UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Diana Namestnik

Kibernetska oblika bojevanja v Iraku (2003–2016) in Siriji (2011–2016)

Diplomsko delo

Ljubljana, 2016

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Diana Namestnik

Mentor: izr. prof. dr. Uroš Svete

Kibernetska oblika bojevanja v Iraku (2003–2016) in Siriji (2011–2016)

Diplomsko delo

Ljubljana, 2016

Zahvala!

Zahvaljujem se svojim staršem za vso podporo in potrpljenje skozi študijska leta, da verjameta vame in v moje delo, cilje, sposobnosti ter za "nenehno opominjanje", da je ta naloga dobila končni epilog.

Hvala mentorju, izr. prof. dr. Urošu Svetetu za pomoč in pravo usmeritev pri diplomski nalogi, za nasvete in podporo ter za dobro sodelovanje nasploh v zadnjih letih mojega študija.

Kibernetska oblika bojevanja v Iraku (2003–2016) in Siriji (2011–2016)

Kibernetska bojevanje predstavlja danes novodobno obliko bojevanja v kibernetskem prostoru, ki je peta domena vojskovanja (poleg zemlje, zraka, morja in vesolja). Kibernetska oblika bojevanja se prvotno uporablja kot podporni sistem vojaškega posredovanja. Bojevanje se izvaja preko računalnikov in informacijske strukture, zatorej ne prihaja do neposrednega fizičnega kontakta z nasprotnikom. Ampak je presegla državne okvire, saj jo za svojo dosego ciljev in namenov uporabljajo tudi nedržavni akterji (hektivistične skupine, posamezniki, kriminalne skupine, teroristične organizacije ipd.). Kibernetski napadi velesil (ZDA, Rusija, Kitajska) imajo lahko učinek orožja za množično uničevanje, saj zaradi prepletenosti civilne in vojaške strukture lahko naredijo ogromno škodo na lokalni in globalni ravni. Irak in Sirija sta postala poligon za preizkušanje metod in novih kibernetskih orožij svetovnih velesil. V obeh primerih so se s strani napadalcev (IS, SEA), ki so te napade najbolj izvajali na zahodne medijske in druge organizacije, predvsem uporabljali za propagandne namene in pritegnitev svetovne javnosti o dogodkih, ki so se in se še dogajajo v državah danes. Bo pa kibernetska oblika bojevanja v prihodnosti postala glavna domena bojevanja tistih držav, ki v konvencionalnem smislu ne morejo konkurirati velesilam.

Ključne besede: kibernetsko bojevanje, kibernetski prostor, tehnologija, kibernetski napad in obramba

Cyber warfare in Iraq (2003–2016) and Syria (2011–2016)

Cyber warfare is presenting today new age form of warfare in cyberspace, which is the fifth domain of warfare (in addition to land, air, sea and space). Cyber warfare is originally used as a supporting system of the military intervention. Warfare is performed by computers and information infrastructure, so there is no direct physical contact with an opponent. But it exceeded the national sphere, since it is also used by non-state actors (hactivist groups, individuals, criminal groups, terrorist organizations, etc.) to achieve the objectives and purposes of their actions. Cyber attacks of world powers (USA, Russia, China) can have the effect of weapons of mass destruction because of the intertwining of civil and military structures. They can do enormous damage locally and globally. Iraq and Syria have become a testing ground for methods and new cyber weapons world powers. In both cases the attackers (IS, SEA) that mainly carry on the cyber attacks on Western media and other organizations, are in the vast majority used for propaganda purposes and to get world public attention about the events that have been and are still happening in the countries today. Cyber warfare will in the future become a major domain of warfare of those countries with small army forces and can not compete with the conventional supremacy of world powers.

Key words: cyber warfare, cyber space, technology, cyber attack and defense

KAZALO

KAZALO SLIK

SEZNAM KRATIC

AFCYBER:	Kibernetsko poveljstvo zračnih sil (*ang. Air Force of Cyber Command*)
ATP:	Obstojna napredna grožnja (*ang. Advanced Persistent Threat*)
CENTCOM:	Ameriško Glavno poveljstvo (*ang. US Central Command*)
CIA:	Centralna preiskovalna agencija (*ang. Central Investigation Agency*)
CNA:	Računalniško omrežni napadi *(ang. Computer Network Attack)*
CND:	Računalniško omrežna obramba *(ang. Computer Network Defense)*
CNE:	Računalniško omrežno izkoriščanje *(ang. Computer Network Explotation)*
CNO:	Računalniško omrežne operacije (*ang. Computer Network Operations*)
CPM:	Nepretrgana vztrajna kontrola (*ang. Continuos Persistent Monitoring*)
CYBERCOM:	Ameriško kibernetsko poveljstvo (*ang. U.S. Cyber Command*)
CW:	Kibernetsko vojskovanje (*ang. Cyberwarfare)*
C2I:	Vodenje, poveljevanje in obveščevalna (*ang. Command, Control and Intelligence*)
C3I:	Vodenje, poveljevanje, komunikacije in obveščevalna (*ang. Command, Control, Communication and Intelligence*)
C4I:	Vodenje, poveljevanje, komunikacije, računalništvo in obveščevalna (*ang. Command, Control, Communications, Computer and Intelligence*)
DDoS:	Distribuirani napadi onemogočanja storitev (*ang. Distributed Denial of Service*)
FBI:	Zvezni preiskovalni urad (*ang. Federal Bureau of Investigation*)
FSA:	Svobodna sirska vojska *(ang. Free Syrian Army)*
GPS:	Sistem za globalno lokacijo (*ang. Global Positioning System*)
HIC:	Konflikt visoke intenzivnosti (*ang. High intensity conflict*)
IKT:	Informacijsko – komunikacijska tehnologija
IO:	Informacijske operacije *(ang. Information Operations)*
iOS:	Operacijski mobilni sistem za iPhone (*ang. iPhone OS*)
IP:	Internetni protokol *(ang. Internet Protocol)*
IS, ISIS:	Islamska država (*ang. Islamic State*)
IW:	Informacijsko vojskovanje *(ang. Information Warfare)*
JFCC:	Skupna funkcionalna komponenta poveljevanja (*ang. Joint Functional Component of Command)*
LIC:	Konflikt nizke intenzivnosti (*ang. Low intensity conflict*)
MNZ:	Ministrstvo za notranje zadeve
NSA:	Nacionalna agencija za varnost (*ang. National Security Agency*)
NYT:	New York Times
OMU:	Orožje za množično uničevanje (*ang. Weapons of Mass Destruction*)
PYG:	Kurdska stranka v Siriji
RMPA:	Revolucija na področju vojaške tehnologije in civilno-vojaških razmerij (*ang.Revolution in the Military and Political Affairs*)
SEA:	Sirska elektronska armada *(ang. Syrian Electronic Army)*
USSTRATCOM:	Ameriško strateško poveljstvo (*ang. U.S. Strategic Command*)
VB:	Velika Britanija (*ang. United Kingdom*)
ZDA:	Združene Države Amerike (*ang. United states of America*)
YPG:	Ljudske zaščitne enote v Siriji
WTC:	Svetovni trgovinski center *(ang. World Trade Center)*

1 UVOD

»*Vojskovanje ni več potiskanje vojakov in orožja po bojišču,*
ampak je vse bolj potiskanje elektronov in protonov«
(Loren Thompson, ameriški obrambni analitičar) (Thinkexist 1999).

Ko sta bila napadena Pentagon in WTC septembra 2001, je v svetu internet uporabljalo približno 500 milijonov prebivalcev (8% svetovne populacije). Danes se ta številka približuje 3 milijardam (okoli 40% celotnega prebivalstva), kar kaže na to kako hitro se razvija tehnologija napredka informacijskih sistemov in omrežja (Kindamo 2015, 48).

Začetki interneta segajo v sedemdeseta leta prejšnjega stoletja, ko se je pri Američanih rodila ideja o ARPANET-u, prvem predhodniku interneta. Ta pionirski paket preklapljanja omrežja je s časoma prerasel v tisti internet, ki ga poznamo danes. V prvih računalniških mrežah so bile vključene predvsem ameriške vojaške in državne ustanove, kasneje pa tudi civilne. Sprva so informacije izmenjavali zgolj preko skrbnikov sistemov, z razvojem interneta pa so se začele informacije prenašati preko poštnih programov, programov za pregledovanje vsebin (brskalnikov) (Leiner in drugi 2016). Dandanes pa večina izmenjave informacij poteka preko multimedijskih aplikacij kot so npr. Whatsapp, Facebook Messenger, Skype, Viber ipd. V teh letih so se razvijala različna orodja in programi ne samo za računalnike, ampak tudi za pametne telefone in tablice, skratka naprave, ki omogočajo komunikacijo med ljudmi in so danes v splošni rabi ter nekaj povsem običajnega.

Na nastanek interneta je vplivala še izgradnja njegove omrežne arhitekture, namreč internet nima načrtnega strukturiranja, kakor tudi ne hierarhične delitve. Sestavlja ga veliko število neodvisnih mrež, ki so med seboj povezane z enotnim protokolom TCP (ang. *Transfer Control Protocol*) / IP (ang. *Internet Protocol*)). Pomemben je pa tudi HTML (ang. *Hypertext Markup Language*) jezik, ki je osnova današnjega širjenja informacij preko interneta. Vsak uporabnik interneta je potencialni proizvajalec informacij, internet pa prostorsko dopušča neomejeno in sinhrono komuniciranje med pošiljatelji in prejemniki (Svete 2005, 20).
Internet danes omogoča globalno povezavo celotnega sveta in se je z leti preoblikoval iz akademskega igrišča v globalno redno poslovanje in komunikacijski medij. Ta sprememba je ena najpomembnejših oblik razvoja v zgodovini. Internet je globalni živčni sistem, kjer se informacije pošiljajo iz enega dela sveta v drugega (Boni in Kovacich 2000, 3, 7).

Ampak internet se ne uporablja samo za iskanje in prenašanje informacij, temveč je tudi postal pomebno orodje za nov sodobni način vojskovanja. Tisti, ki poseduje najbolj točne in ažurne informacije in spretno uporablja veščine informacijsko-komunikacijskih naprav, ima večje možnosti za zmago in tako posledično nadzor nad bojiščem in nasprotnikovimi namerami.

Če se osredotočim na pojem kibernetska oblika bojevanja, bi lahko rekla, da gre za bojevanje, ki se odvija v virtualnem svetu, nam poznanem kot internet. Kajti če dobesedno prevedem besedo cyber in jo združim z bojevanjem, dobim končni rezultat »kibernetsko bojevanje«. Če pa povzamem definicijo po Slovarju slovenskega knjižnega jezika (2000, 393), je kibernetika veda, ki raziskuje podobnost med delovanjem strojev in živo naravo. Torej, gre za primerjavo delovanja komunikacijskih mehanizmov v živih bitjih s tistimi v napravah za zbiranje informacij in izvajanje ukrepov. Namreč predpona kiber (*angl. cyber*) se nanaša na umetne organizme, računalništvo. To je bila tudi moja prva asociacija na katero sem pomislila pri kibernetskem bojevanju. Vendar pojem kibernetika zajema veliko definicij, ki se ne nanašajo samo na virtualni svet, ampak tudi na družbeni. Ena izmed takšnih definicij opredeljuje, da je kibernetika interdisciplinarna znanost, ki se ukvarja z obnašanjem tehničnih, sociotehničnih in družbenih sistemov (Wikipedia 2001).

Moje diplomsko delo se bo osredotočalo na tisto kibernetiko, ki je povezana z informacijsko-komunikacijsko tehnologijo, namreč digitalizacija informacijskih procesov je omogočila združitev telekomunikacij, televizije, računalnikov in interneta v enotno multimedijsko okolje in se tako posledično razširila v vse družbene sektorje, od zdravstva do transporta in izobraževanja (Wilson v Svete 2005, 17).

2 METODOLOŠKO - HIPOTETIČNI OKVIR

2.1 Opredelitev predmeta preučevanja

Predmet preučevanja diplomskega dela, je opredelitev koncepta kibernetskega bojevanja kot enega izmed oblik informacijskega vojskovanja. Namreč področje kot takšno, je zastavljeno širše in v povezavi z drugimi oblikami informacijskega vojskovanja gre za medsebojno povezanost delovanja. Diplomska naloga najprej opredeljuje definicije in njegovo splošno vlogo v današnji družbi, za osnovno razumevanje tega področja. V nadaljevanju pa se predmet preučevanja osredotoči na kibernetsko obliko bojevanja v Iraku in Siriji. Kibernetsko bojevanje se v obeh primerih uporablja kot neke vrste podporni sistem, ki se izvaja pred ali hkrati z vojaškimi napadi, ki potem posledično temu sledijo na terenu. Lahko bi rekla, da gre za nekakšno »predpripravo terena«, pred oboroženimi spopadi.

2.2 Cilji in namen diplomskega dela

V diplomskem delu, želim opredeliti koncept vključevanja kibernetske oblike bojevanja v širšo obliko informacijskih operacij na primerih ameriškega napada na Irak (2003) in kibernetskih napadov na Sirijo. Obe področji napadov bom analizirala, opredelila in medsebojno primerjala.

Hkrati pa bom še predstavila metode in orožje kibernetskega bojevanja, značilnosti, tarče napadov, na katerih področjih se uporablja oziroma za kakšen namen (gospodarski, politični, vojaški ipd.) ter ali je bila ta oblika bojevanja v obeh primerih, v Iraku in Siriji uspešna.

2.3 Hipoteze

- Hipoteza 1: Kibernetsko bojevanje, je eden izmed elementov informacijskega vojskovanja.
- Hipoteza 2: Uporablja se izključno samo za vojaške namene (tarče napada so samo vojaški objekti in vojaška infrastruktura), ker so glavni akterji oborožene sile, ki se bojujejo med seboj.
- Hipoteza 3: Kibernetski napadi na Irak, so bili izvršeni v okviru informacijskih operacij, v prvi fazi napadov. Irak in Sirija (državni in nedržavni akterji) nista izvajali povračilnih ukrepov s kibernetskimi napadi.
- Hipoteza 4: Kibernetski napadi v obeh državah, so bili s strani napadalcev (IS, SEA) uspešni.

2.4 Uporabljena metodologija

Metode, ki sem jih uporabila pri diplomskem delu so sledeče:

- **Metoda zbiranja ustreznih virov** (primarnih in sekundarnih)

- **Deskriptivna (opisna) metoda**

Opisna metoda je v mojem diplomskem delu najširše in najpogosteje uporabljena metoda, saj sem jo uporabila pri opredeljevanju glavnih značilnosti, ciljev in delovanja posameznih prvin kibernetskega bojevanja v ameriškem napadu na Irak in Sirijo.

- **Analiza vsebine**

Zbrala sem več pisnih virov s področja kibernetskega bojevanja, kako so ga uporabili v primerih napada na Irak in Sirijo in ali so bili napadi s strani napadalcev uspešni. Interpretirala sem predvsem sekundarne vire kot so objavljene publikacije, članke, raziskovalna področja ipd.

- **Komparativna metoda**

Zbrane definicije kibernetskega bojevanja, značilnosti, akterje in cilje sem primerjala med seboj glede na različne avtorje oziroma vire. S pomočjo te metode, sem iskala podobnosti in razlike med kibernetskim bojevanjem na področju Iraka in Sirije (načini bojevanja, metode ipd.) ter ju na koncu dela primerjala med seboj.

2.5 Temeljni pojmi

Kibernetika: veda, ki raziskuje podobnost med delovanjem strojev in živo naravo: nagel razvoj kibernetike / strokovnjak za kibernetiko (SSKJ 2000, 393). Gre za interdisciplinarno vedo, ki se ukvarja z nadzornimi in komunikacijskimi sistemi. Raziskuje tehnike, s katerimi se informacija pretvarja v želeno akcijo, primerja krmilne in komunikacijske mehanizme v živih bitjih s tistimi v napravah in išče analogije (Slovenski veliki leksikon (H-O) 2004).

Kibernetsko bojevanje: John Chipman (v Tisdall 2010) je podal eno izmed definicij, ki pravi da gre za obliko bojevanja, ki se uporablja za uničevanje nasprotnikove državne infrastrukture, za vmešavanje pri notranjih vojaških zadevah, finančnih transakcijah z namenom da bi onesposobili sovražnika.

Bratuša (2006, 1) pravi da gre za obliko bojevanja, v katerem udeleženci fizično niso omejeni na določeni prostor, saj virtualni prostor nima državnih meja.

Arquilla in Ronfeldt (1997, 28–30) pa navajata da pri kibernetski obliki bojevanja gre predvsem za konflikt na vojaški ravni. Kibernetski napad na vladne organizacije, izvršen s strani nedržavnega akterja (predvsem organiziranih skupin) pa opredeljujeta s tako imenovano internetno vojno (»netwar«), kjer gre v prvi vrsti za nenasilne akcije kot je propaganda, različne psihološke kampanje, politične in kulturne prevrate in podobno. Slednja se lahko sprevrže v kibernetsko vojno.

Drugače pa na splošno kibernetsko bojevanje zajema uporabo nezakonitega izkoriščanja različnih metod na internetu, uničenje ali prekinitev delovanja računalniških omrežij in programske opreme, hekerstvo, računalniško forenziko in vohunstvo. Gre za obliko delovanja, ki je lahko podprt s strani države ali posameznih skupin (Tisdall 2010).

3 KIBERNETSKA OBLIKA BOJEVANJA

3.1 Začetki in zgodovina kibernetske oblike bojevanja

Prva oblika kibernetskega bojevanja oziroma zametki njenih značilnosti v zgodovini so se kazali v strategiji in taktiki vojskovanja mongolske vojske (13. in 14. stoletje). Njihova moč se je kazala v znanju, ne v številčni premoči vojaških sil, medsebojni hitri komunikaciji o lokacijah njihovega sovražnika, a hkrati dobrem prikrivanju svojih sil. Tako kot danes kibernetsko bojevanje nima moč samo v močnejši in naprednejši tehnologiji, temveč je poglavitno znanje, kako nekdo razmišlja o konfliktu in strateških namerah proti nasprotniku (Arquilla in Ronfeldt 1997, 34).

Mongolska vojska pod taktirko Velikega Khana, je s svojo vojsko obvladoval največji imperij (z začetkom v Vzhodni Evropi pa območje vse do Japonskega morja) v človeški zgodovini (Wikipedia 2001). Njihov največji uspeh, je bil bojni pohod na veliki muslimanski imperij (današnji Bližnji vzhod in bivša Sovjetska zveza), kjer jim je uspelo s peščico vojske (125,000 vojaki) premagati skorajda pol milijonsko vojsko na drugi strani (Arquilla in Ronfeldt 1997, 34) Kako? Preprosto, z zavajanjem o svoji številčnosti, dobri medsebojni komunikaciji, pridobivanju informacij o lokaciji vseh nasprotnikovih sil na bojišču, zasedami, izčrpavanjem sovražnika, hitrimi učinkovitimi napadi. Khanova taktika je bila takšna, da je vedno deloval okoli sovražnika, preučeval njegove namere, nikoli ni šel direktno nanj. S tem je dokazal, da številčna premoč sil ni nujno zmaga, pomembno je znanje, pogum in veščina (Nell 2008).

Mongolsko bojevanje je tako postala osnova za kibernetsko in internetno bojevanje (Arquilla in Ronfeldt 1997, 37), kjer se napada na največja podjetja in države lahko loti majhna skupina ljudi ali celo posameznik, ki lahko povzroči milijonske finančne škode, če poseduje dovolj znanja, veščin in seveda tehnologije, da doseže svoj zadan cilj. Ko pogledamo zadevo iz vojaškega vidika, glede na to, da se kibernetsko bojevanje izvaja na vojaški ravni, morajo oborožene sile isto posedovati kar se da največ informacij o nasprotniku, ampak ne samo o vojaškem statusu temveč tudi o političnem, civilnem, kulturnem, skratka vseh ravneh države, da lahko zadajo čim močnejši udarec oziroma povzročijo čim večjo škodo, da se nasprotnik preda. Ker pa sta dandanes civilni in vojaški del sistemov prepletena in soodvisna, napadalci nimajo težav z izbiranjem tarč in ciljev.

