kot "živčni sistem javnih in zasebnih institucij – kontrolni sistem dežele. Sestavljen je iz stotine tisoče medsebojno povezanih računalnikov, strežnikov, usmerjevalnikov, stikal in kablov optičnih vlaken, ki omogočajo delovanje naše kritične infrastrukture" (Department of Homeland Security 2003, 1). Tudi dokument Pregled politik kibernetskega prostora (*Cyberspace Policy Review*) poudarja fizične platforme, sisteme in infrastrukture, ki omogočajo globalno povezljivost, potrebno za vstopanje in delovanje v kibernetskem prostoru. Pri opredeljevanju kibernetskega prostora uporablja podobno definicijo, ki ga definira kot "medsebojno odvisno omrežje infrastruktur informacijske tehnologije in vključuje internet, telekomunikacijska omrežja, računalniške sisteme ter vgrajene procesorje in kontrolnike v kritičnih industrijah" (The White House 2009a, 1). Podobno meni tudi Kuehl, ko pravi, da je "kibernetski prostor globalni prostor delovanja, znotraj informacijskega okolja, katerega razločevalna in unikatna značilnost je zajeta z uporabo elektronike in elektromagnetnega spektra za ustvarjanje, hrambo, spreminjanje, izmenjavo in izrabljanje informacij preko medsebojno odvisnih in medsebojno povezanih sistemov, z uporabo informacijsko-komunikacijskih tehnologij" (Kuehl 2009, 28).

Vseeno ne obstaja standardna, univerzalno sprejeta definicija kibernetskega prostora, zato je uporabno razmišljati o načinih, kako celostno pristopiti h konceptu. Eden izmed novejših načinov konceptualizacije kibernetskega prostora je ta, da ga opredelimo v smislu več medsebojno odvisnih ravni oz. slojev delovanja.

3.1.1 Štiriravenski model konceptualizacije kibernetskega prostora

- Fizična raven

Fizična raven je najbolj materialna raven kibernetskega prostora. V grobem jo sestavljata dve komponenti. *Komponenta fizičnega omrežja* predstavlja celoto vseh fizičnih elementov in naprav, ki omogočajo delovanje kibernetskega prostora. Gre za strojno opremo ter mobilno in stacionarno infrastrukturo, ki jo najdemo na kopnem, morju, zraku in vesolju. Kibernetski

prostor je namreč prostor, ki nastaja znotraj medsebojno povezane infrastrukture računalniških naprav, katere gradniki so kabli, žice, optična vlakna, radijske frekvence, integrirana vezja, procesorji, stikala, usmerjevalniki, strežniki, računalniki, sateliti, senzorji, naprave za shranjevanje podatkov, oddajniki, sprejemniki in električna energija. Vsi ti elementi imajo naravne značilnosti širine, višine, mase in prostornine.
Geografska komponenta predstavlja fizično lokacijo vseh gradnikov, ki sestavljajo fizično omrežje. Vsi elementi namreč obstajajo v prostoru, zato so lahko geografsko locirani in so v pristojnosti različnih organizacij in držav (Clark 2010).

- Logična raven

Logična raven zajema programsko opremo in programsko kodo, ki je potrebna za njeno delovanje. Gre za številne sisteme navodil, dogovore in postopke, ki jih je umetno ustvaril človek in omogočajo delovanje in komunikacijo med računalniškimi napravami. Številni računalniški programi namreč v veliki meri nadzirajo fizične sestavne dele, preko programskih navodil pa se procesirajo tudi informacije, ki so shranjene na računalniku. Logično raven sestavljajo kompleksne aplikacije in storitve, kot so operacijski sistemi, spletni iskalniki, socialna omrežja, internetna telefonija in spletni zemljevidi, kot tudi storitve nižjih ravni, ki zajemajo mehanizme prenosa podatkov, programske standarde glede oblike podatkov in okolja, v katerih se programi izvajajo. Sem spada tudi zlonamerna programska oprema v obliki virusov, črvov in trojanskih konjev.
Prednosti in omejitve kibernetskega prostora v večini izhajajo iz odločitev, sprejetih na logični ravni. Z uporabo drugačnega pristopa pri logiki medsebojnega povezovanja bi lahko kljub enakim fizičnim elementom ustvarili popolnoma drugačen kibernetski prostor (Clark 2010).

- Informacijska raven

Tretja raven kibernetskega prostora je podatkovna plast, kjer nastajajo informacije. To je najmanj oprijemljiva raven, saj se značilnosti informacij močno razlikujejo od značilnosti fizičnih objektov. Gre za vsebinsko raven, ki obsega vse informacije, ki so ustvarjene, pridobljene, shranjene in obdelane znotraj kibernetskega prostora.
Informacijska raven zajema celotno vsebino, ki se nahaja na družbenih omrežjih, spletnih straneh, elektronski pošti, spominskih medijih in virtualnih bazah podatkov. Informacije se pojavljajo v številnih oblikah, kot so glasba, videi, knjige, fotografije, članki, novice,

metapodatki (informacije o informacijah) in ostala sporočila, ki jih lahko prebere človek. Dostop do informacij je lahko sistematično omejen (Clark 2010).

- Družbena raven

Družbena raven je sestavljena iz vseh ljudi, ki uporabljajo in komunicirajo v kibernetskem prostoru. Gre za dejanski internet ljudi in možnih odnosov in ne internet strojne in programske opreme. V osnovi družbena raven zajema vlade, privatni sektor, civilno družbo in akterje tehnološke skupnosti. Ljudje niso zgolj pasivni uporabniki kibernetskega prostora, ampak ga z načini uporabe definirajo in oblikujejo.
Družbeno raven prav tako sestavljata dve komponenti. *Komponenta kiber osebnosti* zajema osebno identifikacijo oz. virtualno identiteto na omrežju. Sem spadajo e-poštni naslov, IP naslov računalniške naprave, številka mobilnega telefona itd. *Komponento osebnosti* sestavljajo dejanski uporabniki spleta. Specifična značilnost vseh akterjev družbene ravni je, da se v resničnem življenju (izven kibernetskega prostora) lahko identificirajo s svojo unikatno DNK kodo, medtem ko je na mreži določitev veliko težja. Posameznik ima lahko več kiber osebnosti (npr. različne e-poštne naslove na različnih računalnikih), posamezna kiber osebnost pa ima lahko večje število uporabnikov (npr. večje število uporabnikov dostopa do enotnega računa v neki spletni trgovini) (Clark 2010).

3.2 Geopolitika

> "V vsakem obdobju, v vsaki civilizaciji, njena geografija, njena vizija in njena predstava o prostoru" (Moreau Defrages 2005, 7).

"Geopolitiko lahko na kratko opredelimo kot preučevanje odnosa človek − politika − geografsko prostorski dejavniki. Gre za samostojno disciplino preučevanja, ki pa nima splošno priznane krovne discipline. Nekateri jo namreč uvrščajo pod okrilje geografske znanosti, drugi jo priključujejo politologiji oz. sami znanosti o mednarodnih odnosih" (Simoniti 1997, 13). Vseobsegajoča definicija geopolitike ne obstaja, saj "pojem zajema preveč vsebin, ki se jih ne da zajeti v nekaj stavkih" (Simoniti 1997, 30). Opredelitve in vsebine geopolitike so se skozi čas spreminjale, tako kot se je spreminjala struktura svetovnega reda, s katerim se geopolitika ukvarja (O'Tuathail in drugi 2006). Geopolitika naj

bi se nanašala na številne načine povezovanja prostora z močjo.

Tvorec termina geopolitika je bil švedski profesor političnih ved in politik Rudolf Kjellén, ki je leta 1899 prvi uporabil besedo za poimenovanje "znanosti o državi kot geografskem organizmu oz. pojavu v prostoru" (Kjellén 1917, 46). Mackinder je menil, da geopolitika išče "formulo, s katero bi izrazili določene vidike geografske vzročnosti v svetovni zgodovini" (Mackinder 1904, 421). Za Cohena geopolitika predstavlja "analizo interakcije med geografskim okoljem in dogodki na eni strani ter političnimi procesi na drugi" (Cohen 2003, 12), Gray jo definira kot "prostorsko preučevanje in prakso mednarodnih odnosov /…/, ki razlaga dinamično prostorsko razsežnost določenih trajnih vzorcev konflikta v mednarodnih odnosih" (Gray 2005, 18, 28), medtem ko Flint govori o "borbi za nadzor nad prostori in kraji, ki se osredotočajo na moč", pri čimer naj bi bila moč včasih "videna kot relativna moč držav v zunanjih zadevah in možnost držav, da vodijo vojne, danes pa postaja bolj sofisticirana" (Flint 2006, 28). Morgenthau o geopolitiki govori kot o "psevdoznanosti, ki povzdiguje dejavnik geografije v absolut, ki na videz določa moč in usodo posameznih držav" (Morgenthau 1966, 153), Ó'Tuathail pa pravi, da je geopolitika pravzaprav "razprava o svetovni politiki, s posebnim poudarkom na tekmovanju med državami in geografskih dimenzijah moči" (Ó'Tuathail in drugi 2006, 1). Kljub različnim definicijam lahko opazimo, da se znotraj vseh definicij geopolitike pojavljata dejavnika moč (vpliv, politika, država) in prostor (geografija, okolje, ozemlje, kraj). Tako naj bi bila geopolitika v svojem bistvu "analiza geografskih vplivov na odnose moči v mednarodni politiki" (Encyclopaedia Britannica 2016).

Po drugi strani naj bi bila geopolitika pravzaprav to, kar etimološko namiguje beseda sama: "geografska politika". Politika, ki je geografsko interpretirana oz. analizirana zaradi svoje geografske vsebine (Kristof 1960, 34). Geopolitika kot veda, v določenih primerih služi politiki za osmišljanje in upravičevanje njenega programa. V tem smislu, je geopolitika lahko (zlonamerna) uporaba geopolitične znanosti v ideološke namene, pri čemer se spreminja v ideologijo in politično doktrino.

3.2.1 Klasična oziroma moderna geopolitika

Klasična geopolitika predstavlja geopolitične razprave in misli, ki so se v mednarodni politiki odvijale od konca 19. stoletja pa vse do konca hladne vojne. Pojem se nanaša na klasično pojmovanje geopolitike kot povezave med fizičnim geografskim prostorom in njegovim vplivom na moč, interese ter politično delovanje držav. Gre za način, kako so bile ideje, povezane s politiko in prostorom, lahko uporabljene znotraj državnih politik. Geopolitika se je

ukvarjala s političnimi odnosi med državami, zunanjimi strategijami držav in z globalnim ravnotežjem moči (Jones in drugi 2004).

Tradicionalna geopolitika se je v veliki meri opirala na objektivne geografske dejavnike, v katerih je videla bistvo moči države. V času njenega nastanka se je pod vplivom socialnega darvinizma razvil koncept organicistične teorije države, ki je državo obravnavala kot prostorski organizem, ki za svojo rast potrebuje prostor, ozemlje, kjer je ta rast možna. Rast države naj bi bila povezana z njeno širitvijo, propadanje in smrt pa naj bi se kazala v statičnosti meja ali izgubi ozemlja. Na ta način so avtorji poudarjali pomen ozemlja ali prostora, saj država brez njega naj ne bi mogla obstajati. Za predstavnike klasične geopolitike je bil značilen geografski determinizem. Njihova razmišljanja so temeljila na predpostavki, da geografija določa omejitve in možnosti v mednarodni politiki: države lahko izkoristijo svoje geopolitične prednosti in možnosti ali pa postanejo žrtve svojega geopolitičnega položaja. Državna politika in njen razvoj sta bila omejena s topografskim okvirjem. To je veljalo tako za definicije kot teoretske razprave, ki so se kasneje odražale kot politične strategije držav. Geografija naj bi tako predstavljala edini pomemben dejavnik pri konceptualizaciji in prakticiranju zunanje politike. Tako je Spykman zapisal: "Geografija je najosnovnejši dejavnik zunanje politike držav, saj je najstalnejši. Ministri se menjajo, celo diktatorji umrejo, gorske verige pa ostajajo na mestu" (Spykman 1944, 41). Značilnost predstavnikov klasične geopolitične misli je v tem, da vidijo bistvo politične moči predvsem v povezavi z zasedbo fizičnega ozemlja in nadzorom nad geografskim prostorom. Razumevanje sveta je v tistem času namreč temeljilo na ideji svetovne moči z osvajanjem ozemelj in njihovemu priključevanju osvajalskim središčem. Klare tako pravi, da se je s terminom geopolitika oz. geopolitična tekma označevalo tekmovanje oz. prizadevanje velesil za nadzor nad ozemljem, viri in pomembnimi geografskimi položaji, kot so pristanišča, kanali, rečni sistemi, oaze in drugi viri bogastva in vpliva (Klare 2003).

V času klasične geopolitične misli se je končalo obdobje odkrivanja Zemlje, saj je prišlo do nastanka popolne geografske slike sveta. To je vodilo v geografsko in zgodovinsko posploševanje in poskus nastanka globalnih pogledov na svet. Zemljevidi so bili obravnavani kot dosleden odraz narave same, objektivna kartografska projekcija ozemeljske resničnosti. Predstavniki klasične geopolitike so zato pričeli z iskanjem univerzalnih geografskih središč sveta, katerih nadzor bi državam omogočil neznansko moč ter spremenil ali ohranil razmerja moči na Zemlji. Admiral Mahan in njegovi somišljeniki so ključ do svetovne moči videli v pomorski moči, v obvladovanju oceanov in svetovnih morij. Sir Halford Mackinder in drugi so verjeli, da so revolucionarna odkritja na področju kopenskega transporta, kot v primeru

železnic, tehtnico prevesila v korist kopnega. Spet tretji, na primer Nicholas Spykman, so menili, da sta pomorska in kopenska moč enakovredni, zato naj bi resnični centri moči ležali na področjih, kjer se stikata tako kopno kot morje. Z nastankom oz. razvojem letalskih in vesoljskih tehnologij je ponovno prišlo do sprememb v vrednotenju geografske pomembnosti določenih področij. Tako so tudi predstavniki klasične geopolitike spoznali, da okvirje in meje te nove znanstvene discipline spreminja in preoblikuje tudi tehnološki razvoj. Razvoj tehnologije namreč spreminja pomen prostora v času, s tem pa je vplival tudi na aktualnost starih in razvoj novih teorij. V različnih zgodovinskih obdobjih so namreč veljali različni geografski koncepti za doseganje konkurenčne prednosti pred drugimi državami, ki pa so se zaradi tehnološkega, družbenega in političnega razvoja spreminjali. Vseeno pa za zagovornike klasične geopolitične misli objektivni fizično-geografski dejavniki predstavljajo bistvene geopolitične dejavnike, ki vplivajo na razmerja in odnose moči v mednarodni politiki. Geografija naj bi izdatno vplivala na oblikovanje politike posameznih držav, zaradi česar naj bi bilo z opazovanjem moč replicirati potek dogodkov in izoblikovati sistemsko teorijo, ki ima splošno in trajno veljavo (Kristof 1960).

3.2.2 Kritična oziroma postmoderna geopolitika

Tudi kritična geopolitika se nanaša na raziskovanje vloge "geografije" v praksah zunanje politike držav. Vendar tu geografije ne smemo razumeti kot čisto fizično ozemlje ali geografske dejavnike, temveč kot geografske razprave, politična in kulturna pisanja o pomenu sveta. V središču njenega proučevanja so načini, s katerimi različne geografske razprave, prakse in vidiki merijo, opisujejo in ocenjujejo svet. Kritična geopolitika kritizira površinske in sebične načine, s katerimi stara geopolitika "prebira svetovni politični zemljevid", tako da nanj projecira svoje lastne kulturne in politične predpostavke in domneve. Za razliko predstavnikov klasične geopolitične misli namreč menijo, da geografija ni neko nespremenljivo dejstvo, ampak gre za subjektivna zgodovinska in družbena pisanja o svetu. Ta pisanja so odraz določenih kulturnih in političnih vrednot in še zdaleč niso splošno veljavne in brezčasne resnice, temveč gre za spremenljive koncepte. Tako naj stari geopolitični zemljevidi ne bi bili več veljavni v svetu naraščajočih finančnih tokov, hipnih informacij in tehno-znanstvenih tveganj (Doods 2007).

Za kritično geopolitiko je prostor prav tako izjemnega pomena. Vendar ga za razliko od klasične geopolitike ne preučuje v smislu geografskega prostora. Namesto tega preučuje družbeno konstrukcijo prostora – načine, s katerimi prostor dobiva svoj pomen s strani

geopolitičnih akterjev in njihovih idej. Geopolitika naj bi omogočala analizo različnih ali nasprotujočih si stališč političnih akterjev glede točno določenega geografskega prostora. Ravnanje, s pomočjo katerega posamezniki in družbene skupine predstavljajo oz. prikazujejo svet na določen način, avtorji kritične geopolitike imenujejo "prostorizacija" (spatialization). Tako Ó'Tuathail meni, da je geopolitika diskurzivni postopek, s pomočjo katerega različni akterji "prostorizirajo" mednarodno politiko, dajejo prostorom politični kontekst. Tudi Simoniti podobno meni, da je "geopolitika torej način razmišljanja, način utemeljevanja, način konceptualizacije prostora, ne zgolj v fizičnem smislu, temveč tudi v človeškem (humanem)" (Simoniti v Paker 1997). Kritična geopolitika deli geopolitično mišljenje na štiri področja. Formalna geopolitika se nanaša na moderne geopolitične teorije ter predstave, ki jih ustvarjajo državniški intelektualci. Praktična geopolitika se nanaša na prakse in ravnanja politikov ter oblikovalcev javnih politik, ki se kaže v dejanski zunanji politiki. Popularna geopolitika se nanaša na poročanja o svetovni politiki znotraj popularne kulture in množičnih medijev določene države. Vsa tri področja pa so rezultat prevladujočih predstav, kultur, tradicionalnih praks in družbeno-zgodovinskega okvirja. Ti predstavljajo četrto področje geopolitike, strukturno geopolitiko (Ó' Tuathail in drugi 2006).

Področje geopolitike se je bistveno razširilo. V skladu z globalno perspektivo sveta se je tudi geopolitična znanost pričela ukvarjati s problemi, ki niso več nujno vezani na politične preslikave prostorskih dimenzij. Deteritorializacija geopolitike postaja vsakodnevna tema v sodobnih razpravah o mednarodnih odnosih. Če je šlo pri tradicionalni geopolitiki predvsem za odnos med fizičnim prostorom in politiko, torej za pogojevanje subjektivnih političnih odločitev z objektivnimi geografskimi danostmi ter geografsko umeščenostjo, gre pri novi geopolitiki za področja novega zanimanja. Razprave o grožnjah so se iz prevladujočih groženj glede "ozemeljsko opredeljenih" sovražnikov razširile na post-teritorialne nevarnosti. Avtorje zanima, kako globalni procesi in izzivi, kot npr. "informacionalizacija", ekološka degradacija ali globalizacija, vplivajo na naša geografska razumevanja sveta. Ozemlje in teritorialnost sta namreč družbena konstrukta, ki se prepletata s tehnološkimi zmogljivostmi, transportnimi napravami, vojaško logistiko, družbenimi institucijami, političnimi avtoritetami in ekonomskimi omrežji. Človeška družba kot taka ustvarja, preureja in uničuje pojem ozemlja in teritorialnosti. Tehnologije pa preoblikujejo naše načine ustvarjanja sveta in načine, na katere geografi, politiki in ostali akterji razmišljajo o prostoru, vizualizirajo kraje, območja, okolja in ljudi na zemlji.

V prostor, ki ga je vedno pokrivala t. i. trda geopolitika in ki temelji na geografskih dejavnikih ter vojaški tehnologiji, je vstopila t. i. mehka geopolitika, ki bolj upošteva gospodarstvo,

kulturo, religijo ter vpliv medijev na ravnanje in sprejemanje političnih odločitev (Simoniti 1997). Agnew pravi, da se geopolitika namreč ukvarja s procesi, ki so vključeni v nastajanje neenakomerne porazdelitve moči na Zemljinem površju in z njihovimi posledicami za človeško populacijo. Ta moč pa naj se ne bi manifestirala samo geografsko, v obliki meja med državami in drugimi politično-teritorialnimi enotami oz. nadzoru, ki ga močnejše države izvajajo nad šibkejšimi, temveč tudi v obliki finančnih, informacijskih in čustvenih povezav, ki jih ljudje tvorijo med seboj ter med kraji in ozemlji, ki jih naseljujejo. Poleg političnega vidika odnosov med državami vedno pomembnejši postajajo ekonomski, kulturni, ideološki vidiki odnosa med državami. Tako kritična geopolitika večji pomen kot samemu geografskemu prostoru in njegovim lastnostim pripisuje področjem, ki so posredno povezana z geografskimi dejavniki, kot so npr. ekonomija, politika, tehnologija ter zgodovinsko-kulturni kontekst. Bistvo razumevanja nove geopolitike je postalo raziskovanje narave odnosa med močjo in prostorom, saj po mnenju avtorjev razmerja in strukture moči v prostoru niso fiksne, ampak so bolj fluidne.

4 TRANSFORMACIJA GEOPOLITIKE

4.1 Informacijska družba

Pojmi, kot so "informacijska revolucija", "informacijska doba" in "informacijska družba", so novi modeli, preko katerih poskušajo strokovnjaki interpretirati geostrateške, gospodarske in družbene implikacije komunikacijskih tehnologij, ki so po svoji naravi resnično globalne, kot npr. internet. Razvoj te kritične informacijske infrastrukture od specializiranega vojaškega omrežja do vse navzoče, povsod razširjene komunikacijske infrastrukture prikazuje potencial digitalnih omrežij, da spreminjajo družbo. Informacijska doba je splošno definirana kot zgodovinsko obdobje, v katerem se lahko neskončne količine informacij globalno in poceni prenašajo preko omrežij. Informacijska doba je posledica nastanka tehnologij, ki omogočajo nizkocenovno komunikacijo na daljavo. Če so države, še posebej tiste, ki so pomembno prispevale k razvoju IKT, glavni upravljavci temeljne infrastrukture, so IKT "gromozansko povečale število in poglobile nadnacionalne načine komunikacije." Zato se je področje delovanja med državami in nedržavnimi nadnacionalnimi akterji povečalo (Keohane in Nye 1998; Rennstich 2008).

Robert Keohane in Joseph Nye definirata informacijsko revolucijo kot "hiter tehnološki

razvoj v računalništvu, komunikacijah in programski opremi, ki je vodil k dramatičnemu upadu stroškov procesiranja in prenašanja informacij /.../ Razlikovalno lastnost informacijske revolucije predstavlja velikansko zmanjšanje stroška prenosa informacije" (Keohane in Nye 2001, 215). Informacijsko revolucijo je po njunem mnenju potrebno razumeti kot rezultat politik ZDA in mednarodnih institucij v obdobju po drugi svetovni vojni, ki so predstavljale okvir za globalizacijo svetovnega gospodarstva.

Kuhn opisuje, kako se konceptualni svetovni nazori spreminjajo skozi čas. Čeprav je Kuhn poskusil opisati napredek znanosti in filozofije skozi zgodovino, je njegov model uporaben za razumevanje odzivanja vlad na izzive, ki jih predstavljajo IKT. Paradigmatični preskok se zgodi kot "niz mirnih obdobij, ki ga prekine intelektualno nasilna revolucija", kar povzroči "da en svetovni nazor nadomesti drug." Kot posledica je resničnost starega nazora popolnoma pozabljena. Revolucionarno obdobje, v katerem se preskok odvija, je zaznamovano z zmedo in strahom (Kuhn 1996).

Dokaz za trenutno zmedo in nerazumevanje novega preskoka je prisotno na področju mednarodnih odnosov in njihovemu podpodročju, varnostnih študijah. Izgleda namreč, da se nobena teorija s področja varnostnih študij ne more ustrezno odzvati na stvarnosti informacijske dobe. Kljub temu da so novi izzivi posledica informacijske revolucije, vpliva IKT na globalno varnost nobena izmed teorij mednarodnih odnosov ne obravnava učinkovito, zato razlaga sodobnih varnostnih odnosov in politik ni mogoča. Čeprav so teoretiki poskusili analizirati moč in varnost v informacijski dobi, so omejeni z mejami svojih teorij, pri čemer je vsaka nezdružljiva z drugo. Zato je potreben pragmatičen pristop, pri katerem strokovnjaki uporabljajo vse teorije mednarodnih odnosov, kot tudi literaturo, ki se osredotoča na različne politike (Eriksson in Giacomello 2006).

Herrera meni, da trenutni okvirji mednarodnih odnosov ne obravnavajo tehnologije kot sestavnega dela mednarodnega sistema. Namesto tega, različni modeli mednarodnih odnosov obravnavajo vire mednarodnih sprememb, vključno s tehnologijo, kot zunanje dejavnike v teoriji mednarodnih odnosov. Njegov holistični pristop poskuša konceptualizirati tehnologijo kot sestavni del mednarodnega sistema, v katerem imata tehnologija in politika "vzajemno konstitutiven" odnos. Vendar niso vse tehnologije bistvene za mednarodne odnose. Sam se osredotoča na sistemske tehnologije, ki jih definira kot tiste sociotehnične sisteme – praviloma komunikacijske, transportne sisteme in sisteme moči – ki strukturirajo interakcijo med mednarodnimi akterji in so po obsegu globalni. Kibernetski prostor je eden takšnih sociotehničnih sistemov, ki ustreza Herrerovi definiciji "mešanice materialnih in družbenih institucij, ki se povezujejo okrog izdelkov" (Herrera 2006). Čas je pomemben dejavnik pri

politiki sociotehničnih sistemov mednarodne pomembnosti: "Kompleksni sociotehnični sistemi bodo v različnih stadijih svojega življenjskega cikla imeli različen političen vpliv. V začetku sistem ne obstaja. Če je uspešno zamišljen in ustvarjen, potem se sociotehnični sistem sprva počasi razširja, dokler ne doseže faze razširitve, po kateri se širi hitro in široko. Na koncu, v svoji zreli fazi, je sistem splošno razširjen, zato se njegova širitev upočasni oziroma celo ustavi" (Herrera 2006, 36).

4.2 Tehnogeopolitika

Butler razvija koncept tehnogeopolitike, ko govori, da je tehnogeopolitika nov način, preko katerega lahko napravimo specifične geopolitične uvide, še posebej v primerih, ko tehnologija predstavlja vodilni dejavnik. Čeprav koncept ni uporaben kot model za razumevanje vseh geopolitičnih dogodkov, "predstavlja specifičen pogled, ki je lahko uporabljen v določenih geopolitičnih oz. tehnoloških primerih za razumevanje diplomatskega položaja udeleženih strani. V svojem članku opredeljuje pet splošnih načel, ki so lahko uporabljena kot učinkovita konceptualna orodja za razumevanje ponavljajočih se diplomatskih pozicij strank, udeleženih v pogajanjih, kjer se prepletata geopolitika in tehnologija (Butler 2001). Ta načela so sledeča:

- Države si prizadevajo za specifične tehnologije, da bi izboljšale svoje geopolitične pozicije.
- Države se na tehnične dosežke drugih držav odzivajo geopolitično, kar vpliva na njihov geopolitični položaj.
- Če je država tehnološko nerazvita, bo uporabila svojo moč za omejitev dostopa drugim državam, s čimer bo pridobila čas, da jih bo tehnološko dohitela in z njimi tekmovala na izenačenem tehnološkem področju.
- Če je država tehnološko naprednejša od svojih trgovskih in vojaških tekmic, bo zasledovala najbolj liberalno politiko, ki ji bo omogočala primerjalno prednost.
- Kadarkoli se lahko tehnološka odkritja razvijejo v takšni meri, da izbrišejo geopolitične koristi oz. slabosti, kar državo prisili v ponovno preučitev njihove geopolitične zunanje politike in pozivanju k mednarodni konferenci oz. zasedanju glede obravnave njihovih skrbi (Butler 2001).

Mednarodno sodelovanje glede kibernetske varnosti in internetnega upravljanja potrjuje Butlerjevo hipotezo, da je teh pet načel vedno prisotno v pogajanjih, kjer se prepletata geopolitika in tehnologija. Prvo načelo se kaže tako, da so Združene države razvile temelje internetne infrastrukture v 1960, da bi zagotovile komunikacijo njihovih jedrskih sil v primeru napada in možnost izvedbe povračilnega napada. Druge države, kot npr. Rusija in Kitajska, so reagirale na prevladujoč vpliv ZDA v kibernetskem prostoru z razvojem lastne IKT. V omejevanju nadzora ZDA nad kritično infrastrukturo se kaže veljavnost drugega in tretjega načela, saj so države razvile svoja lastna omrežja. Četrto načelo se kaže v tem, da ZDA hitijo z implementacijo liberalnih politik, da bi njihove dobrine IKT pridobile prednost na tujih trgih. Nenazadnje velja tudi zadnje načelo, saj izgleda, da tehnološki napredek tako Rusije kot Kitajske počasi zmanjšuje geopolitično prednost ZDA (Butler 2001). Dogovori v zvezi z upravljanjem sestavnih delov kibernetskega prostora se odvijajo že od 19. stoletja naprej, da bi se vzpostavila pravila za upravljanje s številnimi telekomunikacijskimi tehnologijami. Manjka pa mednarodna ureditev glede upravljanja kibernetskega prostora kot celote. Zakoni in ureditve določenih elementov kibernetskega prostora, kot je npr. telegraf, so dobro razvite. Za nekatera druga področja, kot npr. internet, obstaja velikanska vrzel ne samo znotraj zakonskih okvirov posamezne države, ampak tudi na mednarodni ravni.