Industrializacija je vodila k razvoju masivnih vojsk v (1. svetovna vojna), mehanizacija je omogočila v 2. svetovni vojni popolni razvoj tankov, informacijska revolucija oziroma njen tehnološki razvoj pa omogoča vzpon kibernetske oblike bojevanja. Medtem ko je v prvih dveh poudarek na fizični premoči, je pri slednji moč znanje in posedovanje informacije. Kibernetska oblika bojevanja je danes to, kar je bil Blitzkrieg v 20. stoletju. V vojskovanju danes ni več poudarka na tem kdo več vloži denarja, dela in tehnologije na bojišče, temveč kdo poseduje najboljšo informacijo o bojišču. Gre za neke vrste »vojno o znanju«, kdo ve kaj, kdaj, kje in zakaj, in o tem kako zavarovati informacije o nasprotniku. Informacija je postala vir moči, ki je zelo dragocena, saj ima takšno močno veljavo kot kapital in delo v postindustrijski dobi. Zato je pomembno kako je informacija zbrana, ohranjena, procesirana, predstavljena in kako organizacije same izkoristijo to prednost v moči (Arquilla in Ronfeldt 1997, 6–25).

Moramo pa razlikovati med omrežno vojno in kibernetsko vojno, namreč mnogi pomislijo da gre za eno in isto stvar, vendar to ni res. Pri kibernetski obliki gre za splošno informacijsko naravnan pristop bojevanja, kjer govorimo o konfliktu z visoko intenzivnostjo (v ang. HiC – *high intensity conflict*[1]) in večjih regionalnih konfliktih (v ang. MRC – *major regional conflict*) s poudarkom na vojaškem napadu s strani oboroženih sil. Medtem ko gre pri internetni vojni za družbeni konflikt z nizko intenzivnostjo (v ang. LIC – *low intensity conflict*[2]) s strani nedržavnih akterjev kot je posameznik, organizirane civilne skupine, kriminalne skupine, teroristi (Paul 2008, 3).

Glavna značilnost kibernetskega bojevanja je hitri učinkoviti napad, ne da bi nasprotnik odkril od kje je prišel napad, kdo ga je izvršil in da napad povzroči čim več materialne in finančne škode.

[1] Je najbolj učinkovita in logična metoda vojskovanja, kjer konvencionalne sile premagajo nasprotnikovo vojsko, vlada pade in prebivalstvo dobi direktivo da morajo sodelovati z zmagovalcem vojne (primeri vdaje Nemčije in Japonske v II. svetovni vojni) (McCormick v Emery 2004).

[2] Primer gverilnega bojevanja, ki nima ne moči ne sredstev da bi se direktno borila z invazijsko vojsko. Njena bistvena naloga je pridobivati prave informacije o lokacijah sovražnika na terenu in ker gre za manjše sile, same izbirajo lokacijo in čas napada na njih. V bistvu gre za obraten vrstni red od visoko intenzivnega konflikta: prvo se soočijo z ljudmi, potem državo in nazadnje šele vojsko. Cilj jim je zmagati politično, ne vojaško (McCormick v Emery 2004).

3.2 Umestitev kibernetske oblike bojevanja v informacijsko vojskovanje in njene splošne značilnosti

Informacija je strateški vir, ki je bistvenega pomena za nacionalno varnost. Vojaške operacije pa so odvisne od informacij in informacijskih sistemov, ki sočasno izvajajo integrirane dejavnosti (Joint Publication 3-13 2006).

Eden prvih, ki je začel preučevati to področje informacijskega vojskovanja, je bil Martin Libicki (1995, 7) in pravi, da kot samostojna oblika vodenja ne obstaja, obstaja pa sedem oblik informacijskega vojskovanja, ki se prepletajo znotraj tehnik vodenja vojne. Te oblike so:

- vojskovanje na področju vodenja in poveljevanja (Command and Control Warfare)
- vojskovanje na obveščevalnem področju (Information-based Warfare)
- elektronsko vojskovanje (Electronic Warfare)
- psihološko vojskovanje (Psychological Warfare)
- hekersko vojskovanje (Hacker Warfare)
- ekonomsko informacijsko vojskovanje (Economic Information Warfare)
- kibernetsko vojskovanje (Cyberwarfare)

Po Libickem (1995, 75–83) je kibernetsko vojskovanje od vseh oblik najbolj široka kategorija, ki vključuje: informacijski terorizem, semantični napad, simulacijsko vojskovanje in Gibsonovo vojskovanje.

1. **Informacijski terorizem**

Pri informacijskem terorizmu gre za napade na računalniške sisteme z namenom, da bi povzročili škodo posameznikom in ne računalnikom. Ta oblika je učinkovita predvsem v družbah, kjer avtomatizirani računalniški sistemi nadzorujejo pomebne družbene podsisteme (npr. izobraževanje, zdravstvo, poslovanje, vladno delovanje).

2. **Semantični napad**

Glavna razlika med semantičnim napadom in hekerskim je, da pri slednjem računalniški sistem preneha delovati ali pa se v celoti zaustavi. Medtem ko gre pri semantičnem napadu za prelisičenje, namreč z napadom so bile vnešene spremembe v sistem, ampak le-ta še vedno

deluje. Odgovori oziroma delovanje »novega« sistema, pa je seveda v popolnem nasprotju od tiste prave, prejšnje realnosti.

3. Simulacijsko vojskovanje

Simulacijsko vojskovanje je teoretična raven, kako naj bi nek spopad oziroma vojna izgledala v praksi. Gre za realistične simulacije, kjer pa je pravo strelno orožje zamenjano z virtualnim. Vojskovanje temelji na tem, da obe strani, ki to simulacijo uporabljata se skušata naučiti kaj je dobro in slabo ter to uporabita v praksi. Ampak vsi vemo da prava vojna ne deluje po tem konceptu, ampak po konceptu organizatorja igre.

4. Gibsonovo vojskovanje

Ta kategorija temelji bolj na znanstveno fantastičnem vidiku, kjer so osebe spremenjene v virtualne like (film Tron) v neskončnem virtualnem prostoru oziroma mreži, kjer se odvijajo boji. Gibsonovo vojskovanje naj bi predstavljalo 5. dimenzijo kibernetskega vojskovanja in je popolnoma teoretični vidik.

Kibernetska oblika bojevanja ima nekaj posebnih značilnosti, namreč le-ta lahko omogoči akterjem, da dosežejo svoje strateške in politične cilje ne da bi uporabila oborožene sile. Kibernetski prostor omogoča nesorazmerno moč majhnim in relativno nepomembnim akterjem. Napadalci lahko delujejo s popolno anonimnostjo in so lahko državne (OS) ali nedržavne narave (posamezniki, mednarodna kriminalna podjetja ali skupine, hekerske skupine). V kibernetskem prostoru so meje med vojaško in civilno, fizično in virtualno sfero zabrisane. Vojna dejanja v kibernetskem prostoru, se ponavadi pojavijo z drugimi oblikami prisile in spopadov. Ampak načini in sredstva kibernetskega bojevanja, se še vedno razlikujejo od teh oblik spopadov (Carnish in drugi 2010).

Po Arquilli in Ronfeldtu (1997, 30–31) se kibernetska oblika bojevanja nanaša na vodenje in pripravo informacijskih vojaških operacij. Kar pomeni motenje signala oziroma popolno uničenje informacijskih in komunikacijskih sistemov nasprotnika ter da imamo čim več informacij o njem, hkrati pa izvajamo obrambo na ta način, da nasprotnik izve čim manj o nas. Pri tem pametno uporabljamo znanje in informacije tako, da se ob minimalni porabi sredstev (finačnih, delovne sile ipd.), na koncu zmaga prevesi na našo stran. Ta oblika bojevanja uporablja raznolike tehnološke metode zlasti za vodenje in poveljevanje, zbiranje, procesiranje in podajanje obveščevalnih podatkov, za taktično komuniciranje in identifikacijo

sovražnika. Te metode so elektronska oslepitev, zavajanje, preobremenitev strežnikov ter vdor v nasprotnikove informacijske in komunikacijske sisteme. V prihodnosti se bo narava vojskovanja glede na razvoj tehnologije, še spreminjala. Zaradi tega bo kibernetska oblika bojevanja imela čedalje bolj pomembno vlogo, in sicer tako v nizko in visoko intenzivnih konfliktih, konvencionalnem in nekonvencionalnem okolju ter v napadalnem in obrambnem smislu.

Še ena definicija pravi, da je kibernetska oblika bojevanja veja informacijskega vojskovanja, ki izvaja ukrepe v kibernetskem prostoru[3]. Kibernetski prostor je vsak virtualni prostor, ki vsebuje set računalnikov in omrežje. Obstaja veliko kibernetskih prostorov, ampak tisto najpomembnejše za kibernetsko bojevanje je internet in omrežje, ki je dostopno medijem. Vojaška opredelitev kibernetskega bojevanja pa je kombinacija računalniško omrežnega napada (CNA) in računalniško omrežne obrambe (CND) in posebnih informacijskih operacij (Parks in Duggan 2001). Na primer Christopher Paul (2008) v svojem delu Informacijske operacije, doktrina in praksa, kibernetski napad in obrambo šteje pod računalniško omrežne operacije (CNO), ker gledano s strani definicij gre za isto razlago, samo drugo pojmovanje.
Avtorji različno klasificirajo in opredeljujejo koncept kibernetske oblike bojevanja, ampak skupno vsem definicijam je to, da je kibernetska oblika bojevanja element informacijskega vojskovanja, ki se izvaja v kibernetskem prostoru. Za izvajanje te oblike bojevanja, se uporabljajo informacijski, računalniški sistemi in omrežja. Kibernetska oblika bojevanja vključuje različne aspekte obrambe in napadov na informacijsko in računalniško omrežje v kibernetskem prostoru, in hkrati preprečuje nasprotniku, da to počne isto. V večini primerov gre za anonimne napade, zato je večkrat težko določiti izvor in izvajalca napada (Hildreth 2001). Ker ni enotne definicije o kibernetskem bojevanju, bom v svojem delu uporabila pojem kibernetsko bojevanje za vse, kar je povezano z računalniškimi sistemi in omrežji v primeru napada ali obrambe, torej se bom opirala na ameriško vojaško definicijo.

Vsaka konvencionalna oborožena sila države mora biti dobro opremljena in organizirana. Slednja je odvisna od dobre razporeditve pravih informacij v točnem obsegu in času. Zato vsaka vojska potrebuje dobro informacijsko in telekomunikacijsko omrežje, logistiko in vsaka sila mora poznati svojega sovražnika. Čeprav je danes glede na tehnologijo razvoja

[3] Kibernetski prostor je medsebojna povezanost ljudi preko računalniških in telekomunikacijskih naprav ne glede na fizično lokacijo. Izraz se uporablja kot metafora za nefizični teren računalniških sistemov. Tako kot fizični prostor, kibernetski prostor vsebuje predmete (datoteke, maili, slike, sporočila ipd.) in različne načine prenašanja le-teh (Hildreth 2001).

informatike komunikacija hitrejša, je bolj pomembno da so informacije točne. Kajti vojaške enote, da so uspešne pri svoji nalogi, morajo biti na terenu točno razporejene in vse to je odvisno od točnih informacij. To vse kaže, da se vse oborožene sile čedalje bolj nanašajo na hitro komunikacijo in točne informacije, ampak hkrati se ne zavedajo kako hitro lahko le-te postanejo sredstvo z veliko vrednostjo (Cyber Warfare). Računalniška tehnologija je intergirana komponenta skoraj vsakega modernega orožja, od tistih večjih sistemov pa vse do tiste na osebni ravni oborožitve vojaka. Zato prekinitve ali motenje takšnih sistemov, lahko nevtralizirajo celo najbolj načrtovano obrambno strategijo (Kindamo 2015, 48).

3.3 Uporaba ciljev, metod in orožja napadov kibernetskega bojevanja

Kibernetsko bojevanje je lahko konflikt med državami, vendar lahko na različne načine vključujejo tudi nedržavne akterje. V kibernetskem bojevanju je zelo težko natančno predvideti cilj napada. Lahko je vojaški, industrijski, civilni ali pa samo strežnik, ki gosti širok spekter strank, izmed katerih je samo ena tarča napada (Carnish in drugi 2010).
Primeri, kjer so bili cilji tako vojaške kot civilne narave, je bil ruski kibernetski napad na Gruzijo leta 2008[4] in napad na Estonijo[5] leto poprej, kjer so bili cilji bolj gospodarske in politične narave. Če gledamo iz vidika uspešnosti, je bil do danes najbolj uspešen kibernetski napad na domnevni sirski nuklearni reaktor v izgradnji. Zakaj? Ker je v letu 2007 imela Sirija eno najbolj prefinjenih in večplastnih omrežij zračne obrambe na svetu, za katero je skrbelo 60,000 vojakov. Opremljena je bila z najbolj uničujočimi izstrelki zemlja-zrak. Kljub temu je Izraelu uspelo uničiti reaktor, ker so skupaj z vojaškim letalskim napadom izvedli elektronski in kibernetski napad na vojaške sisteme. Izklopili so celoten obrambni sistem države in to samo v nekaj sekundah (Mahon 2016, 68). Najbolj znan kibernetski napad, izveden v popolni tajnosti in ga smatrajo za začetnika kibernetskega bojevanja pa je bila operacija Stuxnet

[4] Množični kibernetiski napadi na vladne in spletne strani so se dogajali v času rusko-gruzijskega spora (Južna Osetija, Abhazija) v avgustu 2008, s čimer je kibernetsko bojevanje dobilo kokretnejšo obliko. S temi dejanji Rusi niso povzročili fizične škode, so pa ohromili delo gruzijske vlade, saj so onemogočili komuniciranje z domačo in mednarodno javnostjo (Theiler 2011).
[5] Številni kibernetski napadi na vladne, bančne, medijske strani zaradi premika kipa (postavljen v bivši Sovjetski zvezi) iz centra prestolnice Talin. Šlo je predvsem za distribuirane napade onemogočanja storitev (ang. distributed denial of service), sledi so vodile vse do vladnih strežnikov v Rusiji, vendar so ruski uradniki sprva zanikali vpletenost v napade. Glede na to, da Estonija velja za eno najbolj omrežno povezanih držav (prva država, ki je omogočila elektronsko glasovanje svojim državljanom leta 2005 na volitvah), so ti trije tedni napadov ohromili vsakdanje življenje Estoncev, namreč kar 97% bančnih transakcij preko spleta, se izvaja na dnevni bazi. Ti dogodki so sprožili debato o varnosti in ranljivosti informacijsko-komunikacijskih sistemov številnih držav (Wikipedia 2001). Zveza NATO je v letu 2014 sprejela kibernetsko bojevanje v obrambno politiko držav članic, čeprav so to predlagali že v letu 2008. »Politika Nata za kibernetsko obrambo« priznava da se načela mednarodnega prava upoštevajo tudi v kibernetski domeni, ne samo fizični (Kindamo 2015, 48).

(zgodila v letu 2010). Šlo je za dobro organizirano in pripravljeno sofisticirano obveščevalno-vojaško operacijo, kjer je bil cilj napada iranski jedrski obrat Natanz, globoko pod zemeljsko površino. Stuxnet[6] je tako postala prva najbolj znana programska oprema, ki so jo uporabili pri kibernetskem bojevanju. S to operacijo so preprečili Iranu, da bi v obdobju 2014–2015 prišel do operativnega jedrskega orožja. Kot alternativo neuspešnemu kibernetskemu napada, so imeli Američani pripravljeno akcijo bojnega letalstva iz Izraela ali iz ZDA ob uporabi najdražje in zelo rušilne bombe MOP (ang. Massive Ordnance Penetrator), ki se uporablja za preboj jedrskih bunkerjev, za vodenje bombe pa se uporablja GPS (Aršič 2015, 33). V tem primeru, je šlo za vojaški-obveščevalni napad na vojaški objekt s strani oboroženih sil Izraela in ZDA.

Kibernetski napadalci (državni ali nedržavni) skušajo destabilizirati družbo na gospodarski, kulturni, finančni in politični ravni, se pravi popolnoma uničiti kritično infrastrukturo, ki so življenjskega pomena vsakega državljana (Mahon 2016, 68). Takšni napadi lahko popolnoma ohromijo državo, če ne celo uničijo. Ampak ravno zaradi te prepletenosti med vojaško in civilno sfero, so države previdne pri uporabi tovrstnega bojevanja. Zato se s kibernetskimi napadi v veliki večini bolj prikazuje premoč neke države, kot pa se dejansko povzroči neka fizična škoda, razen seveda v primerih kjer bi lahko bile posledice globalne narave (npr. Iran - Stuxnet).

Metode kibernetske napadov bodo še naprej imele neposredne nevarnosti za organizacije, ki delujejo v javnem in zasebnem interesu. Po Mukaramu (2014) ločimo 5 metod kibernetskega bojevanja:

- **Vztrajna napredna grožnja (ang. Advanced Persistent Threat - ATP):**

  je bolj značilna za koordinirane napadalce, ki so osredotočeni na en sam cilj. Cilj pa je da bi vdrli v ranljiv operacijski sistem in ostali neopaženi kolikor dolgo je mogoče. ATP je postal priljubljen pristop za tiste, ki opravljajo kibernetsko, korporativno in obveščevalno vohunjenje. Nobena tehnologija ali proces ne more ustaviti ATP, tradicionalne varnostne metode so se izkazale za neučinkovite proti tem grožnjam. Zaščita pred ATP zahteva več plasti obrambe, znanje in veščine za čimprejšnje odkrivanje in reagiranje na tovrstne

[6] Računalniški črv, ki je okužil sisteme v 14 obratih, povezanih s predelavo urana in ostalimi deli iranskega jedrskega programa (Aršič 2013, 33). Od virusa se razlikuje v tem, da se razmnožuje sam brez gostitelja, kar pomeni da zna samodejno preslepiti sovražnika, da ga zažene. Na začetku, ko vstopi v sistem (preko USB ključa) sprva vohuni v ciljnem sistemu. Potem pa ko pridobi ključne podatke, prevzame nadzor in tako poskrbi za neuspeh sistema, še preden ga tvorci sistema sploh opazijo in skušajo odpraviti. Črv ne povzroči samo programsko škodo sistema, ampak tudi fizično (Wikipedia 2001).

napade. Zaradi ATP, se je posledično razvil kibernetski pristop nepretrgana vztrajna kontrola (ang. Continous Persistent Monitoring – CPM).

- **Distribuirani napadi onemogočanja storitev (ang. Distributed Denial Of Service – DDoS):**

Metoda omogoča hekerjem, da »sesujejo« žrtev in ne ukradejo njenih osebnih podatkov. Tu gre za poplavo omrežja z ogromnimi količinami podatkov. Glede na to, da je ta metoda v primerjavi z drugimi tehnično manj zahtevna, je ne bi smeli podcenjevati. Rezultat takšnega napada, je počasno delovanje spletne strani. Uspešno izveden DDoS napad ponavadi onemogoča dostop do internetne domene, vendar to ne vpliva na notranji računalniški sistem organizacije. Če podjetja upoštevajo osnovne varnostne zahteve, njihov finančni in poslovni sistem in druga osnovna struktura, naj ne bi doživela takšnih napadov.

- **Navzkrižna platforma zlonamernih programov (ang. Cross-Platform Malware)**

Zlonamerni programi niso več eksluzivni samo pri napadih na Windows operacijske sisteme, temveč tudi na iOS sisteme (operacijski sistem iPhone). Gospodarska spobuda za izgradnjo zlonamernih platform, narašča z naraščajočim številom sistemov, ki uporabljajo drugačne operacijske sisteme od iOS. Kar bo neizogibno povečalo število napadov na CPM.

- **Metamorfni in polimorfni zlonamerni programi (ang. Metamorphic and Polymorphic Malware):**

Ta kategorija škodljive programske opreme nenehno spreminja svojo kodo, tako da se za vsako od svojih naslednjih različic razlikuje od prejšnje. Metamorfni in polimorfni zlonamerni programi predstavljajo največjo grožnjo vsem organizacij v svetu, saj lahko izogne odkrivanju anti-virusnim programom. Za izdelavo teh programov je potrebno veliko znanja in veščin, saj zahteva zapletene tehnike pisanja kot so preimenovanje registra, koda permutacije, širjenje in krčenje kode, vstavljanje odpadne kode. Ampak to ni ovira za tiste, ki obvladajo ta posel. Več in več podjetij se zanaša na odprtokodne spletne aplikacije, ki odpirajo pot za dovzetnost do metamorfnih in polimorfnih zlonamernih programov. Hootsuite je primer odprtokodne platforme namenjena za javni prenos, katero številna podjetja uporabljajo za upravljanje svojih Twitter računov. Napadalci imajo enostaven dostop do takšnih platform, zato se jim ni težko naučiti vse

ranljivosti, ki jih uporabijo pri pisanju svojih kod in se tako se izognejo varnostnim zahtevam.

- **Ribarjenje (ang. phishing):**

  Ta metoda deluje preko e-pošte in ideja o tej e-pošti temelji na neizključni komunikaciji kar pomeni, da vsakomur omogoča da kontaktira kogarkoli, ne glede na to kdo je. To komunikacijo pa izkoriščajo napadalci, ko pošiljajo e-pošto v imenu nekoga drugega s okuženimi priponkami ali povezavami. Ko nekdo na drugi strani odpre to e-pošto s priponko ali povezavo, avtomatsko omogoči nadzor nad njegovim računalnikom.

Po viru Cyber warfare so orožja, ki se uporabljajo pri kibernetskem bojevanju odražajo glede na namen njihove uporabe (zaznavanje, zavajanje, identifikacija nasprotnika, preprečevanje dostopa do sistema, napad na sistem). Večinoma so prosto dostopna na internetu, razen tista specifična ali novejša ki se nadalje tržijo bodisi za dobiček (zasebni industrijski sektor) ali nikoli ne pridejo na prosti civilni trg prodaje (vojaška). Ta orožja so za:

1. **Zaznavanje nasprotnika**

Sistemi v tej kategoriji imajo cilj, da zaznajo napadalce in jih identificirajo, kaj je njihov namen in kje je njihova lokacija. Zaznavanje temelji na znanju in vedenju strokovnjakov, kdaj se takšna oblika grožnje pojavi. Orodja, ki se uporabljajo pri tem so: sistemi za detekcijo vdora, varnostni pregled, analiza vpisa.

2. **Preprečitev dostopa do sistema**

Ustavitev napadalca, je primarni cilj četudi napad še ni bil identificiran oziroma se ni zgodil. Večina napadov so preprosti in enostavni, v bistvu gre za testiranje ali so virtualna vrata odprta in najboljša preventiva je, da jih zaklenemo. Glavna orodja v tej kategoriji so: požarni zid, sistemi za preverjanje pristnosti in sistemi za preverjanje avtorizacije.

3. **Identifikacijo cilja**

V to kategorijo spadajo skenerji in sicer: omrežni skenerji, sistemski skenerji in skenerji za preverjanje ranljivosti sistema.

4. **Napad**

Sem spadajo vsa orodja, ki izkoriščajo ranljivost sistema in njeno uporabo, da dosežejo končni cilj, ki ga določi napadalec. V tej kategoriji je teh orodij ogromno, zato bom navedla le tiste, ki se najbolj uporabljajo v praksi: internetni črvi, kjer gre za avtomatska orodja, ki izkoriščajo ranljivosti operacijskega sistema in imajo sposobnost samorepliciranja iz enega sistema v drugega. Druga skupina teh orodij so trojanski konji, ki se uporabijo na sistemu za dostop do podatkov preko skritega kanala dostopa, da se pridobijo podatki in informacije. Potem imamo skupino računalniških virusov, ki ob aktivaciji okužijo sistem z zlonamernim programom (ang. malware). Virus se razmnožuje tako, da se reproducira in okuži vse programe v sistemu in jih spreminja. Vohunski program je naslednja skupina, ki se uporablja za napad, njegov cilj je zbiranje podatkov o osebi ali organizaciji (brez njihove vednosti), ki jih pošilja napadalcu oziroma lahko prevzame tudi nadzor nad računalnikom (Wikipedia 2001).

5. **Zavajanje nasprotnika**

Zavajanje se uporablja v primeru, ko se izvede napad na nasprotnika, da se odvrne njegovo pozornost. Sem spadajo: orodja, ki prilagajajo oziroma spreminjajo vpis (ang. log modifiers), porazdeljeni napadalni sistemi (ang. distributed attack systems), rootkiti (ang. rootkits) in prikrita orodja (ang. stealth tools).

Kibernetska orožja so dejansko računalniški programi, ki so sposobni prekiniti delovanje podatkovnih baz ali predelati logično delovanje nasprotnikovih računalniških sistemov. Delijo se na orodja, ki se uporabljajo pri napadih na sistem kot so virusi, trojanci, orodja za onemogočanje dostopa do storitev, druga skupina so t.i. »dvojna uporaba« orodij, kamor uvrščamo skenerje ranljivosti sistema in orodja za nadzor omrežja in navsezadnje še orodja, ki se uporabljajo pri obrambi sistemov kot so požarni zidovi in šifriranje (Wilson 2006).

Del kibernetskega bojevanja so računalniško omrežne operacije (CNO), ki imajo sposobnost napadati in onemogočati nasprotnikovo računalniško omrežje, braniti vojaške informacijske sisteme ter izkoriščati nasprotnikovo omrežje preko zbiranja informacij. Sestavljajo jih 3 elementi, ti so:

- **Računalniško omrežni napad** (*ang. Computer Network Attack*):

Operacije, ki onemogočajo oziroma uničijo računalniške sisteme in omrežja. CNA temelji na toku podatkov, ki se uporablja kot orožje pri izvrševanju napadov. Na primer pošiljanje signalov preko digitalnega toka, da se izklopi energijski tok nasprotnikovega omrežja.

- **Računalniško omrežna obramba** (*ang. Computer Network Defense*):

Obrambni ukrepi, ki varujejo informacije, računalnike in omrežja pred prekinitvijo in uničenjem omrežja. CND vključuje nadzor, odkrivanje in odzivanje na nedovoljene dejavnosti računalnikov. Orodja, ki se uporabljajo pri CND so požarni zidovi in šifriranje podatkov ali ukrepe nadziranja nasprotnikovega računalnika, pri katerem določijo njegove sposobnosti preden le-ta napade vojaško informacijsko strukturo.

- **Računalniško omrežno izkoriščanje** (*ang. Computer Network Exploitation*):

je tehnika s pomočjo katere se uporabljajo računalniška omrežja, da bi prodrli v omrežja in sisteme računalnikov nasprotnika, s ciljem pridobivanja in zbiranja obveščevalnih podatkov. Orodja, ki se pri tem uporabljajo so podobna tistim, ki se uporabljajo za CNA, ampak s to razliko da se samo pridobivajo obveščevalni podatki, se ne prekinja sistem delovanja kot pri CNA. V bistvu gre za vohunjenje, kjer se pridobivajo podatki o ranljivosti nasprotnikovih sistemov in pridobivanja informacij zaupne narave (Wilson 2006).

3.4 Oblike kibernetskega bojevanja

Po Carnishu in drugi (2010) ločimo 4 oblike kibernetskega bojevanja:

- **Kibernetski terorizem in ekstremizem:** pojav asimetričnosti v kibernetskem prostoru in njegovih skritih globinah, postaja dragocen vir za nedržavne akterje kot so teroristične in ekstremistične skupine. Namreč tem skupinam internet predstavlja eden najbolj poglavitnih virov za financiranje, rekrutiranje pripadnikov in širjenje svojega propagandnega sporočila. Kajti živimo v svetu, kjer komunikacija večinoma poteka preko socialnih omrežij, novičarski mediji so večinoma digitalizirani, plačilni promet v veliki meri poteka na spletu, vse je dostopno preko mobilnih aplikacij ipd.[7]

[7] Teroristi (Lashkar-e-Taiba), ki so v Mombaju novembra 2008 izvedli teroristični napad, so pri svojem delu uporabili GPS sisteme in mobilne naprave za pripravo konvencionalnega napada na civiliste. Tehnologijo so uporabili za snemanje in podrobno poizvedovanje o ciljih napada, ter medsebojno komunikacijo in za prejemanje taktičnih navodil strelcem napada (Carnish in drugi 2010).

- **Kibernetsko vohunjenje:** je ena najbolj razširjenih kibernetskih dejavnosti in se uporablja za odkrivanje občutljivih vladnih informacij, krajo poslovnih podatkov ali samo kot izvidovanje nasprotnikovih namer. Vohunjenje je že dolga leta ustaljena praksa fizičnega sveta, ampak v kibernetskem prostoru se skupaj s tehnologijo napredka še vedno razvija. Obstaja pa zavedanje, da je ta oblika bojevanja čedalje pogosteje uporabljena samo iz enega razloga, ker se njeno orožje (trojanci, logične bombe) infiltrira v sistem in tam ostane toliko časa, dokler čas in okoliščine zahtevajo, seveda brez vednosti lastnika. Ko se ta aktivira, omogoči napadalcu, da prevzame popoln nadzor nad sistemom preden se žrtev napada zaveda. Takšni kibernetski napadi, če so časovno pravilno usklajeni, lahko povzročijo ogromno škodo in povzročijo politično napetost ali se uporabijo kot podporni sistem konvencionalnega bojevanja.
- **Gospodarski kibernetski kriminal:** z razvojem tehnologije, je vedno več možnosti, da finančne institucije postanejo tarče kibenetskih napadov. Temu pravijo kibernetski kriminal, ki je dobro organiziran z resnimi napadi na vlado, podjetja in javne institucije z namenom pridobivanja denarja ali blaga. Kot vojno stanje se opredeli takrat, ko gre za obstojne, dolgotrajne napade in predstavlja nevarnost za nacionalno bilanco stanja, ki bi bilo škodljivo za industrijo in družbo kot celoto ter posledično vplivajo na varnost in stabilnost države. To obliko bojevanja, bi morale vse države vključiti v svojo nacionalno strategijo kot je to storila Velika Britanija in ne bi smelo vso breme boja pasti na pleča finančnih institucij. Po besedah Jeffrya Carra (Carnish in drugi 2010), naj bi se tehnike razvoja kibernetskega kriminala odvijale v kriminalnem laboratoriju, kjer njihovi uporabniki testirajo in razvijajo nove različice orodij in prijemov.
- **Psihološko kibernetsko bojevanje:** oblika bojevanja, kjer gre za ukrepe in prijeme psiholoških elementov vplivanja na žrtev kibernetskega napada. Sistemi kritične infrastrukture še v mnogih pogledih predstavljajo nacionalno ranljivost in slabost države. To povzroča občutke negotovosti kot se je že dokazalo v primerih Stuxneta in Titan Rainovih epizod v ZDA in VB. In ravno ta občutek porajanja negotovosti lahko postane cilj napadalca, na enak način kot ga povzroča terorizem**.**

4 UPORABA KIBERNETSKE OBLIKE BOJEVANJA NA PRIMERU IRAKA (2003) IN SIRIJE (2011)

V tem poglavju bom splošno predstavila vsak posamezni konflikt v obeh državah in nato posamezno po točkah opredelila in predstavila časovnico ter značilnosti kibernetskega bojevanja. V času intepretacije primarnih in sekundarnih virov, bom preverila še zadnji dve hipotezi, ki sem si jih zastavila na začetku diplomske naloge, in sicer ali so bili kibernetski napadi na Irak in Sirijo s strani napadalcev uspešni in o tem ali so bili kakšni povračilni kibernetski napadi.

4.1 Operacija Iraška svoboda (2003)

Iraška vojna, znana pod imenom II. Zalivska vojna ali Operacija Iraška svoboda se je začela 20. marca 2003 z vojaško invazijo s strani večnacionalnih sil[8], ki so jo vodile ZDA. Vojaški napad se večinoma opredeljuje kot ameriško-britanski, ker je bila sestava vojaških enot v času invazije v večini samo ameriška in britanska (ob pomoči avstralskih in poljskih OS). Glavni povod za to vojaško operacijo je bila domnevno iraško posedovanje OMU (orožje za množično uničevanje), ki naj bi predstavljajo predvsem grožnjo zahodnem delu sveta. ZN (Združeni narodi), ki so poslali svoje inšpektorje v Irak, da bi preverili obstoj takšnega orožja, niso našli ničesar. S programom OMU so v Iraku končali leta 1991, ampak če bi mednarodne sankcije proti državi dvignili, je obstajala možnost da bi Hussein nadaljeval z nadaljno proizvodnjo OMU. To je bil samo eden izmed številnih razlogov zakaj je ZDA tako vztrajala pri tej invaziji, poleg ostalih da naj bi Saddam Hussein podpiral teroristično organizacijo Al Kaido (povezavo med njima niso nikoli našli), potem finančno podpiral palestniske samomorilce in nenazadnje kršil človekove pravice s svojim diktatorskim režimom[9]. Slednji je bil na koncu poglaviten razlog koalicijskih sil za invazijo, da so širile demokracijo in svoboščine v državi. Kljub nasprotovanju nekaterih velesil (Nemčija, Francija) in nezadostnih dokazov o obstoju OMU (na tem področju popolnoma zatajila ameriška obveščevalna

[8] »Koalicija voljnih« je termin, ki ga je uporabil Colin Powell (ameriški državni sekretar v času Busheve administracije), za tiste države ki so podprle ameriško invazijo na Irak. V tem primeru ni šlo samo za vojaško pomoč v obliki OS, ampak tudi kasneje za povojno pomoč. V to koalicijo so bile ob začetku napada vključene naslednje države: Afganistan, Albanija, Azerbejdžan, Avstralija, Bolgarija, Češka, Danska, Eritreja, Estonija, Etiopija, Filipini, Gruzija, Italija, Japonska, Južna Koreja, Kolumbija, Latvija, Litva, Madžarska, Makedonija, Nizozemska, Nikaragva, Poljska, Romunija, Salvador, Slovaška, Španija, Turčija, Uzbekistan in Velika Britanija (Schiffers v Zupančič 2006).

[9] V Husseinovem režimu, je poglavitno vlogo imela iraška stranka Baas (30 letno neprekinjeno vladanje), s pomočjo katere se je posvetna vlada utrdila in razširila svoj vpliv na vsa področja države, od politike, gospodarstva, šolstva pa vse do policije in OS. Pri tem je imel zelo pomembno vlogo represiven državni aparat, ki je zatrl vse poskuse iraške opozicije, da bi spremenila režim v državi (Žabkar 2003).

agencija – CIA) je marca Operacija Iraška svoboda doživela svojo izvedbo na iraškem terenu (Wikipedia 2001). V primerjavi s prvo zalivsko vojno, kjer so države (Savdska Arabija, Katar, Oman, Bahrajn in Združeni arabski emirati) na Bližnjem vzhodu leta zaveznikom odstopile svoje baze, infrastrukturo, nekatere še svoje vojaške enote, je bila v tej drugi zalivski vojni situacija ravno nasprotna. ZDA so lahko uporabile le kuvajtsko ozemlje, ki pa ni imelo strateške globine. Namreč Kuvajt je tipično puščavsko ozemlje, brez topografskih objektov, ima neugodne razmere za bivanje, dekontaminacijo, maskiranje in za celotno oskrbo OS. Pa glede na to, da je večina prebivalstva zgoščena v luki Kuvajt, so zavezniške vojaške sile pripomogle k visoki gostoti žive sile na kvadratni kilometer, kar je bil nevaren dejavnik tveganja v primeru da bi Irak izvedel protinapade in pri tem uporabil OMU (za katere so bili zavezniki prepričani da jih ima). Izhodiščna črta napada zavezniških sil na Irak, je bila v tej vojni v primerjavi s prvo kar 5-krat krajša, merila je samo 200 kilometrov. Tako da strateško gledano je imela zavezniška vojska kar težko nalogo. Vojaško invazijo na Irak je vodil general Tommy Franks, ki je imel nalogo da čim prej konča vojno, da se stanje v državi ne bi spremenilo v spopad med suniti, šiiti in Kurdi oziroma v humanitarno katastrofo regionalnih razsežnosti. Ker je iraška vlada napovedala, da bodo poglavitni boji potekali v glavnem mestu Bagdad, je bila glavna strateška os premikanja zavezniških sil v smeri Kuvajt-Bagdad skozi puščavo. Pot je bila dolga 500 kilometrov in je bila 2,5-krat daljša od tiste prejšnje v prvi vojni. Glavne zavezniške OS na tej poti je moral general Tommy Franks zavarovati pred iraškimi bočnimi napadi. Na severu Iraka so zavezniki podprli Kurde s specialnimi silami in letalstvom, zato te iraške sile niso sodelovale v bojih proti zaveznikom na jugu države (Žabkar 2003).

Zavezniške sile so imele v primerjavi z iraškimi zračno premoč. V primerjavi s prvo zalivsko vojno, so pri tokratni drugi uporabili spremenjeno vlogo letalstva, in sicer letala ki so v 20 dneh opravili več kot 30.000 poletov niso več podpirala kopenske vojske le posredno (z napadi na logistične baze, radarske, komunikacijske ipd.), temveč tudi neposredno z odzivom na klic kopenskih enot (napadi na iraške cilje, ki so jim zapirali prodor v globino osrednjega iraškega ozemlja). Informacije meteoroloških, navigacijskih in obveščevalnih satelitov je z revolucijo na področju razvoja vojaške tehnologije (angleška kratica RMA[10]), omogočila da podatki niso več bili dostopni samo poveljnikom in vojaškim štabom divizij in brigad, ampak

[10] Revolution in Military Affairs; Če je bil prvi vojni glavni tehnološki napredek GPS in naprave za termalno nočno opazovanje, so bili v drugi vojni vodljivi letalski projektili in bombe (uporaba med 80-90%), ki so bili satelitsko vodeni (Žabkar 2003).

tudi poveljnikom nižjih enot oziroma posameznim vojakom, pilotom. Na ta način so uspešneje izvajali svoje naloge, ker so bile informacije, ki so jih pridobili s pomočjo napredne tehnologije točne, ažurne in hitre. Z razvojem tehnologije se jim je odprla pot uspešnejše uporabe orožja in opreme. V tej vojni so zavezniki uporabili 4-krat manjše število pripadnikov kopenske vojske in 3-krat manjše število letalskih poletov. Vojna je do zasedbe Bagdada trajala 22 dni (kopenske in zračne operacije so se v tej vojni izvajale vzporedno in ne zaporedno kot v prvi) (Žabkar 2003).