Krasner trdi, da se v primeru globalne komunikacijske ureditve države v določenih stališčih lahko razhajajo. Povečanje moči, ki izhaja iz razvoja nove tehnologije, ustvarja nasprotja v mednarodnih pogajanjih. Če sta moč in tehnologija porazdeljeni enakomerno, bodo ustvarjeni mednarodni režimi, da bodo razrešili problem uskladitve delovanja. Pravi, da so "za nastanek mednarodnih komunikacijskih ureditev informacijski tokovi in znanje manj pomembni kot relativna sredstva moči. Kjer prihaja do nesoglasij glede osnovnih načel in norm in je porazdelitev moči izrazito asimetrična, se mednarodna ureditev ne razvije. Močnejše države enostavno počnejo, kar jim paše" (Krasner 1991, 337).

Zato meni, da so institucionalni dogovori bolj posledica distribucije sredstev nacionalne moči kot prizadevanj za rešitev problemov. Tudi ostali raziskovalci menijo, da se lahko multilateralne institucije uporabljajo (predvsem s strani hegemonističnih držav) za spodbujanje lastnih interesov, tako da namerno ustvarjajo politične institucije za zadostitev lastnim interesom. Močnejše in bolj tehnološko razvite države naj bi zato svoje primarne interese raje zaščitile preko unilateralnih oz. bilateralnih dejanj kot preko multilateralne ureditve (Krasner 1991).

4.3 Militarizacija kibernetskega prostora

Informacije in komunikacijske tehnologije so že od nekdaj sredstva strateškega pomena. Skozi zgodovino so narodi, imperiji in ostale oblike političnih vladavin širile svoje delovanje preko svetovnih področij. Politični subjekti so strateško izrabljali prostore kopnega, oceanov in zraka za projekcijo moči. V drugi polovici 20. stoletja je prišlo do nastanka tehnologij, ki so omogočile strateško izrabljanje vesolja in kibernetskega prostora. Te tehnologije so zmanjšale pomembnost geografskih omejitev. Znanstveni in tehnološki napredek sta vesolje in kibernetski prostor spremenila v strateško okolje, ki je dosegljivo državnim akterjem. Militarizacija kibernetskega prostora in njegovo izrabljanje za vojno posledično prinaša povečano število nevarnosti in groženj. Za razliko od ostalih strateških vojaških tehnologij, kot so jedrsko orožje, rakete in letala, so stroški in sredstva, potrebna za militarizacijo kibernetskega prostora, nizka, medtem ko imajo lahko učinki enake posledice kot raketni napad. To znižuje prag za vstopanje tako državnih kot nedržavnih akterjev, vključno s terorističnimi in kriminalnimi mrežami. Trenutna mednarodna prizadevanja glede koordinacije globalnega odziva za zaščito kibernetskega prostora se osredotočajo na grožnje, ki jih predstavljajo nedržavni akterji, ki predstavljajo najvidnejši izziv glede kibernetske varnosti. Strateške grožnje nacionalnega pomena, ki izhajajo iz kibernetskega prostora, so večinoma prezrte kljub trendu militarizacije kibernetskega prostora s strani držav. Širjenje programov za kibernetsko bojevanje in sodelovanje določenih vlad s kibernetskimi tolpami, da bi napadle kritične informacijske infrastrukture, še dodatno otežuje globalna prizadevanja glede kibernetske varnosti (Berkowitz 2003; Armistead 2004; Price 2005; Finn 2007; Johnson 2008).

V preteklosti kibernetsko bojevanje ni bilo mogoče na nobeni stopnji razvoja, vendar so danes informacijski sistemi sposobni izvršiti napade s hitrostjo svetlobe ne glede na geografske dejavnike. Tehnologije, kot so medcelinske balistične rakete in globalne telekomunikacije, so zmanjšale preteklo pomembnost geografskih dejavnikov. Colin S. Gray nasprotuje tem vidikom in trdi, da gre za zmoto. Kljub temu da nove oborožitvene tehnologije v veliki meri zmanjšujejo pomen razdalje, terena in celo podnebja, opredeljuje tri strateške pomanjkljivosti te tehnologije:

- Ohranjanje tehnološkega napredka (Tehnološkega napredka namreč ni zmožna ohranjati in imeti v lasti zgolj ena varnostna skupnost)

- Geografski dejavniki (Spopad se ne more odvijati mimo geografskih dejavnikov, za nadzor nad teritorijem so potrebni ljudje)
- Logistične zahteve (ki so potrebne za nadziranje teritorija) (Gray 1996).

Danes, ko so družbe vedno bolj odvisne od kibernetskega prostora, militarizacija tega področja spreminja naravo spopada. Gre za naraven pojav, saj nas zgodovina uči, da tehnološki napredek preoblikuje način vodenja vojn. S tem ko napredek na področju IKT poganja reorganizacijo vojaških sil, se na globalni ravni odvija revolucija v vojaških zadevah (RMA). Vlade vedno bolj prilagajajo svoje nacionalnovarnostne politike, postopke in doktrine na način, da vključujejo kibernetski prostor kot novo področje delovanja, preko katerega želijo uresničiti svoje strateške interese. Borba za nadzor nad temi tehnologijami je geopolitična. Posledice militarizacije kibernetskega prostora za razvoj informacijske družbe so še večje, ker obstoječa mednarodna zakonodaja ne obravnava problemov kibernetskega bojevanja na ustrezen način. Potrebovali bi nov zakonodajni okvir, ustvarjen posebej za bojevanje v kibernetskem prostoru, ki bo temeljil na določenih osnovnih pravnih načelih, ki bodo omogočala ne samo njegove učinkovitosti, temveč bodo preprečili zlorabe s strani držav, ki bi se znašle na strani prejemnic napadov. Te negotovosti poudarjajo potrebo po sprejetju mednarodne zakonodaje za spopade v kibernetskem prostoru (Molander in drugi 1996; Ferguson in Mansbach 2004). David Lonsdale primerja strateško informacijsko vojskovanje s strateškim bombardiranjem, ko pravi da:

> *"Tako kot strateško bombardiranje, poskuša SIW (strateško informacijsko vojskovanje) zaobiti sovražnikove ozemeljske sile, da bi napadlo neposredno v zaznano središče sil. Vendar za razliko od letalske moči, ki deluje preko uporabe uničevalne ognjene moči in fizične sile, SIW predvsem deluje preko nenasilnih sredstev kot so "zlonamerna programska oprema" in elektromagnetni pulz. V tem smislu SIW niti ne predstavlja dejanja fizičnega nasilja, niti ne zajema nikakršne stopnje fizične izločitve /.../ instrumentalni cilj SIW je bolj pogosto ustvarjanje strateških učinkov s prekinitvijo namesto uničenja" (Lonsdale 2004, 135).*

Lonsdale meni, da ima strateško informacijsko vojskovanje lahko uničevalne učinke, čeprav jih po navadi nima. Njegova klasifikacija SIW kot oblike nenasilnega dejanja, ki ne zahteva fizičnega izvajanja, ko je uporabljeno, strateško ni ustrezna, še posebej, če upoštevamo nedavno spajanje kinetičnih in kibernetskih orožij (Lonsdale 2004). Taktični omrežni napadi

predstavljajo poglavitni dejavnik uspešnega izida vojaških operacij, kar prikazuje izraelski napad na sirsko jedrsko elektrarno iz 2007. Kibernetski sistem, uporabljen v tem napadu, je izraelskim zračnim silam omogočil "vdor v komunikacijska omrežja, vpogled v to, kar vidijo sovražnikovi senzorji in prevzem nadzora upravljanja na način, da so bili sovražnikovi senzorji premaknjeni v položaj, da prihajajočega letala niso mogli zaznati" (Fulghum in Barrie 2007, 28).

Everard pravi, da je razlika med informacijskim vojskovanjem in ostalimi oblikami vojne ta, da se informacijsko vojskovanje osredotoča na nadvlado informacijskih sistemov kot celote. Torej tako na informacije kot tudi sisteme, na katerih so te informacije shranjene in preko katerih se razširjajo (Everard 2000). Lonsdale ponuja elegantno definicijo informacijskega vojskovanja, ko govori o sposobnosti zaključiti vojno z napadom na sovražnikovo nacionalno informacijsko infrastrukturo (NII) preko kibernetskega prostora. Informacijsko vojskovanje naj bi bilo strateško samo v primeru, da se vojna lahko konča zgolj z napadom na nacionalno informacijsko infrasktrukturo preko uporabe kibernetskega prostora in katerega drugega prostora delovanja. Lonsdale pritrjuje, da je kibernetski napad na NII lažje izvesti kot zračni napad na isto tarčo. Sistemi inovacij in usposabljanja, ki so potrebni za izvedbo strateške zračne ofenzive, so dražji, saj zahtevajo znanje številnih veščin, od upravljanja z bombnikom, kontroliranja zračnega prometa do popravljanja vzletnih stez. Vse, kar zahteva izvedba kibernetskega napada, je prenosni računalnik in znanje o omrežnih ranljivostih napadenih računalniških tarč in kako te ranljivosti izrabiti: "Širjenje zmogljivosti SIW je edinstveno v tem, da je programska in strojna oprema, ki je potrebna za njegovo vodenje že dosegljiva, celo posameznikom /.../ Računalnik predstavlja utelešenje tehnologije z dvojno rabo in programska oprema ter potrebni načini za uporabo so široko dostopni na internetu /.../ Zgoščenka s hekerskimi orodji in informacijami predstavlja bojno orožje" (Lonsdale 2004, 140).

5 MOČ V KIBERNETSKEM PROSTORU

5.1 Kibernetska moč

Kibernetska moč – strateška uporaba informacijske in komunikacijske tehnologije za omogočanje gospodarske rasti, krepitev družbe in povečanje varnosti – je postala ključna politična usmeritev v ZDA in po svetu. Razprave glede internetne nevtralnosti, zasebnosti in

kibernetske varnosti so vprašanja, ki so vsa povezana s kibernetsko močjo. Če je kibernetski prostor področje, v katerem se odvijajo kibernetske operacije, je kibernetska moč vsota vseh strateških vplivov, ki jih generirajo kibernetske operacije znotraj in zunaj kibernetskega prostora (Nye 2010).

Kot navaja ena izmed širše uporabljanih definicij, je "kibernetska moč sposobnost uporabe kibernetskega prostora za ustvarjanje premoči in vplivanje na dogodke v ostalih okoljih delovanja in z ostalimi instrumenti moči" (Kuehl 2009, 38). Njen strateški pomen se vrti okrog sposobnosti manipuliranja zaznav strateškega okolja v vojni in miru, medtem pa istočasno zmanjševanje sposobnosti nasprotnika, da bi razumel isto okolje. Spreminjanje učinkov kibernetske moči v politične cilje je umetnost in znanost strategije, ki je definirana kot "upravljanje s kontekstom za vzdrževanje premoči v skladu s politiko." V bistvu je kibernetska moč sposobnost nadzora sistemov informacijske tehnologije in omrežij v kibernetskem prostoru in z uporabo kibernetskega prostora. (Nye 2010).

Kibernetska moč je uporaba, grožnja z uporabo ali vpliv zaradi zmožnosti uporabe kibernetskih napadalnih zmogljivosti. Moč je vedno odvisna od konteksta in kibernetska moč je odvisna od sredstev, ki karakterizirajo področje kibernetskega prostora. Kibernetska moč preko drugih elementov ter instrumentov moči ustvarja sinergije med temi elementi in jih povezuje tako, da izboljšujejo vsakega od njih. Razlikujemo lahko med močjo znotraj kibernetskega prostora in močjo zunaj kibernetskega prostora, tako kot lahko pri pomorski moči razlikujemo med pomorsko močjo v oceanih in projekcijo pomorske moči na kopnem (Booz Allen Hamilton 2011; Schreier 2015).

Kibernetska moč igra izjemno pomembno vlogo pri ekonomski moči. Nacionalno varnostne strategije iz časa Reaganove administracije 80. let prejšnjega stoletja so že vsebovale poglede in omenjale vlogo informacij ter informacijskih tehnologij pri krepitvi ameriškega gospodarstva. Znotraj globalne ekonomije 21. stoletja, ki se odvija v globaliziranem in medsebojno povezanem svetu, kibernetski prostor predstavlja najpomembnejši dejavnik, ki povezuje vse udeležence, pospešuje produktivnost, odpira nove trge in omogoča upravljalske strukture, ki so veliko manj hierarhične in imajo veliko večji doseg (Kuehl 2009).

Vpliv kibernetske moči na zadeve, ki zadevajo politiko in diplomacijo, je enako obsežen. Svetovni, vse navzoč, medij za vplivanje ostaja satelitska televizija, ki se prenaša preko sistemov in omrežij, ki se povezujejo v kibernetskem prostoru. Kampanje za vplivanje, ki jih v spopadih uporabljajo tako vlada ZDA kot tudi teroristične mreže, izkoriščajo kibernetsko moč kot ključno zmogljivost za zmago nad mislimi in idejami. V vojaškem smislu kibernetska moč predstavlja verjetno najvplivnejši instrument moči v zadnjih dveh desetletjih. Od ruskega

koncepta "vojaško tehnične revolucije" v 80. letih, do razvoja konceptov omrežnega vojskovanja in obrambne transformacije vojaških sil ZDA, sta kibernetski prostor in kibernetska moč v središču novih konceptov in doktrin na vseh stopnjah spopada (Kuehl 2009).

Kibernetska moč postaja ključni vzvod za izvajanje in razvoj nacionalnih politik, naj gre za protiterorizem, gospodarsko rast, diplomatske zadeve ali drugo izmed številnih vladnih aktivnosti. Na državni oz. lokalni ravni kibernetska moč oblikuje načine povezovanja vlade s svojimi državljani, ko omogoča storitve na načine, ki so bili še desetletje nazaj nepredstavljivi. Kibernetski prostor dejansko spreminja načine ustvarjanja podatkov, surovine, ki poganja našo družbo in gospodarstvo. Zaradi novih oblik vsebine – podob, zvokov, informacij v tisoč in eni obliki – in povezljivosti, s katero to vsebino prenašamo in izmenjujemo, se spreminja način vplivanja in uporabe moči za dosego strateških ciljev (Kuehl 2009).

Kibernetska moč postaja privlačna tako za vplivne in manj vplivne akterje zaradi relativno nizkih stroškov, velikega potencialnega vpliva in splošnega pomanjkanja transparentnosti. Vplivni akterji, kot so ZDA, lahko kibernetsko moč združijo z obstoječimi vojaškimi zmogljivostmi, ekonomskimi sredstvi in omrežji mehke moči. Manj vplivni akterji, kot so države, organizacije in posamezniki, lahko v kibernetskem prostoru asimetrično pridobijo s povzročitvijo obsežne škode na ranljivih ciljih. Z relativno majhnim vložkom lahko ohromijo omrežja in ukradejo dragocene osebne in lastniške informacije. ZDA že sedaj namenjajo milijarde dolarjev za lastno zaščito, a so tudi tako veliki denarni vložki nezadostni (Nye 2010).

5.1.1 Trda moč v kibernetskem prostoru

Trda moč je enostavna in samoumevna oblika moči. Izkusi se lažje kot mehka moč in jo je v določeni meri preprosteje izvajati. Trda moč je starejša oblika moči in se manifestira na praktičen in konkreten način. Je lažje vidna, njeni učinki so lažje merljivi. Tako kot mehka moč ni zgolj podaljšek lastnega ideološkega pristopa, ampak jo lahko najdemo tudi v drugih kontekstih.

"Trda moč je poznana vsem. Sloni na spodbudah (korenčkih) ali grožnjah (palicah)" (Nye 2004, 5). Trda moč je definirana kot sposobnost doseganja ciljev preko uporabe ekonomske moči ali uporabe vojaške moči na način, da ostalim groziš s svojo ekonomsko superiornostjo

ali fizično prisilo. Trda moč je osnovana na lastništvu virov. V tem smislu se zelo razlikuje od mehke moči, saj gre za obliko moči, ki temelji na zmogljivosti akterjev, da akumulirajo tolikšno količino sredstev, ki je potrebna, da uveljavijo svojo voljo. Sredstva so v tem primeru mišljena kot fizična sredstva v smislu oprijemljivih zadev in ne kot nematerialna sredstva, kot so ideje in mnenja. V tem smislu se trda moč bistveno razlikuje od mehke moči (Pallaver 2011).

V kibernetskem prostoru lahko proizvedemo trdo moč s fizičnimi ali kibernetskimi instrumenti. Primer uporabe kibernetskih sredstev je organizacija DDoS napada s strani države ali nedržavnih akterjev in ostalih ideološko motiviranih vsiljivcev. Druge oblike trde moči vključujejo vstavitev zlonamerne kode v računalniške sisteme za prekinitev delovanja sistemov oz. krajo intelektualne lastnine. Kriminalne združbe to počnejo zaradi profita, vlade držav pa to počnejo za povečevanje svojih gospodarskih sredstev. Kibernetska informacija lahko povzroči škodo tudi na fizičnih ciljih v drugi državi. Številne sodobne industrije in službe izvajajo procese, ki jih nadzirajo računalniki, povezani v SCADA sisteme. Zlonamerna programska oprema, vstavljena v te sisteme, lahko povzroči izključitev, kar povzroči realne fizične učinke, tako kot jih je imel Stuxnet črv za iranski jedrski program.

Seveda pa lahko tudi fizični instrumenti predstavljajo sredstva moči v kibernetskem prostoru. Usmerjevalniki, strežniki in optični kabli, ki prenašajo elektrone, imajo geografske lokacije, ki so v pristojnostih vlad, zato so družbe, ki upravljajo in uporabljajo internet, podrejene zakonom teh istih vlad. Vlade lahko namreč fizično prisilijo družbe in posameznike v sodelovanje. Spoštovanje francoskih zakov omejuje Yahoo pri razširjanju informacij v Franciji, Google je bil prisiljen umakniti sovražni govor med zadetki iskanja v Nemčiji. Čeprav so bila sporočila v ZDA, domovini teh družb, zaščitena s svobodo govora, bi neuklonitev pomenila zaporne in denarne kazni ter izgubo dostopa do teh pomembnih trgov. Vlade nadzirajo obnašanje na internetu preko tradicionalnih fizičnih groženj posrednikom, kot so npr. ponudniki internetnih storitev, brskalniki, iskalniki in finančni posredniki. Seveda pa lahko fizična sredstva uporabimo za napad na fizično infrastrukturo, na kateri je osnovan kibernetski prostor. Fizična infrastruktura je namreč ranljiva za neposredni vojaški napad ali sabotažo s strani vlade ali nedržavnih akterjev, kot so teroristi oz. kriminalci. Strežniki so lahko razstreljeni in kabli so lahko prerezani (Nye 2011).

5.1.2 Mehka moč v kibernetskem prostoru

V primerjavi z zagovorniki trde moči, ki ne priznavajo mehke moči, zagovorniki mehke moči razmišljajo tudi o trdi moči. Zanje trda moč predstavlja obliko moči, vendar vedo, da obstajajo alternative − ena izmed njih je mehka moč (Pallaver 2011).

Veliki zagovornik mehke moči je Nye, ki pravi, da "lahko včasih dosežeš želene rezultate brez vidnih groženj in izplačil. Rečeno drugače, država lahko znotraj svetovne politike doseže rezultate, ki jih želi, ker ji druge države − zaradi spoštovanja istih vrednot, posnemanja njenega zgleda, želje po doseganju enake stopnje blaginje in odprtosti − želijo slediti. To je mehka moč − doseči, da drugi želijo enake rezultate kot ti. Doseči sodelovanje namesto prisile" (Nye 2004, 5).

Mehka moč temelji na sposobnosti oblikovanja preferenc ostalih, brez uporabe sile, prisile ali nasilja. Ta moč se manifestira v različnih kontekstih in z različno stopnjo intenzivnosti in dokazljivosti.

Legitimnost je osrednjega pomena za mehko moč. Nye pravi, da "če bodo ljudje ali države verjeli, da so ameriški cilji legitimni, se jih bo lažje prepričalo, da se pustijo voditi brez uporabe groženj in podkupnin." Po njegovo naj bi "ugajanje vrednotam, interesom in preferencam drugih, v določenih okoliščinah, nadomestilo odvisnost od korenčkov in palic." To še posebej velja v današnjem prostoru mednarodnih odnosov, kjer so "vojske dobro usposobljene za premagovanje držav, vendar so neustrezno orodje za boj proti idejam" (Armitage in Nye 2007, 6). Mnogo organizacij, proti katerim se borimo danes, ne nadzira nikakršnega ozemlja, ima v lasti malo sredstev in ustoliči novega voditelja vsakič, ko je stari ubit. Zmaga v tradicionalnem smislu je zato izmuzljiva. Posledično je zmaga danes odvisna od pritegnitve tuje populacije na svojo stran in pomoči pri izgradnji zanesljivih demokratičnih držav. Mehka moč je ključna za zmago. Lažje je demokracijo narediti privlačno ljudem, kot ljudi prisiliti, da so demokratični.

V kibernetskem prostoru lahko mehko moč proizvedemo tako z informacijskimi orodji, preko "agenda framinga" (sposobnost vplivanja na to, katere zadeve dobijo pozornost in na kakšen način so prikazane), privlačnosti in prepričevanja. Naprimer pritegnitev skupnosti programerjev odprtokodne programske opreme, da upoštevajo nove standarde, je primer uporabe mehke moči. Informacija lahko potuje preko kibernetskega prostora in ustvari mehko moč, tako da pritegne prebivalce druge države. Primer je javna diplomatska kampanja, ki izrablja internet, kot je bil poziv državne sekretarke ZDA, Hillary Rodham Clinton, za svobodo interneta na Kitajskem v 2010 in Egiptu 2011. V splošnem so ameriški uradniki

zavzeli stališče, da internet "legitimizira njihovo delovanje podpiranja proticenzurne tehnologije" (Nye 2011).

Če govorimo o fizičnih sredstvih, ki lahko ustvarijo mehko moč v kibernetskem prostoru, je potrebno omeniti, da imajo vlade moč postavitve posebnih strežnikov in programske opreme, ki je ustvarjena tako, da pomaga razširjati sporočila različnih aktivistov za človekove pravice, kljub prizadevanjem njihovih vlad, da bi ustvarile informacijski požarni zid in blokirala ta sporočila. Podobno so zaradi iranske vladne zadušitve protestov proti rezultatom volitev leta 2009 ZDA investirale v programsko in strojno opremo, ki bi protestnikom omogočila razširjanje njihovih sporočil. Mehka moč pa se lahko s pomočjo fizičnih sredstev manifestira tudi izven kibernetskega prostora. Nevladne organizacije in nedržavni akterji lahko organizirajo fizične demonstracije v protest organizacijam, za katere menijo, da zlorabljajo internet. V letu 2006 so protestniki v Washingtonu demonstrirali proti podjetju Yahoo in drugim internetnim podjetjem, ki so posredovala imena kitajskih aktivistov, kar je vodilo k njihovi aretaciji s strani kitajske vlade (Nye 2011).

Caro Bejarano govori o sedmih ključnih strateških točkah, kjer imajo ZDA velikansko prevlado in moč vplivanja: operacijski sistemi, iskalniki, fizična komunikacijska infrastruktura, računalništvo v oblaku, vladni forumi, kriptografija in internetni protokol.

Čeprav naj bi bil kibernetski prostor splošno razširjen in oblast naj ne bi bila centralizirana, ima eno samo podjetje strahoten globalni vpliv na področju računalništva. Operacijski sistem Microsoft Windows obvladuje 84,2 odstotkov svetovnega trga, medtem ko Applov Mac OS uporablja 9,3 odstotka in Linux 1,6 odstotkov naprav. Kljub pritožbam glede varnostnih pomanjkljivosti in omejene funkcionalnosti podjetja ZDA obvladujejo trg v skladu z zakoni in kulturnimi normami svoje države. Podjetja ZDA dominirajo globalnemu trgu tudi na področju operacijskih sistemov za mobilnike: Google Android 66 %, Apple iOS 19,3 % ter Microsoft 2,2 % (StatCounter GlobalStats).

Drugo strateško točko predstavljajo iskalniki, ki imajo velikanski vpliv na ideje. Gre za način aplikacije mehke moči, ki ga omenja Nye. Čeprav obstajajo številni iskalniki, je med njimi takšen, ki močno izstopa. Iskalnik Google obvladuje 83 odstotkov svetovnega tržnega deleža, v ozadju pa mu sledijo Yahoo, Bind in kitajski Baidu. Googlovi iskalni algoritmi oblikujejo rezultate z indeksiranjem več kot 1000 milijard internetnih naslovov. Ker ljudje po navadi upoštevajo samo prvih tri do pet zadetkov, to Googlu omogoča oblikovanje izbire. Več tisočkrat dnevno Google odloča, kaj je in kaj ni pomembno na internetu. Kitajska je to spoznala v trenutku, ko je prišla v spor s podjetjem. Želela je cenzurirati Googlove zadetke iskanja na kitajskem ozemlju in sprožila napade proti Googlovi infrastrukturi. Podjetje se je

umaknilo in relociralo svoje strežnike v Hong Kong. Cena tega dejanja je bila izguba vpliva v primerjavi z Baidujem, s strani vlade sponzoriranim iskalnikom, ki sedaj obvladuje kitajski trg in omogoča storitve več kot 400 milijonom uporabnikom. (Caro Bejarano 2013).

Tretjo strateško točko predstavljajo fizične komunikacijske infrastrukture, še posebej sistemi, ki podpirajo internetno hrbtenico. Zgolj peščica podjetij oz. ponudnikov interneta namreč nadzira komunikacijsko jedro interneta. Še ne dolgo nazaj je celoten internetni promet potekal preko infrastrukture ZDA. Položaj se danes spreminja zaradi nižjih stroškov informacijske tehnologije in povečane skrbi za zaščito elektronskih komunikacij. Posledično druge države izgrajujejo svoje lastne hrbtenice, da bi preprečile prehod njihovega internetnega prometa preko infrastrukture ZDA. V tem smislu je Patriot Act, ki je omogočil spremljanje zlih kibernetskih aktivnosti, povzročil učinek preusmeritve prometa mimo nadzora ZDA, s čimer je zmanjšal vpliv nad globalnimi komunikacijskimi potmi (Caro Bejarano 2013).

Računalništvo v oblaku predstavlja četrto strateško točko. Trenutni trend gre v smer centralizacije procesiranja in spletne hrambe, kar infrastrukturi računalništva v oblaku omogoča zagotavljanje določenega vpliva na te vrste storitev. Ponudniki storitev računalništva v oblaku, kot so Amazon, Microsoft in Google, omogočajo uporabnikom dostopanje do storitev na zunanjih strežnikih. Gre za naraščajoč trg znotraj kibernetskega prostora. Vedno bolj bodo podatkovne infrastrukture potovale k določenim dobaviteljem, kar predstavlja strateško prednost. Trenutna vodilna podjetja so ameriška, vendar bi lahko bili v bližnji prihodnosti podatki ameriških državljanov locirani na strežnikih zunaj zakonskih meja, kot se že dogaja s prebivalci v drugih državah. Na takšen način ZDA podpirajo razvoj teh storitev v regijah, ki so omejena z nacionalnimi jurisdikcijami (Caro Bejarano 2013).

Peta strateška točka je vladanje. Gre bolj za kulturno vprašanje kot obliko nadzora, čeprav je tudi to odvisno od nazora. Obstajajo številni konzorciji, ki so jih ustanovile zaskrbljene strani, ki vzajemno sodelujejo pri razvoju komunikacijskih standardov v kibernetskem prostoru, med njih spadajo IEEE, ITU, W3C, IANA in mnoge druge, ki imajo ključno vlogo pri razvoju in oblikovanju sestavnih delov kibernetskega prostora. Participacija znotraj teh vladnih forumov omogoča določeno usmeritev teh vladnih teles (Caro Bejarano 2013).

Šesto strateško področje predstavlja kriptografija, ki predstavlja temelje internetne zaščite. Če bi sodobni načini zaščite podatkov odpovedali, bi razpadel celoten motor gospodarstva. Že od leta 1972 NIST v sodelovanju z NSA testira in certificira kriptografske standarde, ki so dostopni javnosti. Ta dejavnost ima gospodarski učinek, ki je bil v letu 2001 že ocenjen na 1,2 milijardi dolarjev. Zaradi eksponentne rasti spletne trgovine je ta številka nedvomno porasla. Kriptografija predstavlja dodaten element mehke moči v kibernetskem prostoru, saj nobena

vlada ne more vsiliti implementacije zunaj svojih lastnih omrežij. Odprt in konkurenčen postopek določanja standardov privlači zasebne varnostne subjekte, ki prepoznajo vrednost tega procesa. S tem se zmanjšuje prevladujoča vloga ZDA glede vpliva na ta ključni sestavni del interneta (Caro Bejarano 2013).

Zadnjo strateško prednost predstavlja internetni protokol, ki predstavlja osnovo internetnega usmerjanja podatkov. Zaradi števila internetnih naslovov je potrebno implementirati nov standard IPv6. Kitajska ima zaradi števila uporabnikov po novem določen vpliv glede standardov, implementacije strojne opreme in nadzornih mehanizmov (Caro Bejarano 2013).