4.1.1 Kibernetska oblika bojevanja v Operaciji Iraška svoboda

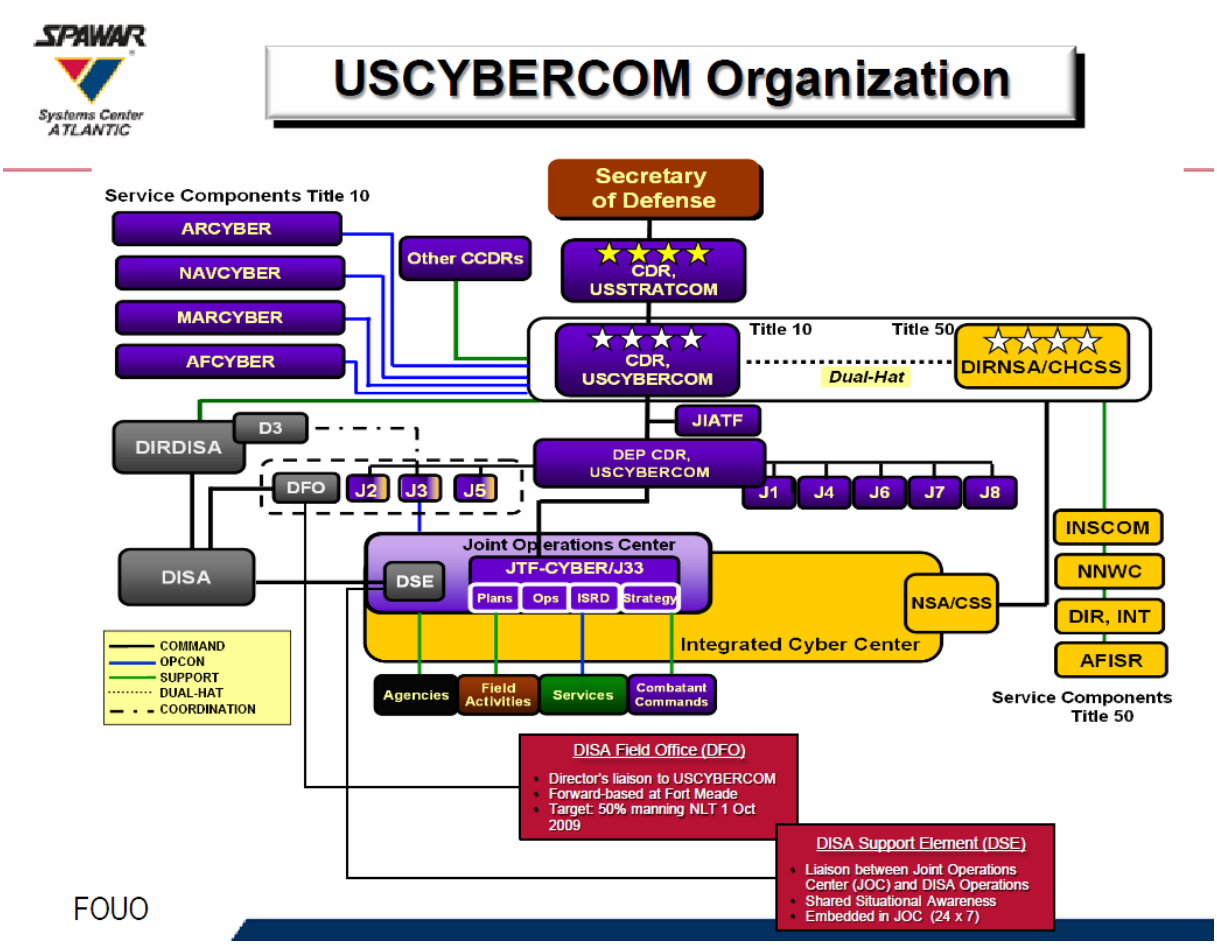
Ameriški predsednik Bush mlajši je pred napadom na Irak, prvič podpisal skrivno direktivo o razvoju kibernetskih napadov na računalniško omrežje nasprotnika na nacionalni ravni, ki je določala kdaj in kako so ZDA izvajale kibernetske napade. Gre za pravilnik o tem, kako naj bi ZDA vdrle in motile delovanje tujih računalniških sistemov. Namesto, da bi tvegali letala in vojaške enote, so si vojaški načrtovalci zamislili vizijo o tem, kako bi vojaki za računalniki potihem vdirali v računalniško informacijske sisteme nasprotnika in tako onemogočali radarje, električne naprave, telefonske storitve, komunikacije poveljstva ipd. Ta direktiva je znana pod imenom Nacionalno varnostna predsedniška direktiva 16 in je zajemala smernice o ofenzivnih kibernetskih operacijah proti Iraku (razvojnim programom kemičnega, biološkega in nuklearnega orožja). Šlo je za sodelovanje med vojaško in civilno sfero (gospodarstvo, akademiki iz MIT[11]). Mnogi civilni strokovnjaki na tem področju, so bili do uporabe kibernetskih napadov v vojaške namene skeptični. In sicer, ravno zaradi prevelike vpletenosti računalniškega omrežja v vseh sferah države, ki je kazala na veliko ranljivost za protinapade. Zato so nekateri zavrnili sodelovanje pri projektu. Pod to direktivo je imel Pentagon 3 naloge: eksperimentirati z kibernetskimi orožji in čim bolje spoznati njihovo učinkovitost, normalizirati uporabo teh orožij in jih uporabljati kot sestavni del ameriške oborožitve ter nenazadnje usposobiti profesionalni kader vojakov kibernetskega bojevanja. Cilji kibernetskega bojevanja so bili v direktivi opredeljeni kot striktno vojaški, v primeru pa da bi prišlo do napada na civilno omrežje in sisteme, je bila naloga vojske čim bolj minimizirati civilno škodo. Učinkovitost in natančnost kibernetskih napadov sta bili odvisni od natačnih obveščevalnih informacij o nasprotnikovem omrežju in sistemih, zato je bilo sodelovanje Pentagona z ameriškimi agencijami (FBI, CIA in NSA) še kako ključno (Graham 2003).

[11] Inštitut tehnologije Massatchusettsa

Ameriška vojska nima enotne definicije kibernetskega bojevanja, poimenuje jo z različnimi termini kot so informacijsko vojskovanje, informacijska varnost, kibernetska varnost in nenazadnje kibernetsko bojevanje, izraz ki je pojem opredeljevanja v mojem diplomskem delu. Če še enkrat povzamem ameriško vojaško definicijo kibernetskega bojevanja (*ang. Cyberware*) po avtorjih Anderssenu in Winterfeldu (2014, 53), ta termin v ameriški vojski zajema vse kar je povezano z CNO, operacije ki sem jih opredelila že predhodno. Glavna doktrina, ki opredeljuje uporabo kibernetskega bojevanja za vse ameriške sile, se imenuje Skupna doktrina za kibernetiko (JP3-13)[12], objavljena 2006. O vprašanju vodenja mednarodnih kibernetskih misij in kateri organ je strateško odgovoren za vodenje le-teh, so razpravljali v vojaških in političnih krogih zadnjih nekaj let. Namreč v ameriški vojski posamezne zvrsti kot so vojska, letalstvo, marinci in mornarica vodijo vsaka zase kibernetske operacije. Ampak ne glede na to, je strateška odgovornost za CNO padla na bremena Ameriškega strateškega poveljstva (ang. USSTRATCOM) in NSA, ki je odgovorna za obrambo celotnega vojaškega omrežja. Povezava med NSA in Strateškim poveljstvom se odraža na ravni Skupne funkcionalne komponente poveljevanja (JFCC) imenovano tudi kot Skupna funkcionalna komponenta poveljevanja kibernetskega bojevanja, katere poveljnik je direktor agencije NSA. Poveljstvo, ki je direktno odgovorno Strateškemu poveljstvu in izvaja kibernetske operacije pa se imenuje Ameriško kibernetsko poveljstvo (*ang. U.S. Cyber Command – CYBERCOM*), zasnovano je bilo v času Busheve administracije, s svojo funkcijo pa je nastopil šele leta 2010 (s predsedniškim mandatom Barracka Obame). Poveljstvo se nahaja v Fort Meadu (Carr 2010, 176) (glej sliko 4.1). Slika 4.1 prikazuje celotno organizacijsko strukturo CYBERCOM, odgovorno Strateškemu poveljstvu in podrejeno ameriškemu Ministrstvu za obrambo. Kibernetska komponenta pa je vpeta v vsako zvrst ameriških OS (vojsko, mornarico, marince in letalstvo).

[12] Doktrina, ki ureja aktivnosti in izvajanje skupnih operacij OS ZDA, določa smernice za vojaško koordinacijo in sodelovanje z drugimi vladnimi službami in agencijami, v času izvajanja mednarodnih vojaških operacij (Joint Publication 3-13 2006).

Slika 4.1: Organizacijska struktura CYBERCOM



Google (1998).

Iraška telekomunikacijska in računalniška strukura v letu 2003 ni bila razvejana po celotni državi, večinoma je bila prisotna samo v večji iraških mestih (telekomunikacije pod nadzorom Husseina, saj je le tako lahko vladal z železno roko nad svojimi državljani). V vojski so imeli ruske računalniške sisteme in optične kable, ki so jih namestili Kitajci (CNN 2003). Dostop do interneta je imelo le 12,000 Iračanov (večinoma iraška vojaška in civilna elita) od 23,5 milijona prebivalcev, država je bila ena zadnjih na Bližnjem vzhodu, ki se je kasneje po ameriški invaziji priključila na internetno omrežje. Vojaški računalniki z občutljivimi podatki pa sploh niso bili povezani na internetno omrežje (BBC News 2003). Iraška vojska ni imela vojaške enote ali oddelka, ki bi se ukvarjal s kibernetskim bojevanjem, tako da so bile v tem pogledu ZDA v veliki prednosti. In zaradi tega bo moja pozornost glede kibernetskih napadov usmerjena v ameriški način kibernetskega bojevanja, ker povračilnih ukrepov s strani Iraka v tej operaciji, ni bilo.

Čeprav je bil Irak v uporabi IKT manj razvit in je imel restriktivno internetno in informacijsko politiko, se je zavedal pomena IKT in interneta, predvsem v smislu vplivanja na mednarodno javnost. Na uradni spletni strani iraškega predsednika so predstavili njegova stališča in izjave o aktualnem dogajanju v državi, ki jo je vodil. Stran je bila napisana tako v angleščini (za mednarodno javnost) kot tudi v arabščini. Poleg tega pa naj bi internet uporabljale iraške obveščevalne službe za strateško pridobivanje informacij o analizah, navodilih in primerih psihološkega bojevanja ameriške vojske. En del kibernetskega bojevanja se je izvajal že pred samim vojaškim napadom na Irak, in sicer ameriški hekerji so v februarju 2003 spremenili povezave na spletni strani iraškega časopisa Iraq Daily in jo preusmerili na svojo stran, kjer so širili svojo resnico o dogajanju v Iraku (Svete in Žabkar 2006, 287, 291).

Kibernetsko bojevanje v Operaciji Iraška svoboda se je izvajalo v sklopu informacijskega vojskovanja, ki je vključevalo:

- metanje letakov z letal vojaškim enotam in iraškim prebivalcem z vsebino o nenapadanju ameriških letal in uporu Saddamovemu režimu,
- »šok in strah« zračno bombandiranje,
- kibernetski in elektronski napadi na vojaške in vladne komunikacijske sisteme.

193. Oddelek za specialne operacije pensilvanijske zračne nacionalne garde je predvajal radijske posnetke iz letala EC-130E Commando Solo[13]. Vojaški uradniki ameriške vojske so pošiljali e-maile in sporočila na mobilne telefone iraškim poveljnikom z namenom, da ne bi upoštevali Husseinove ukaze in dezertirali iz njegove vojske ter svarili pred uporabo OMU proti ZDA (CNN 2003). Po vsakem takšnem napadu so glavni iraški ponudniki internetnih storitev izklopili vse povezave z internetom (Svete in Žabkar 2006, 287). Tarče teh napadov niso bili samo vojaški poveljniki, ampak tudi izbrani člani iraške gospodarske in politične elite. Ameriška in britanska letala so odvrgla preko 8 milijonov letakov na večja mesta v osrednjem in južnem Iraku z istim sporočilom kot pri pošiljanju e-mailov in sms-ov (elementi psihološke vojne) (Buncombe 2003).

Kibernetsko bojevanje v pravem pomenu besede (državo popolnoma uničiti samo s to obliko bojevanja), v tej operaciji ni nikoli prišlo do izraza. Pentagon in ameriške varnostne agencije

[13] Ti radijski posnetki so bili narejeni s strani 4. skupine psiholoških operacij (4th Psychological Operations Group) v Fort Braggu, Severni Karolini. Ta podobna oddajanja so iz istih letal uporabili tudi v Afganistanu, ko so z prepričevali Talibane in Al Kaidine borce, da predajo orožje in da sporočijo civilistom, da zavezniške sile niso sovražniki. Namreč večina prebivalcev ni vedela zakaj so na njihovih tleh, niti za dogodke 11. Septembra (Buncombe 2003).

so sicer imele izdelan načrt o kibernetskem napadu na bančni račun Sadama Husseina (izvedle ga naj bi kibernetske enote letalstva). S tem napadom bi zamrznile milijarde dolarjev, uničile ves vladni finančni sistem, preprečili nabavo vojaškega orožja in opreme, zmožnost plačila vojakom in posledično državo spravili do bankrota. Ampak ZDA se za to potezo niso nikoli odločile, ker bi zaradi tega imel posledice ves svet (Markoff in Shanker 2009). Kajti iraški bančni sistem, je bil povezan s francoskim in s sesutjem bi onemogočili poslovanje bank in bankomatov po celotni Evropi. Zaradi globalne finančne povezanosti pa bi bilo poslovanje moteno še v ZDA in v preostalih državah po svetu (Elliot 2010). Kljub vsemu pa je ameriška vojska dobila zeleno luč, da nevtralizira vojaške in vladne komunikacijske sisteme (napadi so se odvijali v zgodnjih urah vojaškega napada). Ta napad je povzročil veliko kolateralno škodo. Uničili so oddajnike za mobilni signal in omrežne komunikacije. Uporabili pa so tudi elektronsko motenje signalov[14] in kibernetske napade na telefonsko omrežje. Ameriška vojska je celo zaprosila mednarodna komunikacijska podjetja, ki so zagotavljala satelitsko povezavo za mobitel in telefon Iraku, naj določene komunikacijske kanale zaprejo oziroma so jih obvestili da bodo zveze motene. Te posledice niso čutili samo v Iraku, ampak tudi v sosednjih državah (Markoff in Shanker 2009). Ameriške letalske sile so v tej vojni eksperimentirale s tako imenovanimi »E-bombami« (mikrovalovna bomba visoke moči – ang. kratica HPM[15]), ki imajo moč kratkih impulzov s katerimi onemogočijo delovanje računalnikov, radarjev, radijev, skratka ohromijo električno napajanje vseh naprav tudi elektronskih vžigov v avtomobilih in letalih (Roberts 2003). To pa niso edino orožje s takšnim učinkom, ameriška vojska je uporabila še eksplozivne magnetnokumulativne generatorje (ang. EMG[16]), ki proizvajajo veliko magnetno polje, s katerim se onemogoči delovanje vseh elektronskih naprav (Smith 2003).

Operacija Iraška svoboda je bila uspešna vojaška akcija iz naslednjih razlogov:

- *Prevlada v pridobivanju informacij:* zavezniške sile so imele vse informacije o premikih svojih OS in silah nasprotnika (točnost zaradi nadzora iraškega ozemlja iz

[14] Elektronsko bojevanje sta izvajali letalstvo in mornarica, glavno vlogo pri tem pa sta imeli letali EC-130H Compass Call in EA-6b Prowler. Obe letali imata zmožnost motenja komunikacij, mobilnih telefonov in naprav za daljinsko upravljanje. Letalo EC-130H Compass Call lahko moti vojaške in civilne frekvence in ima zmožnost motenja več frekvenc naenkrat. Medtem ko EA-6B Prowler uporabljajo samo za motenje vojaških frekvenc (radarjev) (Cox 2006,106–108).

[15] Ang. High Power Microwave bomb; napad na Iraško satelitsko TV postajo, ki je predvajala Husseinovo propagando 24-ur izven Iraka (Roberts 2003). Gre za bombe, ki ne povzročajo človeških žrtev in spadajo v kategorijo nesmrtonosnih orožij (Smith 2003).

[16] Ang. Explosive Magnetocumulative Generator je konvecionalna bojna glava z učinkom proizvajanja magnetnega polja enakega majhni nuklearni bombi. V ameriški oborožitvi, je ta bojna glava uporabljena v Tomahawkih (Smith 2003). Več kot 802 takšnih raket, je bilo iztreljeno na ključne iraške tarče (Wikipedia 2001).

zraka in vesolja ter računalniško podprtih komunikacij, uporaba GPS sistema). Iraški poveljniki so zaradi zastarane opreme na pamet ugibali lokacije zavezniških sil,

- *dominantnost v zraku in vesolju*: GPS sistemi so odvisni od satelitske povezave in komunikacije, ki so omogočali letalske napade od koderkoli in kadarkoli, tudi v slabih vremenskih razmerah zaradi napredne elektronike,
- *hitrost manevriranja sil*: hitrejši tanki in ostala vojaška vozila, posledično hitrejša reakcija na probleme na terenu. To je omogočilo zmanjšanje potrebe po masivnih letalskih napadih in uporabe helikopterjev, ki so ranljivejša od oboroženih vozil,
- *povezana koordinacija sil*: enote marincev so tesno sodelovale z enotami vojske, kar je pomenilo da je vojska poklicala marince, da izvedejo napade iz zraka, ko je to najbolj potrebovala,
- *točnost orožja:* tehnološki napredek v razvoju orožja je omogočil bolj natančno in uspešno ciljanje vojaških tarč in obenem znižal število civilnih žrtev,
- *racionalizacija logistike:* zmožnost izvajanja letalskih misij iz morja, je zmanjšalo potrebo po postavljanju letalskih baz na kopnem,
- *fleksibilnost:* hitro odzivanje na spremenljive okoliščine na terenu zavezniških sil, je omogočilo da enote niso izgubljale časa z načrtovanjem akcij vnaprej,
- *Specialne enote:* so zbirale informacije na terenu o lokacijah vojaških sil nasprotnika, ocenjevale škodo in prekinitev nasprotnikovih komunikacij, opravljanje iskalnih in reševalnih misij,
- *prednost v psihološkem bojevanju:* pošiljanje sms-ov in klicanje iraških poveljnikov na mobilne telefone, da naj se predajo (mnogi poveljniki in vojaki so se predali ali dezertirali iz enot). Ta tip bojevanja je bil eden najbolj uspešnejših elementov IO (Samuelson 2003).

Čeprav je bila ta vojna kratka in uspešna s strani zavezniških sil, jih je pravi izziv šele čakal po vzpostavitvi povojnega Iraka. Sadama Husseina so zrušili z namenom, da demokratizirajo državo, a zgodilo se je ravno nasprotno. V času okupacije ameriških sil se je stanje v državi spremenilo v kaotično, napetosti med različnimi verskimi skupinami v Iraku (Kurdi, Suniti in Šiiti, dvig radikalne skupine Al Kaide in nato IS) se je sprevrglo v državljansko vojno, ki traja še danes. Glede na celoten uspeh Operacije Iraška svoboda, lahko rečem, da je bila kibernetska oblika vojskovanja v okviru informacijskega vojskovanja uspešna, čeprav ni bila uporabljena v večji meri kot so mnogi pričakovali. Namreč še danes se mnogokrat pri

strokovnjakih pojavlja moralno vprašanje, do katere mere sploh lahko gre država s kibernetskimi napadi. Namreč zaradi prepletenosti vojaškega in civilnega omrežnega (kritična infrastruktura) sistema, se pojavi problem kako napasti vojaške tarče, da pri tem ne bi povzročili škodo v civilni sferi. Seveda pa se pojavi tudi vprašanje, kako izvesti kibernetske napade, da ne bi bilo globalnih posledic. Kajti vsa ta globalna komunikacijska povezanost držav sveta, vojaškim strokovnjakom povzroča marsikatero preglavico pri načrtovanju kibernetskih napadov na nasprotnika. In ravno ta slednja trditev, je bil ključni faktor, da se ZDA niso odločile za glavni kibernetski napad, to je napad na iraški finančni sistem.

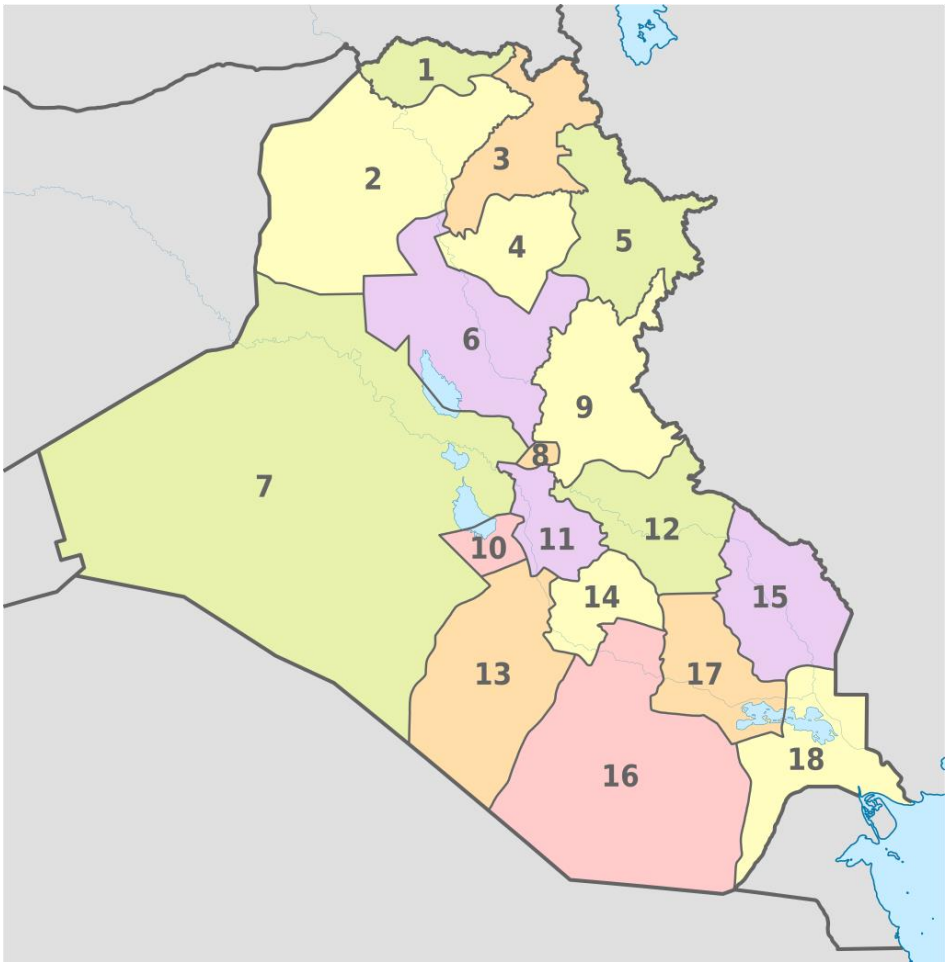
4.1.2 Kibernetski napadi v Iraku od leta 2006 do maja 2016

V tem podpoglavju bo predstavljena časovnica vseh kibernetskih napadov in njihovih akterjev ter na kakšen način so te napade izvajali. Pred letom 2003 so gospodarske mednarodne sankcije v Iraku povzročile kolaps računalnikov, ker jih je bilo težko vzdrževati (Levinson 2008). Po letu 2003 pa se je število uporabnikov interneta postopoma povečalo, ljudje so dobili dostop do mobilnih in internentih komunikacij, ki je bila v času Husseinovega režima prepovedana. Povečalo se je število televizijskih in radijskih hiš, ki jih je upravljala javno financirana Iraška medijska mreža. Če povzamem podatke na spletni strani o sedanjem stanju države na področju komunikacij[17], je v primerjavi s prejšnjo v času Husseinovega režima, ogromna razlika. Če so bili prej Iračani na dnu svetovne lestvice po uporabi mobilnih komunikacijskih naprav na prebivalca, so danes v ospredju na 59. mestu, po uporabi interneta pa na 87. mestu (CIA World Factbook 2016). Skratka Iračanom so se po ameriški invaziji odprla vrata v svet mobilnih in internetnih komunikacij. Pravo kibernetsko bojevanje pa se je začelo šele z letom 2014, pred tem so se dogajali le občasni napadi.