5.2 Akterji in njihova sredstva moči

Način, kako je moč razpršena v kibernetskem prostoru, se kaže v velikem številu akterjev in zmanjševanju razlik v njihovi moči. V kibernetskem prostoru lahko škodo povzroči vsakdo, od najstniškega hekerja do vlade večje države. Za moč v kibernetskem prostoru je značilno, da različna sredstva moči, ki jih imajo različni akterji, v mnogih primerih zmanjšujejo razliko med državnimi in nedržavnimi akterji. Vendar relativno zmanjšanje razlik v moči ne pomeni enakosti. Velike vlade imajo še vedno več sredstev. Na internetu niso vsi enakopravni. Nye pravi, da lahko akterje v kibernetskem prostoru glede na strukturo v grobem razdelimo v tri kategorije:

- vlade,
- organizacije z visoko strukturiranimi omrežji,
- posameznike ter rahlo strukturirana omrežja (Nye 2011).

Ko se zgodi določen škodljiv napad, je pogosto težko določiti, ali gre za rezultat zlonamernega napada, prenehanje delovanja nekega sestavnega dela, ali nesrečo. Čeprav so njihovi cilji različni, so orodja in taktike, ki jih uporabljajo vojska, teroristi in kriminalci v kibernetskem prostoru zelo podobne, če ne enake. To pomeni, da je akterje kibernetskega napada izredno težko odkriti:

> *"Tako kot vsako streljanje ni nujno vojno dejanje, vsak uspešen kibernetski napad ni nujno dejanje kibernetske vojne. Kibernetski napad, ki izklopi električno omrežje, je lahko del kibernetske vojne ofenzive, lahko pa je tudi kiberteroristično dejanje, oblika kibernetskega kriminala, oziroma, če ga izvede 14-letnik, ki ne razume, kaj sploh*

počne – kibernetski vandalizem. Za katerega gre, je v veliki meri odvisno od namenov napadalca in okoliščin napada /.../ tako kot v resničnem svetu"(Schneier 2007).

Schneier razločuje med *kibernetskim vandalizmom*, kamor vključuje popačenje spletnih strani; *kibernetskim kriminalom*, ki zajema krajo intelektualne lastnine, izsiljevanje z grožnjo DDOS napada, prevare, ki temeljijo na kraji identitete itd.; *kibernetski terorizem*, npr. vdor v računalniški sistem, da bi povzročili raztalitev reaktorske sredice v jedrski elektrarni, dvig zapornic na jezu oz. namerno povzročitev nesreče dveh letal in *kibernetsko vojno*. Schneier uporablja izraz "kibervojna", ko se nanaša na uporabo računalnikov za prekinitev aktivnosti sovražne države, še posebej z namernimi napadi na komunikacijske sisteme (Schneier 2007).

Tudi Ben Israel in Tabansky menita, da vsi akterji, ki delujejo v kibernetskem prostoru uporabljajo enaka orodja in načine. Med tehnično stranjo, ki ima v lasti napadalne zmogljivosti (programerji, hekerji, lastniki "zajetih omrežij") in tistimi, ki naročajo storitve (zasebni preiskovalci, organiziran kriminal, vohunske organizacije), naj bi pogosto obstajalo nekakšno komercialno sodelovanje. Da bi lahko določili, ali je kibernetski napad dejanje vojne, pravita, je treba preučiti par vidikov:

- *organizacijski in geografski vir napada:* ali za dejanjem stoji država;
- *motiv:* ali je mogoče identificirati ideološki, politični, gospodarski ali religiozni motiv napada;
- *stopnja kompleksnosti:* ali je napad zahteval kompleksno planiranje in koordinirane vire, ki so prvenstveno na voljo državnim službam;
- *posledice:* ali je napad povzročil škodo in žrtve in ali bi povzročil škodo, če ni bi bili napravljeni zaščitni ukrepi (Ben Israel in Tabansky 2011).

Nye pravi, da lahko v grobem grožnje nacionalni varnosti v kibernetskem prostoru razdelimo v štiri širše kategorije. Za vsako od njih veljajo različni časovni vidiki. Čeprav gre za relativno nove grožnje, so vse globoko zakoreninjene v človeški zgodovini. Kibernetski prostor zgolj omogoča nove načine za dosego starih ciljev, naj gre za kriminal, vohunjenje, aktivnosti agitacije ali vojno. V praksi se pogosto prepletajo med seboj in niso popolnoma samostojne (Lord in Sharp 2011). Te zlonamerne aktivnosti pogosto smatramo kot kibernetske napade oz., bolj ustrezno, kibernetska dejanja, preko katerih državne in nedržavne organizacije izvajajo

informacijske operacije, kot so vohunjenje, sabotaža ali kriminalna dejanja. Zaradi kompleksnosti informacijskih infrastruktur in stalne uporabe novih tehnologij lahko te operacije vodijo k odkrivanju novih vstopnih točk v sovražnikova omrežja, preko uporabe zlonamerne programske opreme poškodujejo specifične sisteme informacijske tehnologije in kradejo zaupne ali uporabne podatke za zasebne ali državne aktivnosti (Valeri 2013).

Kibernetski kriminal uporablja računalnike in z njimi povezane sisteme za krajo in ogrozitev zaupnih informacij v kriminalne namene, najpogosteje zaradi finančne koristi. Čeprav ima lahko seštevek stroškov, ki izhaja iz oškodovanja, strateške učinke, so žrtve po navadi posamezniki in organizacije. Z uporabo razširjenih oblik napadov kriminalnim združbam uspeva pridobivati finančne dobičke, ki izhajajo iz cvetočega digitalnega gospodarstva. Čeprav strokovnjaki poskušajo oceniti škodo, ki jo povzroča kibernetski kriminal, je ta težko izmerljiva. Podjetja zaradi grožnje po izgubi zaupanja investitorjev in javnosti oklevajo pri poročanju dejanskih izgub. Poleg tega je tudi širše ekonomske učinke kibernetskega kriminala, kot so oportunitetni stroški, težko izmeriti. Vseeno McAfee ocenjuje, da naj bi škoda, ki jo je globalno gospodarstvo utrpelo zaradi izgub na področju intelektualne lastnine, kot posledica kibernetskega kriminala, v letu 2008 znašala 1000 milijard dolarjev. Gospodarske izgube zaradi kibernetskega kriminala naj bi v prihodnosti še naraščale, saj kibernetski kriminalci pri svojem delovanju postajajo vedno bolj sofisticirani. S pomočjo ustvarjanja lažnih profilov na straneh družbenih omrežij kriminalci izboljšujejo svoje aktivnosti zbiranja osebnih informacij, s katerimi nato napadajo posebej izbrane uporabnike. Ti načini jim omogočajo učinkovitejše kraje bolj varovane intelektualne lastnine podjetij (Lord in Sharp 2011).

Kibernetsko vohunjenje uporablja računalnike in z njimi povezane sisteme za zbiranje obveščevalnih podatkov oz. omogočanje določenih operacij tako v kibernetskem kot fizičnem prostoru. Za razliko od kibernetskega kriminala, kjer so incidenti finančno motivirani, ima kibernetsko vohunjenje strateške učinke, ki ogrožajo širšo skupnost. Motivi za kibernetsko vohunjenje so številni, vendar gre po navadi za pridobivanje vojaške, politične, industrijske oz. tehnološke prednosti. Vohunjenje se pojavlja že od nastanka človeške zgodovine, vendar kibernetsko vohunstvo predstavlja cenejši način izgradnje informacijskega profila konkurentov in sovražnikov, tako za državne in nedržavne akterje, vključno z zasebnimi podjetji. Kibernetski vohuni lahko ukradene informacije uporabijo za številne namene, vključno z izsiljevanjem, zastraševanjem, predvidevanjem ali motenjem delovanja političnih

nasprotnikov. Med kampanjo za predsedniške volitve v 2008 so tedanjima senatorjema Barracku Obami in Johnu McCainu kibernetski napadalci vdrli v računalniška omrežja, da bi pridobili občutljive informacije glede njunih načrtov. Državni in nedržavni akterji lahko z ukradenimi informacijami pridobijo uvid v načrte, operacije in ranljivosti oboroženih sil ZDA in njihovih zaveznic. Prav tako kibernetsko vohunjenje ogroža najnovejšo tehnologijo, ki jo ustvarja obrambno-industrijski kompleks ZDA. Kibernetski vohuni so ukradli podatke podjetij, ki so načrtovali večnamensko bojno letalo F-35 Joint Strike Fighter, katerega razvoj temelji na milijonih vrsticah programske kode in predstavlja najdražji program oborožitve v zgodovini ZDA. Namestnik obrambnega sekretarja je razkril, da je okužen prenosni disk, ki je bil leta 2008 vstavljen v vojaški prenosnik, povzročil "digitalno zasedbo, preko katere bi bili lahko podatki prenešeni na strežnike pod tujim nadzorom. Koda, ki se je neopaženo razširjala, je bila ustvarjena z namenom, da bi operacijski načrti padli v roke neznanega sovražnika." Tako kot kibernetski kriminal, se tudi kibernetsko vohunjenje pojavlja po celem svetu. V letu 2009 so kanadski raziskovalci razkrili GhostNet, omrežje 1295 okuženih gostiteljskih sistemov, ki so napadali tuja zunanja ministrstva, ambasade in multilateralne organizacije v Iranu, Indiji, Južni Koreji, Nemčiji, Pakistanu in mnogo drugih. GhostNet je svojim upravljalcem omogočal aktivacijo kamer in avdio naprav v okuženih računalnikih za nadzorovanje uporabnikov. Gre za primer kibernetskega vohunjenja, ki je omogočil fizični nadzor. Med vohunjenjem in napadom v kibernetskem prostoru obstaja tanka linija. Države so že davno sprejele dejstvo, da vohunijo druga za drugo in razvile neformalna pravila delovanja, ki zadržujejo te vrste aktivnosti pod stopnjo spopada. Vendar je meja med vohunjenjem in napadom, ki lahko onemogoči celotno električno omrežje, za kar bi bil v preteklosti potreben večji kinetični napad, danes v zgolj nekaj pritiskih na tipkovnico. Ker lahko zlonamerna koda daljše obdobje neopaženo potuje po omrežjih, lahko med vdorom in napadom dejansko mine več let (Lord in Sharp 2011).

Kibernetska agitacija uporablja računalnike in z njimi povezane sisteme za nadlegovanje, motenje, vplivanje, ustrahovanje oz. zavajanje nasprotnikov ali ciljev napada. Po navadi motivacijo za napad predstavljajo politični ali ideološki cilji, za dosego ciljev pa se uporabljajo nelegalna sredstva. Kibernetsko agitacijo uporabljajo anarhistične hekerske združbe. Organizacija Anonymous je izvedla številne opazne kibernetske napade kot odziv na zaprtje voditelja WikiLeaksa Juliana Assangea. Za razliko od kibernetskega kriminala in kibernetskega vohunjenja, pri katerih gre za krajo ali spreminjanje podatkov, kibernetska agitacija poskuša kaznovati ali vplivati na prepričanje in obnašanje napadenega subjekta. V

procesu kibernetske agitacije sicer lahko pride do kraje ali spreminjanja podatkov, izginotja večjih vsot denarja (kot posledice prekinitve delovanja omrežij), vendar je cilj kibernetskih agitatorjev škodovati oz. prepričevati (Lord in Sharp 2011).

Resnost dejanj kibernetske agitacije se močno razlikuje. Lahko gre za zgolj za digitalen grafit na sovražnikovi spletni strani, da bi širši javnosti javno naznanili obžalovanje. Takšni incidenti predstavljajo nevšečnost, vendar so večinoma bolj neškodljivi kot kibernetski kriminal ali kibernetsko vohunjenje. Resnejši primeri kibernetske agitacije pa lahko povzročijo množično zmedo ali spodkopavajo zaupanje v učinkovitost pomembnih institucij, kot so nacionalne vlade, multilateralne organizacije in finančne institucije (Lord in Sharp 2011).

WikiLeaksova objava 250.000 zaupnih dokumentov ameriške vlade predstavlja primer kibernetske agitacije. Čeprav se je namerni vdor v podatke zgodil znotraj vojske ZDA, je bila WikiLeaksova odločitev, da objavi ukradene dokumente, politično motivirana, z namenom diskreditacije držav, ki naj bi po njihovo prakticirale pretirano varovanje podatkov. Razkritje je povečalo politične napetosti med ZDA in njenimi zaveznicami ter škodovalo ugledu številnih ameriških funkcionarjev. Incident prikazuje strateško grožnjo, ki jo kibernetska agitacija predstavlja za države, kot so ZDA, ki morajo ohranjati mednarodne odnose za dosego svojih širših globalnih političnih interesov (Lord in Sharp 2011).

Kibernetska agitacija različnim akterjem omogoča učinkovite, vendar nepredvidljive načine za oblikovanje mednarodne percepcije, ki služi doseganju njihovih ciljev in diskreditira njihove sovražnike. Tako državni kot nedržavni akterji lahko uporabljajo ta sredstva, vendar so do sedaj kibernetsko agitacijo večinoma izvajali t. i. hektivisti − posamezniki, ki so ohlapno povezani in vdirajo v računalniške sisteme in omrežja za dosego političnih ciljev. Hekerji, ki niso politično motivirani, kot so najstniki, ki zaradi zabave kradejo ali ogrožajo zaupne informacije, se udejstvujejo v kibernetskem kriminalu in ne kibernetski agitaciji. Ker so zlonamerna programska oprema in avtomatizirana napadalna orodja široko dostopna na internetu, danes hektivisti ne potrebujejo naprednih računalniških znanj. Vse, kar potrebujejo, je želja po delovanju (Lord in Sharp 2011). Kibernetski terorizem, uporaba kibernetskih sredstev za ustvarjanje strahu in panike v družbi predstavlja različico kibernetske agitacije. Njegovi učinki imajo lahko sicer za posledico fizično uničenje, vendar je končni cilj vedno psihološki. Kibernetski terorizem je vedno napravljen z namenom doseganja političnih, verskih ali ideoloških ciljev. Do sedaj so dejanja kibernetskega terorizma v veliki meri ostala nesofisticirana in so zajemala preobremenitev ideoloških nasprotnikov z e-poštnimi sporočili, izvajanjem DDoS napadov ali skrunjenjem spletnih strani. Vseeno vlado ZDA vedno bolj

skrbi možnost uporabe bolj naprednih groženj, saj kibernetski prostor ponuja naravno zatočišče za teroriste. FBI je preiskoval posameznike, ki so povezani ali simpatizirajo z Al-Kajdo, ki so izrazili zanimanje za izvedbo kibernetskih napadov na kritično infrastrukturo ZDA in od zunaj pridobili bolj sofisticirane kibernetske zmogljivosti. ZDA morajo predvidevati, da teroristične skupine lahko in bodo iznašle načine za uporabo kibernetskih sredstev v prihodnosti. (Lord in Sharp 2011).

Kibernetsko vojno sestavljajo vojaške operacije za odvračanje sovražnika, ki se izvajajo v kibernetskem prostoru s strani državnih in nedržavnih akterjev, in učinkovita uporaba informacijskih sistemov in orožij oz. sistemov, ki jih nadzira informacijska tehnologija, za dosego političnih ciljev. Kibernetska vojna se lahko odvija na "regularen" način, med uradnimi vojaškimi silami držav, ali "neregularen" način, med uradnimi in neuradnimi silami državnih ali nedržavnih akterjev, ki se spopadajo za legitimnost in vpliv. Zajema lahko celoto spopada, ali pa se odvija kot del širše vojne, ki vključuje kopenske, pomorske, zračne ali druge vojaške sile. V prvem primeru se odvija zgolj v kibernetskem prostoru, čeprav lahko proizvaja učinke v realnem svetu, medtem ko se v drugem primeru istočasno odvija tako v kibernetskem kot fizičnem prostoru (Lord in Sharp 2011).
Kibernetsko vojno je lažje definirati v teoriji kot v praksi, predvsem zato, ker se prava kibernetska vojna do danes še ni zgodila. Kibernetski napadi imajo lahko kinetične učinke, vendar še niso povzročili uničenja in prelivanja krvi, ki ju tradicionalno povezujemo z vojskovanjem v fizičnem svetu. Biti informacij, ki so del kibernetskih napadov, ne ubijajo ljudi neposredno, čeprav lahko uničijo ali reprogramirajo digitalne sisteme tako, da posledično povzročijo izgubo življenj. Kibernetski napadi lahko povzročijo velikansko škodo, vendar ne dosegajo stopnje kibernetske vojne, pogosto zato, ker je sovražna stran nezmožna ali ne želi priznati napada oz. se odzvati nanj. Vojna vključuje dinamično interakcijo med vsaj dvema subjektoma. Kibernetski napad, sprožen proti subjektu brez volje ali zmogljivosti za obrambo oz. povračilne ukrepe, nedvomno predstavlja pomemben dogodek, vendar tu ne gre za vojno. Meja med dejanjem kibernetske vojne in dejanjem, ki ne dosega te označbe, je tanka. Odvisna ostaja od tega, ali se napadeni subjekt šteje za žrtev vojnega dejanja in zaključkov, ki jih bodo sklenile tretje osebe. Čeprav pravni strokovnjaki verjamejo, da bi morale države kibernetsko vojno definirati v ožjem smislu, tako da bi zajemala le dejanja, ki imajo za posledico veliko stopnjo uničenja kot pri ostalih oblikah konflikta, še vedno obstaja nezanesljivost in subjektivnost glede definiranja. (Lord in Sharp 2011).

Convertino, DeMattei in Knierim v svojem članku govorijo o posredovalcih groženj in jih opredeljujejo kot ljudi in organizacije, ki želijo izrabiti ranljivosti in naj bi v velikem številu naraščali. Govorijo o štirih glavnih oblikah akterjev, ki jih delijo po načinu delovanja in njihovem namenu: hekerje, organiziran kriminal, teroriste in nacionalne države (Convertino in drugi 2007).

5.2.1 Hekerji

Prvo kategorijo akterjev predstavljajo hekerji, posamezniki, ki za vdiranje v računalniška omrežja in sprožanje napadov uporabljajo programska orodja, ki so jih zasnovali in omogočili drugi oz. sami posedujejo znanje in veščine, ki jim omogočajo vdiranje v sisteme. Za nekatere hekanje predstavlja bolj ali manj samostojno aktivnost na področju kibernetske varnosti; drugi menijo, da nima večjega pomena in ni v nobeni meri primerljiv z resnejšimi področji kibernetskih groženj (Convertino in drugi 2007).

Hekanje je tudi v medijih in javnosti zmotno predstavljeno kot arhetipična kibernetska grožnja. Po navadi so hekerji stereotipno predstavljeni kot težavni in zdolgočaseni najstniki brez družabnega življenja, čeprav so lahko v resničnem življenju visoko izobraženi in usposobljeni v programiranju. Na žalost je njihova motiviranost v tem, da tekmujejo proti sebi in svojim kolegom tako, da vdirajo v informacijsko komunikacijska omrežja zaradi svoje zabave ali povzročitve nepotrebne škode, manjših tatvin in da bi dosegli določeno slavo med svojimi kolegi. Tako imenovani "digitalni domorodci", ki so zrasli z digitalno tehnologijo in v svetu interneta, si želijo "doseči piflarsko nesmrtnost" s poskušanjem "ustvarjanja predmeta zlonamerne programske opreme, ki bi bil deležen pozornosti medijev." Bolj nevarno obliko predstavlja razočarana stranka oz. nezadovoljni "insajder" kot npr. odpuščeni zaposleni, ki vdre v omrežje svojega bivšega delodajalca zaradi maščevanja z željo povzročitve škode oz. sodelovanja z zunanjimi sodelavci kot posledica podkupnine oz. prisile. Najnevarnejšo obliko pa predstavljajo posamezni hekerji, ki delujejo na mednarodnem prizorišču in sodelujejo v velikih političnih oz. ideoloških kampanjah (Acohido 2008).

Glede hekerskih groženj se pogosto dramatizira in se jim pripisuje prevelik pomen. IKT infrastruktura je prikazana, kot da ji neprestano grozi uničenje zaradi nenehnih prizadevanj omrežij zdolgočasene mladine, ki potrebuje rekreativni stimulus. Kot kaže poročilo Symanteca, je hekanje v letu 2014 predstavljalo 34 odstotkov vdorov. Vseeno je jasno, da lahko posledice individualnega hekanja predstavljajo veliko hujšo obliko kibernetskih groženj. Včasih je motiv za delovanje daleč od rekreativnega, heker pa deluje z jasnim

namenom. Gary McKinnon, ki je bil obtožen vdora v številne vladne računalniške sisteme med letoma 2001 in 2002, je priznal, da je napade načrtoval kot odziv na po njegovem mnenju "teroristična dejanja ZDA, po 11. septembru" (Poulsen 2008; Symantec Corporation 2014).

5.2.2 Skupine organiziranega kriminala

Internet je postal vozlišče zasebne, politične in komercialne aktivnosti ter tudi zelo pomemben medij za finančne in intelektualne transakcije. Zato ni presenečenje, da se je v skladu s tem razvil tudi kriminalni interes. Kibernetski prostor je postal mamljiv in donosen cilj napadov za sodobna kriminalna podjetja, saj se preko internetne infrastrukture in drugih IT sistemov vsak dan prenaša več sto milijard dolarjev ekonomske vrednosti. Skupine organiziranega kriminala za izvajanje nalog, ki prinašajo denarne koristi, vse bolj koristijo hekerske storitve. Za izvajanje številnih kriminalnih aktivnosti v kibernetskem prostoru je na voljo mnogo programske opreme in aplikacij. Tako kot za ostala področja varnosti in obrambne politike je značilen odnos akcije − reakcije, ko vsak kibervarnostni ukrep povzroči poskus kriminala, da bi zaobšel ta isti ukrep, kar posledično prinese nove protiukrepe. V takšnih okoliščinah je vsak opis kibernetskih kriminalnih aktivnosti bolj ilustrativen kot dokončen (Howard in drugi 2009).

Internet Security Threat Report opisuje številna orodja in sisteme, ki se uporabljajo za dosego kriminalnih ciljev, pogostost uporabe in glavne tarče teh aktivnosti. Vsiljena pošta, eno izmed najosnovnejših orodij, v letu 2014 še vedno predstavlja približno 60 odstotkov vsega nadziranega prometa po elektronski pošti in še naprej ostaja najučinkovitejše sredstvo za raznašanje virusov, trojanskih konjev in kot orodje za kriminalne aktivnosti "phisinga". V letu 2014 se je pojavilo okrog 317 milijonov novih oblik zlonamerne programske opreme, kar predstavlja skoraj en milijon dnevno, skupno število različnih oblik zlonamerne programske opreme pa znaša že 1.7 milijarde. To predstavlja veliko povečanje zle aktivnosti v primerjavi s prejšnjimi leti, kar pripisujejo "povečani profesionalizaciji zlonamerne kode in nastanek organizacij, ki zaposlujejo programerje, ki so namenjeni ustvarjanju teh groženj." Cilj te aktivnosti je jasen. Večina teh groženj je namenjena finančni pridobitvi, saj lahko z izvajanjem dejanj, kot je kraja zaupnih informacij, ki se lahko prodajo na spletu, finančno pridobijo. Kriminalci se zanašajo na velikanski spletni črni trg, kjer prodajajo in kupujejo zlonamerno programsko opremo, ukradene podatke kreditnih kartic, dokumentov, sezname e-mail naslovov in napadalne storitve. Spreminjajoče se cene prikazujejo določene podatke

glede ponudbe in povpraševanja. Šestmesečni najem zlonamernega programa spletnega bančništva Spyeye (zaznan kot Trojan.Spyeye) se ponuja za 150 do 1250 dolarjev, DDoS napadi stanejo med 10 in 1000 dolarji dnevno (Symantec Corporation 2015).
Seveda je za implementacijo ustreznih ukrepov potrebno razumeti, kako in v kakšni meri se organiziran kibernetski kriminal izvaja. Vendar je organiziran kibernetski kriminal več kot skupek zgoraj opisanih aktivnosti. Da bi razumeli, kakšne so posledice hujšega organiziranega kriminala za kibernetsko varnost, je treba definirati pojem organiziranega kriminala. Pojem kriminala zajema pridobitev bogastva ali katere druge koristi preko nelegalnih sredstev, kot so tatvina, prevara ali izsiljevanje. Organiziran kriminal je težje določljiv. Konvencija Združenih Narodov proti mednarodnemu organiziranemu kriminalu pojem "organizirane kriminalne združbe" definira kot:

> *"strukturirano skupino treh ali več oseb, ki v daljšem časovnem obdobju usklajeno deluje z namenom storitve enega ali več hudih kaznivih dejanj po tej konvenciji, da bi neposredno ali posredno pridobila finančne ali druge premoženjske koristi; »strukturirana skupina« pomeni skupino, ki se ni naključno oblikovala za neposredno storitev kaznivega dejanja, za katero pa ni nujno, da so vloge članov formalno določene, da je članstvo v njej trajno ali da ima zahtevno strukturo" (Generalna skupščina Združenih Narodov 2001).*

Hudo kaznivo dejanje je jasnejši koncept in vključuje tihotapljenje ljudi, drog in orožja; prostitucijo in seks z otroki; oborožen rop in številne finančno motivirane zločine. Ti vključujejo pranje denarja, prevare, prekrške v zvezi z javnimi sredstvi, korupcijo in podkupovanje, ponarejanje, izsiljevanje in prekrške v zvezi z intelektualno lastnino. Za analizo kibernetske varnosti je pomembno, da se večina teh hujših kaznivih dejanj zgodi v kibernetskem prostoru oz. se izvede s pomočjo in podporo aktivnosti v kibernetskem prostoru. Vendar je potrebno razumeti, da v kibernetskem prostoru "resen in organiziran kriminal" izgublja določene značilnosti. Možno je tudi, da se razvije v skladu z edinstvenimi okoliščinami kibernetskega prostora.
Za organizirani kibernetski kriminal je značilno, da zanj ni potrebna visoka stopnja organiziranosti niti ni nujna uporaba najnaprednejših sofisticiranih sredstev. Primer tega je predstavljen z računalniško zlorabo nizke stopnje, ki je lahko individualna aktivnost ali v določeni meri usklajena, da doseže bolj dramatičen učinek. Ne glede na stopnjo organiziranosti, v kateri se odvija, je lahko takšna aktivnost povezana s hujšo kibernetsko

kriminaliteto. Podjetja s prevladujočim internetnim položajem, kot so eBay, CNN, Yahoo, in Amazon, so preko vsiljene pošte že mnogo let izpostavljena napadom za zavrnitev storitev. Poleg tega se lahko organizirani kriminal na področju kibernetskega prostora manifestira na dva načina. Organizirana kriminalna združba lahko uporablja kibernetski prostor, da nadaljuje s svojimi kriminalnimi aktivnostmi, ali pa se razvije popolnoma nova oblika organiziranega kriminala, ki je edinstvena za kibernetski prostor. Choo and Smith razlikujeta med "tradicionalnimi organiziranimi kriminalnimi združbami" in "organiziranimi kiberkriminalnimi združbami". Hujše kriminalne združbe, kot so azijske triade, japonske jakuze in vzhodnoevropske organizacije, lahko izkoriščajo kibernetski prostor zaradi številnih predvidljivih namenov, vključno s pranjem denarja, tihotapljenjem droge, izsiljevanjem, prevarami z bančnimi avtomati in kreditnimi karticami, piratstvom programske opreme, industrijskega vohunstva, ponarejanjem dokumentacije in podobno. Fenomen je pogosto opisan kot migracija organiziranega kriminala iz realnega sveta v kibernetski prostor. Za te skupine kibernetski prostor ponuja nove priložnosti za hitro povečanje bogastva. Z drugimi besedami, kriminalna dejanja, ki jih je omogočila tehnologija, so nova sredstva za stare cilje (Brenner 2002; Choo in Smith 2008).

Skrivne in visoko učinkovite organizacije, kot so te, ki so pogosto sposobne ekstremnega nasilja v podporo ali zaščito njihovim aktivnostim, predstavljajo resen izziv službam nacionalnih organov pregona, še posebej kadar kriminaliteta prečka državne meje: "Spletni nepridipravi lahko hitro preskakujejo iz ene jurisdikcije v drugo, medtem ko se morajo oblasti različnih držav naučiti, kako sodelovati med seboj" (The Economist 2008). Četudi operirajo v novem svetu kibernetskega prostora, te skupine ohranjajo večino svojih tradicionalnih elementov, kot je hierarhična struktura, zgrajena na kulturi zvestobe in pripadnosti, zato so v določeni meri predvidljive v svoji organizaciji, interesih in v načinu svojih "poslovnih praks".

Večji izziv nacionalnim in mednarodnim organom pregona predstavljajo organizirane kriminalne skupine, ki izvajajo "kibernetska kazniva dejanja tretje generacije", ki se v celoti odvijajo s pomočjo nove tehnologije. Skupine, ki spadajo v to kategorijo, imajo interese zelo podobne svojim tradicionalno organiziranim bratovščinam, čeprav je kibernetska kriminaliteta bolj primerna za prikrite zločine, kot je npr. pedofilija. Te organizacije veliko manj poudarjajo fizično moč in uporabo sile in so manj osredotočene na razvoj eksluzivnosti in izjemno zvestega članstva. Člani kiberkriminalnih organizacij se lahko srečujejo samo na spletu. Povod njihovega združevanja predstavlja potreba po tem, da v ustreznem trenutku združijo potrebne tehnološke veščine. V kibernetskem prostoru fizična sila ni pomembna ... moč je v programski opremi in ne v številu posameznikov. Potreba po kompleksni organizaciji je zelo

majhna. Če kibernetska kriminaliteta že potrebuje nekakšno obliko organizacije, je to samo nekakšna "mafija določenega trenutka", ki izgine, ko je ne potrebujemo več (Brenner 2002; Choo in Smith 2008).