Povojni Irak se je razdelil na 18 provinc oziroma 4 okupacijske cone (glej sliko 4.2).

[17] 33. 559 milijona uporabnikov mobilnih telefonov, 6.381 milijona uporabnikov, ki imajo dostop do interneta, kar je 17,2 % celotnega prebivalstva (Central Intelligence Agency).

Slika 4.2: 18 provinc v Iraku (Dokuh, Nineveh, Erbil, Kirkuk, Sulaymaniyah, Saladin, Al Anbar, Bagdad, Diyala, Karbala, Babil, Wasit, Najaf, Al-Qadisiyyah, Maysan, Muthanna, Dhi Qar, Basra, Halabja)



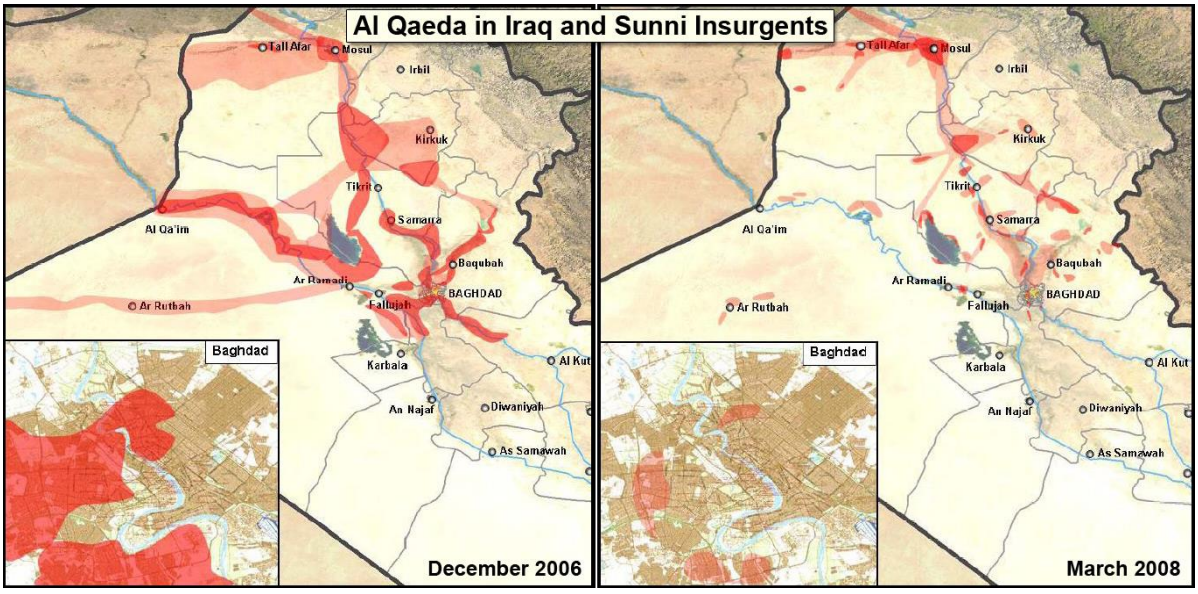
Wikipedia (2001).

V letu 2006 je iraška vlada v tranziciji nastopila s svojo začasno funkcijo 20. maja, dokler se ni oblikovala prava vlada. Verska razklanost in etnična pripadnost določenim skupinam, je segala že daleč v zgodovino (v Iraku večinski delež prebivalstva predstavljajo Suniti, Šiiti in Kurdi). Oslabljena teroristična organizacija Al Kaida, se je po uboju njihovega iraškega voditelja Abbu Mussaba al-Zarkavija[18] v zračnih napadih preimenovala v Islamsko državo v Iraku (ang. ISI). V istem letu so se začeli oblikovati zametki državljanske vojne, zavezniške

[18] Jordanec, ki je sklenil zavezništvo z Bin Ladnom in po ameriški invaziji na Irak ustanovil Al Kaido (STA 2015).

sile pa so se znašle vmes med temi boji. Samomorilci in avto bombe[19] so postali del vsakdana iraških prebivalcev. Iraška vlada je v mesecu decembru obesila Sadama Husseina zaradi zločina nad lastnim ljudstvom. Začel se je boj za mesto Bagdad med suniti in šiiti, ki se je vlekel vse do leta 2008, ko so ga zavzeli šiiti (kontrolirali so ¾ mesta). Šiitsko vodena vlada in njene milice so v glavnem mestu in po državi izvajale etnično čiščenje sunitske skupnosti (glej sliko 4.3). Kibernetski napadi v tem letu niso bili zabeleženi (Wikipedia 2001).

Slika 4.3: Prisotnost Sunitov (z Al Kaido) na območju Iraka in Bagdada od 2006–2008 (temno rdeča barva opredeljuje mesta, kjer so uporniki še sposobni izvajati operacije, svetlo rdeča pa predstavlja tranzitne poti upornikov)



Wikipedia (2001).

V letu 2007 se je nasilje med etničnimi skupinami in napadi na zavezniške sile nadaljevali. Province so se počasi iz rok Američanov in Britancev predajale iraškim varnostnim silam. Velika Britanija je napovedala umik svojih sil do 2008. Al Kaida je v jeseni leta 2007 ubila pomembnega ameriškega zaveznika, Iračana Abdula Sattarja Abu Risha v bombnem napadu v mestu Ramadi. Vodil je sunitski upor proti Al Kaidi. Britanci so predali 9. Iraško provinco, Basro iraškim varnostnim silam. Pojavile so se tudi napetosti med iraškimi Kurdi in Iranom

[19] Eksplozija bombe v mošeji, v Samari ki jo je nastavila Al Kaida (februar 2006, nato je sledilo maščevanje v jeseni ko so Sunitski Arabci z avto bombami in streljanjem napadli sunitsko naselje in organizacije (Wikipedia 2001).

ter Kurdi in Turčijo (Wikipedia 2001). V letu 2007[20] je ameriški predsednik George W. Bush mlajši pooblastil NSA, da je izvedla sofisticiran kibernetski napad na mobitele, računalnike in druge komunikacijske naprave upornikov. Mobilne naprave so uporabljali za postavljanje cestnih bomb na zavezniško vojsko (Harris v Elliot 2010). Ti napadi so bili usklajeni z vojaškimi napadi na terenu. Pošiljali pa so jim tudi napačne informacije, ki so jih peljale v zavezniške zasede (Elliot 2010).

Iraška vojska je v letu 2008 ustanovila enoto za kibernetski kriminal. Ker se je iraška vlada z vsemi silami borila proti Al Kaidi, so bili njihovi računalniki glavni cilji napadov. Ker enota imela bolj malo opreme in računalnikov, je bil ta kibernetski boj izredno težek. Namreč vsa denarna sredstva, je iraška vlada raje namenjala za nakup orožja kot računalnikov. Iraška vlada je začela uporabljati računalnike na vseh ministrstvih (v času Husseina na primer Ministrstvo za notranje zadeve ni posedovalo nobenih računalnikov), ampak tu je nastal problem, namreč ti niso bili zaščiteni pred napadi. V maju istega leta so zabeležili napad na računalnike Ministrstva za notranje zadeve, ki se je zgodil preko neškodljivega pop-up okna. Ta se je prikazal na zaslonu zaposlenega na MNZ, kjer se je pojavilo vprašanje o namestitvi posodobitve sistema. Zaposlenemu se je zazdelo, da nekaj ni v redu, zato je takoj obvestil enoto za spletni kriminal. Ugotovila je, da je napad izvedel napadalec imenovan »Iraški heker« in če bi ta dobil dostop do občutljivih podatkov MNZ, vključno z e-pošto in naslovi tisočih uradnikov, bi to lahko pomenilo katastrofo za državo. Kajti te informacije bi lahko prišle v roke teroristov. Zaradi tega primera so ZDA zasegle trde diske v Afganistanu in Iraku, kjer so bili načrti za sabotažo naftovodov (Kartz v Levinson 2008). Drugače pa je v Iraku najbolj znani heker »Iraški potapljač«. Gre za neidentificiranega prebivalca Wasit province južnega Bagdada. Od leta 2005 je vdrl že v preko 1500 spletnih strani, trdijo na spletni strani Zone-H.org (neodvisna organizacija, kjer beležijo hekersko aktivnost širom sveta). Spletne strani je popačil in puščal sporočila za predsednika Busha, ki so bile žaljive narave. Med drugim je vdiral tudi v iraške spletne strani ministrstev – MNZ, Ministrstvo za električno energijo in komunikacije ter v nekaj bank. S tem početjem je dokazoval ranljivost vladnih računalnikov in omrežja (Levinson 2008).

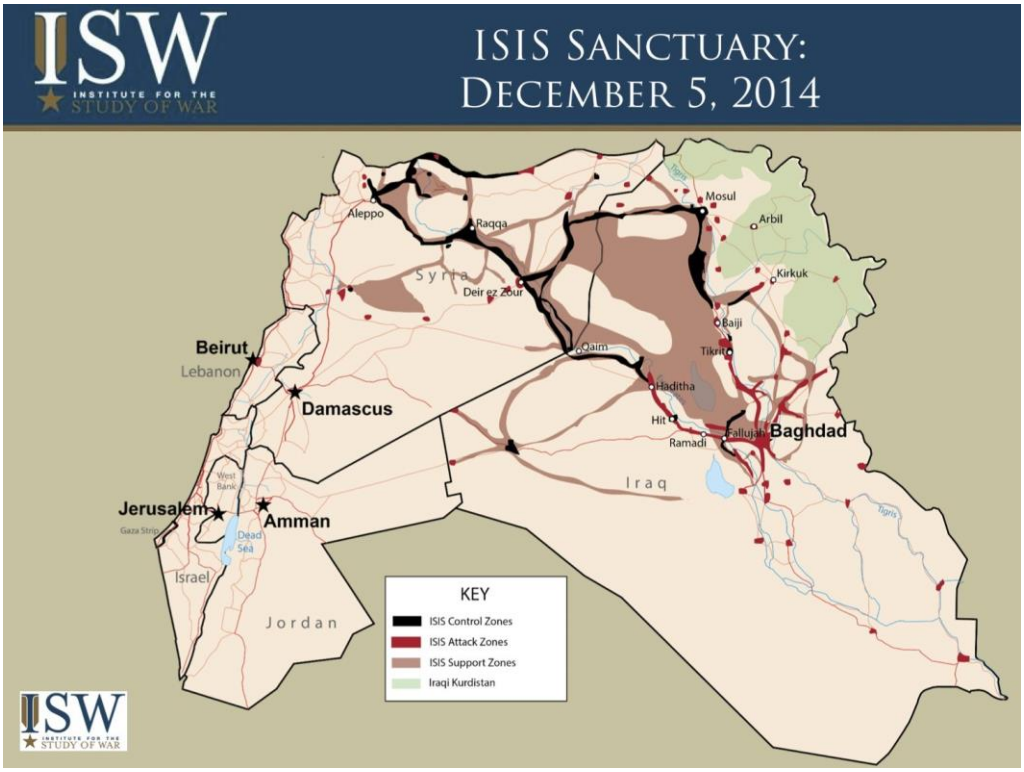
[20] 14. avgusta 2007 so se zgodile serije samomorilskih napadov z največjimi civilnimi žrtvami do sedaj (v provinci Qahtaniya na severu Iraka). Umrlo je 800 ljudi. Več kot 100 domov in trgovin je bilo uničenih. Ameriški uradniki so napad pripisali teroristični organizaciji Al Kaida. Tarča napadov, je bila nemuslimanska etnična skupina Yazidi, napad so izvedli pripadniki Al Kaide zaradi maščevanja. Namreč skupnost Yazidi, naj bi do smrti kamenjala najstnico, ker je bila v partnerski zvezi z muslimanom, sunitskim Arabcem (Wikipedia 2001).

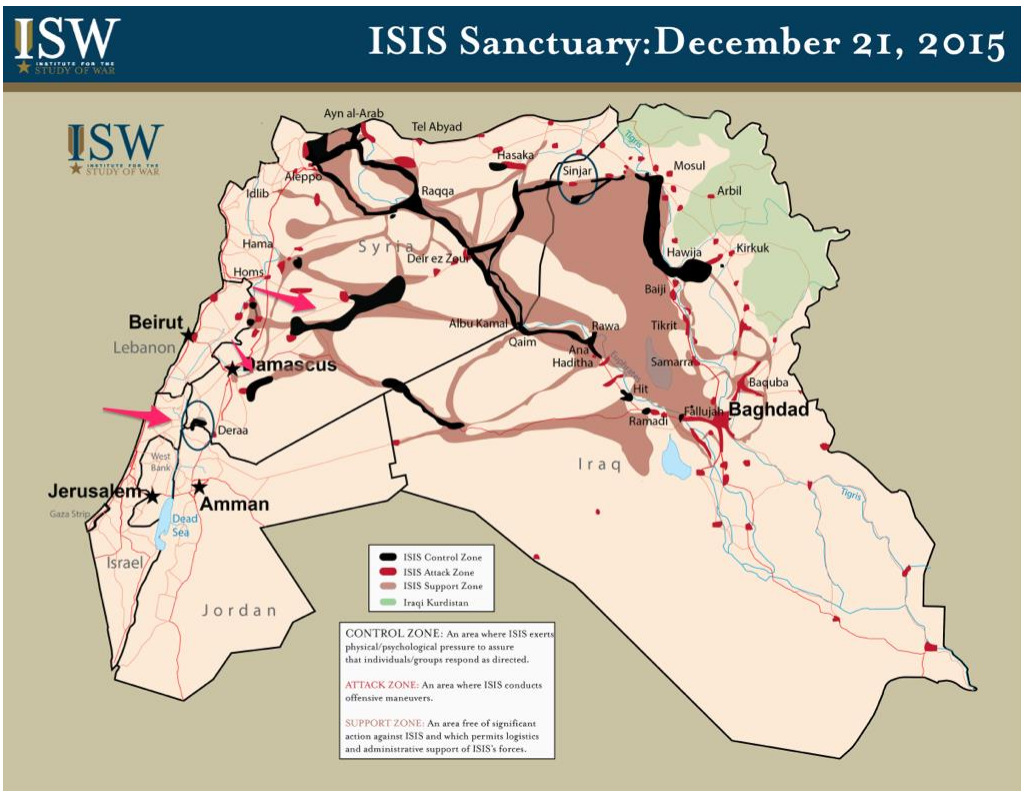
V letih 2009–2011: so ZDA nadzor nad Zeleno cono[21] in Husseinovo predsedniško palačo predale iraški vladi (2009), iraški premier je označil ta dan za simbol iraške neoodvisnosti. V provincah so izvedli volitve, ki pa niso minile brez nasilja (zgodile so se z najnižjo volilno udeležbo v zgodovini Iraka). Barrack Obama, ki je nasledil Busha mlajšega, je javno obljubil, da bodo ZDA bojno misijo v Iraku končale do 31. avgusta 2010. Po tem letu so ostale samo tako imenovane »tranzicijske sile« (50.000 vojakov), ki so usposabljale iraške varnostne sile in skupaj z njimi vodile protiteroristične operacije do konca leta 2011, ko se je tudi uradno končala ameriška okupacija Iraka (Wikipedia 2001). V letu 2010, so ZDA ustanovile prvo Kibernetsko poveljstvo (CYBERCOM), v Fort Meadu, državi Teksas. Na čelo te vojaške organizacije, so vladni organi postavili generala s štirimi zvezdicami Ketha Alexanderja, ki je zaprisegel pred senatskim odborom. Po ustanovitvi te organizacije, so 30.000 vojakov iz zračnih sil premestili iz tehnične podpore »v prve bojne linije kibernetskega bojevanja«. Od prevzema predsedniške funkcije, je Barrack Obama sprejel temo kibernetske varnosti kot eno najbolj resnih ekonomskih in nacionalnih varnostnih izzivov ZDA. Kajti informacijsko omrežje ZDA, je bilo vsakodnevno napadeno s strani Kitajcev, Severne Koreje in Rusov. Ena izmed prvih nalog, ki jih je poveljstvo izvedlo, je bilo »dot-mil« operacije, zapiranje nizov spletnih strani tako imenovanih »medenih pasti« (angl. honeytrap). To so lažne spletne strani, ki so bile ustanovljene s strani CIE in Savdijcev, z namenom pridobivanja podatkov o islamskih skrajnežev, ki so načrtovali napade v Savdski Arabiji. Kibernetsko poveljstvo je te operacije ustavilo, ker so džihadisti uporabljali spletne strani za novačenje borcev v Iraku. Kljub nagovarjanju CIE naj strani ostanejo, se je Kibernetsko poveljstvo odločilo, da bo strani zaprlo. Posledično je po zaprtju teh strani, bilo ustavljenih tudi preko 300 strežnikov v Savdski Arabiji, Nemčiji in Teksasu. Ker so hekerji v letu 2009 pregledali ogromno občutljivih podatkov programa Joint Strike Fighter (orig.) v Pentagonu, je bilo ustanovitev Kibernetskega poveljstva nujno. Je pa nastal problem v smislu regulative, namreč kibernetska tehnologija se razvija tako hiro, da ameriška vlada nima časa, da bi razvila smernice in pravila usklajene politike kibernetskega bojevanja (Beaumont 2010).

V nadaljnjem pisanju diplomskega dela, bom predstavila teoristično organizacijo Islamsko državo, ker je eden izmed ključnih akterjev kibernetskega bojevanja od leta 2014 naprej na spletu. IS je v letih 2014 in 2015 dosegla svoj vrhunec (glej sliko 4.4), tako v nadzoru ozemlja (severni Irak in deli ozemlja v Siriji) kot tudi v aktivnostih na spletu.

[21] Zelena cona je bilo zazidano ozemlje s stolpi (oboroženi s strojnicami), ločeno od Bagdada (Wikipedia 2001).