5.2.3 Teroristi

Za teroriste in ostale ekstremistične skupine je značilna obsežna uporaba interneta. Na kibernetski prostor vse bolj gledajo kot na sredstvo za dosego svojih ciljev, zavedanje teroristov pomena uporabe informacijske tehnologije in kibernetskega prostora v teroristične namene pa narašča že od leta 2000 dalje. Tudi Osama bin Laden je dejal, da "je zelo pomembno, da se koncentriramo na napad na gospodarstvo ZDA, preko vseh možnih sredstev" (Verton 2003, xv). FBI definira kibernetski terorizem kot "ustrahovanje civilnega prebivalstva preko uporabe visoke tehnologije za izvajanje dejanj, ki imajo za posledico onesposobitev ali izbris podatkov in informacij kritične infrastrukture; za dosego političnih, verskih in ideoloških ciljev" (Tafoya 2001, 2). Naraščajoča tehnična usposobljenost terorističnih in drugih skupin povečuje možnost za izvedbo omrežnih napadov. Zaradi naraščanja fizične in obmejne varnosti pa se teroristi spreminjajo v kibernetske bojevnike in hekerske službe, da bi lahko sodelovali v kibernetskem terorizmu proti ZDA (Wilson 2005).
Popularnost interneta za ideološki in politični ekstremizem lahko razložimo na številne načine. Tako bo glede na nastanek, zasnovo in delovanje, internet v prihodnosti še bolj uporabljen kot medij za ekstremistične organizacije in aktivnosti. Ker je nastanek interneta povezan s potrebo po odpornih vladnih in vojaških komunikacijskih sistemih za primer jedrskega napada, je internet kot sistem − zaradi v svoji zgradbi vdelane odpornosti in anonimnosti − privlačen za ekstremiste. Privlačnost sistema je tudi v tem, da je relativno poceni in da so že bile napravljene investicije, potrebne za razvoj in vzdrževanje globalne komunikacijske infrastrukture. Internet predstavlja anarhistično ozemlje, prostor izven nadzora vlade, ki ga lahko ekstremisti izkoriščajo na neverjetne načine, tako kot ga izkorišča družba za komunikacijo in delitev informacij (Barno 2006; Stenersen 2008). Zasnova interneta je ravno tako izjemno primerna za organizacije, ki so namerno netransparentne glede svoje strukture in namenov. S tem, ko organizacije postajajo bolj netransparentne in kompleksne, vrednost interneta narašča, saj je identifikacija organizacij in sledenje njihovemu napredku še bolj oteženo. Opravka imamo z "omrežji znotraj omrežij, povezavami v povezavah in zvezami med posamezniki, ki prečkajo lokalne, nacionalne in mednarodne meje" (The Economist 2007). Zaradi narave svojega delovanja internet omogoča številne

uporabne storitve za ekstremiste. Gre namreč za komunikacijski medij s številnimi oblikami prikritega delovanja. Preko zaščitenih in kodiranih podatkov se lahko posredujejo navodila, načrtujejo operacije in organizirajo kampanje za zbiranje sredstev. Preko uporabe forumov, oglasnih desk, blogov in spletnih objav pa so lahko prikazane tehnike, načini ter ideje, o katerih poteka interaktivna debata. Preko procesa spletne evalvacije se lahko izboljšujejo taktike in postopki ter kritizira določena ideologija oz. doktrina delovanja. S takšnim pristopom pa je lahko celo nekaj tako določenega, kot je teroristična kampanja, predstavljeno (vsaj za potencialne rekrute) kot nekaj vključujočega in konsenzualnega. Ker gre za prilagodljiv komunikacijski medij, je internet primeren za produkcijo in razširjanje propagande. Ekstremistične skupine so vedno uporabljale velike količine propagande v obliki tiskanih gradiv in v zadnjem času video posnetkov. Internet je povzročil, da je ta material zaradi spletnih objav in interaktivnih klepetalnic veliko dostopnejši in bolj reproduktiven. S pomočjo interneta lahko propagandno sporočilo doseže nesmrtno veljavo, s čimer besede zaprtega ali pokojnega radikalnega vodje ostajajo vir inspiracije. Deluje lahko tudi kot propagandna knjižnica; odlagališče za versko, politično in ideološko literaturo, priročnike navodil in videoposnetke taktike in tehnik delovanja (Sterensen 2008).

Zaradi lahko dosegljivih priročnikov za delovanje je internet postal prostor za učenje in poučevanje. Na voljo so interaktivni priročniki, ki se dotikajo velikega števila tem, od rokovanja z orožjem do veščin, potrebnih za pisanje zlonamerne kode ali sabotiranje računalniškega omrežja. Taktična in operativna usposabljanja se lahko izvajajo preko simulatorjev in celo spletnih računalniških iger, vključno z MMORPG (Masive Multyplayer Online Role-Playing Games). Ob svojemu obsegu aktivnosti, se internet pogosto opisuje kot "virtualni tabor za usposabljanje" oz. "odprto univerzo" za ekstremiste, kjer so rekruti lahko usposobljeni do stopnje, potrebne za izvedbo terorističnega ali uporniškega napada. (The Economist 2007; Sterensen 2008)

5.2.4 Nacionalne države

Trenutni dokazi kažejo na to, da kibernetsko področje hitro postaja središčna točka nacionalnih držav za vojskovanje v prihodnosti. Serabian je pred kongresom pričal, da "opažajo naraščajoč pojav doktrine in napadalno usmerjenih programov kibernetskega vojskovanja v drugih državah. Identificirane so številne države, ki s pomočjo vlade razvijajo napadalne kibernetske programe. Tuje države so začele z vključevanjem informacijskega vojskovanja v svoje vojaške doktrine, kot tudi v učbenike svojih vojnih fakultet, v primerih

napada in obrambe. Razvijajo strategije in orodja za izvajanje informacijskih napadov" (Serabian 2000). Jasno je, da so tuje vlade zainteresirane za izvajanje strukturnih napadov zaradi dostopa do tehnologije, obveščevalnih informacij, sredstev financiranja, organizirane doktrine in pripravljenosti na daljnoročne cilje (National Communications System 2000). Kibernetski prostor je postal polno razvito bojevališče, ko se vlade po svetu spopadajo za digitalno premoč v novem, večinoma nevidnem prostoru operacij. Če so bili nekoč kibernetski napadi omejeni na kriminalno dejavnost, danes postajajo ključno orožje vlad pri zaščiti nacionalne suverenosti in projekciji nacionalne moči (Geers in drugi 2013).

Človeški in mednarodni konflikti vstopajo v novo fazo, pa naj gre za strateške kibernetske vohunske kampanje, kot sta Moonlight Maze in Titan Rain, ali uničevalske napade, kot so bili vojaški kibernetski udari na Gruzijo in Iran. Kibernetski konflikt pogosto posnema tradicionalni konflikt. Kitajska uporablja kibernetske napade velikega obsega, tako kot je uporabljala svoje pehotne sile med korejsko vojno. Na drugi strani pa Izrael, ZDA in Rusija uporabljajo bolj precizno kibernetsko taktiko, ki temelji na naprednih tehnologijah. Največji izziv pri odvračanju, obrambi in povračilnih ukrepih zaradi kibernetskih napadov predstavlja problem pravilne identifikacije povzročitelja. John Arquilla pravi, da "balistične rakete pridejo s podatki o pošiljatelju, medtem ko računalniški virusi, črvi in DOS napadi izhajajo iz tančice anonimnosti." Kibernetska pripisljivost, ki se nanaša na identifikacijo verjetnega krivca za napade, je izjemno zahtevna, še posebej v primeru posameznih napadov. Države so pogosto napačno identificirane kot nedržavni akterji in obratno. Vezi med njimi pa se dejansko zmanjšujejo, saj se velikansko število "patriotskih kiberkriminalcev" bori v imenu vlad, drugi razlog pa je, da kiberkriminalne organizacije vsem, vključno posameznim državam, ponujajo storitve kibernetskih napadov in dostop do kompromitiranih omrežij (Geers in drugi 2013).

Kibernetski napadi, izvedeni proti Estoniji v 2007, so pritegnili pozornost mednarodne javnosti. Estonske vladne in bančne strani ter ponudniki interneta so bili tarče DDOS napada. Ti napadi, imenovani "klikskrieg", so izredno onemogočili državo, ki je veljala za začetnico elektronske državne uprave. Prišlo je do negotovosti o tem, kdo stoji za napadi. Nekateri so trdili, da je šlo za hudodelske računalniške uporabnike iz Rusije, spet drugi so obtoževali rusko vlado, čeprav je Estonija na koncu kazensko preganjala posameznega hekerja. Pomembna lekcija primera Estonije je bila, da so lahko tudi zelo velike organizacije in vladna ministrstva ranljiva na prekinitvene napade te vrste (Cornish in drugi 2009).

Zaradi izkušenj iz elektronskega vojskovanja so kibernetske operacije postale značilnost konvencionalnih vojaških napadov. V septembru leta 2007 je bil izraelski zračni napad na tarčo v Siriji izveden s pomočjo vzporednega kibernetskega napada proti sirski zračni

obrambi, kar je omogočilo izraelskemu letalu, da je priletel v sirski zračni prostor brez strahu, da bi bil opažen in onemogočen (Reilly 2008). V prihodnosti naj bi "kibernetski napadi na vladne strežnike vedno bolj predstavljali opozorilo pred bližajočim se fizičnim napadom" (Ficke 2008). Med rusko-gruzijskim konfliktom glede Južne Osetije v letu 2008, ki so ga opisali kot "prihajajočo dobo nove dimenzije bojevanja" (Skinner 2008), smo bili priča zasebni računalniški moči, organizirani in koordinirani tako, da je nacionalnemu sovražniku povzročila strateške posledice. Ni jasno, ali je ruska vlada stala neposredno za napadom ali je uradno odobrila DDOS napade na Gruzijo, vendar je jasno, da napadov vsaj uradno ni preprečila. Čeprav ni bila zabeležena nikakršna dolgotrajna kibernetska škoda, je koordiniran napad prikazal neizkoriščen potencial uporabe interneta za povzročitev množične zmede, pri doseganju političnih ciljev." Dejstvo je, da bo kibernetsko vojskovanje v prihodnjih letih predstavljalo izjemno pomemben dejavnik v konfliktih med državami. Z zmanjševanjem pomembnosti fizičnih in ozemeljskih dejavnikov se značaj bojevanja temeljito spreminja (Cornish in drugi 2009).

Prelomno točko na področju geopolitičnih spopadov predstavlja Stuxnet. Gre namreč za prvo uporabo kibernetskega orodja za dosego strateških ciljev s strani države, ki predstavlja verjetno ravnanje držav v prihodnosti. Stuxnet je črv, odkrit junija 2010, s katerim je bila napadena iranska jedrska ustanova v Natanzu. Ustvarjen je bil z namenom izvedbe kibernetskega udara proti iranskemu jedrskemu programu. Deloval je tako, da je spremenil frekvenco električnega toka, ki je napajal Siemensove centrifuge za bogatenje urana, kar je povzročilo njihovo premikanje naprej in nazaj, z intervali, za katere naprave niso bile ustvarjene. Gre za prvi in do danes edini primer kibernetskega napada, ki je povzročil fizično uničenje infrastrukture, ki so jo nadzirali okuženi računalniki. Zaradi velikosti in sofisticiranosti črva, strokovnjaki menijo, da je bil lahko ustvarjen samo s financiranjem in podporo nacionalnih držav. Čeprav uradno nihče ni prevzel odgovornosti, se predvideva, da sta ga ustvarili ZDA in Izrael. Kljub materialni škodi, ki jo je povzročil črv, so pomembnejši politični učinki in strateški kontekst uporabe tega črva. Če je bil kibernetski prostor do sedaj uporabljan za industrijsko vohunjenje ali podporo fizičnim akcijam, napad prikazuje zmožnost kibernetske vojne med državami z napadi na fizične cilje zgolj z uporabo kibernetskega prostora (Farwell in Rohozinski 2011).

Scot Borg, direktor US Cyber Consequences Unit, ocenjuje, da bi "DDOS napadi velikega obsega, ki bi bili uperjeni proti ZDA, lahko povzročili uničenje. V primeru, da bi bilo električno omrežje ali druge storitve prekinjene za obdobje treh mesecev, bi bila škoda ekvivalentna hkratnemu udaru 40 do 50 orkanov" (Fickes 2008).

6 NACIONALNA VARNOST IN ZAŠČITA KRITIČNE INFRASTRUKTURE

6.1 Nacionalna varnost ZDA v kibernetskem prostoru

Kibernetska varnost je ključnega pomena za zaščito in uveljavljanje ameriških nacionalnih interesov. Kot je zapisano v Nacionalni varnostni strategiji ZDA iz leta 2010, dolgoročne prioritete vključujejo:

- varnost ZDA, njenih državljanov, zaveznic in partneric,
- močno, inovativno in rastoče gospodarstvo znotraj odprtega mednarodnega ekonomskega sistema, ki poudarja blaginjo in priložnost,
- spoštovanje univerzalnih vrednot doma in po svetu (The White House 2010, 7).

Vse bolj je sposobnost ZDA, da doseže te cilje, odvisna od zanesljivega in varnega dostopa do interneta, za katerega je državna sekretarka Hillary Rodham Clinton dejala, da predstavlja "omrežje, ki povečuje moč in potencial vseh ostalih omrežij" (Clinton 2010). Sposobnost ZDA, da uveljavijo svoje interese je odvisna od zaupanja v delovanje interneta, varnost sistemov, ki so povezani z njim, in njegove uporabnike. Vendar je obstoj varnega in zaščitenega interneta ogrožen s strani različnih akterjev in groženj, zato ga ustvarjalci politik ne smejo jemati kot nekaj samoumevnega (Lord in Sharp 2011).
Informacijska tehnologija predstavlja povečevalca moči za vojsko ZDA in obveščevalno dejavnost po svetu. DOD sedaj upravlja že z več kot 15.000 omrežji in 7 milijoni računalniških naprav na več kot 4000 lokacijah v 88 državah. Ta napredna informacijska infrastruktura omogoča ZDA predvidevanje, zaznavanje in odzivanje na nacionalno-varnostne grožnje z neverjetno natančnostjo in učinkovitostjo. Vojaška uporaba kibernetske tehnologije lahko uveljavlja ameriške interese, vendar hkrati ustvarja ranljivosti. Vojaške sile ZDA so v veliki meri odvisne od dostopa do civilnih omrežij. Četudi so vojaška in civilna omrežja medsebojno ločena, gibanje podatkov in uporabnikov med njimi povzroča nepredvidene nevarnosti. Vsak dan so oborožene sile izpostavljene milijonom kibernetskih napadov in vdorov. Vsako uro pride do 250.000 poskusov vdorov in pregledovanj vojaških omrežij ZDA, v sisteme poskuša prodreti več kot 100 obveščevalnih agencij in tujih vojaških sil. Čeprav so ti poskusi napadov večinoma odbiti, je potreben samo en sam uspešen vdor, da pride do ogrozitve občutljivih informacij (Lynn 2010).

Dostop do kibernetskega prostora je prav tako omogočil novo priložnost za ustvarjanje blaginje. Po podatkih Information Technology and Innovation Foundation je informacijska tehnologija omogočila povečanje letnega bruto domačega proizvoda ZDA za 2000 milijard dolarjev. Številne študije kažejo, da je internet izboljšuje učinkovitost, znižuje stroške, potrošnikom povečuje izbiro, pospešuje produktivnost, izboljšuje dostop na tržišča za mala podjetja, spodbuja inovativnost in povečuje rast prihodkov (Atkinson in drugi 2010). Vseeno ekonomske pridobitve, ki jih je omogočil internet, niso trajne. Kibernetski kriminal in vohunjenje ogrožata zaupne informacije, trgovske skrivnosti in intelektualno lastnino, ki predstavljajo gonilno silo vojaške moči in globalne konkurenčnosti ZDA. V primeru, da ZDA in njihova podjetja zaradi posledic kibernetskih napadov postanejo manj zanesljive gospodarske partnerice, bo ameriški vpliv začel bledeti, kar bi ogrozilo nacionalno varnost. Celo najnaprednejše organizacije postajajo ranljive za kibernetske nevarnosti. Če bi bile resno ogrožene, bi se škodljive posledice razširile povsod. V letu 2011 je prišlo do dveh kibernetskih napadov, ki bi lahko predstavljala "požar pete stopnje" za kibernetsko varnostno skupnost. Prvi je bil napad na RSA Security, največji ponudnik kibernetskih varnostnih naprav za avtentikacijo za zvezne oblasti in podjetja Fortune 500. Napad je uporabil zlo programsko opremo za pridobitev pomembne intelektualne lastnine, kar bi lahko ogrozilo delovanje sistema za večino strank podjetij. Drugi napad je bil usmerjen na Comodo Group, ki zagotavlja digitalne certifikate, ki potrjujejo avtentičnost spletnih strani. Napadalec se je vtihotapil v italijansko računalniško podjetje in zlorabil svoj dostop do Comodovih sistemov za ustvarjanje lažnih certifikatov popularnih spletnih strani, kot so Google, Yahoo in Skype. Taki vdori lahko omajejo zaupanje v internetno delovanje, saj uporabniki ne vedo, ali sporočajo svoje podatke legitimnim stranem (Nakashima 2011; Richmond 2011).

Nacionalna kritična infrastruktura, ki omogoča pravilno delovanje dinamičnemu gospodarstvu, še vedno ostaja nezadostno zaščitena. Ponudniki kritične infrastrukture še vedno ugotavljajo obseg njihovih ranljivosti za kibernetske grožnje. Večji ponudnik vodovodnih storitev v južni Kaliforniji je najel računalniškega hekerja, da preizkusi ranljivosti računalniškega omrežja podjetja – kar je hekerju in njegovi ekipi uspelo v enem dnevu, s čimer so pridobili nadzor nad opremo, ki dodaja kemikalije v pitno vodo Kalifornijcev (Dilanian 2011).

Dostop do interneta zagotavlja spoštovanje univerzalnih vrednot, ki so pomembne za državljane ZDA, kot sta svoboda govora in združevanja. Internet zagovornike teh vrednot oskrbuje z novimi orodji za dosego njihovih ciljev. Opornikom daje možnost izražanja, zatirani javnosti sredstva za organiziranje, nemočnim posameznikom pa priložnost za

globalno zbirališče. Čeprav se opazovalci ne strinjajo glede vpliva interneta na bližnjevzhodne in severnoafriške revolucije v letu 2011, nihče ne dvomi, da so spletne strani družabnih omrežij, kot sta Twitter in Facebook, igrale pomembno vlogo. Zaradi internetne moči in prizadevanj avtoritarnih režimov po zadušitvi njegove proste uporabe ameriška administracija poudarja zavezanost ZDA k svobodi interneta. To zavezo so podprli z denarnimi sredstvi, tako da so investirali velike vsote v tehnologije, ki lahko zaobidejo vladne cenzorje. Državna sekretarka Clinton je izrazila zavezo po "svobodi povezovanja – ideji, da vlade ne preprečujejo ljudem povezovanja na internet, na spletne strani ali med seboj" (Clinton 2010). Poudarila je tudi ameriško "globalno zavezanost k internetni svobodi in zaščiti človekovih pravic na spletu, kot to počnemo brez povezave, "vključno s svobodo izražanja, združevanja in zbiranja (Clinton 2011).

6.2 Kritična informacijska infrastruktura

Svetovna velesila ZDA je začetnica in vodilna na področju razprav glede svoje kibernetske ranljivosti. Njena kritična infrastruktura predstavlja očiten cilj napada v kateremkoli spopadu. Razprave o zaščiti kritične infrastrukture so se začele s pojavom novih groženj, ki v prejšnjem obdobju niso bile izvedljive. Razvoj kibernetskega prostora je povzročil, da je prvič v zgodovini možno napasti sisteme kritične infrastrukture z uporabo kibernetskega prostora, brez fizičnega dostopa do lokacije in brez izpostavljenosti med napadom in po njem. Zaščita kritične infrastrukture je eden izmed ključnih problemov kibernetske varnosti, zato zahteva specifično razpravo (Ben-Israel in Tabansky 2011).

Moderna družba je postala veliko bolj odvisna od dosegljivosti, zanesljivosti, varnosti in zaščitenosti mnogih tehnoloških infrastruktur. Tako zaradi velikih družbenih in ekonomskih koristi, ki jih omogočajo, kot tudi zaradi resnih posledic, ki bi jih prineslo njihovo nedelovanje, so informacijski sistemi postali nujni za človeško blagostanje. Infrastruktura je sistem, ki združuje številne strukture in omogoča določene aktivnosti, npr. vodovodna cev, ki prenaša vodo od zajetja do naselbin, asfaltirane ceste, mostovi in križišča, ki omogočajo gibanje ljudi in dobrin, letala, komunikacije, gorivo in zdravstvene storitve. Ena izmed značilnosti infrastruktur je odvisnost številnih aktivnosti od njenega delovanja. V preteklosti je odvisnost izhajala zgolj iz fizičnih in geografskih odnosov. Z razvojem kibernetskega prostora, ki vključuje komunikacijske sisteme podatkov in računalniška sredstva avtomatizacije nadzora in poveljevanja, so se pojavila nova razmerja, ki ustvarjajo nove

ranljivosti. Infrastrukture, ki jih smatramo za kritične, so tiste fizične in informacijske zmogljivosti, omrežja in sredstva, ki bi ob poškodovanju povzročila resne posledice za blagostanje državljanov, ustrezno delovanje vlad ter industrij in ostale škodljive učinke. Za številne države so značilne različne definicije kritične infrastrukture. V splošnem pa velja, da so "kritične infrastrukture tiste strukture, katerih prekinitev vodi k veliki družbeno-ekonomski krizi, ki lahko ogrozi stabilnost družbe in zato povzroči politične, strateške in varnostne posledice" (Nickolov 2005; Tabansky 2011).

Nickolov našteva infrastrukture, ki morajo delovati na minimalni ravni za preživetje ostalih javnih in zasebnih sektorjev:

- preskrba z elektriko, gorivom in vodo,
- transportni in komunikacijski sistemi,
- preskrba s hrano in upravljanje z odpadki,
- finančne službe in zavarovalništvo
- informacijska in telekomunikacijska omrežja,
- vojaški in obrambni sistemi, civilna zaščita,
- urgentne, zdravstvene in reševalne službe,
- javne agencije in administracija, sodni sistem,
- mediji, glavne raziskovalne ustanove, ipd. (Nickolov 2005).

Čeprav je bila večina teh sistemov fizično ločena med seboj, so se kritične infrastrukture zaradi komunikacije, upravljanja z različnimi informacijami in kontrolnih funkcij skozi čas začele združevati in postale odvisne od informacijskih struktur, kot je javno telefonsko omrežje, internet, zemeljska in satelitska brezžična omrežja. Prišlo je tudi do nastanka novih kritičnih infrastruktur, ki predstavljajo popolne informacijske infrastrukture: računalniške podatkovne baze, ki vsebujejo pomembne podatke, kot so zapisi o kapitalu v bančnem sistemu, znanstvena in tehnična intelektualna lastnina ter programi, ki upravljajo produkcijske procese in številne poslovne procese. V informacijski dobi koncept "infrastrukture" vsebuje tudi računalniške sestavne dele, zato se danes infrastruktura vedno nanaša na informacijsko infrastrukturo. Tehnološki napredek je vodil k večji avtomatizaciji v delovanju in nadzoru kritične infrastrukture in nastanku posebne informacijske infrastrukture (Nickolov 2005; Tabansky 2011).

Napad na infrastrukturo ima učinek "ojačevalca sile" in omogoča majhnim napadom doseči velik učinek, zato so se strukture in omrežja kritične infrastrukture zgodovinsko pokazale kot

privlačne tarče napada za številne akterje. Koncepti zaščite strateško pomembne infrastrukture in objektov so del nacionalnega obrambnega načrtovanja že desetletja, čeprav se stopnja pomembnosti spreminja. Proti koncu hladne vojne in v naslednjih letih je možnost prekinitve delovanja infrastrukture zaradi napadov ali drugih oblik prekinitev igrala majhno vlogo v razpravi glede varnosti. Informacijska infrastruktura igra pomembno vlogo v razpravi o zaščiti kritične infrastrukture. Ranljivosti kritične infrastrukture v glavnem izhajajo iz informacijske infrastrukture. Ta podpira številne elemente kritične infrastrukture, ki je za svoje gladko, zanesljivo in neprekinjeno delovanje postala odvisna od močno medsebojno odvisnih nacionalnih in mednarodnih nadzornih sistemov programske opreme. To vodi h kompleksnim oblikam medsebojne odvisnosti. Zato del globalne in nacionalne informacijske infrastrukture, ki je nujen za kontinuiteto delovanja storitev kritične infrastrukture, imenujemo *kritična informacijska infrastruktura* (Dunn 2007).

Dejavnik medsebojne odvisnosti pomeni, da kritične infrastrukture niso nujno napadene fizično, ampak so lahko napadene preko elektronskih in virtualnih sredstev, kar bi v najslabšem primeru pomenilo, da lahko skupina izurjenih hekerjev s sovražnimi nameni spravi celotno državo na kolena. Danes je lahko obstoječa računalniška infrastruktura izrabljena z vdorom v komunikacijska omrežja ali preko strojne ali programske opreme računalnikov za nadzor in upravljanje, da bi dosegli prekinitev, prenehanje delovanja ali fizično uničenje kritičnega sistema. Zaradi teh značilnosti se kibernetske grožnje v osnovi razlikujejo od izzivov tradicionalnih groženj (Dunn 2007).

7 STRATEŠKI DOKUMENTI ZDA, KI ZADEVAJO KIBERNETSKI PROSTOR

7.1 Nacionalna strategija za zašito kibernetskega prostora – 2003

Nacionalna strategija za zaščito kibernetskega prostora predstavlja prvo nacionalno pobudo za premislek o internetni varnosti. Februarja 2003 je bila razglašena s strani *President's Critical Infrastructure Protection Board*, političnega subjekta, ki je nastal s sprejetjem predsedniške izvršne odredbe 13231. Čeprav odredba ni omenjala nikakršne potrebe po načrtu kibernetske zaščite, razlogi verjetno ležijo v potrebi po javnem odzivu na teroristični napad 11. septembra in nepoznavanju interneta v povezavi z nacionalnimi javnimi politikami, še posebej v smislu kibernetske varnosti (Casey 2003).

O nacionalni strategiji za zašito kibernetskega prostora lahko razmišljamo kot o treh ločenih dokumentih, ki vsebujejo podobno vsebino. Prvi del, *Povzetek,* je sestavljen iz sedmih strani in povzema vsako od prednostnih nalog strategije. Sledi *Uvod,* kjer se ponovi besedilo iz povzetka in dva manjša odstavka "*Kibernetske grožnje in ranljivosti*" ter "*Nacionalna politika in vodilna načela*". Prvi odstavek omenja pretekle napade, kot sta NIMDA in Code Red, ter skuša opisati mogoče napade v prihodnosti. V drugem odstavku je kratko in jedrnato opisana nacionalna politika do kibernetskega prostora, ki ji sledijo jasno zapisana vodilna načela. Ta dva odstavka skupaj z uvodom predstavljata drugi dokument. Zadnji del, ki ga obravnavamo kot tretji samostojni dokument, predstavlja srce strategije in bolj podrobno predstavlja ukrepe. Sestavljen je iz petih delov, kjer je vsak del posvečen eni izmed nacionalnih prednostnih nalog (Casey 2003).
V Nacionalni strategiji za zaščito kibernetskega prostora je izraženih pet nacionalnih prednostnih nalog:

1. Nacionalni sistem odzivanja za zaščito kibernetskega prostora.
2. Nacionalni program za zmanjšanje varnostnih groženj in ranljivosti v kibernetskem prostoru.
3. Nacionalni program usposabljanja in ozaveščanja glede zaščite kibernetskega prostora.
4. Zaščita vladnega kibernetskega prostora.
5. Nacionalna varnost in mednarodno sodelovanje na področju zaščite kibernetskega prostora.

Nikjer v strategiji ni izraženo, da bi bila katera izmed prednostnih nalog pomembnejša od ostalih, kljub številčnemu zaporedju, v katerem so zapisane. Prva prednostna naloga se osredotoča na izboljšanje odzivanja na kibernetske incidente in zmanjševanje morebitne škode, ki bi jo povzročili ti dogodki. Druga, tretja in četrta prednostna naloga se nanašajo na zmanjšanje groženj zaradi kibernetskih napadov in zmanjšanje ranljivosti na te napade. Peta prednostna naloga je preprečevanje kibernetskih napadov, ki bi lahko ogrozili sredstva nacionalne varnosti ter izboljšanje mednarodnega upravljanja in odzivanja na njih.

Vodilna načela strategije lahko povzamemo z naslednjimi tematskimi področji:

1. Nacionalna pobuda za sodelovanje in delitev informacij o grožnjah ter opravljanje lastnih zadolžitev pri zaščiti lastnih sistemov.