Slika 4.4: Ozemljski teritorij v Iraku pod nadzorom IS (rjava barva podpora IS, črna barva popolni nadzor terena) v decembru 2014, 2015



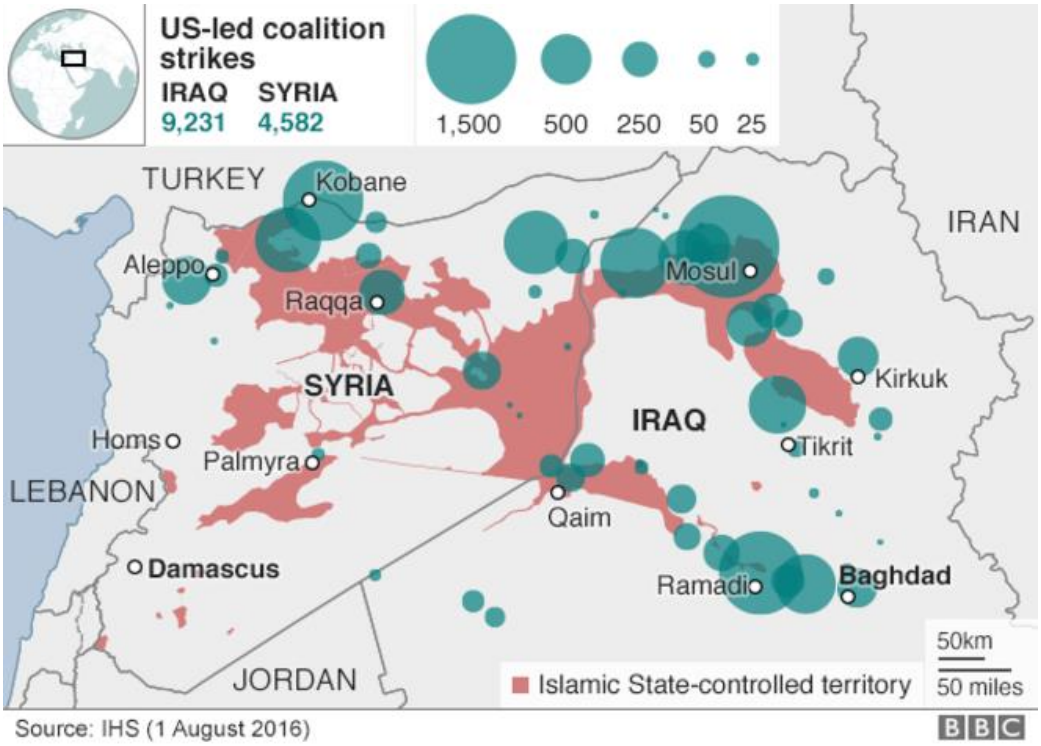


Google (1998).

Do leta 2013 je v večini mirovala, ker so se jim uprli sunitski Iračani in druge uporniške skupine. Takrat so svoje ime preimenovali v ISIL (Islamska država Iraka in Levanta), vodenje organizacije pa je prevzel Abu Bakr al-Baghdadi. V Iraku je dobil močno podporo s strani sunitskih Iračanov, ker naj bi jih novo nastala iraška vlada (večinsko šiitska) diskriminirala. In ker so bili pri izvajanju svojih operacij pretirano brutalni in neobvladljivi (obglavljanja množične ustrelitve, križanja), je Al Kaida prekinila vse stike z njimi. Junija 2014 se je preimenovala v Islamsko državo (IS) (Wikipedia 2001). IS (imenovana tudi ISIS ali Daesh) je nedržavni objekt z lastnostmi države, imajo svoje ozemlje (ki jih je iztrgala vladam v Damasku (Sirija) in Bagdadu (Irak)), svojo »vlado«, šolstvo, sodstvo, OS in upravni aparat. Taktika bojevanja, ki jo uporabljajo, je zmes simetričnih (uporaba ognjene podpore, vojaške mehanizacije, pehotni boj) in asimetričnih prostopov (samomorilski napadalci, podtaknjene bombe). OS naj bi štele nekje od 10-15.000 pripadnikov od katerih je dve tretjini borcev, ostalo so pripadniki sunitskih plemen Iraka in Sirije, ki opravljajo rekrutacijo in usposabljanje novih borcev (Barle 2016, 39). Približno 12.000 borcev, naj bi bilo tujcev iz približno 81 držav, med katerimi so tudi iz Evrope (cca. 2500) (STA 2015). Večina pripadnikov te skupine so sunitski borci, člani strmoglavljene iraške stranke Baas in izpuščeni kriminalci iz zaporov v času ameriške invazije na Irak. Organizacija je počasi doživljala svoj uspeh zaradi varnostnega vakuma in nezmožnostjo iraških varnostnih sil, da bi branile celovitost iraškega ozemlja pred napadi uporniški sil. Iraška vojska je skoraj razpadla zaradi boja z IS, namreč sunitski pripadniki so prebegnili na njihovo stran, šiitski pripadniki pa so se umaknili v glavno mesto Bagdad (Barle 2016, 40). Junija 2014 so skrajneži IS zasedli severno iraško mesto Mosul, nato pa so prodirali proti jugu in mestu Bagdad ter s pohodom grozili o odpravi številnih etničnih in verskih manjšin v državi (BBC News 2016). Skupina je razglasila versko avtoriteto nad vsemi muslimani sveta, v svoj kalifat pa je želela vključiti še Sirijo, Izrael, Jordanijo, Ciper, Libanon in južno Turčijo (Wikipedia 2001). Borci IS so imeli v posesti širok spekter orožja, od lahke oborožitve do težje (strojnice, jurišne puške, ostrostrelske puške, topništvo, protitankovske raketomete, protiletalske topove, protiletalske raketne sisteme, celo topovske granate polnjene z iperitom (kemično orožje), orožja za ognjeno podporo). Zasegli so tudi tanke in oklepna vozila, hummerje in vojaške tovornjake iraške in sirske vojske (STA 2015). Skratka imeli so mešanico zastarelega sovjetskega in zaplenjenega sodobnega zahodnega orožja. Tipično bojno vozilo, predelanega izvora, je bil poltovornjak opremeljen s težkim mitraljezom in obdan z provizoričnim oklepom. Ta vozila so v večinski meri tvorila motorizacijo IS, s katerimi so izvajale vojaške akcije »udari in se umakni« vzdolž prometnic. Sama organizacija OS ni bila tipično vojaška, saj so imeli pokrajinski in lokalni poveljniki

avtonomijo pri samem izvajanju vojaških akcij. Vrh IS je dodelil nalogo, samo izvedbo pa so prepustili poveljnikom na terenu (Barle 2016, 41). Po navedbah mnogih strokovnjakov in medijev, naj bi bila IS ena izmed najbogatejših organizacij, saj naj bi imela 2 milijardi dolarjev v gotovini in drugih sredstvih. Od začetka so ji pri financiranju pomagali določeni posamezniki iz bližnjih zalivskih držav, danes pa naj bi se financirala sama s pomočjo ilegalne prodaje nafte in plina s polj, ki jih ima v lasti, prispevkov in davkov, tihotapljenja, ugrabitev in izsiljevanj. ZDA so za boj proti IS oblikovale mednarodno koalicijo približno 60 držav, v katero je vključena tudi Slovenija (STA 2015). Ko je IS začela prodirati proti kurdskemu mestu Erbilu, je ZDA sprožila zračne napade na njihove položaje. Septembra so jih razširili še na Sirijo (BBC News 2016). Zračna ofenziva ZDA s koalicijo (glej sliko 4.5)

Slika 4.5: Koalicijski napadi (države, ki so vključene v koalicijo: Avstralija, Belgija, Kanada, Danska, Francija, Jordanija, Nizozemska, Bahrajn, Turčija, Savdska Arabija, Združeni Arabski Emirati) na položaje IS (2016)



BBC News (2015).

je v Iraku in Siriji od avgusta 2014 pa do danes zdesetkala vrste IS (Rusija, ki ni del ameriške koalicije, je začela z zračnimi napadi na Sirijo leto kasneje). Na terenu so se oblikovale močne

skupine in milice, ki so na dnevni bazi uničevale njihove komunikacijske, transportne in ekonomske poti. Zaradi teh ofenzivnih napadov na položaje IS, se je skupina kljub dobri organizaciji znašla v defenzivnem bojevanju (Barle 2016, 41). Od takrat naj bi IS izgubila približno 40% poseljenega območja v Iraku, kjer je vladala ter 10-20% območja v Siriji (BBC News 2016).

Že v svojih prvi dneh nastanka, je Al Kaida pokazala izjemen interes za uporabo interneta za propagandne namene. Namreč njena prva spletna stran je bila ustanovljena pred dvajsetimi leti (Azzan.com). Začetne ideje o uporabi spleta za kibernetsko bojevanje so radikalne islamistične skupine osvojile po ubojih nekaterih glavnih voditeljev Al Kaide med leti 2010 in 2012 na arabskem polotoku in Somaliji. Takrat so opustili tradicionalno komunikacijo in posvojile idejo pokojnega Anwarja al-Awlakija, da se je njihova propaganda in ideologija širila preko socialnih omrežij (Facebook, Twitter, Skype ipd.). Tako so dosegli ciljno publiko na lokalni in globalni ravni (na ta način so džihadisti povečali svojo moč v zahodnih državah). In ravno sveži konflikti v Iraku in Siriji so ponudili priložnost, da so to tehniko preizkusili. Glavno orodje bojevanja radikalnih islamističnih skupin na spletu, so postala socialna omrežja, kjer so tudi podajali napotke za sestavo eksplozivnih sredstev doma - preko skritih sporočil »kako narediti torto ali branje kuharice« (npr. lonec na pritisk, ki ga uporabljamo za kuho, je bil uporabljen v terorističnem napadu na Bostonskem maratonu leta 2013). Ta strategija pa se jim je najbolj izplačala, ko so začeli novačiti ljudi z vseh koncev sveta, zbirali denarna sredstva za svojo kampanjo[22] in za vodenje novih vrst napadov preko spleta. Spletni komunikacijski programi in aplikacije na mobilnih telefonih, so omogočili neposredno komuniciranje e-hadistov (podporniki skupine na spletu) in tistimi na bojišču. Internet so uporabljali za spodbujanje svojih privržencev, da so napadali spletne strani zahodnih vladnih organizacij in institucij. Kibernetska kampanja ISIL je bila uspešna že v tem, da so mnogi posnemali njihova dejanja. Ena od teh je Sirska elektronska armada (SEA), ki je od leta 2011 pa do danes izvedla mnogo kibernetskih napadov na zahodne medije. Predstavila jo bom v naslednjem poglavju. Manj znani kibernetski skupini kot sta Elektronska vojska Al Kaide in Tunizijska kibernetska vojska, sta napadli ameriške spletne strani Urada za carinsko in mejno

[22] Mišljeno z uporabo podobnih prijemov kot se jih poslužujejo kibernetski kriminalci: t. i. ribarjenjem (ang. phishing attacks) in krajo kreditnih kartic. V Angliji so na ta način (Younis Tsouli znan pod hekerskim vzdevkom »Irhabi007« in njegovi sodelavci) pridobili 2,5 milijona funtov protipravno pridobljenega denarja. To pa ni edini način pridobivanja sredstev, namreč zbirajo denar tudi preko globalnih internetnih dobrodelnih nevladnih organizacij. Komunikacija donatorjev in islamskih skrajnežev poteka preko socialnih omrežij in spletnih forumov. ISIL je ustvarila svojo mobilno aplikacijo (ang. Dawn of glad tidings), preko katere uporabniki redno objavljajo in posodabljajo dogodke skupine iz terena in na tak način pomagajo širiti glas do čim večjega števila morebitnih vlagateljev.

zaščito ter Urada za upravljanje kadrov. Podpornik skupine IS Boke Harama pa je vdrl v zapise nigerijske obveščevalne službe in objavil podatke šestdesetih državnih varnostnih operativcev. Zaradi teh povečanih aktivnosti radikalnih islamističnih skupin (ISIL, Jabhat al-Nusrah) na internetu, so oktobra 2013 nekatere evropske in arabske države (Egipt, Francija, Savdska Arabija, Velika Britanija in Združeni arabski emirati) skupaj z ZDA združile moči in ustanovile Informacijsko koalicijo za bojevanje proti IS na spletu (Berton in Pawlak 2015). Na območju Iraka se je kibernetsko bojevanje razmahnilo z letom 2014, ko se je sočasno z vojaškimi napadi (koalicijski napadi so se začeli avgusta) na terenu, uradno še začela vojna na spletu. Glede na to da živimo v obdobju, ko so socialna omrežja v porastu, uporaba takšnih orodij pri terorističnih organizacijah ni nič novega. Tako kot OS razvijajo kibernetsko tehnologijo in ustanavljajo posebne enote za tovrstno bojevanje, tudi ekstremistične verske skupine na črnem trgu (na »*Darknetu*«) najemajo plačane hekerje, ki opravljajo določene storitve v njihovem imenu.

V Iraku so uporniške skupine (predvsem IS) zaposlovale hekerje, ki so spletne programske opreme za boj na spletu uporabljali predvsem za zbiranje obveščevalnih podatkov in motenje usmerjevalnikov ter drugih sistemov. Pošiljali so zavajajoča sporočila (t.i. »minska sporočila«), ki so v priponki imela pripeto zlonamerno programsko opremo. Ta se je ob odprtju takšnega sporočila inštalirala na žrtvine računalnike in tako zbirala ter kradla vse podatke iz sistema. Tarče napadov so bile različne lokalne skupine v sporu, posamezniki tudi ožji člani sorodnikov vpletenih v konflikt. Kdo točno je avtor teh zakodiranih sporočil, ni bilo nikoli znano, saj so bila sporočila poslana iz javnih omrežij (Ward 2014). Znana je bila samo lokacija znotraj Iraka. Po podatkih podjetja IntelCrawler za kibernetsko varnost, so se napadi izvajali v večjih iraških mestih: Bagdadu (več kot polovica primerov), Erbilu (četrtina vseh napadov), občasni napadi pa so se dogajali še Basri in Mosulu. Iraški akterji, ki so delovali v teh dejavnostih, so bili povezani z egipčanskimi, libanonskimi, libijskimi, iranskimi in sirskimi islamističnimi skupinami. Te skupine namreč, so izvajale kibernetske napade zaradi verskih in političnih prepričanj, podprte pa so bile tudi s strani nekaterih strank (Osman 2014). Zlonamerni programi, ki so jih uporabljali hekerji so bili večinoma trije (Njrat, Bitfrost in DarkComet). Imeli so isti končni cilj, dobiti popoln nadzor nad računalnikom na daljavo. Preko teh programov niso dobili samo nadzor, vklopili so lahko tudi kamero in mikrofon, da so dobili še video in zvokovno povezavo. Teme poslanih sporočil uporabnikom (v katerih so bili ti zlonamerni programi), s katerimi so prepričali uporabnika da je odprl sporočilo, so bile v povezavi z dogodki na terenu. Na primer, vse kar je bilo povezano z šiitskimi muslimani,

sirskim predsednikom Assadom, IS in z njo povezane aretacije, skratka z vsemi informacijami o kriznih žariščih na Bližnjem vzhodu. Zlonamerne programe so infiltrirali v sporočila na socialnih omrežjih kot je Facebook, Skype, Twitter, Youtube, Whatsapp in preko e-pošte ter političnih forumov. Ustvarjali so tudi spletne strani, ki so izkoriščale ranljivosti brskalnikov (Ward 2014). Varne vtičnice in FTP/HTP povezavo so vstavili v datotečni sistem Google Chrome brskalnika in javno dostopno programsko opremo ter na tak način okužili strežnike preko katerih so prestrezali in manipulirali podatke (Osman 2014). Za dosego svojih ciljev so uporabljali različne metode in orodja kibernetskega bojevanja.

V začetku leta 2015 so simpatizerji IS (skupina poimenovana kot Kibernetski kalifat) vdrli v twitterjev račun ameriškega vojaškega Glavnega poveljstva (*ang. Centcom*[23]). Na računu so objavili občutljive informacije o vojaških operacijah Kitajske in Severne Koreje ter osebne podatke častnikov višjega čina (naslove in telefonske številke) (Guion 2015). Profilno sliko Centcom so zamenjali z zamaskiranim obrazom moškega (glej sliko 4.6).

Slika 4.6: Napad na twitterjev račun ameriškega Glavnega poveljstva

Usborne (2015).

[23] Je odgovoren za vojaške operacije med Evropo in Pacifikom, osrednje območje sveta, ki zajema 20 držav: Afganistan, Bahrajn, Egipt, Iran, Irak, Jordanija, Kazahstan, Kuvajt, Kirgizistan, Libanon, Oman, Pakistan, Katar, Savdska Arabija, Sirija, Tadžikistan, Turkmenistan, Združeni arabski emirati, Uzbekistan, in Jemen. Ustanovljeno je bilo v času Reaganove administracije, 1. januarja 1983. Glavno oporišče Glavnega poveljstva se nahaja v zračni bazi MacDill, blizu Tampe na Floridi. Poveljstvo vodi general Lloyd Austin (Gion 2015).

Vojaškemu osebju so grozili, da vedo vse podatke o njih in njihovi ožji družini in da jih opazujejo. Stran so napadli, ker je Centcom dnevno objavljal sporočila o koalicijskih napadih na lokacije IS. Ta kibernetski napad je bil za Pentagon bolj sramotne narave kot varnostna grožnja. Zato so na ta primer gledali kot na kibernetski vandalizem, saj ni prišlo do objave tajnih podatkov. Vdor v račun je trajal cca. 40 minut, preden so račun zaprli. Medtem ko se je Pentagon odzval na napad, so hekerji vdrli še v youtubov račun in še tam objavljali svoja propagandna sporočila in video posnetke. Račun so sčasoma prav tako zaprli. En teden pred napadom na Centcom so podporniki IS uspešno vdrli v twitterjeve račune medijskih hiš: Albuquerque Journal v Novi Mehiki in na televizijsko hišo WBOC-TV v Marylandu (Usborne 2015). Glavni osumljenec za ta napad je bil britanski heker Junaid Hussain – alias Aku Hussain al-Britani, ki je leta 2013 pobegnil v Sirijo. Leta 2012 je bil zaprt zaradi kraje in objav podatkov na spletu bivšega britanskega premierja Tonya Blaira (Myers 2015). Posledično so konec januarja na zahtevo britanskih varnostnih sil in ameriške agencije CIE, v antiteroristični operaciji na socialnem omrežju zaprli približno 400 twitterjevih računov podpornikov IS in džihadistov ter tako deloma zmanjšali radikalno mreženje na spletu (Wright in drugi 2015). Ampak računi se vedno znova pojavljajo pod drugimi imeni ali vzdevki, nekateri imajo odprtih celo 10 računov in več, tako da dokončno izkoreninjenje prisostnosti radikalnih skupin na socialnih omrežjih in internetu ne bo nikoli mogoče.

Po terorističnih napadih na francosko satirično novinarsko hišo Charlie Hebdo januarja 2015, je skupina Anonimni (*ang. Anonymous*), ki je v tem primeru nedržavni akter kibernetskega bojevanja, sprožila svojo spletno vojno proti proti IS. Maščevala se je tako, da je vdrla v račune na Twitterju in Facebooku, ki so bili odprti s strani podpornikov IS in jih 1500 zaprla ter na koncu pustila še video sporočilo, da jih bodo polovili in izpostavili javnosti. Hkrati pa so s to akcijo sesuli še spletno stran CIE in kot posledica tega se je zgodil domino efekt – sesule so se džihadistične spletne strani, vključno s francosko spletno stran ansar-ahaqq.net. Glavni cilj te hektivistične skupine, je bil ustaviti širjenje spletne propagande IS in rekrutacijo mladih iz zahodnih držav (Berton in Pawlak 2015). Vzajemno sodelovanje med hektivisti in administracijo socialnih omrežij, je bil koristen proces (preprečevali so objave obglavljenja, mučenja in javnih usmrtitev ljudi in s tem posledično zmanjševali sledenje takšnim profilom). Twitterjeva administracija je zaradi rasti takšnih profilov uvedla dodatne ukrepe, namreč postavila je filtre, ki so onemogočali objave nasilnih video posnetkov in groženj na podlagi rase, narodnosti in vere. Kljub vsemu so se podporniki IS znašli in začeli objavljati video posnetke pod imeni drugih vsebin, ki so zaobšli filte. Na arabskih računih, kjer je mnogo več

sledilcev pa so množično začeli deliti te posnetke na svojih osebnih profilih takoj po objavi na spletu. Tako je IS zopet dosegla svojo ciljno publiko z novimi pristopi objavljanja (Griffin 2015). V februarju so hekerji Kibernetskega kalifata napadli twitterjev račun revije Newsweek in preko njega grozili ameriškemu predesedniku, njegovi družini ter celotnemu nacionalnemu sistemu, da ga bodo uničili od znotraj (Chiacu 2015).

Ker je Francija del ameriške koalicije, ki z letalskimi napadi izvaja boj proti IS v Iraku in Siriji, je bilo samo vprašanje časa, kdaj bo postala žrtev kibernetskega napada. Hekerji Kibernetskega kalifata (podporniki IS) so v spomladanskem času napadli francosko TV mrežo TV5 Monde (oddaja program v več kot 200 državah po svetu) in popolnoma ustavili predvajanje rednega vsebinskega programa (televizija ni predvajala niti slike niti zvoka približno 3 ure dokler je trajal napad). Napadli pa so tudi spletno stran in račune socialnih omrežij, na facebookov profil televizije pa so objavili dokument s podatki vseh sorodnikov francoskih vojakov (identitete in življenjepise), ki so sodelovali v antiterorističnih operacijah v Iraku in Siriji (približno 1500 vojakov, kar je več kot polovica vseh evropskih sodelujočih sil). Pustili so sporočila z grožnjami naj se francoska vojska umakne iz Bližnjega vzhoda in da bodo nadaljevali kibernetski kalifat proti vsem sovražnikom skupine IS. Obtožili so francoskega predsednika, da je zaradi sodelovanja v vojni proti IS, odgovoren za vse teroristične napade, ki so se zgodili in se še bodo (Charlie Hebdo, Hyper Cacher). Hekerji so zamenjali profilno sliko TV mreže podobno tisti, ki so jo uporabili pri napadu na Centcom v ZDA (glej sliko 4.7) (Campbell 2015).