2. Zaščita zasebnosti in javnih svoboščin.
3. Strategijo naj vodijo tržne zakonitosti in ne vladni ukrepi.
4. Prevzemanje odgovornosti v obliki seznamov organov in opisov področij delovanja.
5. Prilagodljivost sistemov odzivanja na načrtovanje in izvedbo.
6. Večletna prizadevanja vključno z rednimi ponovnimi pregledi (Department of Homeland Security 2003).

V skladu z Nacionalno strategijo za domovinsko varnost so strateški cilji te strategije naslednji:

- preprečevanje kibernetskih napadov na kritično infrastrukturo ZDA;
- zmanjševanje nacionalne ranljivosti za kibernetske napade;
- minimizacija škode in časa, potrebnega za povrnitev v stanje pripravljenosti zaradi kibernetskih napadov od trenutka, ko se zgodijo (Department of Homeland Security 2003).

Grožnje in ranljivosti, ki najbolj ogrožajo ZDA naj bi bile glede na strategijo sledeče:

- glavno grožnjo predstavljajo organizirani kibernetski napadi, ki lahko povzročijo izčrpavajoče prekinitve nacionalne kritične infrastrukture, gospodarstva in nacionalne varnosti;
- vohunjenje za vladnimi organizacijami, univerzitetnimi raziskovalnimi centri in zasebnimi podjetji (Department of Homeland Security 2003).

Čeprav Ministrstvo za domovinsko varnost prevzema večino odgovornosti pri izvajanju strategije, je Urad za upravljanje in proračun (*Office of Management and Budget - OMB*) naveden "kot organ, ki nadzira implementacijo vladnih politik, načel, standardov in priporočil za programe zvezne vlade v zvezi z računalniško varnostjo." Ministrstvo za domovinsko varnost združuje 22 zveznih organov, katerih skupnih cilj je povečanje domovinske varnosti. Minister bo imel pomembne zadolžitve glede varnosti kibernetskega prostora. Te naj bi zajemale:

- razvoj vseobsegajočega državnega načrta za zaščito ključnih virov in kritične

infrastrukture ZDA;

- zagotavljanje kriznega upravljanja v primeru napada na sisteme kritične infrastrukture;
- zagotavljanje tehnične podpore zasebnemu sektorju in ostalim vladnim organom, upoštevajoč nujne ukrepe za povrnitev stanja v primeru odpovedi delovanja kritičnih informacijskih sistemov;
- usklajevanje z ostalimi zveznimi agencijami za zagotavljanje informacij in nasvetov v zvezi z ustreznimi zaščitnimi ukrepi in protiukrepi državnim, lokalnim in nevladnim organizacijam, vključno z zasebnim sektorjem, izobraževalno skupnostjo in javnostjo;
- izvajanje in financiranje raziskav ter razvijanje skupaj z ostalimi agencijami, kar bo vodilo do novega znanstvenega razumevanja in novih tehnologij v podporo domovinski varnosti. (Department of Homeland Security 2003)

Prednostna naloga I.: Nacionalni sistem odzivanja za zaščito kibernetskega prostora

Ker nikakršen načrt kibernetske zaščite ni odporen na jasen in premišljen napad, morajo biti informacijski sistemi zmožni delovanja med napadom in biti tako odporni, se hitro povrnejo v polno delovanje.

Nacionalna strategija za zaščito kibernetskega prostora prepoznava osem glavnih ukrepov in pobud za varnostno odzivanje v kibernetskem prostoru:

1. Ustanovitev javno-zasebne arhitekture za odzivanje na kibernetske incidente na nacionalni ravni.
2. Zagotavljanje razvoja tehnične in strateške analize kibernetskih napadov in ocen ogroženosti.
3. Vzpodbujanje razvoja zmogljivosti zasebnega sektorja, da se doseže enoten pogled na stanje kibernetskega prostora.
4. Razširitev omrežja za kibernetsko odzivanje in informiranje v podporo Ministrstvu za domovinsko varnost pri koordiniranju kriznega upravljanja zaščite v kibernetskem prostoru.
5. Izboljšanje upravljanja v primeru državnih incidentov.
6. Koordiniranje procesov za prostovoljno sodelovanje pri razvoju nacionalnih javno-zasebnih načrtov kontinuitete in načrtov za primere kriznih stanj.
7. Izvajanje načrtov kontinuitete kibernetske zaščite za zvezne sisteme.

8. Izboljšanje in povečanje izmenjave informacij med javnim in zasebnim sektorjem glede kibernetskih napadov, groženj in ranljivosti (Department of Homeland Security 2003).

Prednostna naloga II.: Nacionalni program za zmanjšanje varnostnih groženj in ranljivosti v kibernetskem prostoru

Ranljivosti izhajajo iz šibkih točk tehnologije in neustrezne implementacije in nadzora tehnoloških produktov. Nacionalni program poskuša vzpostaviti načrt za identifikacijo internetnih ranljivosti s pomočjo številnih vladnih organov in tehnologije.

Nacionalna strategija za zaščito kibernetskega prostora prepoznava osem glavnih ukrepov in pobud za zmanjšanje groženj in z njimi povezanimi ranljivostmi:

1. Krepitev zmogljivosti organov nadzora za preprečevanje in kazensko preganjanje napadov v kibernetskem prostoru.
2. Ustvarjanje procesov za ocenjevanje nacionalne ranljivosti za boljše razumevanje potencialnih posledic groženj in ranljivosti.
3. Varovanje internetnih mehanizmov z izboljševanjem protokolov in povezovanja.
4. Spodbujanje uporabe zaupanja vrednih digitalnih sistemov nadzora in sistemov prevzemanja podatkov.
5. Zmanjševanje in izboljševanje ranljivosti programske opreme.
6. Razumevanje medsebojne odvisnosti infrastrukture in izboljševanje fizične varnosti kibernetskih sistemov in telekomunikacij.
7. Priotizacija zveznih programov raziskav in razvoja kibernetske zaščite.
8. Ovrednotenje in zavarovanje nastajajočih sistemov (Department of Homeland Security 2003).

Prednostna naloga III.: Nacionalni program usposabljanja in ozaveščanja o zaščiti kibernetskega prostora

Enega izmed najpomembnejših kosov varnostne sestavljanke prestavlja izobrazba. Večina kibernetskih ranljivosti izhaja iz pomanjkanja ozaveščenosti o kibernetski varnosti pri računalniških uporabnikih, upravljalcih sistemov, razvijalcih tehnologije, upravnih odborih ...

Tretja prioriteta je verjetno ena izmed najbolj praktičnih in bo zato najlažje izvedljiva. Tri komponente te prioritete so *zavedanje, usposabljanje in certificiranost.*

Nacionalna strategija za zaščito kibernetskega prostora prepoznava štiri temeljne naloge in pobude glede ozaveščanja, izobraževanja in usposabljanja:

1. Spodbujanje vseobsegajočega nacionalnega programa ozaveščanja, da bi krepili zavedanje vseh Američanov – podjetij, zaposlenih in splošne populacije – da zaščitijo svoje dele kibernetskega prostora.
2. Spodbujanje ustreznih programov usposabljanja in izobraževanja v podporo potreb države glede kibernetske zaščitenosti.
3. Povečanje učinkovitosti obstoječih programov usposabljanj zveznih oblasti o kibernetski varnosti.
4. Spodbujanje podpore zasebnega sektorja za izdajanje koordiniranih, prepoznavnih, profesionalnih potrdil glede kibernetske varnosti. (Department of Homeland Security 2003).

Prednostna naloga IV.: Zaščita vladnega kibernetskega prostora

Čeprav vlada upravlja zgolj z manjšinskim deležem računalniških sistemov državne kritične infrastrukture, vlade na vseh ravneh opravljajo bistvene storitve na področjih kmetijstva, prehrane, vode, javnega zdravstva, nujnih storitev, obrambe, socialne blaginje, informacij in telekomunikacij, energije, transporta, bančništva in financ, kemikalij, poštnih in dostavnih storitev, za katere je kibernetski prostor ključnega pomena za delovanje. Vladni organi morajo predstavljati zgled, ko gre za vprašanje kibernetske varnosti. Ponudniki tehnologije bi morali biti zadovoljni z izjavo, da bodo "zvezne oblasti postale zgodnji uporabniki novih, bolj varnih sistemov in načinov delovanja, kjer je to potrebno" (Department of Homeland Security 2003, 43).

Nacionalna strategija za zaščito kibernetskega prostora prepoznava pet temeljnih nalog in pobud glede zaščite vladnega kibernetskega prostora:

1. Neprestano ocenjevanje groženj in ranljivosti zveznih kibernetskih sistemov.
2. Avtentikacija in ohranjanje pooblaščenih oseb za zvezne kibernetske sisteme.

3. Zaščita zveznih brezžičnih lokalnih omrežij.
4. Izboljšanje varnosti pri zunanjih izvajalcih in preskrbi vlade.
5. Spodbujanje državnih in lokalnih oblasti pri ustanavljanju programov zaščite informacijske tehnologije in sodelovanju z ostalimi podobnimi vladami pri delitvi informacij in analitičnih centrih (Department of Homeland Security 2003).

Prednostna naloga V.: Nacionalna varnost in mednarodno sodelovanje na področju zaščite kibernetskega prostora

Ameriški kibernetski prostor povezuje ZDA z ostalim svetom. Omrežje vseh omrežij se razteza po celotnem planetu, kar zlonamernim akterjem omogoča, da upravljajo s sistemi tisoče kilometrov stran. Kibernetski napadi prečkajo meje s svetlobno hitrostjo in razpoznavanje vira zlonamerne dejavnosti je težko. Zato ZDA potrebujejo sistem mednarodnega sodelovanja, ki bo olajšal delitev informacij, zmanjšal ranljivosti in odvrnil napadalce.

Nacionalna strategija za zaščito kibernetskega prostora prepoznava šest temeljnih nalog in pobud za krepitev mednarodnega sodelovanja in nacionalne varnosti ZDA:

1. Krepitev protiobveščevalnih naporov, povezanih s kibernetskim prostorom.
2. Izboljšanje zmogljivosti za pripis napada in odziv na napad.
3. Izboljšanje koordinacije pri odzivanju na kibernetske napade znotraj nacionalne varnostne skupnosti v ZDA.
4. Sodelovanje z industrijo in mednarodnimi organizacijami, da bi olajšali dialog in partnerstvo med mednarodnimi javnimi in zasebnimi sektorji, katerih glavni namen je zaščita informacijske infrastrukture in promocija globalne varnostne kulture.
5. Spodbujanje ustanavljanja nacionalnih in mednarodnih "watch-and-warning" omrežij za zaznavanje in preprečevanje kibernetskih napadov, ko se ti pojavijo.
6. Spodbujanje drugih držav, da se pridružijo konvenciji Sveta Evrope glede kibernetskega kriminala, ali da zagotovijo, da so njihovi zakoni in postopki najmanj tako celoviti (Department of Homeland Security 2003).

7.2 Pregled politik kibernetskega prostora – 2009

Januarja 2008 je administracija predsednika Georga Busha začela s celovito nacionalno iniciativo glede kibernetske varnosti. V pobudi, da bi dosegli večjo varnost ZDA, kar zadeva kibernetske grožnje, je iniciativa vzpostavila večstranski pristop zvezne vlade pri identifikaciji tedanjih in pojavljajočih se kibernetskih groženj z utrditvijo kibernetskih in telekomunikacijskih ranljivosti ter s proaktivnim delovanjem in z odzivanjem na subjekte, ki želijo ukrasti ali upravljati z zaščitenimi podatki na zaščitenih zveznih sistemih. *Homeland Security Presidential Directive 23* in *National Security Presidential Directive 54*, s katerima je bila vzpostavljena CNCI imata še vedno oznaki zaupno, čeprav je nekaj podrobnosti iniciative postalo javnih preko sporočil za javnost, izjav voditeljev izvršne veje oblasti in analiz s strani posameznikov, ki spremljajo zadeve, povezane s kibernetsko varnostjo in terorizmom.

V govoru med svojo predsedniško kampanjo je predsednik Obama obljubil, da bo "kibernetsko varnost napravil za najvišjo prednostno nalogo, kar bi v 21. stoletju morala biti /.../ in imenoval nacionalnega kibernetskega svetovalca, ki bo poročal neposredno predsedniku" (Obama 2008). Kmalu po prevzemu položaja, je Obama v februarju 2009 zahteval od Sveta za nacionalno varnost *(National Security Council)* in Sveta za domovinsko varnost *(Homeland Security Conucil)* pregled načrtov, programov in aktivnosti zvezne vlade, vključno s projekti CNCI, povezanimi s kibernetsko varnostjo. Pregled naj bi predstavil priporočila za razvoj strateškega okvirja in koordinacijo iniciativ znotraj vlade ZDA. Pregled je imel za posledico 29. maja 2009 objavljeno poročilo, ki je predlagalo ukrepe za dosego bolj zanesljive, odporne in zaupanja vredne digitalne infrastrukture. Poročilo je spodbudilo Državno ministrstvo ZDA (*US State Departement*), Ministrstvo za trgovino ZDA (*US Commerce Departement*), Ministrstvo za domovinsko varnost ZDA (*US Departement of Homeland Security*) in Ministrstvo za obrambo ZDA (*US Departement of Defense*), da so izdali nove strateške dokumente, in kongres, da je začel v večji meri sprejemati zakonodajo na področju kibernetskega prostora.

Pregled je bil oblikovan kot na novo zastavljen program, ki je v razpravo vključil številne javno-zasebne partnerje. V to je bilo všteto več kot štirideset sestankov z industrijo, znanstveno srenjo, državnimi vladami, skupinami za civilne svoboščine, sindikati, mednarodnimi vladami, zakonodajno in izvršno vejo ter ostalimi. To je na strani partnerjev sprožilo "transparentnost in vključenost brez primere" (Hathaway 2009), saj so prejšnje politične iniciative v zvezi načrtom za kibernetsko varnost postale tarče kritik zaradi pretirane skrivnostnosti. Cilj te razširjene vključitve številnih subjektov je zajemal

identifikacijo ključnih zahtev, opozarjanje na vrzeli v tedanjih politikah, predlaganje področij, kjer je potrebno izboljšano sodelovanje, in določitev odgovornosti za politike kibernetskega prostora. Kot je zapisala Bela Hiša:

> *"V takšnem okolju status quo ni več sprejemljiv, zato se mora nacionalni dialog glede kibernetske varnosti začeti danes. Vlada ZDA sama ne more biti uspešna pri zaščiti kibernetskega prostora, ni pa popolnoma izvzeta iz zaščite naroda pred kibernetskimi incidenti oz. nesrečami. Zagotavljanje, da bo kibernetski prostor dovolj odporen in zanesljiv, da bo podpiral cilje ZDA glede gospodarske rasti, civilnih svoboščin in zaščite privatne lastnine, nacionalne varnosti ter nadaljnjega razvoja globalnih demokratičnih institucij, zahteva sodelovanje s posamezniki, znanstveno srenjo, industrijo in vladami. Kibernetska varnost mora postati nacionalna prednostna naloga in biti usmerjana iz Bele Hiše" (*The White House 2009c, iii*)*

Ta vsesplošna vključenost je izpostavila nekatere temeljne napetosti, ki so del nacionalnih politik glede kibernetske varnosti v 21. stoletju. Poleg zadev, ki so obravnavane v pregledu politik, so bili problemi *zasebnosti, javno-zasebnega partnerstva in nacionalnega dialoga* zaradi prepletenosti narave problema in predlaganih odzivov deležni posebne pozornosti (Center for Democracy & Technology 2009).

Zagovorniki zasebnosti so dolgo časa vztrajali, da vlada grožnja zasebnosti in da "prevelika količina zakonodaje igra ključno vlogo pri zmanjševanju zasebnosti" (Harper 2004). Čeprav obstoji splošno prepričanje, da je vložek državljanov za politiko zasebnosti pomemben, obstaja tudi prepričanje, da trenutna zakonodaja ZDA na področju zasebnosti ni v koraku z grožnjami, ki ogrožajo tako vlado kot zasebni sektor (The White House 2009a).

Ena izmed ugotovitev pregleda politik glede kibernetskega prostora je, da so interesi javnega in zasebnega sektorja prepleteni in da morajo vladni in industrijski voditelji, tako nacionalni kot mednarodni, razviti celovite rešitve. Predlogi vključujejo izboljšanje vladne učinkovitosti, vključenosti zasebnega sektorja, javno-zasebna partnerstva in delitev informacij. To se lahko doseže z vladno prerazporeditvijo sredstev, ovrednotenjem preprek za dosego partnerstev, integriranim pristopom k formulaciji politik in koordinaciji/širjenju mednarodnih partnerstev. Nacionalni dialog glede kibernetske varnosti je z vključitvijo zasebnega sektorja v 60-dnevno pripravo poročila izjemno napredoval. Potreba po opredelitvi izzivov in razpravi o tem, kaj lahko država stori za kolektivno reševanje problemov, je ustvarjena z namenom izboljšanja procesa, kjer bodo državljani ZDA cenili potrebo po delovanju. Ključna ugotovitev

dokumenta Pregled politik glede kibernetskega prostora je izpostavitev dejstva, da ZDA ne bodo uspele pri zaščiti kibernetskega prostora, če bo vlada delovala samostojno. Predstavlja tudi edinstveno priložnost za ZDA, da sodelujejo z državami po svetu pri spodbujanju inovativnosti in vsakemu poskusu napraviti kibernetska omrežja varna (The White House 2009a).

Politika kibernetske varnosti vključuje strategije, politike in standarde, ki zadevajo varnost in delovanje v kibernetskem prostoru in zajemajo vse oblike zmanjševanja groženj, zmanjševanja ranljivosti, odvračanja, mednarodnega angažmaja, odzivanja na incidente, odpornosti, aktivnosti politik za obnovitev stanja, vključno z nalogami delovanja v računalniškem omrežju, nalogami zavarovanja informacij, diplomatskimi, vojaškimi, policijskimi in obveščevalnimi nalogami, ki so povezane z varnostjo in stabilnostjo globalne informacijske in komunikacijske infrastrukture.

Ta dokument povzema zaključke in predstavlja okvir za nastanek zanesljive, odporne, zaupanja vredne digitalne infrastrukture za prihodnost. Pregled politik kibernetskega prostora sestavlja 10 iniciativ glede kratkoročnega načrta delovanja in 14 iniciativ za srednjeročno delovanje na področju zaščite kibernetskega prostora.

Kratkoročni načrt delovanja:

1. Imenovanje uradnika za politike kibernetske varnosti, ki bo odgovoren za koordiniranje državnih politik in dejavnosti, ki zadevajo kibernetsko varnost; ustanovitev močnega direktorata nacionalnega varnostnega sveta, ki mu bo predsedoval uradnik za politike kibernetske varnosti, ki bo hkrati tudi predsednik nacionalnega gospodarskega sveta, tako da bo koordiniral medresorski razvoj strategij in politik, povezanih s kibernetsko varnostjo.

2. Priprava na s strani predsednika odobreno posodobljeno nacionalno strategijo za zaščito informacijske in komunikacijske infrastrukture. Ta strategija bi morala vključevati stalno vrednotenje dejavnosti CNCI in kjer je to ustrezno, graditi na njenih uspehih.

3. Določitev kibernetske varnosti kot ene izmed predsednikovih ključnih prednostnih upravljalskih nalog in vzpostavitev načina merjenja učinkovitosti delovanja.

4. Določitev uradnika za zasebnost in državljanske svoboščine pri direktoratu za kibernetski prostor pri Nacionalno varnostnem svetu.

5. Sklic ustreznih medresorskih mehanizmov za preučevanje prednostnih zadev s področja kibernetske varnosti, ki so identificirane tekom procesa razvoja politike in formulacija enotne, razumljive politike svetovanja, ki jasno določa vloge, naloge in uporabo pooblastil resorjev glede dejavnosti, povezanih s kibernetsko varnostjo pri zvezni vladi.

6. Vzpodbuditev nacionalne javne kampanje o ozaveščenosti in izobraževanju za promocijo kibernetske varnosti.

7. Razvoj vladnih stališč ZDA glede okvirja mednarodne politike kibernetske varnosti in krepitev mednarodnih partnerstev za nastanek pobud, ki obravnavajo vse dejavnosti, politike in priložnosti, povezane s kibernetsko varnostjo.

8. Priprava načrta odzivanja na incidente glede kibernetske varnosti; vzpodbuditev dialoga za okrepitev javno-zasebnih partnerstev, usmerjenih k racionalizaciji, usklajevanju in zagotovitvi sredstev, da bi optimizirali njihov prispevek in zavezanost.

9. V sodelovanju z ostalimi subjekti predsedniških izvršnih odborov, razvijati okvir za raziskave in razvoj strategij, osredotočenih na prelomne tehnologije, ki imajo potencial za izboljšanje varnosti, zanesljivosti, odpornosti in zaupanja v digitalno infrastrukturo; raziskovalni skupnosti omogočiti dostop do podatkov, za lažji razvoj orodij, hipotez in identifikacijo delujočih rešitev.

10. Izgradnja vizije upravljanja z identitetami glede kibernetske varnosti in strategije, ki obravnava interese zasebnosti in civilnih svoboščin, s čimer podpira tehnologije izboljševanja zasebnosti za državljane (The White House 2009a)

Srednjeročni načrt delovanja:

1. Izboljšanje procesa razrešitve medresorskih sporov glede interpretacije zakonov in uporabe politik in pooblastil glede kibernetskega delovanja.

2. Uporaba okvirja ocenjevanja izvrševanja programov, kot jih uporablja Urad za upravljanje in proračun, s čimer bi zagotovili financiranje ministrstev in agencij glede na uspešnost delovanja pri zasledovanju ciljev pri doseganju kibernetske varnosti.
3. Povečanje podpore ključnim izobraževalnim programom, raziskavam in razvoju za zagotovitev stalne konkurenčnosti v ekonomiji informacijske dobe.
4. Razvoj strategije za razširitev in usposabljanje delovne sile, vključno s privabljanjem in ohranjanjem strokovnjakov glede kibernetske varnosti v zvezni vladi.
5. Določitev najučinkovitejšega in uspešnega mehanizma za strateško opozarjanje, ohranjanje ozaveščenosti ter informiranje zmogljivosti za odzivanje na incidente.
6. Razvijanje skupine grozečih scenarijev in načinov merjenja, ki se lahko uporabijo pri odločitvah kriznega upravljanja, načrtovanju povrnitve in prednostnih nalogah pri raziskavah in razvoju.
7. Razvijanje procesov med vladnim in zasebnim sektorjem za podporo preprečevanju, odkrivanju in odzivanju na kibernetske incidente.
8. Razvijanje mehanizmov za izmenjavanje informacij, povezanih s kibernetsko varnostjo, ki obravnavajo probleme zasebnosti in lastnine informacij, ter izmenjavo informacij delajo vzajemno koristno.
9. Razvijanje rešitev za zmogljivosti komuniciranja v sili − v primeru naravnih katastrof, kriz ali konfliktov skladno z zagotavljanjem omrežne nevtralnosti.
10. Povečanje deljenja informacij glede omrežnih incidentov in ranljivosti s ključnimi zavezniki in iskanje bilateralnih in multilateralnih dogovorov, ki bodo izboljšali gospodarske in varnostne interese hkrati s ščitenjem civilnih svoboščin in pravic zasebnosti.
11. Vzpodbujanje sodelovanja med akademskimi in industrijskimi laboratoriji za razvijanje načrtov prehoda in spodbud za hitro prevzemanje raziskav in tehnoloških razvojnih inovacij.
12. Uporaba ciljev infrastrukture in okvirja delovanja raziskav ter razvoja za opredelitev ciljev državnih in mednarodnih organov.
13. Implementacija nabora interoperabilnih sistemov upravljanja z identitetami za izgradnjo zaupanja v spletne transakcije in izboljšanje zasebnosti, v podporo dejavnostim visoke vrednosti.
14. Izboljšanje vladnih strategij javnega naročanja in izboljšanje tržnih spodbud za varne in odporne izdelke strojne in programske opreme, nove varnostne inovacije in varne upravljalske storitve. (The White House 2009a)

7.3 Mednarodna strategija za kibernetski prostor – 2011

Administracija predsednika Obame je 16. maja 2011 izdala Mednarodno strategijo za kibernetski prostor, s podnaslovom Blaginja, varnost in odprtost v omreženem svetu. Predsednik Obama je pri tem dejal, da mednarodna strategija predstavlja prvo uporabo pristopa, ki bo poenotil sodelovanje ZDA z mednarodnimi partnerji na vseh področjih glede kibernetskih zadev. Pri oblikovanju pristopa za maksimizacijo prednosti in zmanjševanje groženj v kibernetskem prostoru predsednikova ekipa stavi na potrebo po izgradnji vladavine zakona z vključevanjem mednarodnih norm in procesov (The White House 2011),

Varnost ne predstavlja edine skrbi glede prihodnosti kibernetskega prostora. Naraščajoče rivalstvo med ZDA in Kitajsko je izpostavilo različnost odnosov glede pomena kibernetskega prostora in namena interneta. Administracija predsednika je zato pohitela, da bi vzpostavila normativen pogled na kibernetski prostor kot globalni politični prostor, pri čemer je vrhunec predstavljal govor sekretarke Clinton iz januarja 2010 o internetni svobodi. Clintonova je dejala, da ZDA "zavzemajo stališče o enotnem internetu, kjer ima celotno človeštvo enakovreden dostop do znanja in idej" (Clinton 2010). Za dosego tega cilja je potrebno izboljševati svobodo izražanja in veroizpovedi. Politična agenda glede "svobodnega interneta" je dobila zalet z vzponom zavedajoče uporabnosti interneta med demokratičnimi vstajami v severni Afriki in na Bližnjem Vzhodu v prvi polovici leta 2011. Predsednikov urad je videl priložnost za uveljavitev ideologije glede možnosti, ki jih je tehnologija ustvarila za ljudi po svetu.

V mednarodni strategiji, ki zadeva kibernetski prostor, poskuša administracija predsednika Obame integrirati gospodarske, varnostne in politične dele politike ZDA v vseobsežen, povezan strateški pristop. Ta pristop poskuša izboljšati družbene, gospodarske in politične prednosti, ki jih omrežni svet ustvarja za posameznike, skupnosti in narode, medtem ko se hkrati odziva na grožnje, ki zmanjšujejo vrednost interneta za komunikacijo, trgovino in mednarodno sodelovanje. Pri tem naj bi ZDA sledile osrednjim zavezam za ohranitev temeljnih svoboščin, zasebnosti in prostega pretoka informacij. Mednarodna strategija prepoznava starodavne napetosti med varnostjo in svobodo in se zavzema za večjo kibernetsko varnost ter razširjene internetne svoboščine. Zagovarja, da uporabljen pristop preko vladavine zakona hkrati podpira nacionalno varnost in razširja skupne vrednote.

Mednarodna strategija poskuša zagotoviti, da bodo kibernetske tehnologije odprte, interoprabilne, zaščitene, zanesljive in trdne. Zasledovanje teh ciljev na globalni ravni od ZDA zahteva prizadevanja na področju diplomacije, obrambe in pri razvojnih politikah.

Mednarodna strategija predstavlja načrt, ki vladnim organom ZDA omogoča boljše opredelitve in koordiniranje njihove vloge pri "izvrševanju nadaljnjih aktivnosti in načrtovanju implementacije teh aktivnosti v prihodnosti." Za podporo tem aktivnostim strategija deli vladna prizadevanja ZDA na sedem medsebojno odvisnih področij aktivnosti, pri čemer zahteva, da vsako področje sodeluje z vlado, mednarodnimi partnerji in zasebnim sektorjem (The White House 2011).

Motiv, ki se ponavlja skozi celotno mednarodno strategijo, je potreba po *vladavini zakona* na področju kibernetskega upravljanja tako doma kot po svetu. *Vladavino zakona* definira kot družbeni red, kjer spoštovanje zakonov ščiti ljudi in interese, prinaša stabilnost globalnim trgom in zlonamerne akterje mednarodno preganja. Glede na izzive kibernetskega prostora spoštovanje zakona zahteva vzpostavitev okolja oz. pravil obnašanja, ki gradijo na soglasju o sprejemljivem obnašanju in partnerstvih med tistimi, ki razumejo delovanje kibernetskega sistema kot ključni element za nacionalne in skupne interese.

Mednarodno pravo in zakonski procesi igrajo ključno vlogo pri viziji blaginje, varnosti in odprtosti omreženega sveta. Na področju materialnega prava mednarodna strategija jasno določa, da številna načela mednarodnega prava, ki veljajo v času miru in vojne, veljajo tudi v kibernetskem prostoru. Ta obstoječa mednarodna zakonska pravila vključujejo spoštovanje temeljnih državljanskih in političnih pravic glede svobode izražanja in združevanja, zasebnosti, lastnine, odgovornosti države, da odreče zatočišče kriminalcem ter pravico do uporabe sile pri obrambi oz. skupni samoobrambi v primeru oboroženih napadov.

Mednarodna strategija hkrati prepoznava edinstvene značilnosti omrežne tehnologije, ki zahtevajo večjo jasnost glede delovanja obstoječih zakonskih pravil v kibernetskem prostoru in v določenih primerih nova pravila. Ta nastajajoča pravila, ki so specifična za kibernetski prostor, zahtevajo razvoj in implementacijo na področjih globalne interoperabilnosti, omrežne stabilnosti, zanesljivega dostopa, večstranskega upravljanja in stalnih nadzorov (The White house 2011).