Slika 4.7: Napad skupine Kibernetski kalifat na TV mrežo TV5 Monde

Campbell (2015).

Francoski preiskovalni organi so kasneje po zaključeni preiskavi pripisali ruskim hekerjem APT28, saj naj bi se napad zgodil preko Brazilije, izviral pa iz Rusije (Runkle 2015). Ampak ne glede na to, kdo je bil glavni napadalec, so v končni fazi naredili uslugo IS, saj so na ta način preusmerili pozornost javnosti na njih. V juliju je skupina Kibernetski kalifat izvedla napad na sirsko Organizacijo za človekove pravice in grozila njegovemu direktorju, spremenila je njihovo spletno stran, profilno sliko in pustila grozilna sporočila. Uničila je podatke na strežnikih, jih popolnoma izbrisala, ampak na srečo so imeli v organizaciji kopijo podatkov. Grožnje in podobne napade je doživela že s strani sirske vlade in Al Kaide (AFP 2015).

Napad, ki je v avgustu postavil na prežo ameriško Ministrstvo za obrambo in FBI, je bil tokrat izveden s strani podporne skupine imenovane »Hekerska divizija IS«. Vdrla je v 1481 računov socialnih omrežij posameznikov zaposlenih na ministrstvu in objavila vse njihove osebne podatke na spletu, od e-poštnih računov, v katerih oddelkih delajo, telefonskih številk do naslovov ter pustila sporočilo, da vsakega posameznika nadzirajo. Na koncu so ameriški preiskovalci ugotovili, da je bil ta seznam bolj zbiranje podatkov na brskalniku Google kot resnični vdor v sistem Ministrstva za obrambo (Bunkle 2015). Da bi bil zaključek leta 2015 za IS popoln, so skušali vdreti v ameriški nacionalni računalniški sistem električnega omrežja, vendar neuspešno (Marks 2015).

Če do sedaj medsebojno primerjam vse kibernetske napade IS, lahko ugotovim, da imajo v večini primerih »isti podpis«: napadli so spletne strani in socialna omrežja ter uporabili račune za medijsko kampanjo o sebi, kradli so podatke in jih objavili na spletu ali jih brisali s strežnikov, popačili originalne spletne strani (zamenjali profilne slike s svojimi) in pustili grozilna sporočila tistemu, ki so ga napadli. Skratka metoda in tehnika sta isti, le tarče napadov se razlikujejo.

Benjamin Runkle (2015) navaja 3 razloge zakaj je potrebno pozorno spremljati IS na spletu:

- gradnja konvencionalne vojske je izjemno draga, medtem ko je kibernetsko bojevanje tako poceni, da si jo lahko privoščijo ne samo nedržavni akterji, ampak tudi šibkejše države od velesil (ZDA, Kitajska, Rusija). Teroristične skupine nimajo izobraževalnih ustanov, da bi množično proizvajale kibernetske vojake kot to počneta Rusija in Kitajska, ampak enostavno usluge kupijo na črnem trgu (takšen primer je bil, ko so kupili storitve Juanida Hussaina). To je malo zaskrbljujoče glede na to, da IS dnevno zasluži IS 1-2- milijona dolarjev samo s prodajo nafte,
- četudi so bili prvi napadi IS osnovnošolski, ne pomeni da bo skupina ostala v takšnem primitivnem stanju ves čas (začela je že uporabljati šifriran sistem komunikacije in s tem zamaskirala pogovore tako, da so ostali prikriti obveščevalnim službam; svojim pripradnikom so dajali napotke, kako ustvariti račun na spletu s ponarejeno telefonsko številko),
- kibernetski napadi omogočajo neposredno napade na civilno strukturo in gospodarske cilje, kar lahko na državni ravni povzroči katastrofo. Rusija in Kitajska imata vse sposobnosti, da izvedeta katastrofalni kibernetski napad na ZDA, ampak bi same sebi povzročile gospodarsko škodo, ravno zaradi prepletenosti sistemov z ameriškim. Zato se raje posvečata kibernetskemu vohunjenju in kraji ameriških vojaških podatkov.

V začetku leta 2016 so ZDA (Ministrstvo za obrambo) prvič javno naznanile kibernetsko vojno proti IS. Glavni cilj jim je bil fizično in virtualno izolirati IS, povzročiti motnje ali preprečiti komunikacijo[24] med vodilnimi v skupinami (Poveljstvo IS) in borci na terenu, obremeniti omrežje s povečanim tokom podatkom[25], onemogočiti premikanje finančnih

[24] napad na komunikacijsko infrastrukturo mest (Mosul in Raka); izvajali so motenje radijskih signalov, dešifrirali pogovore med pripadniki IS, vdirali v račune socialnih omrežij in zvajali še ostale elektronske sabotaže (Shekar 2016).
[25] IS je mislila, da imajo težave z omrežjem, v resnici pa je šlo za ameriški kibernetski napad (metoda zavajanja nasprotnika) (Carey 2016).

sredstev, preprečiti novačenje borcev zunaj meja Iraka in Sirije ter tako v celoti omejiti delovanje skupine na lokalni taktični ravni, da bi izgubili nadzor vpliva nad prebivalci in gospodarstvom. Kibernetsko bojevanje je ameriški vojski služilo kot podporni sistem vojaškim operacijam, da bi skupaj z iraškimi in kurdskim silami pridobili nadzor nad mestom Mosul v Iraku in Raka v Siriji. Podrobnosti o kibernetskih napadih niso izdajali, da ne bi nasprotnik kopiral in proučeval metode njihovega bojevanja ter pridobival podatke o lokacijah in času napadov. Zato Kibernetsko poveljstvo[26] ostaja ena najbolj skrivnostnih vojaških organizacij na svetu. Po objavi te novice v medijih, so podporniki skupine IS začeli z grožnjami o napadih na ustanovitelja Facebooka Marka Zuckerberga in Twitterja Jacka Dorseya. Namreč oba socialna medija sta v zadnjem času zatrla uporabo računov na njihovih platformah. Ampak Kibernetsko poveljstvo ni skrbelo, da so te akcije zapiranja računov ogrozile njihovo zbiranje obveščevalnih podatkov o skupini. Ravno nasprotno, uporniki so začeli uporabljati druge komunikacijske kanale, ki so vojski omogočali še lažji dostop do prestrezanja njihovih pogovorov (Gertz 2016). ZDA so ves ta čas imele prednost v kibernetskih bojih v Iraku (ne samo zaradi boljše tehnologije in številčnosti kibernetskih vojakov), ker so pomagale pri gradnji celotnega telekomunikacijskega omrežja[27], tako da so točno vedele kje in kdaj napasti nasprotnika (Carey 2016). Ko so koalicijske sile začele izvajati vojaške operacije skupaj s kibernetskimi, se je po oceni ameriške vlade število borcev IS (aprila) zmanjšalo na najnižjo številko doslej od leta 2014. Ker pa se je številčnost zmanjšala v Iraku in Siriji, se je dvojno povečevala v Libiji (nekje med 4000-6000 borcev). Kajti slednja, je postala od padca režima Gadafija vroča točka za vojaške skupine. Kljub vsemu se je organiziranost IS, vključno z rekrutiranjem novih članov, vzpostavitvijo baze in načrtovanjem napadov na ZDA poslabšala. Odkar so ubili vodjo IS v Libiji, Abu Nabila se IS nikakor ni mogla postaviti nazaj na noge (Tomkin 2016). Februarja 2016 je koalicija pospešila kampanjo proti IS in kljub temu, da niso povedali javnosti kako točno bodo izvajali kibernetske napade, je prišla na plano informacija (preko medija New York Times), da je vojska uporabljala t. i. »kibernetske bombe« in v omrežje IS vgradila vsadke (ang. implants). Preko slednjih, je ameriška vojska spremljala delovanje skupine in posnemala ter spreminjala sporočila poveljnikov, da bi uporniki nevede zašli na območja, kjer so jih napadli z letali in

[26] Do leta 2018 bodo v 133 kibernetskih enotah, ki bodo razporejene v vseh zvrsteh vojske, zaposlili več kot 6000 vojaških in civilnih tehničnih strokovnjakov (AFP 2016). Vsaka od teh enot naj bi štela od 40-60 vojakov, velika večina civilnega dela so arabski jezikoslovci, saj IS za svoje delovanje razumljivo uporablja arabski jezik (Gertz 2016).

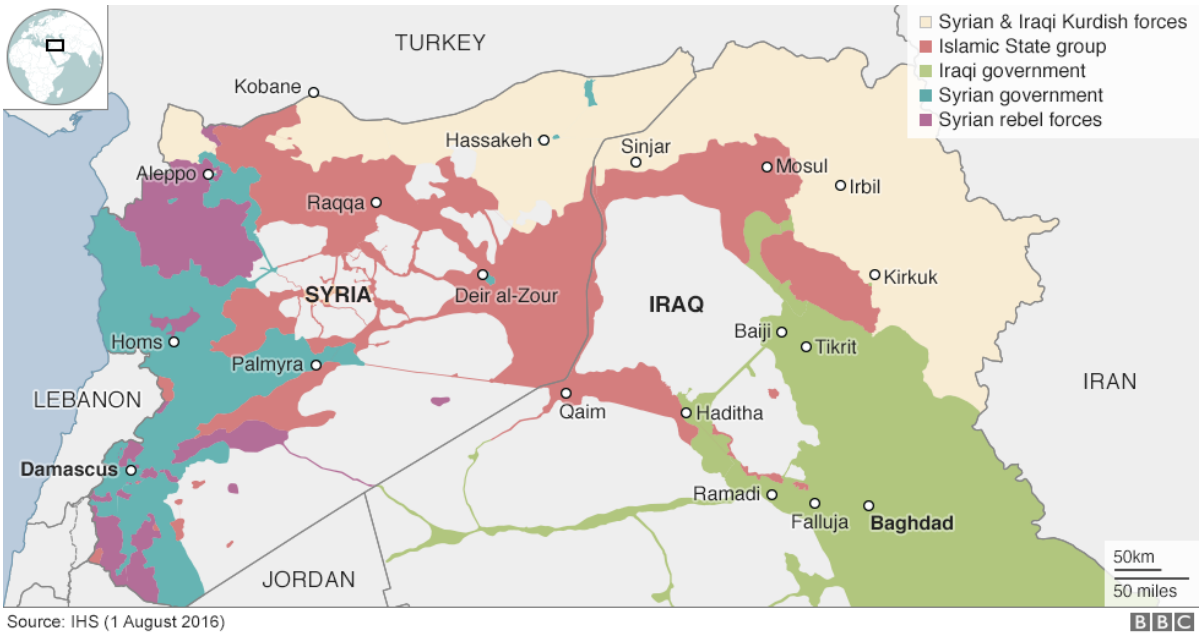
[27] NSA in vojska so jo uporabljale za potrebe pridobivanja obveščevalnih podatkov, da so lažje bile bitko z uporniki (Shekhar 2016).

droni (AFP 2016). Glavno poveljstvo vojske ZDA je podalo oceno, da je bilo ubitih okoli 25.000 skrajnežev (BBC News 2016).

4.2 Sirski konflikt (2011)

Zmagoslavje tunizijske in egiptovske revolucije, je navdihnilo arabsko mladino, da je sprejela izziv in val revolucije. V Libiji, Bahrajnu, Jemnu in Siriji so zahtevali od vlade reforme in javno svobodo. 15. marca 2011 je veter arabske pomladi zajel tudi Sirijo. Začeli so se protesti na ulicah (mirne narave), vladajoči režim predsednika Bašarja al-Assada (s stranko Baas) pa je odgovoril s silo. Sirska država ima drugače že dolgo zgodovino z začaranim krogom represije. Že oče Bašarja (Hafyz Assad) je v letih 1971-2000 vladal z železno roko. Z avtoritativnim vladanjem je brutalno zatiral opozicijo, tako da ni bilo prostora za politične nasprotnike. Assadova družina spada k manjšini alavitov, ki predstavlja le 15% prebivalstva poleg 10%, ki so kristjani, ostalo 75% pa večinski suniti. Alaviti nadzorujejo v Siriji vse vidike političnega sistema (medije, vojsko in policijo, gospodarstvo). Sirska opozicija pa je razdeljena, šibka, razdrobljena in neučinkovita. Kljub nasilnemu odgovoru na mirne proteste, se je glas revolucije širil še v druga sirska mesta. Mesto Homs so poimenovali za glavno mesto revolucije. Assadova vlada je nad mesto poslala vojsko, ki je v upanju da bo zatrla gibanje, uporabila nad uporniki težko artilerijo in orožje, vključno z zračnimi napadi (Shehabat 2012). Na severu Sirije so se istega leta oblikovale Ljudske zaščitne enote (YPG) (od 30.000-50.000 borcev tudi tujih), kot oboroženo krilo kurdske stranke PYG, da bi zaščitile možnost vzpostavljanja kurdske avtonomije na severu Sirije (ima podporo Zahoda, sodeluje pa tudi z Rusijo). Poleg Kurdov pa si je sirijska vlada nakopala še sovražnika v radikalnih islamističnih vrstah, to je IS (nadzor ozemlja tudi na severu države) (Gaube 2016).

Slika 4.8: Sirsko ozemlje pod različnimi nadzori (vlade, Kurdov, upornikov in IS)



BBC News (2016).

Ko se je revolucija prelevila v vojaški konflikt (julija 2011), so sunitski vojaki zapuščali Assadovo vojsko in ustanovili t.i. Svobodno sirsko vojsko (ang. FSA – Free Syrian Army), ki se je borila na strani upornikov režima (Shehabat 2011). Če pogledamo podporo vojskujočih strani še iz strani zunanje pomoči pa je zadeva sledeča, glavni podporniki upornikov v Siriji sta Savdska Arabija in Katar, ki nudita oporo v orožju in drugimi sredstvi bojevanja. Potem je še na isti strani Turčija, ki podpira ideologijo Muslimanske bratovščine[28]. ZDA nudijo podporo v obliki hrane, orožja in nenazadnje tudi letalsko podporo proti boju z IS. Nekatere evropske države (Velika Britanija, Nemčija, Francija) oskrbujejo upornike z vojaškim materialom in letalsko podporo proti IS. Na drugi strani pa podporo sirski vladi nudita Iran in Rusija (vojaški interesi s prodajo orožja in trgovinsko sodelovanje med državama), ki se boji da bi s padcem režima nastala nova fronta na njenem ozemlju, če bi se nestabilnost začela širiti na Kavkaz (Berginc 2014).

Ravno zaradi različnih interesov tako akterjev znotraj države in mednarodnih podpornikov bo ta vojna trajala še nekaj časa. So se pa zedinili vsaj pri eni stvari, to je da so začeli boj proti Islamski državi in s skupnimi močmi deloma ustavili širjenje njenega vpliva znotraj Sirije in izven.

[28] Je predstavljala največjo opozicijo za časa vladavine Hafyza Assada, ki se je zaključila z uporom leta 1982, ko je vlada pobila med 25.000 in 40.000 ljudi v Hammi (Shehabat 2011).

4.2.1 Kibernetsko bojevanje v Siriji (2011–maj 2016)

Sirska telekomunikacijska infrastruktura je ena od najmanj razvitih na Bližnjem vzhodu, podobno kot v Iraku pred ameriško invazijo. Internet v Siriji je bil na voljo državljanom šele leta 2000, ko je oblast prevzel Bašar al-Assad. Problem je bil, da se državljani niso mogli svobodno izražati preko spleta, ker je vlada pozorno spremljala vse aktivnosti in seveda pri tem uporabljala filtriranje in cenzuro[29] (ukinjanje, blokiranje spletnih strani ki so povezane s politiko, manjšinami, človekovimi pravicami in zunanjimi zadevami ter blokiranje mobilnih sporočil[30]), da bi tako ohranila svoj legitimni položaj (Shehabat 2011). Če je bilo leta 2000 le 30.000 uporabnikov interneta, se je do konca leta 2010 razširilo na 1/5 prebivalstva (5 milijonov uporabnikov). Uporabniki so se povezovali preko povezave na klic in telefonskih naročnin, kjer je bil omejen prenos podatkov (256 kb/s) in zelo počasno predvajanje video vsebin. Širokopasovna povezava je bila omejena iz 2 razlogov: pomanjkanje fizične infrastrukture v ruralnih območjih in previsoka cena storitev za večino Sircev. Zato je mobilna povezanost v primerjavi z internetnim, znatno višja in bolj priljubljena (63%). Povezanost z mednarodno skupnostjo, je še vedno centralizirana in nadzorovana s strani vlade. Samostojne satelistke povezave so prepovedane. V Siriji sta 2 ponudnika mobilnih storitev, enega od njih je lastnik Assadov bratranec, kar zopet nakazuje, da je v večini vseh podjetij v lasti Assadove družine. Sirska vlada, je regulirala in nadzirala internet preko vladnega telesa Sirske telekomunikacije (ang. STE), ki ima v lasti vso telekomunikacijsko infrastrukturo in ponuja internetne storitve v državi. To vladno telo pa je del Ministrstva za telekomunikacijo. Situacija telekomunikacijskih storitev se je poslabšala v letih 2011, 2012 ko se je povečala inflacija in električni izpadi zaradi protestov ter represije sirske vlade. Komunikacijska infrastruktura je bila v nekaterih mestih (Homs) zelo poškodovana zaradi letalskih napadov in bombandiranja sirske vojske, zato so bile povezave motene in prekinjene (Freedomhouse 2012).

[29] Cenzura se je izvajala preko komercialno dostopnih programov. Neodvisni viri v zadnjih letih, so pokazali na uporabo programa ThunderCache (orig.), ki je sposoben spremljati in nadzorovati uporabnika. Sirska vlada pa je uporabljala tudi ameriški program Blue Coatsystems (orig.) za nadzor nad socialnimi omrežji in objavljenimi video posnetki (10.000 poskusov dostopa do opozicijskih Facebook spletnih strani, od tega so bili 3 od 5 blokirani in 2 od 5 dovoljeni, ampak zabeleženi) (Freedomhouse 2012).

[30] Dokumenti objavljeni na spletu so razkrili, da je posebna vladna enota Veja 225 ukazala Sirijatelu in ostalim mobilnim ponudnikom, da blokirajo sporočila, ki vsebujejo besede revolucija in demonstracija (Freedomhouse 2012).