Strategija je sestavljena iz treh delov. Prvi del, *Strateški pristop,* prepoznava prednosti, slabosti kibernetskega prostora in omenja temeljna načela, na katerih bo temeljilo delovanje ZDA:

- ZDA naj bi bile zavezane k ohranjanju in izboljševanju koristi digitalnih omrežij za družbo in gospodarstvo.

- ZDA se zavedajo, da rast teh omrežij prinaša nove izzive za njihovo nacionalno in

gospodarsko varnost in globalno skupnost.

- ZDA se bodo spopadle z izzivi tako, da bodo ohranjale svoja temeljna načela.

Politike ZDA izhajajo iz zaveze ohranjati tako najboljše, kar kibernetski prostor omogoča, kot tudi braniti svoja načela. Mednarodna politika glede kibernetskega prostora odseva njihovo osnovno zavezanost k *temeljnim svoboščinam, zasebnosti in prostemu pretoku informacij*.
Drugi del strategije, imenovan *Prihodnost,* definira cilje in načine, preko katerih bo ZDA poskušala doseči svoje interese.

Cilj:

ZDA bodo mednarodno delovale za spodbujanje *odprte, interoperabilne, zaščitene in zanesljive informacijske in komunikacijske infrastrukture*, ki bo podpirala mednarodno izmenjavo in trgovino, krepila mednarodno varnost in spodbujala svobodno izražanje in inovacije. Za dosego tega cilja bodo ZDA gradile in vzdrževale okolje, v katerem bodo standardi odgovornega obnašanja vodili dejanja držav, ohranjali partnerstva in podpirali vladavino zakona v kibernetskem prostoru (The White house 2011).

Vloga ZDA:

- Diplomacija: Krepitev partnerstev

Diplomatski cilj – ZDA si bodo prizadevale ustvarjati pobude in gradile konsenz glede mednarodnega okolja, pri katerem bodo države, prepoznavajoč pravo vrednost odprtega, interoperabilnega, varnega in zanesljivega kibernetskega prostora, delovale skupaj in kot odgovorni deležniki.

- Obramba: Odvračanje in zastraševanje

Obrambni cilj – ZDA bodo skupaj z ostalimi narodi spodbujale odgovorno vedenje in se postavile v bran tistim, ki bi želeli onesposobiti omrežja in sisteme, odvračale in zastraševale zlonamerne akterje in si pridržale pravico do obrambe teh vitalnih nacionalnih virov kot nujno in primerno.

- Razvoj: Izgradnja blagostanja in varnosti

Razvojni cilj – ZDA bodo pospešile izgradnjo kapacitet kibernetske varnosti v tujini, bilateralno in preko multilateralnih organizacij tako, da bo imela vsaka država sredstva za zaščito lastne digitalne infrastrukture, da bodo krepile globalna omrežja in gradile bližnja partnerstva tekom konsenza za odprta, interoperabilna, varna in zanesljiva omrežja (The White house 2011).

Tretji del, imenovan *Politične prioritete,* predstavlja osrednji del strategije, saj opredeljuje področja in aktivnosti vlade ZDA za dosego teh ciljev.

Da bi dosegli prihodnost, v kateri kibernetski prostor izkorišča svoj potencial za vse, je vlada ZDA organizirala svoje aktivnosti preko sedmih medsebojno odvisnih področij, ki vsako posebej zahtevajo sodelovanje z vlado, mednarodnimi partnerji in zasebnim sektorjem. Obravnavane kot celota, tvorijo osnove našega strateškega okvirja.

Gospodarstvo: Pospeševanje mednarodnih standardov in inovativnih odprtih tržišč

- Vzdrževanje okolja proste trgovine, ki spodbuja tehnološke inovacije na dostopnih, globalno povezanih omrežjih.
- Zaščita intelektualne lastnine, vključno s poslovnimi skrivnostmi, pred krajo.
- Zagotavljanje prevlade interoperabilnih in varnih tehničnih standardov, ki jih določajo tehnični strokovnjaki (The White house 2011).

Zaščita omrežij: Izboljševanje varnosti, zanesljivosti in odpornosti

- Pospeševanje sodelovanja v zvezi s kibernetskim prostorom, predvsem glede standardov obnašanja za države in kibernetske varnosti, bilateralno in s številnimi multilateralnimi organizacijami in večnacionalnimi partnerstvi.
- Zmanjševanje prekinitev in vdorov v omrežja ZDA.
- Zagotovitev robustnih zmogljivosti za obvladovanje incidentov, odpornosti in sposobnosti obnovitve informacijske infrastrukture.
- Izboljšanje varnosti visokotehnološke oskrbovalne verige, v dogovoru z industrijo

(The White house 2011).

Organi pregona: Razširitev sodelovanja in vladavina zakona

- Polno sodelovanje pri razvoju mednarodnih politik glede kibernetskega kriminala.
- Mednarodna uskladitev zakonov glede kibernetskega kriminala z razširitvijo pristopanja k budimpeštanski konvenciji.
- Pri zakonih o kibernetskem kriminalu se je potrebno osredotočiti na boj proti nezakonitim aktivnostim in ne omejevanju dostopa do interneta.
- Teroristom in drugim kriminalnim skupinam onemogočati zmožnost izrabe interneta za operativno planiranje, financiranje in napade (The White house 2011).

Vojska: Priprava na varnostne izzive 21. stoletja

- Prepoznati in se prilagoditi na povečano potrebo vojske po zanesljivih in varnih omrežjih.
- Graditi in izboljševati obstoječa vojaška zavezništva za soočanje s potencialnimi grožnjami v kibernetskem prostoru.
- Razširiti sodelovanje glede kibernetskega prostora z zavezniki in partnerji za povečanje kolektivne varnosti (The White house 2011).

Internetno upravljanje: Zavzemanje za učinkovite in vključujoče strukture

- Priotizacija odprtosti in inovativnosti na internetu.
- Ohranitev varnosti in stabilnosti globalnih omrežij, vključno s sistemom domenskih imen.
- Spodbujanje in povečevanje prizorišč za diskusijo o problemih upravljanja interneta za zainteresirane skupine (The White house 2011).

Mednarodni razvoj: Izgradnja kapacitet, varnosti in blaginje

- Zagotavljanje potrebnega znanja, usposabljanj in drugih sredstev za države, ki želijo zgraditi tehnične zmogljivosti in zmogljivosti glede kibernetske varnosti.

- Nenehno razvijati in stalno deliti mednarodne dobre prakse glede kibernetske varnosti.
- Povečati sposobnost držav za boj proti kibernetskemu kriminalu – vključno z usposabljanjem organov pregona, forenzičnih specialistov, sodnikov in zakonodajalcev.
- Razvijanje odnosov z oblikovalci politik za izboljšanje izgradnje tehničnih kapacitet, omogočanje rednega in trajajočega stika s strokovnjaki in njihovimi sogovorniki znotraj vlade ZDA (The White house 2011).

Internetna svoboda: Podpora temeljnim svoboščinam in zasebnosti

- Podpora akterjem civilne družbe pri doseganju zanesljivih, varnih in zaščitenih platform za svobodno izražanje in zbiranje.
- Sodelovanje s civilno družbo in nevladnimi organizacijami pri ustanavljanju varovalnih mehanizmov, ki bodo zaščitile njihovo internetno delovanje pred nezakonitimi digitalnimi vdori.
- Spodbujanje mednarodnega sodelovanja na področju učinkovite zaščite zasebnosti komercialnih podatkov.
- Zagotavljanje neprekinjene interoperabilnosti interneta, ki bo dostopna vsem (The White house 2011).

7.4 Okvir za izboljšanje kibernetske varnosti kritične infrastrukture – 2014

NIST je 12. februarja 2014 izdal prvotno verzijo Okvirja za izboljšanje kibernetske varnosti kritične infrastrukture. Okvir lastnikom kritične infrastrukture in ostalim zainteresiranim omogoča usmeritve glede najboljšega načina zaščite informacij in sredstev pred kibernetskimi napadi.

Okvir je nastal kot posledica predsedniške odredbe 13636 iz 12. februarja 2013, imenovane "Izboljševanje kibernetske varnosti kritične infrastrukture", kjer je zapisano "da je politika ZDA izboljšanje varnosti in odpornosti nacionalne kritične infrastrukture in ohranjanje kibernetskega okolja, ki spodbuja učinkovitost, inovativnost in gospodarsko blaginjo, medtem ko istočasno povečuje varnost, zaščitenost, poslovno zaupnost, zasebnost in civilne svoboščine." V odredbi je predsednik pozval NIST k razvoju "nabora standardov,

metodologije, postopkov in procesov, ki bodo uskladili politične, poslovne in tehnološke pristope za odzivanje na kibernetska tveganja." (The White House 2013) Ministrstvo za domovinsko varnost je identificiralo 16 različnih industrijskih področij kot del kritične infrastrukture, vključno z obrambo, komunikacijami, hrano in kmetijstvom, zdravstveno oskrbo in seveda informacijsko tehnologijo. Nastali okvir, ki je ustvarjen s sodelovanjem vlade in zasebnega sektorja, uporablja skupni jezik pri obravnavanju in upravljanju tveganj glede kibernetske varnosti na stroškovno učinkovit način, upoštevajoč potrebe podjetij, brez da bi postavljal dodatne zakonske zahteve za podjetja. Okvir se osredotoča na uporabo podjetniških dejavnikov pri upravljanju aktivnosti kibernetske varnosti in upoštevanju tveganj glede kibernetske varnosti kot del organizacijskih procesov upravljanja s tveganji. Okvir je razdeljen na tri dele: jedro okvirja, profil okvirja in stopnje uresničevanja okvirja (National Institute of Standards and Technology 2014).

Jedro se v nadaljevanju deli na pet dejavnosti: identifikacija, zaščita, zaznavanje, odzivanje in povrnitev. Gre za dejavnosti v zvezi s kibernetsko varnostjo, rezultate in informativna priporočila, ki veljajo za vsa področja kritične infrastrukture in omogočajo podrobnejše usmerjanje razvoja individualnega organizacijskega profila. Uporabljene skupaj, so te dejavnosti ustvarjene za pomoč organizacijam pri razumevanju in oblikovanju njihovega programa kibernetske zaščite v funkcionalnejši in učinkovitejši sistem.
Profil okvirja je namenjen uskladitvi dejavnosti organizacij v zvezi s kibernetsko varnostjo z njihovimi poslovnimi zahtevami, dovoljenimi tveganji in sredstvi. Na ta način lahko organizacije dosežejo višjo stopnjo sofisticiranosti glede kibernetske varnosti.
Stopnje uresničevanja omogočajo mehanizem, s katerim organizacije vidijo in razumejo značilnosti njihovega pristopa pri upravljanju s tveganji v zvezi s kibernetsko varnostjo. Organizacijam omogočajo analizirati raven, do katere njihov sistem upošteva cilje, ki so določeni v okvirju.
S pomočjo teh standardov, priporočil in praks okvir omogoča skupno sistematizacijo in mehanizme organizacije pri:

- opisu trenutnega odnosa do kibernetske varnosti,
- opisu želenega stanja glede kibernetske varnosti,
- identifikaciji in priotizaciji priložnosti za izboljšanje v kontekstu stalnega in ponovljivega postopka,

- oceni napredka glede želenega stanja,

komunikaciji med notranjimi in zunanjimi udeleženci glede kibervarnostnih tveganj (National Institute of Standards and Technology 2014).

Okvir omogoča organizacijam – ne glede na velikost, stopnjo tveganj v zvezi s kibernetsko varnostjo oz. kompleksnosti – da vpelje načela in dobre prakse upravljanja s tveganji v izboljšanje varnosti in odpornosti kritične infrastrukture. Okvir omogoča organiziranje in strukturiranje zdajšnjih številnih pristopov k kibernetski varnosti z zbiranjem standardov, smernic in praks, ki danes učinkovito delujejo v industriji. Še več, ker se navezuje na globalno prepoznane standarde kibernetske varnosti, se lahko okvir uporablja tudi v organizacijah, lociranih izven ZDA, in služi kot model za mednarodno sodelovanje pri krepitvi kibernetske varnosti kritične infrastrukture.
Okvir ne predstavlja univerzalnega pristopa pri upravljanju s tveganji glede kibernetske varnosti kritične infrastrukture. Organizacije bodo še naprej soočene z unikatnimi tveganji – različnimi grožnjami, različnimi ranljivostmi, različnimi mejami tveganja − in načini, kako se bodo implementirale prakse v okvir, se bodo razlikovali. Organizacije lahko določijo aktivnosti, ki so pomembne za zagotavljanje nujne storitve in določijo prednostne investicije za maksimizacijo porabljenih sredstev. Konec koncev je namen okvirja zmanjšanje in boljše upravljanje s tveganji v zvezi s kibernetsko varnostjo. Okvir je živ dokument in bo še naprej posodobljen in izboljšan, ko industrija zagotovi povratne informacije glede na izvajanje. Ko bo okvir udejanjen, bodo izkušnje integrirane v prihodnje verzije. To bo zagotovilo izpolnjevanje zahtev lastnikov in uporabnikov kritične infrastrukture znotraj dinamičnega in zahtevnega okolja novih groženj, tveganj in rešitev. Uporaba tega prostovoljnega okvirja je nadaljnji korak pri izboljševanju kibernetske varnosti kritične infrastrukture ZDA – zagotavljanje smernic za individualne organizacije, hkrati z izboljševanjem kibervarnostnega položaja nacionalne kritične infrastrukture kot celote.

7.5 Kibernetska strategija Ministrstva za obrambo ZDA – 2015

V aprilu 2015 je Ministrstvo za obrambo ZDA izdalo novo kibernetsko strategijo, da bi "usmerjali razvoj kibernetskih sil DOD in okrepili kibernetsko obrambo ter stališče glede kibernetskega odvračanja." Osredotoča se na izgradnjo kibernetskih zmogljivosti in organizacijo DOD zaradi treh primarnih nalog:

(1) obrambe svojih lastnih omrežij, sistemov in podatkov; (2) obrambe nacionalnih interesov ZDA pred kibernetskimi napadi s "hujšimi posledicami", vključno z izgubo življenj, hujšo škodo na lastnini, resnimi sovražnimi zunanjepolitičnimi posledicami in resnimi gospodarskimi posledicami, ter (3) po ukazu predsednika ali obrambnega sekretarja, zagotovitev podpore vojaškim operacijam in kriznim načrtom, vključno z onesposobitvijo sovražnikovih vojaških omrežij.

Strategija v nadaljevanju določa pet strateških ciljev, ki naj bi jih ministrstvo doseglo v naslednjih petih letih in so namenjeni zagotavljanju izvajanja treh osnovnih nalog. Te cilji zajemajo:

- Izgradnja in ohranjanje obstoječih sil in zmogljivosti za izvajanje operacij v kibernetskem prostoru.
- Obramba informacijskega omrežja DOD, zaščita podatkov DOD in zmanjšanje nevarnosti za operacije DOD.
- Pripravljenost za obrambo ozemlja in vitalnih interesov ZDA pred motečimi oz. uničujočimi kibernetskimi napadi s hujšimi posledicami.
- Izgradnja in ohranjanje mogočih kibernetskih možnosti in načrtovanje uporabe teh možnosti za nadziranje stopnjevanja spopadov in oblikovanje okolja spopada v vseh fazah.
- Izgradnja in ohranjanje močnih mednarodnih zavezništev in partnerstev za odvračanje skupnih groženj in povečevanje mednarodne varnosti in stabilnosti (Department of Defense 2015).

Izgradnja in vzdrževanje kvalificirane delovne sile podpira vse ostale cilje znotraj strategije. Kibernetsko poveljstvo ZDA poroča, da je močno obremenjeno z identifikacijo, usposabljanjem in zadržanjem kvalificiranega osebja. Pojavljajo se namreč problemi nižje stopnje izobraženosti, višine plač v primerjavi z ostalimi zasebnimi sektorji. Za učinkovito delovanje v kibernetskem prostoru Ministrstvo za obrambo potrebuje sile in osebje, ki bodo usposobljeni po najvišjih standardih, pripravljeni in opremljeni z najboljšimi tehničnimi zmogljivostmi. V letu 2012 je ministrstvo začelo z izgradnjo Sil za izvajanje kibernetskih

nalog ministrstva (*Cyber Mission Force*). Popolnoma operativne bodo sile vključevale skoraj 6200 pripadnikov vojaškega, civilnega in pogodbenega podpornega osebja iz vseh vojaških oddelkov in obrambnih organov v sestavi. CMF predstavljajo velikansko investicijo za ministrstvo in ZDA kot celoto in osrednji cilj te strategije je določitev specifičnih ciljev, ki bodo vodili razvoj CMF in ostalega osebja ministrstva za podporo kibernetskim nalogam za zaščito in obrambo nacionalnih interesov ZDA (Department of Defense 2015).

CMF bodo obsegale izvajalce kibernetskih aktivnosti, organizirane v 133 ekip, razvrščene sledeče: (1) sile za kibernetsko zaščito bodo izboljševale tradicionalne obrambne ukrepe in branile prioritetna omrežja in sisteme ministrstva pred prioritetnimi nevarnostmi; (2) sile za nacionalne misije in z njimi povezane podporne ekipe bodo branile ZDA in njihove interese pred kibernetskimi napadi s hujšimi posledicami; (3) sile za bojne misije in z njimi povezane podporne ekipe bodo podpirale bojna poveljstva z generiranjem integriranih učinkov v kibernetskem prostoru v podporo kriznim operacijam in načrtom.

Bojna poveljstva integrirajo sile za bojne misije in sile za kibernetsko zaščito v načrte in operacije in jih uporabljajo v kibernetskem prostoru, medtem ko sile za nacionalne misije delujejo pod Kibernetskim poveljstvom ZDA. Zunaj tega sestava so lahko ekipe uporabljene tudi v podporo ostalim misijam, kot zahteva ministrstvo.

V 2013 je ministrstvo začelo z integracijo CMF v širše večnamenske vojaške sile ZDA za dosego sinergije znotraj področij, zagotovitev pripravljenosti sil znotraj enote in prestrukturiranje vojaške in civilne delovne sile in infrastrukture za izvajanje nalog ministrstva. V obdobju implementacije te strategije bo ministrstvo nadaljevalo z izgradnjo CMF in z izboljševanjem potrebnega poveljevanja, nadzora in usposabljanjem organizacij, potrebnih za učinkovito delovanje. Ministrstvo se bo osredotočalo na zagotavljanje, da bodo njegove sile usposobljene in pripravljene na delovanje, uporabljajoč zmogljivosti in arhitekturo, ki jo potrebujejo za izvajanje kibernetskih operacij, še naprej bo gradilo politične in zakonske okvirje za vodenje CMF in skrbelo za integracijo CMF v vsesplošno načrtovanje in razvoj sil. (Department of Defense 2015).

Strategija prepoznava, da bo učinkovita kibernetska zaščita zahtevala tesno sodelovanje znotraj ministrstva in v zvezni vladi, z industrijo, mednarodnimi zavezniki in partnerji, z državnimi in lokalnimi oblastmi. Zagotavljanje varnosti v kibernetskem prostoru zahteva celostni vladni in mednarodni pristop zaradi številnosti in raznolikosti interesnih skupin v

prostoru, pretoka informacij preko mednarodnih meja in porazdelitvi zadolžitev, pooblastil in zmogljivosti znotraj vlad in zasebnega sektorja. Za vsako od misij mora ministrstvo še naprej razvijati običajne postopke in procese za koordiniranje svojih kibernetskih operacij (Department of Defense 2015).

8 ORGANIZIRANOST MINISTRSTEV PRISTOJNIH ZA KIBERNETSKI PROSTOR IN POMEMBNEJŠI STRATEŠKI UKREPI

ZDA imajo zaradi številnih zveznih vladnih akterjev na področju kibernetskega prostora določene koristi, po drugi strani pa ta številnost predstavlja izzive. Prednost velikega števila akterjev je hkratni odziv različnih agencij, kar predstavlja agilnost in izboljšano obrambno zmogljivost. Obenem pa takšen pristop povzroča veliko večje stroške in lahko vodi k zmedi glede odgovornosti in povečani stopnji tekmovalnosti za omejena proračunska sredstva in izkušeno delovno silo. Številčnost zveznih vladnih akterjev ni posledica načrtovanja, ampak je večina organizacij nastala kot posledica pobud znotraj mnogih oddelkov, ki so se poskušali odzvati na nastajajoče, slabo opredeljeno področje kibernetskih groženj. Dopisi, politične izjave in strategije izvršilnih oblasti prinašajo neke vrste organiziranost na področje ukrepov ministrstev in vladnih služb (Crowther in Ghori 2015).

Na ravni implementiranja nacionalnih politik in strategij so se razvile razlike med številnimi zveznimi agencijami, službami in ministrstvi, pristojnimi za zaščito in upravljanje s kibernetskim prostorom. Vsaka izmed institucij je pomembna, vendar opravljajo različne vloge v zvezi s kibernetskimi grožnjami. Ministrstva poleg predsednika predstavljajo najvišjo izvršilno raven. Na ravni ministrstev, pristojnih za zaščito kibernetskega prostora, so najpomembnejša Ministrstvo za domovinsko varnost *(Department of Homeland Security – DHS)*, Ministrstvo za pravosodje *(Department of Justice - DoJ)* in Ministrstvo za obrambo *(Department of Defense - DoD):*

8.1 Ministrstvo za domovinsko varnost

DHS predstavlja najpomembnejši vladni organ na področju zaščite kibernetske kritične infrastrukture. Koordinira namreč nacionalno zaščito, preprečevanje, zmanjševanje ter vrnitev

v prvotno stanje po kibernetskih incidentih; razširja analize domačih kibernetskih groženj in ranljivosti; ščiti kritično infrastrukturo, varuje zvezna civilna omrežja (domeno .gov); in preiskuje kibernetska kriminalna dejanja, ki so v njegovi pristojnosti. Vizija DHS je zagotavljanje varnosti, zaščitenosti in odpornosti domovine pred terorizmom in drugimi nevarnostmi. Ena izmed petih glavnih misij DHS je zaščita in obramba kibernetskega prostora, ki vsebuje sledeče komponente:

1. Krepitev varnosti in odpornosti kritične infrastrukture.
2. Zaščita zveznih civilnih vladnih informacijskih tehnoloških podjetij.
3. Izboljšanje uveljavljanja zakonodaje, odzivanja na incidente in poročanja o kibernetskih zmogljivostih.
4. Krepitev (kibernetskega) ekosistema (Department of Homeland Security).

Osrednja enota DHS, ki se ukvarja z kibernetskimi grožnjami, je Direktorat za nacionalno zaščito in programe (*National Protection and Programs Directorate - NPPD*), katerega glavni cilj je zmanjšanje tveganj za grožnje domovini in nastanek odpornejše in varnejše fizične in digitalne infrastrukture vlade ZDA. Najpomembnejši trije uradi znotraj NPPD, ki se ukvarjajo s kibernetsko varnostjo, so Urad za kibernetsko varnost in komunikacije *(Office of Cybersecurity and Communication)*, Urad za zaščito infrastrukture *(Office of Infrastructure Protection)* in Urad za kibernetsko in infrastrukturno analizo *(Office of Cyber and Infrastructure Analysis)*. Izven direktorata NPPD se kibernetske varnostne dejavnosti ministrstva odvijajo tudi znotraj Tajne službe ZDA *(U.S. Secret Service)* in Službe za imigracije in uveljavitev carin ZDA *(U.S. Immigrations and Custom Enforcement)* (Department of Homeland Security).

- Urad za kibernetsko varnost in komunikacije

Naloga Urada za kibernetsko varnost in komunikacije je preprečevanje in minimizacija prekinitev omrežij kritične infrastrukture za zaščito javnih, gospodarskih in vladnih storitev. Vodi tudi prizadevanja varovanje zvezne domene civilnih vladnih omrežij (.gov) in sodeluje z zasebnim sektorjem za povečevanje varnosti kritičnih omrežij. Urad izvaja svoje naloge preko svojih petih oddelkov: Urada za nujne komunikacije (*The Office of Emergency Communications)*, Nacionalnega centra za kibernetsko varnost in integracijo komunikacij

(The National Cybersecurity and Communications Integration Center - NCCIC), Udeležbe zainteresiranih strani in odpornosti kibernetske infrastrukture *(Stakeholder Engagement and Cyber Infrastructure Resilience - SECIR)*, Odpornosti zveznih omrežij *(Federal Network Resilience)* in Razvrščanja omrežne zaščite *(Network Security Deployment)* (Department of Homeland Security).

Oddelek SECIR je primarna točka DHS za udeležbo in koordiniranje nacionalne varnosti/nujne pripravljenosti komunikacij in kibervarnostnih pobud tako za vlado kot industrijske partnerje ter je izvršni sekretariat za pisarno združenega programa komiteja za nacionalno varnost/nujno pripravljenost komunikacij. Od SECIR se pričakuje poročanje o usklajevanju in udeležbi zunanjih partnerjev, medtem ko izkorišča zmogljivosti in veliko strokovno znanje iz tega področja za reševanje zahtev zainteresiranih strani (Department of Homeland Security).

Oddelek NCCIC služi kot središčna točka za uskljajevanje izmenjave informacij glede kibernetske varnosti z zasebnim sektorjem, omogoča tehnično pomoč in analize na samem prizorišču, podporo žrtvam in zmanjševanju kibernetskih napadov, zmogljivost prepoznavanja situacije, ki vključuje integrirane, dejanske informacije o pojavljajočih se trendih, trenutnih grožnjah in statusu incidentov, ki bi lahko prizadeli kritično infrastrukturo in koordinira nacionalni odziv na večje kibernetske incidente, ki imajo vpliv na kritično infrastrukturo. Glede na okvir Nacionalnega načrta za zaščito infrastrukture aktivnosti NCCIC sovpadajo skupaj z medsebojno odvisnimi nalogami Nacionalnega koordinacijskega centra za telekomunikacije *(National Coordinating Center for Telecommunications)*, Računalniške skupine ZDA za nujno pripravljenost *(U.S. Computer Emergency Readiness Team - US-CERT)*, Urada DHS za obveščevalne informacije in analize *(DHS Office of Intelligence and Analysis)* in Nacionalnega centra za kibernetsko varnost *(National Cyber Security Center)*. NCCIC naloga je zmanjševanje možnosti in resnosti incidentov v zvezi z nacionalno kritično tehnologijo in komunikacijskimi omrežji ter izgradnja kibernetske zmogljivosti in odpornosti v drugih organizacijah, ki jo izvaja preko štirih podružnic: Operacije in integracija *(Operations and Integration)*, US-CERT, Skupina za nujen kibernetski odziv za industrijske nadzorne sisteme *(Industrial Control Systems Cyber Emergency Response Team - ICS-CERT)* in Nacionalni koordinacijski center za komunikacije *(National Coordination Center for Communications - NCC)* (Department of Homeland Security).

- US-CERT predstavlja edini element, ki je odgovoren za izboljšanje nacionalnega položaja glede kibernetske varnosti, koordinira izmenjavo kibernetskih informacij in proaktivno upravlja s kibernetskimi nevarnostmi za narod, medtem ko ščiti ustavne pravice Američanov. Dodatno US-CERT sodeluje z zveznimi agencijami, zasebnim sektorjem, raziskovalno skupnostjo, akademsko sfero, državnimi, lokalnimi in plemenskimi oblastmi ter mednarodnimi partnericami. Preko koordinacije s številnimi nacionalnimi centri za varnostne incidente se odziva na potencialne varnostne dogodke in grožnje tako zaupnih kot nezaupnih omrežij in tako javnosti razširja informacije glede kibernetske varnosti (Department of Homeland Security).

- ICS-CERT upravlja s centri za kibernetske varnostne operacije, ki se osredotočajo na analizo in odzivanje na incidente povezane z nadzornimi sistemi, izvaja analizo zlonamerne programske opreme, digitalnih medijev in kibernetskih pomankljivosti, omogoča storitve odzivanja na incidente na kraju samem, omogoča prepoznavanje situacije v obliki dejanskih obveščevalnih podatkov, koordinira odgovorno razkrivanje pomankljivosti in z njimi povezano zmanjševanje nevarnosti, razširja in usklajuje informacije o pomankljivostih in analizi groženj preko informacijskih produktov in opozoril (Department of Homeland Security).

- NCC stalno nadzoruje nacionalne in mednarodne incidente in dogodke, ki bi lahko vplivali na nujne komunikacije. NCC sodeluje tako z US-CERTom in ICS-CERTom pri nadziranju in reševanju problemov, ki vplivajo na komunikacije v nujnih primerih (Department of Homeland Security).

- Urad za zaščito infrastrukture

Urad za zaščito infrastrukture vodi koordinacijo nacionalnih prizadevanj za zmanjševanje tveganj za kritično infrastrukturo ZDA in pomaga pri odzivanju ter vračanju v prvotno stanje v primeru terorističnih napadov, naravnih katastrof in ostalih nujnih stanj. Urad izvaja ocenjevanja in zmanjšuje ranljivosti ter posledice, ki pomagajo lastnikom in upravljalcem kritične infrastrukture, kot tudi državnim, lokalnim, plemenskim in teritorialnim partnericam razumeti nevarnosti in se odzvati nanje. Urad pokriva šest področij kritične infrastrukture: kemikalije, komercialne ustanove, kritična proizvodnja, jezovi, urgentne storitve in jedrsko področje (Department of Homeland Security).

- Urad za kibernetsko in infrastrukturno analizo

Naloga urada za kibernetsko in infrastrukturno analizo je podpiranje prizadevanj za zaščito nacionalne kritične infrastrukture z omogočanjem analitične podpore vodstvu DHS, ostalim operativnim enotam in osebju na terenu, med državnimi operacijami in krizami pri pojavljajočih se grožnjah in incidentih, ocena in sporočanje nacionalnih strategij upravljanja s tveganji glede možnosti in posledic pojavljajočih se in prihodnjih nevarnosti, razvoj in izboljšanje zmogljivosti za podporo kriznih operacij z identifikacijo in priotizacijo infrastrukture preko uporabe analitičnih orodij in vzorčnih zmogljivosti (Department of Homeland Security).

- Preiskovalni oddelek domovinske varnosti

Preiskovalni oddelek domovinske varnosti *(Homeland Security Investigations - HSI)* upravlja s Centrom za kibernetski kriminal *(Cyber Crime Center - C3),* ki je odgovoren za omogočanje domačih in mednarodnih usposabljanj, usklajevanje, podporo in razreševanje kibernetskih preiskav povezanih s spletnim gospodarskim kriminalom, digitalnimi tatvinami nadziranih izvoznih podatkov, digitalnih tatvin intelektualne lastnine in spletnih preiskav izkoriščanja otrok. Najsodobnejši center zveznim, državnim, lokalnim in mednarodnim agencijam organov pregona ponuja usposabljanje in podporo pri preiskovanju kibernetskega kriminala. Najpomembnejši sektor v C3, ki se ukvarja s kibernetsko varnostjo, je Enota za kibernetska kriminalna dejanja *(Cyber Crimes Unit)*, ki omogoča vodenje in pregled nad kibernetskimi preiskavami ministrstva s poudarkom na transnacionalnih kriminalnih organizacijah, ki uporabljajo kibernetske zmogljivosti za povečevanje njihovih zmogljivosti. Enota omogoča usposabljanje, preiskovalno podporo in priporočila ostalim HSI oddelkom glede prihajajočih kibernetskih tehnologij kot tudi strokovno znanje iz področja kibernetskih preiskav povezanih s prevarami v zvezi s krajami identitete in ponarejanjem listin, pranjem denarja, finančnimi prevarami, komercialnimi prevarami, tihotapljenjem mamil in nelegalnimi izvozi (Department of Homeland Security).

- Tajna služba ZDA

Tajna služba vodi mrežo skupin za elektronski kriminal, ki povezuje zvezne, državne in

lokalne organe pregona, tožilce, zasebno industrijo in akademsko skupnost s skupnim ciljem preprečevanja, zaznavanja, zmanjševanja in preiskovanja številnih oblik zlonamerne kibernetske aktivnosti. Tajna služba vodi tudi Nacionalni inštitut za računalniško forenziko *(National Computer Forensics Institute)*, center usposabljanja, ki državnim in lokalnim organom pregona ter zakonodajnim in pravosodnim zaposlenim zagotavlja brezplačno, vseobsegajočo izobrazbo glede tekočih trendov kibernetskega kriminala, preiskovalnih metod in tožilskih in pravosodnih izzivov (US Secret Service).

8.1.1 Izvedeni ukrepi DHS

- DHS zbira javne predloge in pripombe ter organizira delavnice za informiranje o razvoju standardov, za potrebe razvoja Organizacij za izmenjavo podatkov in analize ***(****Information Sharing and Analysis Organizations – ISAOs),* za katere je predsednik izdal odredbo o nastanku in naj bi služile kot vozlišča za izmenjavo kritičnih informacij glede kibernetske varnosti in izboljševanju sodelovanja pri analizi teh informacij znotraj posameznih industrijskih sektorjev in med sektorji samimi. DHS z zasebnim sektorjem in vlado razvija sistem za avtomatsko izmenjavo kazalnikov kibernetske ogroženosti. Razvoj sistema vključuje zaščito zasebnosti in civilnih svoboščin. V začetku je bil sistem namenjen zgolj pošiljanju kazalnikov ogroženosti, od jeseni leta 2015 pa tudi sprejema informacije. Zainteresirana podjetja lahko pri pripravi njihovih omrežij za avtomatizirano izmenjavo indikatorjev kibernetske ogrnoženosti sodelujejo z oddelkom NCCIC. Preko programa sodelovanja in izmenjave kibernetskih informacij *(Cyber Information Sharing and Collaboration Program)* je DHS zgradil zaupanja vredno okolje za izmenjavo informacij o kibernetskih grožnjah z zasebnim sektorjem, ki poteka s pomočjo formaliziranih dogovorov o sodelovanju pri raziskavah in razvoju *(Cooperative Research and Development Agreements)*. Od julija 2015 je v veljavi že 125 dogovorov in DHS je od nastanka programa s podpisnicami dogovora izmenjal že več kot 28.000 kazalnikov ogroženosti. Še dodatnih 156 dogovorov je trenutno v fazi pogajanj, kar bo povečalo komunikacijski doseg DHS.
- Junija 2015 je Zvezni informacijski direktor *(Federal Chief Information Officer)* pričel z akcijo tridesetdnevnega kibervarnostnega sprinta *(Cybersecurity sprint)*, da bi pospešil napredek pri povečevanju zvezne vladne kibernetske varnosti. Preliminarna

poročila sprinta kažejo velikanski napredek v prizadevanjih zveznih agencij da zaščitijo informacije in sredstva ter izboljšajo odpornost zveznih omrežij. Za potrebe akcije je DHS pregledal več kot 40.000 sistemov glede kritičnih ranljivosti, ki jih zvezne agencije že popravljajo.

- DHS pospešuje uvedbo 2. stopnje Programa za stalno diagnostiko in zmanjševanje tveganj *(Continuous Diagnostics and Mitigation program - CDM),* da bi boljše zaščitili uporabnike vladnih računalnikov. Ta stopnja CDM bo zveznim agencijam omogočila orodja za nadziranje aktivnosti njihovih uporabnikov, identificirala ali imajo uporabniki zadostne privilegije in zaznavala nepooblaščene dostope do občutljivih informacij v skoraj realnem času. Do konca leta 2016 bodo tudi vsi zvezni civilni organi implementirali 1. stopnjo CDM, ki prepoznava ranljivosti v računalnikih in programski opremi in jim določa pomembnost, tako da organom omogoča prednostno odpravo hujših ranljivosti.
- DHS preko organov zveznih civilnih oblasti pospešeno uvaja EINSTEIN 3A sistem za preprečevanje vdorov. EINSTEIN 3A zaznava in blokira vse znane kibervarnostne grožnje, tudi zaupne narave, preden lahko vplivajo na zvezne civilne agencije. Sistem je v letu 2015 pokrival 15 zveznih ministrstev in agencij, do konca leta 2016 pa bodo zaščiteni vsi zvezni vladni organi. Del EINSTEINA bo tudi poskusni analitični sistem vrednotenja, ki bo kazalnike rangiral glede na resnost in identificiral nove potencialne grožnje.
- DHS poskuša v sodelovanju s kongresom še nadaljnje okrepiti prizadevanja za zaščito kritične infrastrukture na način, da bi direktorat NPPD preobrazili v novo operativno enoto imenovano Kibernetska in infrastrukturna zaščita *(Cyber and Infrastructure Protection)*, kar bi vključevalo povečanje oddelka NCCIC na raven vodenja s strani pomočnika sekretarja in večjo uporabo terenskih sil, da bi podjetjem pomagali izboljšati sposobnost upravljanja kibernetskih nevarnosti.
- DHS je pristojen za izvajanje največje nacionalne kibernetske vaje simulacije napada Kibernetska nevihta *(Cyberstorm)*, ki se na vsaki dve leti odvija že od leta 2006 (The White House 2015).

8.2 Ministrstvo za pravosodje

DoJ je najpomembnejši vladni organ na področju preiskovanja, preprečevanja in kazenskega pregona kibernetskega kriminala. Poleg tega ima vodilno vlogo pri domačih operacijah nacionalne varnosti, saj izvaja zbiranje, analizo in razširanje domačih obveščevalnih podatkov o kibernetskih grožnjah, podpira nacionalno zaščito, preprečevanje, zmanjševanje in povrnitev od kibernetskih incidentov in koordinira preiskave glede kibernetskih groženj. Ministrstvo razvija svojo kibernetsko strategijo 2014-2018, ki bo vključevala prednostne naloge in programe, ki upoštevajo prioritetne cilje, kot jih je določil predsednik. Najpomembnejši cilj DoJ naj bi predstavljalo »preprečevanje terorizma in izboljšanje nacionalne varnosti v skladu z vladavino zakona«, kamor spadajo tudi prizadevanja za kibernetsko varnost. Proti kibernetskim grožnjam in napadom se nameravajo boriti z uporabo vseh razpoložljivih orodij, preko močnih javno-zasebnih partnerstev in preiskovanjem ter kazenskim pregonom akterjev kibernetskih groženj. Kibernetska strategija vključuje celostni pristop, vključno s preiskavami in kazenskim pregonom, s poudarkom na preprečevanju groženj (US Department of Justice).

- Zvezni preiskovalni urad

Zvezni preiskovalni urad (*Federal Bureau of Investigation – FBI)* vodi nacionalna prizadevanja za preiskovanje visokotehnoloških kriminalnih dejanj, vključno z kibernetskim terorizmom, vohunstvom, računalniškimi vdori in večjimi kibernetskimi prevarami z zbiranjem in deljenjem informacij in obveščevalnih podatkov z javnimi in zasebnimi partnerji po celem svetu. Znotraj urada obstaja Kibernetski oddelek *(Cyber Division)*, ki združuje številne kibernetske pobude in naloge FBI in je poenotil Sile za izvajanje kibernetskih nalog *(Cyber Task Forces)* iz vseh 56 terenskih pisarn, da se osredotočajo zgolj na grožnje kibernetske varnosti in usklajujejo domače preiskave lokalnih skupnosti glede kibernetskih groženj (Federal Bureau of Investigation).

Skupina za kibernetske akcije *(Cyber Action Team - CAT)* je preiskovalna skupina kibernetske divizije FBI za hitro posredovanje, ki je lahko na prizorišču zločina v 48 urah. Naloga CAT je zmožnost globalne namestitve glede na ukaz divizije, da v primerih in nujnih stanjih, ki se zdijo kritična in pomembna, omogoča poglobljeno strokovno znanje glede kibernetskih vdorov in specializiranih preiskovalnih veščin. Po namestitvi so cilji CAT omogočanje

podpore lokalnim terenskim uradom, z namenom hitrega in učinkovitega reševanja preiskave in omogočanja podrobne analize vdora z uporabo različnih FBI preiskovalnih tehnik (Federal Bureau of Investigation).

Nacionalne združene sile za izvajanje preiskovalnih nalog *(National Cyber Investigative Joint Task Force - NCIJTF)* predstavljajo osrednjo točko za usklajevanje, integracijo in izmenjavo informacij povezanih z domačimi preiskavami kibernetskih groženj za vse organe vlade. FBI predstavlja izvršilno enoto NCIJTF pri kateri sodeluje skupaj z NSA, CIA, tajno službo, DHS in USCYBERCOM. Področja nalog NCIJTF obsegajo koordinacijo vsevladnih kampanj proti znanim kiber grožnjam, izrabljanje dragocenih kiber podatkov, analizo in poročanje o teh podatkih, uporabo tradicionalnih finančnih preiskovalnih pristopov na kibernetskem področju in redni nadzor upravljanja kibernetskih incidentov. Ker imajo članice združenih sil mnogo različnih državnih, zveznih in mednarodnih pooblastil, je sodelovanje NCIJTF ključnega pomena za zagotovitev uporabe vseh možnih legalnih sredstev in virov za sledenje, pripisovanje in ukrepanje proti kibernetskim grožnjam, s čimer je povečana možnost za zaprtje menarodnih kibernetskih kiminalcev in njihova odstranitev iz globalnih omrežij (Federal Bureau of Investigation).

Druge oblike kibernetskega sodelovanja, ki jih spodbuja FBI, so:

- Infragard *(InfraGard)*; združenje predstavnikov podjetij, akademskih institucij, državnih in lokalnih organov pregona in ostalih udeležencev zainteresiranih za izmenjavo informacij in obveščevalnih podatkov za preprečevanje sovražnih dejanj proti Združenim državam. To lahko storijo preko portala *iGuardian*, ki predstavlja platformo, ki je bila razvita z namenom poročanja o potencialnih grožnjah povezanih s terorizmom in sumljivih aktivnostih in je dostopno za uporabnike omrežja InfraGuard.

- Nacionalno zavezništvo za kiberetsko forenziko in usposabljanje *(The National Cyber-Forensics and Training Alliance)*, ki je postalo mednarodni model združenja organov pregona, zasebne industrije in akademske sfere za izmenjavo informacij glede preprečevanja pojavljajočih se kibernetskih groženj in zmanjševanja že obstoječih groženj.

- Delovna skupina strateškega zavezništva za kibernetski kriminal *(The Strategic Alliance Cyber Crime Working Group)*, ki je nastala v 2006, in je sestavljena iz kibernetskih enot organov pregona iz Avstralije, Kanade, Nove Zelandije, Velike Britanije in ZDA (Federal Bureau of Investigation).

  - Oddelek za nacionalno varnost

Oddelek za nacionalno varnost *(National Security Division)* Ministrstva za pravosodje se spopada z kibernetskimi grožnjami nacionalni varnosti. Ustanovila je omrežje Kibernetskih strokovnjakov za nacionalno varnost *(National Security Cyber Specialist network)*, ki je novo orodje vladnih kibernetskih sredstev in predstavlja ključni del prizadevanj ministrstva za boljše odzivanje na kibernetske vdore in napade, ki jih izvajajo nacionalne države in teroristične organizacije (United States Department of Justice).

  - Oddelek za kriminalna dejanja

Oddelek za kriminalna dejanja *(Criminal Division)* ministrstva za pravosodje vsebuje Sekcijo za računalniški kriminal in intelektualno lastnino *(Computer Crime and Intellectual Property Section - CCIPS)*, ki implementira nacionalne strategije ministrstva za pravosodje v svetovnem boju proti računalniškemu kriminalu in kriminalnim dejanjem v zvezi z intelektualno lastnino. CCIPS preprečuje, preiskuje in kazensko preganja računalniški kriminal s sodelovanjem z ostalimi vladnimi agencijami, zasebnim sektorjem, akademskimi institucijami in tujimi partnerji. Pri zasledovanju vseh teh ciljev odvetniki sekcije redno izvajajo kompleksne preiskave, razrešujejo edinstvene zakonodajne in preiskovalne probleme, ki jih povzročajo nastajajoče računalniške in telekomunikacijske tehnologije, opravljajo sodni pregon, usposabljajo zvezno, državno in lokalno osebje organov pregona in omogočajo podporo ostalim državnim tožilcem, komentirajo in predlagajo zakonodajo, spodbujajo in sodelujejo pri mednarodnih prizadevanjih za boj proti računalniškemu kriminalu in kriminalnim dejanjem v zvezi z intelektualno lastnino (United States Department of Justice).

  - Urad tožilcev ZDA

Urad tožilcev ZDA *(The Offices of the U.S. Attorneys)* je zadnji pomembnejši del

pravosodnega ministrstva, ki se ukvarja z kibernetskimi zadevami. Enega izmed njihovih desetih prednostnih področij delovanja predstavlja kibernetski kriminal. Posebej so osredotočeni na internetno zalezovanje, računalniško hekanje ter pravice intelektualne lastnine in forenziko. Pri opravljanju nalog pomagajo tudi Nacionalnemu inštitutu za računalniško forenziko *(National Computer Forensics Institute)* (United States Department of Justice).

8.2.1 Izvedeni ukrepi DoJ

- V zadnjem letu je Ministrstvo za pravosodje sodelovalo pri precedenčnih operacijah za zaprtje kriminalnih trgov omrežja darkweb, osvobodilo na tisoče računalnikov izpod nadzora kriminalcev in doseglo uničenje botneta Gameover Zeus ter doseglo privedbo več pomembnejših kibernetskih kriminalcev v ZDA, kjer jim bodo sodili. Ministrstvo deli najboljše prakse z zasebnim sektorjem ZDA na podlagi preteklih izkušenj boja proti kibernetskemu kriminalu preko portala cybercrime.gov.
- NCIJTF skupaj z ostalimi zveznimi kibernetskimi centri in področnimi agencijami izboljšuje FBI-jev Cyber Guardian sistem za izboljšanje procesa upravljanja poročil glede kibernetskih groženj in obveščanja podjetij, da so bila tarče zlonamerne kibernetske aktivnosti. Kibernetski centri so v prvi polovici leta 2015 zabeležili več kot 10.000 poročil glede kibernetskih groženj in omogočili 2000 obvestil.
- FBI Center za prijavo internetnega kriminala *(Internet Crime Complaint Centre – IC3)* vsako leto izdaja letno poročilo. V letu poročilu iz leta 2015 so zabeležili že več kot 3 milijone prijav. Center, ki deluje od leta 2000 ima v zadnjih letih približbo 300.000 prijav letno.
- V fiskalnem letu 2015 je Kibernetski oddelek FBI sprejela odločitev o ustanovitvi treh novih stalnih položajev imenovanih Ataše za pomoč glede kibernetske zakonodaje *(Cyber Assistant Legal Attache - ALAT)* v Londonu, Ottawi in Canberri ter jim dodala pet novih začasnih delovnih mest. ALAT je vključen v tuje obveščevalne agencije in organe pregona države gostiteljice za izboljšanje izmenjave informacij, povečanje sodelovanja pri preiskavah in izboljšanje odnosov s tujimi partnericami. To sodelovanje in partnerstva bodo v sledečih letih razširili. Že v letu 2016 bodo ustanovljene še štiri začasne pozicije (Federal Bureau of Investigation).

8.3 Ministrstvo za obrambo

Ministrstvo za obrambo je odgovorno za obrambo svobode delovanja ameriškega naroda v kibernetskem prostoru in pomoč pri zmanjševanju tveganj za nacionalno varnost, ki izhajajo iz naraščujoče odvisnosti ZDA od kibernetskega prostora. Specifične naloge obsegajo poveljevanje, varovanje in obramba operacij Informacijskega omrežja Ministrstva za obrambo *(DOD Information Network - DODIN)* (vključno z domeno .mil), ohranjanje svobode manevriranja v kibernetskem prostoru, izvajanje vseh oblik vojaških operacij v kibernetskem prostoru, omogočanje skupnega poznavanja situacije glede kibernetskih operacij, vključno z indikacijami in opozorili ter zagotavljanje podpore civilnim oblastem in mednarodnim partnerjem. Glavna naloga DOD je doseganje in vzdrževanje superiornosti v kibernetskem prostoru, ki je definirana kot "stopnja prevlade neke sile v kibernetskem prostoru, ki tej sili in njenim sorodnim silam na kopnem, vodi, zraku in vesolju, kadarkoli in kjerkoli, omogoča varno, zanesljivo izvajanje operacij, brez možnosti sovražnikovega posredovanja za preprečevanje le-teh". DOD imajo pravico izvajati obrambne kiber operacije; Druge oblike kibernetskih operacij (vključno z napadalnimi kiber operacijami) mora odobriti predsednik in jih lahko odreja obrambni sekretar (US Department of Defense).

- Bojna poveljstva

Bojna poveljstva *(Combatant Commands - CCMDs)* odrejajo navodila za delovanje, poveljujejo in izvajajo nadzor nad oboroženimi silami, zato imajo velikanski vpliv na to, kako so sile organizirane, usposabljane in popolnjene. CCMD izmenjujejo kibernetske informacije preko Kibernetskega poveljstva ZDA *(U.S Cyberspace Command – USCYBERCOM)* in lastnih združenih kibernetskih centrov, vendar se številno osebje glede izmenjave informacij redno srečuje na zasedanjih (US Department of Defense).

- Nacionalna varnostna agencija

Nacionalna varnostna agencija *(National Security Agency - NSA)* je državna kriptološka organizacija, ki koordinira, odreja in izvaja visoko specializirane aktivnosti za zaščito informacijskih sistemov ZDA in pridobiva obveščevalne podatke s prestrezanjem informacij tujih obveščevalnih služb. Deluje v podporo vojaškim odjemalcem, nacionalnim ustvarjalcem politik, protiteroristični in protiobveščevalni skupnosti kot tudi ključnim mednarodnim

zaveznikom. Prav tako NSA s proizvajalci in uporabniki izmenjuje informacije o ranljivosti programske opreme kateregakoli komercialnega produkta in sistema, ki ga uporabljajo ZDA in njene zaveznice, s poudarkom na obrambi in zmanjševanju nevarnosti. (National Security Agency).

- Agencija za obrambne informacijske sisteme

Agencija za obrambne informacijske sisteme *(Defense Information Systems Agency - DISA)* omogoča, izvaja in zagotavlja nadzor ter poveljevanje, zmogljivosti za izmenjavo informacij in globalno dosegljivo informacijsko infrastrukturo za direktno podporo združenim vojaškim bojevnikom, nacionalnim voditeljem in ostalim koalicijskim partnerjem pri vseh oblikah operacij. Odgovorna je za delovanje DODIN v splošnem, čeprav ima vsaka veja oboroženih sil svoj ekvivalent DISA, ki upravlja z določenim delom DODINa (Defense Information Systems Agency).

- Obrambni center za kibernetski kriminal

Obrambni center za kibernetski kriminal *(The Defense Cyber Crime Center)* omogoča zahtevnejše dejavnosti digitalne forenzike in multimedijskega laboratorija, kibernetsko tehnično usposabljanje, raziskave, razvoj, testiranje, ocenjevanje in zmogljivosti kibernetske analize v podporo kibernetski protiobveščevalni in protiteroristični dejavnosti, kriminalnim preiskavam, forenzičnim preiskavam v zvezi z vdori, organom pregona, obveščevalni skupnosti, partnerjem kritične infrastrukture in informacijskim operacijam za DOD (Defense Cyber Crime Center).

- Kibernetsko poveljstvo ZDA

USCYBERCOM je bilo ustanovljeno leta 2010 z združitvijo dveh podrejenih organizacij Strateškega poveljstva ZDA *(U.S. Strategic Command - USSTRATCOM)*: enote za omrežno bojevanje Združenega poveljstva za funkcionalne komponente *(Joint Functional Component Command - Network Warfare)* in enote Združenih sil za izvajanje globalnih omrežnih operacij *(Joint Task Force - Global Network Operations)*. Gre za podrejeno združeno poveljstvo znotraj poveljstva USSTRATCOM, ki načrtuje, koordinira, integrira, sinhronizira in izvaja

aktivnosti za vodenje operacij in obrambe specifičnega dela DODIN. Prav tako pripravlja izvedbo vseh oblik vojaških operacij v kibernetskem prostoru za vsa strateška področja delovanja in zagotavlja svobodo delovanja v kibernetskem prostoru za ZDA in njene partnerice, medtem ko istočasno preprečuje svobodo delovanja sovražniku (US Strategic Command).

Sile za izvajanje kibernetskih nalog *(Cyber Mission Force - CMF)* izvajajo kibernetske operacije za prekinjanje in preprečevanje sovražnikovih napadov na nacionalno kritično infrastrukturo in prestavljajo osrednje sredstvo moči. Gre za prvo združeno taktično poveljstvo ZDA osredotočeno na nalogo opravljanja operacij v kibernetskem prostoru. Do konca leta 2018 je predvidenih 133 skupin za izvajanje kibernetskih nalog, ki jih bodo sestavljale:

- skupine za nacionalne misije, ki izvajajo vse oblike kibernetskih operacij za potrebe USCYBERCOM,
- skupine za podporo, ki bodo nudile neposredno podporo Skupinam za nacionalne misije in Skupinam za bojne misije,
- skupine za kibernetsko zaščito, ki bodo namenjene zaščiti kateregakoli dela DOD in bodo dodeljene tam, kjer je to potrebno,
- skupine za bojne misije bodo izvajale naloge v kibernetskem prostoru za zagotovitev ciljev bojnih poveljnikov in bodo geografsko in funkcionalno dodeljene enemu izmed štirih poveljstev združenih kibernetskih sil *(Joint Force Headquarters–Cyber - JFHQ-C)* za direktno podporo geografskim in funkcionalnim bojnim poveljstvom:
  JFHQ-C Washington nudijo podporo Poveljstvu specialnih operacij ZDA, Pacifiškemu poveljstvu ZDA in Južnemu poveljstvu ZDA
  JFHQ-C Georgia nudijo podporo Centralnemu poveljstvu ZDA, Afriškemu poveljstvu ZDA in Severnemu poveljstvu ZDA
  JFHQ-C Texas nudjo podporo Evropskemu poveljstvu ZDA, USSTRATCOM in Transportnemu poveljstvu ZDA
  JFHQ-DODIN brani informacijsko omrežje DOD za USCYBERCOM
  (US Department of Defense).

Vsaka od vej oboroženih sil ima tudi svoje kibernetske enote. Za potrebe zagotavljanja sil za bojne poveljnike, veje oboroženih sil rekrutirajo, usposabljajo, izobražujejo in ohranjajo svoje vojaške kibernetske formacije:

- kibernetsko poveljstvo kopenske vojske/2. pehotna armada ZDA,
- kibernetsko poveljstvo mornarice/10. flota ZDA,
- kibernetsko poveljstvo letalskih sil/24. zračne sile,
- kibernetsko poveljstvo ameriških marincev,
- kibernetsko poveljstvo Obalne straže ZDA (čeprav je neposredno podrejeno DHS) (US Cyber Command).

8.3.1 Izvedeni ukrepi DoD

- DOD je povečal svoje sodelovanje v kibernetskih vajah in pomagal pripraviti NATO in zaveznice, da se soočijo z naraščajočimi kibervarnostnimi izzivi preko nove pobude za pomoč pri razvoju kibernetskih obrambnih strategij, načrtovanja zaščite kritične infrastrukture in izvajanja samoocenjevanja kibernetske obrambne sposobnosti.
- Izgradnja CMF
- Izvedba vsakoletnega usposabljanja Cyber Guard skupaj z DHS in FBI

(The White House 2015).

9 SKLEP

V diplomski nalogi sem skušal analizirati geopolitično pomembnost kibernetskega prostora za ZDA. Prišel sem do zaključka, da je kibernetski prostor zaradi svoje globalne razširjenosti in pomembnosti za vsa področja človekovega delovanja postal ključnega pomena za uresničevanje geopolitičnih interesov ZDA.

Informatizacija družbe, ki je povzročila razširitev kritične komunikacijske infrastrukture po celem svetu, ima velikanske posledice na področju geopolitike. Prišlo je do pojava tehnogeopolitike, ko se države borijo za ohranitev prevlade na določenem tehnološkem področju, da bi na ta način poskušale ohranjati svoj geopolitični položaj in prednosti, ki jih prevlada prenaša. Znanstveni in tehnološki napredek je povzročil, da je postal kibernetski prostor strateški prostor delovanja, ki ga države poskušajo militarizirati za projekcijo svoje moči.

Kibernetska moč, sposobnost uporabe kibernetskega prostora za ustvarjanje premoči in vplivanje na dogodke v ostalih okoljih delovanja in z ostalimi instrumenti moči je postala ključna politična usmeritev v ZDA in po svetu. Varnost in učinkovito delovanje kritične infrastrukture ZDA – vključno z energetiko, bančništvom in financami, transportom, komunikacijami in obrambno industrijo – je odvisno od kibernetskega prostora, industrijskih nadzornih sistemov in informacijske tehnologije, ki je občutljiva na prekinitve in izrabljanje. Preko kibernetskega prostora ameriška in mednarodna podjetja trgujejo z dobrinami in storitvami, hkrati pa je kiberprostor omogočil hipen prenos sredstev ne glede na razdaljo. Poleg pospeševalca prodaje na ostalih področjih je kibernetski prostor sam po sebi ključni sektor svetovnega gospodarstva. Postal je inkubator za nove oblike podjetništva, napredke v tehnologiji, razširitev svobodnega izražanja in nova socialna omrežja, ki poganjajo gospodarstvo ZDA in odsevajo njihova načela. Kibernetski prostor je postal ključnega pomena tudi pri vodenju sodobnih oboroženih spopadov.

Pri strateški uporabi informacijske in komunikacijske tehnologije lahko uporabljamo trdo in mehko moč. Če je trda moč sposobnost doseganja ciljev preko uporabe ekonomske moči ali uporabe vojaške moči in je povezana z zaščito kritične infrastrukture ter kibernetskim bojevanjem, je mehka moč sposobnost oblikovanja preferenc ostalih, brez uporabe sile, prisile ali nasilja. Kibernetski prostor s svojo zmožnostjo razširjanja informacij predstavlja pomemben dejavnik pri uporabi mehke moči in širjenju lastnih vrednot. Karakteristike kibernetskega prostora so privedle do tega, da prihaja do večjega števila akterjev in

zmanjševanju razlik v njihovi moči. Nizka sredstva, potrebna za vstopanje, hitrost in relativno zmanjšanje pomembnosti razdalje ter nedorečena pravila delovanja, so privedla do pojava novih asimetričnih oblik nevarnosti in groženj. Povečana uporaba kibernetskih napadov kot političnega instrumenta odraža nevaren trend v mednarodnih odnosih. Ranljivi podatkovni sistemi predstavljajo mamljivo priložnost za državne in nedržavne akterje, da napadejo ZDA in njihove interese. Prekinitveni, manipulativen ali uničevalen kibernetski napad lahko predstavlja veliko tveganje za gospodarsko in nacionalno varnost ZDA, če pride do izgube življenj, uničevanja lastnine, škodovanja političnim ciljem ali gospodarskim interesom.

Čeprav se je že administracija predsednika Clintona že pred tridesetimi leti zavedala potencialne strateške moči kibernetskega prostora in govorila o nujnosti in pomembnosti razvoja "informacijske avtoceste", so se ZDA šele po terorističnih napadih na *World Trade Center* začele resneje zavedati grožnje, ki jo ogroženost kibernetskega prostora predstavlja za sodobno varnostno okolje in se bolj resno posvečati vprašanjem zaščite tega prostora. Tako sta bila v času vladavine predsednika Busha napravljena dva izjemno pomembna koraka. Ustanovljeno je bilo Ministrstvo za domovinsko varnost, ki danes predstavlja osrednji vladni organ za zaščito kibernetske kritične infrastrukture, hkrati pa je bila sprejeta Nacionalna strategija za zaščito kibernetskega prostora, ki predstavlja prvo nacionalno pobudo za premislek o internetni varnosti. Vendar pa so se ZDA v mandatu zdajšnjega predsednika Obame še aktivneje lotile ureditve področja kibernetskega prostora na deklarativni ravni, saj je število strateških dokumentov, usmeritev, priporočil in smernic, ki so nastale po letu 2008 močno povečalo. Kljub številnim strategijam in implementacijskim načrtom, ki se osredotočajo na specifične probleme povezane s kibernetsko varnostjo in so bili izdani v zadnjih letih, v zadnjem obdobju ni bil pripravljen nikakršen nov vseobsegajoč dokument glede nacionalne kibernetske varnostne strategije, ki bi predstavljal izvleček pomembnih delov posameznih nastalih dokumentov. Posledica tega je, da z izjemo Nacionalne strategije za zaščito kibernetskega prostora iz leta 2003, ki je stara že več kot deset let, ne obstaja enotna strategija, ki bi zajemala številne cilje in aktivnosti, ki so zapisane v trenutnih posameznih dokumentih. Menim, da poenotenje vseh politik in strategij znotraj nove nacionalne strategije predstavlja največji izziv za ZDA v prihodnjih letih.

Vseeno je potrebno priznati, da so ZDA v zadnjih letih napravile velikanski napredek na področju obravnave kibernetskega prostora kot ključne strateške dobrine. Prioritetne naloge in cilji, zapisani v dokumentih Nacionalni strategiji za zaščito kibernetskega prostora in Pregledu politik glede kibernetskega prostora, so bili v večini izpolnjeni. Imenovanje koordinatorja za kibernetsko varnost, imenovanega tudi "kibernetski car", ki usklajuje delo

številnih zveznih uradov in agencij, ki so bile ustanovljene znotraj posameznih ministrstev, predstavlja enega najvidnejših ukrepov, ki dokazuje, da so ZDA odločene preko najvišje veje izvršilne oblasti voditi prizadevanja glede zaščite kibernetskega prostora.

Kibernetska strategija Ministrstva za obrambo je dokaz, da vojska ZDA kibernetski prostor obravnavava popolnoma enakovredno ostalim prostorom bojevanja. Zavedanje, da kibernetski prostor predstavlja nov strateški prostor, se kaže v ustanovitvi samostojnega poveljstva kibernetskih sil, preko katerega bodo ZDA v prihodnjih letih usposobile in izurile pripadnike oboroženih sil za izvajanje vseh oblik kibernetskih operacij. Mednarodna strategija za kibernetski prostor odraža naraščajoče zavedanje o nujnosti mednarodnopravne ureditve področja kibernetskega prostora, saj se ZDA zavedajo, da bo za uresničevanje lastnih interesov v prihodnosti potrebno sodelovanje z ostalimi državami. Vendar lahko vidimo, da prizadevanja ZDA za zagotovitev širše mednarodne podpore glede zadev, povezanih s kibernetsko varnostjo, niso dosegla večjih uspehov. Delno je to posledica netransparentnega delovanja ZDA na področju kibernetskega prostora. Primeri Wikileaksa in afera Snowden kažejo na to, da ZDA ne upoštevajo pravil transparentnega ravnanja, ki jih na deklarativni ravni zagovarjajo. Po drugi strani pa neusklajena mednarodna zakonodaja in politike na področju kibernetskega prostora ustrezajo državam in ostalim nedržavnim političnim akterjem, saj lahko na ta način izvajajo svoje dejavnosti brez nevarnosti, da bi bili sankcionirani.

Dokument Okvir za izboljšanje kibernetske varnosti kritične infrastrukture pomembno izboljšuje sodelovanje z zasebnim sektorjem, saj zaradi odprte arhitekture kritične informacijske infrastrukture učinkovita zaščita kibernetskega prostora ni mogoča brez sodelovanja podjetij v zasebni lasti. Vseeno v praksi še vedno prihaja do problemov zaradi velikih stroškov, ki jih predstavlja prilagajanje standardom zasebnim podjetjem, in problemov, povezanih z zaščito zasebnosti in državljanskih pravic. Obstajajo štirje glavni problemi. Prvi je sama velikost in kompleksnost infosfere ZDA, ki še vedno predstavlja največji nacionalni sestavni del globalnega sistema. Drugi problem predstavljajo nasprotujoči si politični cilji. Na eni strani si ZDA želijo omogočiti učinkovito izmenjavo informacij za identifikacijo potencialnih groženj, ki na drugi strani nasprotuje pravici do zasebnosti in nezaupanju ljudi do pretiranega vladnega vmešavanja. Velikost in oblika gospodarstva ZDA predstavljata tretji izziv. Zasebna podjetja se namreč bojijo, da bo izmenjava informacij vodila k izpostavljenosti ali potencialnemu kazenskemu pregonu, izgubi lastniških informacij v primerjavi s konkurenco ter izgubo zaupanja njihovih strank. Četrti izziv je problem "zastonjkarstva", ko večina udeležencev v shemah izmenjave informacij absorbira več

informacij kot jih prispeva, in ko mnogo udeležencev obravnava izmenjavo informacij kot marketinško priložnost za njihove lastne varnostne rešitve.
V začetku svoje diplomske sem postavil dve hipotezi, ki ju lahko, glede na napisano, obe potrdim.

Hipoteza 1: Nadzor nad kibernetskim prostorom postaja strateškega pomena za uresničevanje geopolitičnih ciljev ZDA. Varnost ZDA, močno, inovativno in rastoče gospodarstvo in spoštovanje univerzalnih vrednot doma in po svetu predstavljajo nacionalne interese ZDA. Vsi ti cilji so sedaj postali odvisni od varnega, zanesljivega in svobodnega kibernetskega prostora. ZDA v vseh analiziranih strateških dokumentih poudarjajo, da si bodo prizadevale za zaščito kibernetskega prostora in ohranjale pravico do njegove obrambe kot nujno in primerno. V prihodnjih letih bodo ZDA preko programov kadrovskega popolnjevanja in štipendij, kot je npr. Cyber Corps, zaposlile več kot 6000 pripadnikov vojaškega in civilnega osebja za zagotovitev informacijske prevlade.
Hipoteza 2: V zadnjih desetih letih smo priča porastu smernic, strategij in politik, s katerimi si ZDA želijo zagotoviti oz. ohraniti nadzor nad vodenjem in upravljanjem kibernetskega prostora. V diplomskem delu sem analiziral pet strateških dokumentov, od katerih so štirje nastali v zadnjih desetih letih. S silovitim razvojem tehnologij in naraščanjem števila groženj in zlonamernih napadov v zadnjih letih se je okrepilo tudi stremenje ZDA k usklajeni politiki glede delovanja in prihodnosti v kibernetskem prostoru.

10 LITERATURA

1. Acohido, Byron. 2008. *Zero Day Threat: The Shocking Truth of How Banks and Credit Bureaus Help Cyber Crooks Steal Your Money and Identity.* New York: Union Square Press.
2. Armistead, Leigh., ur. 2004. *Information Operations: Warfare and the Hard Reality of Soft Power: A Textbook Produced in Conjunction with the Joint Forces Staff College and the National Security Agency.* Washington, D.C.: Potomac Books.
3. Armitage, Richard L. in Joseph S. Nye Jr. 2007. *CSIS Commission on Smart Power : A smarter, more secure America.* Washington, DC: Center for Strategic and International Studies.
4. Atkinson, Robert D., Stephen J. Ezell, Scott M. Andes, Daniel D. Castro in Richard Bennett. 2010. *The Internet Economy 25 Years After.Com: Transforming Commerce & Life.* Washington: The Information Technology and Innovation Foundation.
5. Barno, David W. 2006. Challenges in Fighting a Global Insurgency. *Parameters* 36 (2): 15−29.
6. Bein - Israel Isaac in Lior Tabansky. 2011. An Interdisciplinary Look at Security Challenges in the Information Age. *Military and Strategic Affairs* 3 (3): 21−39.
7. Benedikt, Michael. 1991. Cyberspace: Some Proposals V *Cyberspace: First Steps*, ur. Michael Benedikt, 119−224. Cambridge, MA: The MIT Press.
8. Berkowitz, Bruce. 2003. *The New Face of War: How War Will be Fought in the 21st Century.* New York: The Free Press.
9. Betz, David. 2012. *Cyberpower and International Security.* Dostopno prek: http://www.fpri.org/articles/2012/06/cyberpower-and-international-security (24. januar 2016).
10. Booz Allen Hamilton. 2011. *The Road to Cyberpower: Seizing Opportunity While Managing Risk in the Digital Age.* Dostopno prek: http://www.boozallen.com/content/dam/boozallen/media/file/road-to-cyberpower.pdf (23. marec 2016).
11. Brenner, Susan W. 2002. Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships. *North Carolina Journal of Law & Technology* 4 (1): 1−50.
12. Butler, David L. 2001. Technogeopolitics and the Struggle for Control of World Air Routes, 1910−1928. *Political Geography* (20): 635−658.

13. Caro Bejarano, María José. 2013. *Cyberspace: Hard Power vs. Soft Power.* Dostopno prek: http://www.ieee.es/en/Galerias/fichero/docs_analisis/2013/DIEEEA33-2013_PoderDuroPoderBlandoEnCiberespacio_MJCB_ENGLISH.pdf (7. februar 2016).
14. Casey, Tim. 2003. *The National Strategy to Secure Cyberspace: an In-depth Review.* Dostopno prek: http://www.senki.org/wp-content/uploads/2015/03/national-strategy-secure-cyberspace-in-depth-review_2875.pdf (21. marec 2016).
15. Center for Democracy & Technology. 2009. *Privacy and the White House Cyberspace Policy Review*. Dostopno prek: https://www.cdt.org/files/security/20090619_cybersec_actions.pdf (21. marec 2016).
16. Choo, Kim - Kwang Raymond in Russell G. Smith. 2008. Criminal Exploitation of Online Systems by Organised Crime Groups. *Asian Criminology* 3 (1): 37−59.
17. Clark, David. 2010. *Characterizing cyberspace: past, present and future.* MIT CSAIL, Version 1.2. Dostopno prek: https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf (23. maj 2016).
18. Clinton, Hillary Rodham. 2010. *Remarks on Internet Freedom*. Dostopno prek: http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm (8. februar 2016).
19. --- 2011. *Internet Rights and Wrongs: Choices & Challenges in a Networked World.* Dostopno prek: http://www.state.gov/secretary/20092013clinton/rm/2011/02/156619.htm (8. februar 2016).
20. Cohen, Saul Bernard. 2003. *The geopolitics of the world system.* Lantham, MD: Rowman and Littlefield Publishers, Inc.
21. Convertino, Sebastian M., Lou Anne DeMattei in Tammy M. Knierim. 2007. *Flying and Fighting in Cyberspace*. Maxwell Air Force Base, Alabama: Air University Press.
22. Cornish, Paul, Rex Hughes in David Livingstone. 2009. *Cyberspace and the National Security of the United Kingdom: Threats and Responses.* Chatham House Report. London: Royal Institute of International Affairs.
23. Couchri, Nazli in David Clark. 2011. *Cyberspace and International Relations : Toward an Integrated System.* Dostopno prek: http://ecir.mit.edu/images/stories/Salience%20of%20Cyberspace%208-25.pdf (23. marec 2016).
24. Crowther, Alexander G. in Shaheen Ghori. 2015. Detangling the Web: A Screenshot of U.S. Government Cyber Activity. *Joint Force Quarterly* 78 (3): 75−83.
25. *Defense Cyber Crime Center*. Dostopno prek: www.dc3.mil/ (8. maj 2016).
26. *Defense Information Systems Agency*. Dostopno prek: http://www.disa.mil/ (8. maj

2016).

27. Department of Defense. 2015. *The Department of Defense Cyber Strategy*. Dostopno prek: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (21. marec 2016).
28. Department of Homeland Security 2003. *National strategy to secure cyberspace.* Dostopno prek: http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf (16. januar 2016).
29. Dilanian, Ken. 2011. Virtual War a Real Threat. *Los Angeles Times,* 28. marec. Dostopno prek: http://articles.latimes.com/2011/mar/28/nation/la-na-cyber-war-20110328 (8. februar 2016).
30. Dodds, Klaus. 2007. *Geopolitics: A Very Short Introduction.* Oxford, UK: Oxford University Press.
31. Dunn, Myriam. 2007. Securing the Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory. V *International Relations and Security in the Digital Age,* ur. Johan Eriksson in Giampiero Giacomello, 85−106. Abingdon, Oxon: Routledge.
32. Encyclopaedia Britannica. 2016. *Geopolitics*. Dostopno prek: http://www.britannica.com/topic/geopolitics (16. januar 2016).
33. Eriksson, Johan in Giampiero Giacomello. 2006. The Information Revolution, Security, and International Relations: (IR)relevant Theory? *International Political Science Review* 27 (3): 221−244.
34. Everard, Jerry. 2000. *Virtual States: The Internet and the Boundaries of the Nation-State*. London, UK: Routledge.
35. Farwell, James P. in Rafal Rohozinski. 2011. Stuxnet and the Future of Cyber War. *Survival* 53 (1) Dostopno prek: https://www.cs.duke.edu/courses/common/compsci092/papers/cyberwar/stuxnet2.pdf (5. april 2016).
36. *Federal Bureau of Investigation*. Dostopno prek: https://www.fbi.gov/ (8. maj 2016).
37. Ferguson, Yale in Richard Mansbach. 2004. *Remapping Global Politics: History's Revenge and Future Shock.* Cambridge: Cambridge University Press.
38. Fickes, Michael. 2008. Cyber Terror. *Government Security*, 1. julij. Dostopno prek: http://americancityandcounty.com/security/homeland/cyber_terror_attacks (4. februar 2016).
39. Finn, Peter. 2007. Cyber Assaults on Estonia Typify a New Battle Tactic. *The Washington Post*, A1 (19. maj).

40. Flint, Colin. 2006. *Introduction to Geopolitics*. New York: Routledge.
41. Fulghum, David A. in Douglas Barrie. 2007. Off The Radar; Israel used electronic attack in air strike against Syrian mystery target. *Aviation Week & Space Technology* 167 (14): 28.
42. Geers Kenneth, Darien Kindlunf, Ned Moran in Rob Rachald. 2013. *World War C : Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks*. FireEye Report. Dostopno prek: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf (4. februar 2016).
43. Geers, Kenneth. 2014. *Cyberspace as Battlespace*. Dostopno prek: https://www.blackhat.com/html/webcast/10092014-cyberspace-as-battlespace.html (24. januar 2016).
44. Generalna skupščina Združenih narodov. 2001. *Konvencija združenih narodov proti mednarodnemu organiziranemu kriminalu*, 55/25. Dostopno prek: https://www.kpk-rs.si/download/t_datoteke/2320 (2. februar 2016).
45. Gibson, William. 1997. *Nevromant.* Ljubljana: Cankarjeva založba.
46. Gray, Colin S. 1996. The Continued Primacy of Geography. *Orbis* 40 (2): 247.
47. --- 2005. In Defence of the Heartland: Sir Halford Mackinder and his Critics a Hundred Years on V *Global Geostrategy: Mackinder and the Defence of the West*, ur. Brian W. Blouet, 17−35. London: Routledge.
48. Hansen, Lene in Helen Nissenbaum. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly* (53): 1155–1175.
49. Harper, Jim. 2004. *Understanding privacy and the real threats to it*. Washington: Cato Institute.
50. Hathaway, Melissa. 2009. *Remarks by Melissa E. Hathaway, Delivery at RSA Conference.* Dostopno prek: http://voices.washingtonpost.com/securityfix/Melissa%20Hathaway%20Speech%20at%20RSA.pdf (21. marec 2016).
51. Herrera, Geoffrey L. 2006. *Technology and International Transformation: The Railroad, the Atom Bomb and the Politics of Technological Change*. New York: State University of New York Press.
52. Internet Live Stats - Internet Usage & Social Media Statistics. 2016. *Internet users.* Dostopno prek: http://www.internetlivestats.com/internet-users/ (24. januar 2016).
53. Johnson, Bobbie. 2008. NATO says cyber warfare poses as great a threat as a missile attack: Concern follows strikes by 'Titan Rain' hackers. State-sponsored online aggression said to be rising. *The Guardian*, 2 (6. marec).
54. Jones, Martin, Rhys Jones in Michael Woods. 2004. *An Introduction to Political*

Geography: Space, Place and Politics. London: Routledge.

55. Keohane, Robert O. in Joseph S. Nye Jr. 1998. Power and Interdependence in the Information Age. *Foreign Affairs* 77 (5): 81−94.
56. --- 2001. *Power and Interdependence: World politics in transition, 3rd edition.* Boston: Little-Brown.
57. Kjellén, Rudolf. 1917. *Der Staat als Lebensform.* Leipzig: Hirzel.
58. Klare, Michael. 2003. The new geopolitics. *Monthly Review* 55 (3). Dostopno prek: http://monthlyreview.org/2003/07/01/the-new-geopolitics (1. februar 2016).
59. Krasner, Stephen D. 1991. Global Communications and National Power: Life on the Pareto Frontier. *World Politics* 43 (3): 336−366.
60. Krenn, Philipp. 2003. *Strategic Information Warefare in Cyberspace.* Vien: Bundesre algymnasium Wien XIX.
61. Kristof, Ladis K. D. 1960. The Origins and Evolution of Geopolitics. *The Journal of Conflict Resolution* 4 (1): 15−51.
62. Kuehl, Daniel T. 2009. From Cyberspace to Cyberpower: Defining the Problem V *Cyberpower and National Security,* ur. Franklin D. Kramer, Stuart Starr in Larry K. Wentz, 24−42. Washington: National Defense University Press.
63. Kuhn, Thomas. 1996. *The Structure of Scientific Revolutions.* Chicago, IL: University Of Chicago Press.
64. Lonsdale, David J. 2004. *The Nature of War in the Information Age: Clausewitzian Future.* London, UK: Frank Cass.
65. Lord, Kristin M. in Travis Sharp, ur. 2011. *America's Cyber Future: Security and Prosperity in the Information Age, Volume I.* Washington, DC: Center for a New American Security.
66. Luke, Timothy W. 1998. Running Flat Out on the Road Ahead: Nationality, Sovereignty and Territoriality in the World of the Information Superhighway. V *Rethinking Geopolitics,* ur. Gearoid O'Tuathail in Simon Dalby, 274−294. New York: Routledge, Taylor & Francis Group. Dostopno prek: http://frenndw.files.wordpress.com/2010/03/geopolitics-a-rethinking.pdf (16. januar 2016).
67. Lynn III., William J. 2010. *Defense Dept. Outlines New Infosec Approach.* STRATCOM Cyber Symposium. Omaha, NE. Dostopno prek: http://www.govinfosecurity.com/articles.php?art_id=2580&opg=1 (8. februar 2016).
68. Mackinder, Halford John. 1904. The Geographical Pivot of History. *Geographical Journal 13* (4): 421−437.

69. Maliukevičius, Nerijus. 2007. Geopolitics and information warfare: Russia's approach. V *Lithuanian annual strategic review 2006*, ur. Raimundas Lopata, Jūratė Novagrockienė in Gediminas Vitkus, 121−147. Vilnius: Lithuanian Military Academy.
70. Mitchell, William J. 1995. *City of bits: space, place and the infobahn*. Cambridge, MA: MIT Press.
71. Molander, Roger C., Andrew S. Riddile in Peter A. Wilson. 1996. *Strategic Information Warfare: A New Face of War.* Santa Monica, CA: RAND.
72. Moreau Defarges, Philippe. 2002. *Introduction à la Géopolitique.* Paris: Éditions du Seuil.
73. Morgenthau, Hans Joachim. 1966. *Politics among Nations.* New York: Alfred A. Knopf, Inc.
74. Nakashima, Ellen. 2011. U.S. Agencies Respond to Cyberattack on Information Security Firm. *The Washington Post,* 23. marec. Dostopno prek: https://www.washingtonpost.com/world/us_agencies_respond_to_cyberattack_on_information_security_firm/2011/03/23/ABDhjoKB_story.html (8. februar 2016).
75. National Communications System. 2000. T*he Electronic Intrusion Threat to National Security and Emergency Preparedness Internet Communications: An Awareness Document.* Arlington, VA: National Communications System.
76. National Institute of Standards and Technology. 2014. *Framework for Improving Critical Infrastructure Cybersecurity.* Dostopno prek: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (21. marec 2016).
77. National Research Council. 1991. *Computers at Risk: Safe Computing in the Information Age.* Washington: National Academies Press.
78. Nickolov, Eugene. 2005. Critical Information Infrastructure Protection: Analysis, Evaluation and Expextations. *Information & Security: An International Journal* (17): 105−119.
79. National Security Agency | Central Security Service. Dostopno prek: https://www.nsa.gov/ (8. maj 2016).
80. Nye Jr., Joseph S. 2004. *Soft Power: the means to success in world politics.* New York: Public Affairs.
81. --- 2010. *Cyber power.* Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School.
82. --- 2011. Power and National Security in Cyberspace V *America's Cyber Future: Security and Prosperity in the Information Age, Volume II,* ur. Kristin M. Lord and

Travis Sharp, 5−25. Washington, DC: Center for a New American Security.

83. Obama, Barrack. 2008. *Remarks of Senator Barack Obama, Summit on Confronting New Threats, Purdue University*. Dostopno prek: http://www.cfr.org/elections/barack-obamas-speech-university-purdue/p16807 (21. marec 2016).
84. Organisation for Economic Co-operation and Development. 2008. *The Future of the Internet Economy.* Dostopno prek: http://www.umic.pt/images/stories/ocde/Policy%20Brief.pdf (1. februar 2016).
85. O'Tuathail, Gearóid, Simon Dalby in Paul Routledge. 2006. *The geopolitics reader: Second Edition.* London: Routledge.
86. Pallaver, Matteo. 2011. *Power and Its Forms: Hard, Soft, Smart.* London: Department of International Relations of the London School of Economics.
87. Poulsen Kevin. 2008. British UFO hacker Gary McKinnon is coming to America. *Wired, 30 Julij*. Dostopno prek: http://www.wired.com/2008/07/british-ufo-hac/ (31. januar 2016).
88. Price, Alfred. 2005. *Instruments of Darkness: The History of Electronic Warfare 1939−1945.* London: William Kiner and Co.
89. Reilly, Michael. 2008. When nations go to cyberwar. *New Scientist*, 2−3 (23. februar).
90. Rennstich, Jachim K. 2008. *The Making of a Digital World: The Evolution of Technological Change and How it Shaped our World.* New York: Palgrave Macmillan.
91. Richmond, Riva. 2011. An Attack Sheds Light on Internet Security Holes. *The New York Times,* 6. april. Dostopno prek: http://www.nytimes.com/2011/04/07/technology/07hack.html?_r=0 (8. februar 2016).
92. Rush, Howard, Chris Smith, Erika Kraemer-Mbula in Puay Tang. 2009. *Crime online: Cybercrime and illegal innovation.* Dostopno prek: http://eprints.brighton.ac.uk/5800/1/Crime_Online.pdf (1. februar 2016).
93. Schneier, Bruce. 2007. *Schneier on Security: A Blog Covering Security and Security Technology, Cyberwar.* Dostopno prek: http://www.schneier.com/blog/archives/2007/06/cyberwar.html (31. januar 2016).
94. Schreier, Fred. 2015. On cyberwarefare. *DCAF Horizon 2015 working paper No. 7.* Dostopno prek: http://www.dcaf.ch/Publications/On-Cyberwarfare (25. januar 2016).
95. Serabian Jr., John A. 2000. *Cyber Threats and the U.S. Economy*. *Statement for the Record before the Joint Economic Committee*. Dostopno prek: https://www.cia.gov/news-information/speeches-testimony/2000/cyberthreats_022300.html (4. februar 2016).

96. Simoniti, Iztok. 1997. Uvod k Zahodna geopolitična misel v XX. Stoletju. V *Zahodna geopolitična misel v XX. stoletju.* Geoffrey Parker, 1−57. Ljubljana: Fakulteta za družbene vede.
97. Skinner, Tony. 2008. War and PC. *Jane's Defence Weekly*, (24. september).
98. Spykman, Nicholas J. 1944. *The Geography of the Peace.* New York: Harcourt, Brace.
99. StatCounter GlobalStats. *Top 5 Desktop browsers from Apr 2015 to Apr 2016.* Dostopno prek: http://gs.statcounter.com/#browser-ww-monthly-201504-201604 (22. maj 2016).
100. Stenersen, Anne. 2008. The Internet: A Virtual Training Camp? *Terrorism and Political Violence* 20 (2): 215−233.
101. Sterner, Eric. 2011. Retaliatory Deterrence in Cyberspace. *Strategic Studies Quarterly* 5 (1): 62−80.
102. Strehovec, Janez. 1997. V svetu visokoadrenalinske tehnologije (spremna beseda), v: Gibson, William. *Nevromant*. Ljubljana: Cankarjeva založba (spremna beseda).
103. Symantec Corporation. 2014. *Internet Security Threat Report 2014.* Dostopno prek: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf (29. februar 2016).
104. --- 2015. *Internet Security Threat Report 2015.* Dostopno prek: https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf (2. februar 2016).
105. Tabansky, Lior. 2011. Critical Infrastructure Protection against Cyber Threats. *Military and Strategic Affairs* 3 (2): 61−78.
106. Tafoya, William L. 2011. Cyber Terror. *FBI Law Enforcement Bulletin* 80 (11): 1−7.
107. *The Economist.* 2007. A world wide web of terror, 12. julij. Dostopno prek: http://www.economist.com/node/9472498 (3. februar 2016).
108. --- 2008. Clouds and judgment, 23. oktober. Dostopno prek: http://www.economist.com/node/12471098 (2. februar 2016)
109. The White House. 2009a. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* Dostopno prek: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (16. januar 2016).
110. --- 2009b. *Remarks by the President on Securing Our Nation's Cyber Infrastructure.* Dostopno prek: https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (24. februar 2016).

111. --- 2009c. *Cybersecurity event fact sheet and expected attendees*. Dostop prek: https://www.whitehouse.gov/the-press-office/cybersecurity-event-fact-sheet-and-expected-attendees (23. Marec 2016).
112. --- 2010. *National Security Strategy.* Dostopno prek: https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (8. februar 2016).
113. --- 2011. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.* Dostopno prek: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (21. marec 2016).
114. --- 2013. *Executive Order -- Improving Critical Infrastructure Cybersecurity,* (12. februar 2013). Dostopno prek: https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (21. marec 2016).
115. --- 2015. *FACT SHEET: Administration Cybersecurity Efforts 2015,* (9. julij 2015). Dostopno prek: https://www.whitehouse.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015 (8. maj 2016).
116. Trček, Franc. 1997. *Dostopnost in izključnost v kiberprostoru: računalniško posredovano komuniciranje in spremembe prostorsko-časovne organizacije družbe.* Magistrska naloga, Ljubljana: FDV.
117. *United States Department of Defense*. Dostopno prek: http://www.defense.gov/ (8. maj 2016).
118. *United States Department of Justice*. Dostopno prek: https://www.justice.gov/ (8. maj 2016).
119. *United States Secret Service*. Dostopno prek: http://www.secretservice.gov/ (8. maj 2016).
120. United States Strategic Command. 2016. *United States Cyber Command*. Dostopno prek: https://www.stratcom.mil/factsheets/2/Cyber_Command/ (8. maj 2016).
121. Valeri, Lorenzo. 2013. *Countering Threats in Space and Cyberspace: A Proposed Combined Approach.* London: Chantam House. Dostopno prek: https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/0113discussionpaper_Valeri.pdf (9. februar 2016).
122. Verton, Dan. 2003. *Black Ice: The Invisible Threat of Cyber-Terrorism* (New York: McGraw-Hill / Osborne Media.
123. Wamala, dr. Frederick. 2011. *The ITU national cybersecurity strategy guide.* Dostopno prek: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrat

egyGuide.pdf (3. februar 2016).

124. Wentz, Larry K., Charles L. Barry in Stuart H. Starr, ur. 2009. *Military Perspectives on Cyberpower.* Washington, DC : National Defense University Center for Technology and National Security Policy.

125. Whittaker, Jason. 2004. *The Cyberspace Handbook.* London: Routledge, Taylor & Francis Group.

126. Wilson, Clay. 2005. *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, Congressional Research Service Report for Congress*. Washington, DC: Library of Congress.