Posebnost sirske revolucije v primerjavi z drugimi arabskimi pomladnimi revolucijami, je da so IKT izkoristili obe strani v sporu, Sirska elektronska armada[31] (ang. SEA - Syrian Electronic Army), ki je podprla režim Assada in Svobodna sirska vojska (ang. FSA - Free Syrian Army), ki podprla upornike režima. Rezultat tega je bila prva kibernetska vojna na socialnih omrežjih. Obe strani sta uporabljali naslednje metode bojevanja: napade na profile socialnih omrežij, dezinformacije, propagando in nadzor nad spletnimi aktivnostmi. Glavni povod aktivnega nesoglasja na internetu, je povzročila smrt 13-letnega dečka Hamzela Al-khateeba, katerega truplo so uporniki prikazali v videoposnetku na Youtubu, nato pa so v njegovem imenu odprli profil Mi vsi smo Hamza Al-khateeb (orig.»We are all Hamza Al-khateeb«) na Facebooku kot opomin kaj počne sirijska vlada civilistom. Od takrat naprej so se uporniki obrnili na vsa socialna omrežja in internetne multimedijske aplikacije (Skype, Yahoo Messenger, Whatsapp ipd.), kjer so v živo predvajali novice in informacije o uporu ter širili glas revolucije. V odgovor na te objave na spletu, je sirska vlada izklopila telekomunikacijske storitve v mestih Darra in Homs, da bi preprečila nadaljnje objave. Kljub temu to upornike ni ustavilo, namreč proxy modeme, satelitske telefone in mednarodne mobilne SIM kartice[32] so začeli tihotapiti iz sosednjih držav (Shehabat 2011). Ker so bili pametni telefoni in dostop do 3G brezžičnega omrežja pomembno orodje revolucionarjev, je sirska vlada šla še en korak dlje, prepovedala je uporabo in uvoz telefonov iPhone (omogočajo visoko kakovostne fotografije in videoposnetke). Dokumentarec Al Jazeere naj bi v celoti bil posnet s takšnim telefonom, saj je nošenje kamer ogrožalo življenja novinarjev (BBC v Shehabat 2011). Tako so uporniki za nadaljno spletno aktivnost uporabljali povezave na klic in proxy internetne modeme. Za svojo komunikacijo so uporabljali celo golobe pismonoše (v oblegani provinci Baba Amer v Homsu) in komunikacijo na osebni ravni (orig. »face to face«). Te metode so večinoma uporabljali za dostavljanje občutljivih informacij Sirskemu nacionalnemu svetu, ki je imel sedež v Turčiji. Objave na socialnih omrežjih so imele v zgodnji fazi revolucije veliko moč. Dvignile so zavest večinsko zatiranih Sunitov, ki so bili že leta zatirani. Vsaka enota FSA je ustanovila svojo Facebook stran in tiskovno središče. Kasneje pa so ustanovili Odbor za lokalno koordinacijo. Njegova glavna naloga je bila: širiti novice o stanju na bojišču mednarodnim medijskih hišam, štetje umrlih in širjenje strahu med Assadovimi vojaki, da bi

[31] SEA je bila registrirana 5. maja 2011 s strani Sirske računalniške družbe, organizacije ki jo je 1995 vodil sam predsednik Bašar, kar pomeni da naj bi bila podaljšana roka režima. Ampak še vedno obstaja nejasnost ali so člani te skupine zaposleni s strani vlade, ali so samo njeni priprvženci in podporniki (Fisher in Keller 2011). Njihove povezave oziroma registracijske domene so vladne, predsednik Bašar jih javno podpira, pozitivno o njih in njihovih akcija poročajo v državnih medijih (Freedomhouse 2012). Kakorkoli že, vodijo daleč najbolj izpopolnjeno in organizirano spletno podporo sirskemu režimu.

[32] V mestu Darra, ki je blizu jordanske meje, so uporabljali jordanske SIM kartice, na severu v mestu Aleppo pa turške (Shehabat 2011).

dezertirali v čim večjem številu in se pridružili upornikom[33]. Zaradi represivnih posledic vlade, so socialna omrežja postala glavni vir novic v arabskem in mednarodnem svetu medijev. Družbeni mediji so dobili tudi odločilno vlogo pri organiziranju protestov na ulicah (600 uličnih protestov je bilo organizirano preko socialnih omrežij v enem samem dnevu). Sirska vlada je želela čim bolj preprečevati akcije spletnih upornikov, zato so strokovnjaki uporabili več strategij kibernetskega bojevanja, da bi onemogočili širjenje informacij o uporu, ulovili aktiviste in uničili njihove komunikacijske kanale:

- *ustanovitev lažnega youtuba kanala*:

Uporaba Youtuba, je bila ključna platforma v pomladnih uporih, s katerim so dokumentirali vse dogodke in prikazali brutalnost sirske vlade nad protestniki (oprejemljivi dokazi in zločini posneti nad sirskim ljudstvom). Hkrati pa je deloval kot alternativni tisk, ki je imel svetovne razsežnosti. Youtube je predstavljal veliko nevarnost za režim in njegovo stabilnost v državi.

Iz maščevanja je SEA klonirala spletno stran, da bi ujela spletne aktiviste na 2 načina:

a) če je želel uporabnik komentirati pod videoposnetkom, je moral pustiti prijavne podatke,
b) namestili so zlonamerno programsko opremo (orig. DarkComet RAT), ki je bila zamaskirana kot posodobitev programa Adobe flash predvajalnika. Preko nje so dobili popolni nadzor nad računalnikom na drugi strani povezave (ESR v Shehabat 2011).

- *Facebook vmesnik in profili ter Twitter:*

Facebook je za upornike drugi najbolj pomemben spletni vir za izpostavljanje Assadovega režima. Ustanovili so 3 najbolj popularne spletne profile (Mi vsi smo Hamza Al-khateeb, Sirska revolucija 2011 in Mrežna revolucija Evrata), preko katerih so podajali vse informacije lokalnemu in svetovnemu občinstvu. Te strani so bile nenehna tarča SEA. Z zlonamerno programsko opremo je spremenila vmesnik Facebooka in s tem posledično prijavno povezavo Facebooka v Siriji z namenom, da bi pridobila imena in gesla ter podatke o uporniških facebook računih. Uspešno je odstranila uporniški profil Sirska revolucija 2011, ki je bil kasneje obnovljen s strani Facebook administracije. Isto

[33] Ko se je zgodil bombni napad na člane vlade 18. julija 2012, je Odbor lažno poročal, da so vojaki zapustili orožje in začeli bežati za svoja življenja. To je povzročilo, da je več kot 100 vojakov zapustilo vrste sirske vojske in se pridružilo upornikom (Shehabat 2011).

je SEA počela na Twitterju, ko je puščala komentarje na uporniški strani #Sirija (orig. #Syria) v prid režimu, ki pa jih je administracija sproti odstranjevala. Na Facebooku SEA ni bila dejavna od aprila do avgusta 2012, saj so izgubili spletno bitko proti upornikom, ki so poleg svojih množičnih aktivnostih na spletu, uživali še podporo s strani administracij vseh večjih socialnih omrežij. SEA je šele s septembrom ponovno nadaljevala boj pod imenom Pro-bataljon (ang. the Pro-Battalion) (Shehabat 2011).

- *Skypova šifrirna orodja:*

S programom Skype, so uporniki poročali v živo prek satelitskega programskega kanala Al Jazeera in ta je bil tarča SEA. Okužili so kanal s trojanskim konjem, ki je napadalcu omogočil nadzor nad računalnikom (kamero, kraja podatkov in gesel, onemogočanje protivirusnih programov da ga zaznajo) (Galbren v Shehabat 2011).

- *Informacijska vojna in akterji:*

Sirska država je bila bitko na 3 ravneh, s tremi različnimi nedržavnimi akterji, in sicer:

a) sirska država proti tujim medijskim organizacijam, ki podpirajo upornike (Al Jazeera, Al-Arabya, Reuters)
b) država proti posameznikom in skupinam na lokalni in mednarodni ravni (fizični in virtualni boj)
c) tuje organizacije ozirome skupine proti sirski državi (skupini Anonimni in Telcomix proti sirskemu režimu) (Shehabat 2011).

V kontekstu informacijskega bojevanja, je obilica kibernetskih napadov v letih 2011 in 2012 na obeh straneh spremenila dinamiko bojevanja v velikem obsegu. Platforme socialnega omrežja je preoblikovala v političnega. Napadi in dezinformacije so povzročile transformacijo socialnih omrežij v bojni prostor in tako spremenile njen prvotni namen uporabe. Na eni strani, je sirski režim s pomočjo SEA predstavljal svoje nasprotnike kot teroristične oborožene skupine, ki so kradli vojaško opremo, da bi ubijali sirski narod. Medtem ko je na drugi strani, FSA uporabljala moč socialnih mrežij za psihološko in kibernetsko vojno, s katero so prikazovali brutalnost vladnega režima (deloma so preko njih dosegli svoj cilj – vlada je nehala z letalskimi napadi nad civilisti) (Shehabat 2011).

V nadaljevanju bom na primeru časovnice prikazala samo bolj odmevne primere napadov, kjer je SEA s podporo sirskega režima napadla arabske in zahodne organizacije (medijske,

izobraževalne, finančne ipd.) in kjer so tuje hektivistične organizacije vračale udarec proti sirski državi oziroma SEA. Kajti uporniki so uporabljali splet bolj za širjenje glasu revolucije in poročanje o aktualnih dogodkih v državi, kot pa za obliko maščevanja na SEA in vlado. To so v veliki večini namesto njih opravljali drugi.

Kibernetska vojna med skupino Anonimni in SEA se je pričela že v letu 2011, ko so pripadniki SEA napadli alternativno socialno omrežje skupine Anonimni AnonPlus. Preusmerili so spletno stran AnonPlus na svojo Facebook stran, ki je podpirala ideologijo vladnega režima. Anonimni so takoj vrnili udarec z napadi (DDoS napadi, propagandna sporočila v obliki videoposnetkov nasilja in spletnih povezav protestnikov) na vladne strani sirskih veleposlaništev po svetu in na sirsko Ministrstvo za obrambo v sklopu Operacije Sirija. Svet hekanja in hektivizma se je s temi napadi skupine Anonimni spremenil (Hackmageddon 2011). Postavile so se nove meje kibernetskega bojevanja in arabska pomlad je postala primer, ko se je politično motivirano hekanje izkazalo za ključni dejavnik spreminjanja politične krajine na Bližnjem vzhodu. Hkrati pa je prvič skupina Anonimni napadla nekoga, ki ni v povezavi z njihovimi aretacijami ali podporo Wikiliksa (Limer 2011). Pričakovali so da bo SEA udarila nazaj, vendar se to ni zgodilo. Nepričakovano, je raje septembra usmerila svoj napad na Harvardsko univerzo, kjer so popolnoma spremenili spletno stran (vsebinsko in slikovno) in pustili sporočilo o svoji prisotnosti. Stran ni delovala nekaj ur. Napad so izvedli, ker se je ZDA vmešala v sirsko politiko in nasprotovala Assadovemu režimu (Coughlan 2011). Nato je skupina Anonimni zadala povračilni napad in postavila Assadovo vlado v neprijeten položaj, ko je ukradla na tisoče vladnih e-mailov, vključno s privatno e-pošto predsednika in njegove žene ter jih kasneje objavila na Wikiliksu (Apps 2012).

V začetku leta 2012 je vlada omejila dostop do mobilnih aplikacij, ki so jih uporabljali uporniki. Najbolj do tistih, ki so omogočali video prenose v živo (orig. Bambuser, Whatsapp) ter blokirali aplikacije, ki so prenašale sporočila preko internetne povezave (orig. Nimbuzz, MiG33). O blokadi in cenzuri spletnih strani ter sporočil, je odločal varnostni aparat Veja 225 ali izvršna veja oblasti. V februarju so sprejeli Zakon o regulaciji spletne komunikacije in spletnega zločina. Vsi lastniki spletnih strani, so morali podati vse svoje osebne podatke, shraniti kopijo vsebine spletne strani in njenega spletnega prometa, da je vlada lažje preverjala uporabnike, ki so dostopali do teh strani. V nasprotnem primeru, da lastniki ne bi upoštevali tega zakona, potem bi jih čakala zaporna kazen in globa (od 3 mesece-2 leti

zaporne kazni in od 3400-17.000$ denarne globe). Vlada je izvajala kontrolo tudi nad novinarskim poročanjem. Novinarji so dobili navodila od vladnih predstavnikov, da navajajo informacije uradne novinarske agencije SANA. Marca so uporniki in novinarji objavili preko 40.000 posnetkov na Youtube, ki so jih povzemale največje medijske hiše (CNN, Al Jazeera, BBC, Reuters). Zato so vladni strokovnjaki za internet in SEA zmanipulirali posnetke ter izvedli številne napade na računalnike spletnih sirskih aktivistov (metode ribarjenja in podtikanje zlonamerne programske opreme na povezave) in račune socialnih omrežij medijev, ki so objavljali njihove posnetke (Freedomhouse 2012). SEA je vdrla v twitterjev račun Reutersa (orig. @ReutersTech Twitter), da bi ustvarila vtis zloma upornikov. Račun je popolnoma zasegla, preimenovala (@ReutersME[34]) in iz njega pošiljala vrsto lažnih sporočil oziroma tweetov, da je sirska vojska porazila upornike v mestu Aleppu, da je upornikom zmanjkalo streliva ter objavila da je Washington financiral Al Kaido in da je medij Reuters v »železnem prijemu« Rotschield bančne industrije. Potem so se lotili twitterjevega računa medijske hiše Al Arabya in preko njega objavljali sporočila, da je v Katarju (ki je podpornica upornikov) politična kriza, premier ne opravlja več svojih dolžnosti in da je bila njegova hči aretirana v Londonu ter da se je zgodil državni udar s strani vrhovnega vojaškega poveljnika (Apps 2012).

V istem času je SEA sesula spletni blog socialnega omrežja LinkedIn in povezavo preusmerila na stran, ki je podpirala predsednika Assada (Holt 2012). Aprila so izvedli napad na osebni e-mail račun in Facebook profil opozicijskega predsednika Sirskega nacionalnega odbora Burhana Ghaliouna, v libanonskem spletnem časopisju so objavili naslove in telefonske številke upornikov. Ta objava je ogrozila mnoga življenja upornikov, vendar so se znašli in začeli po tem dogodku uporabljati SIM kartice in računalnike ubitih prijateljev, kar je onemogočilo vladi, da jih je izsledila (Freedomhouse 2012). Junija je SEA zopet izvedla podoben napad na Al jazeero in na njen twiterjev račun, kjer so objavljali sporočila v prid sirskemu režimu ter obtožili enega od katarskih medijev, da so ponaredili prispevek o civilnih žrtvah v Siriji. Skupno vsem tem napadom na medije je to, da imajo naslove, ki so zelo udarni in hitro opazni s strani javnosti, čeprav morebiti samo za kratek čas. Je pa cilj, da dosežejo milijonsko občinstvo po vsem svetu (Apps 2012).

Leto 2012 pa je zabeleženo tudi kot leto, ko je ZDA preko upornikov preizkušala novo tehnologijo, ki se je izognila vladnemu nadzoru. Uporniki so na svojih mobilnih telefonih uporabljali t.i. »panični gumb«, s katerim so v trenutku izbrisali imenik in sporočila ter

[34] ME kratica pomeni Bližnji vzhod (Apps 2012).

»internetni kovček«, ki je omogočal vzpostavitev internetne povezave ko na državni ravni ni povezave, uporablja pa se tudi z namenom izogibanja vladnemu nadzoru (Abbas 2012).

V letu 2013 je spomladi SEA izvedla enega najbolj odmevnih kibernetskih napadov, in sicer napad na Mednarodno tiskovno agencijo (ang. Associated Press), s sedežem v New Yorku. Ko je prevzela njihovo stran je objavila novico, da sta v Beli hiši odjeknili 2 bombi in da je predsednik Obama poškodovan. To je povzročilo paniko na ameriškem borznem trgu, kjer je bilo na ta dan izgubljenih 136 milijard dolarjev. Napad se je zgodil z metodo ribarjenja preko e-pošte, ko je eden od zaposlenih odprl priponko na sporočilu in na ta način omogočil napadalcem dostop do administratorskega sistema. Prav tako je napadla twitterjeve račune, zato jih je podjetje začasno odstranilo, dokler jih niso zopet spravili nazaj v normalo. To je bil zadnji napad v seriji kibernetskih napadov na ameriške medije in Twitter, ki so se zgodili pred tem (Foster 2013). Napad na časopisni medij New York Times, je izvedla celo dvakrat v roku dveh tednov. Zopet je uporabila metodo ribarjenja, ko je okužen mail poslala enemu od zaposlenih. V prvem napadu je bila stran nedosegljiva samo 90 minut, ker so tehniki hitro vzpostavili stran nazaj. Medtem ko v drugem, je SEA nadgradila napad in se lotila registracijskega sistema imenovanja domene (ang. »Domain name system registrars«). Tokrat stran ni delovala več kot 20 ur, ker se je direktno lotila upravljalcev povezave NYT, podjetja Melbourne IT, preko katerega je bil spletni naslov registriran. Vsem zaposlenim je poslala okuženo e-pošto (so narejene tako avtentično, da zaposleni zlahka nasedejo in odprejo priponko) in dovolj je bilo da je pošto odprl samo eden. Na ta način je SEA pridobila vsa gesla in dobila dostop do strežnika, kjer je stran popolnoma sesula (Todd in Brown 2013). Melbourne IT so ponovno vzpostavili stran in pravilno ime naslova, spremenili geslo in zaklenili zapise, da so preprečile nadaljnje spremembe spletne strani (Chonney 2013).

Napad na Twitter je bil podobne narave, isto so se lotili spreminjanja registracijske domene (glej sliko 4.9) preko podjetja Melbourne IT, saj ima Twitter istega upravljalca spletnih strani kot NYT. S to razliko da stran niso popolnoma sesuli, ampak je bil samo moten dostop do nje. Namreč to, da nekaj ni v redu s stranjo so administracijo opozorili uporabniki (Aguilar 2013).

Slika 4.9: Napad na Twitter, na registracijsko domeno

Aguilar (2013).

Po napadu na NYT, Twitter in Mednarodno tiskovno agencijo so ameriške varnostne agencije posumile, da po določenih lastnostih napada (takšni napadi zahtevajo določeno strokovnost in znanje v računalništvu), so sledi vodile na iransko stran. Možen scenarij je tudi, da je sirska vlada plačala za iranske hekerske storitve (Riley in Strohm 2013).

Z metodo ribarjenja in prevzemi računov socialnih omrežij, so člani SEA napadli še sledeče ameriške in britanske novičarske medije: Thomson Reuters, UK Guardian news paper, Daily Telegraph, The Onion, ITV, NBC news, Huffington Post, Wall Street Journal, Global Post. Razlog napadov je pri vseh medijih isti, ker objavljajo neresnične novice o sirskem konfliktu

(Foster 2013). Tarča pripadnikov SEA, je bila tudi ena najbolj svetovno popularnih multimedijuskih aplikacij Viber (glej sliko 4.10).

Slika 4.10: Napad na Viber aplikacijo

Buscemi (2013).

Uporabili so isto metodo kot pri napadih na medije. Z napadom so želeli opozoriti uporabnike, da je večinski del sistema Viberja vohunil za uporabniki in sledil vsakemu IP naslovu. Do podatkovnih baz niso dostopali, želeli so samo pozornost javnosti (Buscemi 2013). Tudi račun socialnih omrežij (Facebook in Twitter) Barracka Obame, ni bil izvzet iz teh sirskih operacij na spletu. Vdrli so v račun od Gmail e-pošte uslužbenca Organizacije za ukrepanje (ki je skrbel za medijsko kampanjo Obame). Nato so spremenili objavljene povezave na profilih socialnih omrežij (povezave so vodile do 24-minutnega propagandnega videoposnetka na Youtubu) (Paulson 2013).

Konec leta je zaznamoval napad še na eno svetovno popularno aplikacijo, to je Skype. Vdrli so v spletno stran bloga in začasno prevzeli kontrolo nad twitterjevimi in facebookovimi računi. Razlog so navedli, da je podjetje podajalo informacije vladnim organizacijam ter izvajalo nadzor nad uporabniki. Ker je podjetje, ki je prevzelo Skype tudi lastnik Microsofta, so nagovarjali uporabnike naj ne uporabljajo njihovih e-mail računov (Hotmail in Outlook), ker so nad njimi tudi izvajali nadzor (Ovide 2014).

Po kibernetskih napadih v letu 2013, so ameriške banke in nekatera podjetja poostrile spletno varnost svojih sistemov in začele vlagati ogromno sredstev v to področje (Npr.: banka JP Morgan Chase je v tem letu namenila 200 milijonov dolarjev). ZDA so zaradi rednih kibernetskih napadov s strani SEA in uporabe kemičnega orožja nad sirskim ljudstvom v Damasku, resno razmišljale o povračilnih ukrepih[35] (da bi vojaško posredovale) proti Siriji. Vendar se za to niso odločile, ker so se bale posledic, ki bi jih prinesla naveza Sirija-Iran-Rusija (Foster 2013). V zvezi z ameriškim vojaškim posredovanjem proti Siriji, so nato dosegli diplomatsko rešitev. Sirski režim naj bi se na pobudo Rusije odrekel kemičnemu orožju in se pridružil državam podpisnicam Konvencije o kemičnem orožju (Prelc Dakič 2013, 19). Je pa ZDA v tem letu izvajala operacijo »podtikanja vsadkov-vohunskih programov« v sirske strežnike, ki je ameriški agenciji NSA omogočilo spremljanje sirskih internetnih in mobilnih komunikacij (Haynard 2015).

Kibernetsko vohunjenje je bila v času sirskega konflikta pomembna strateška taktika s strani sirske vlade. Namreč s to metodo si je zagotovila prednost na bojišču. Med novembrom 2013 in januarjem 2014 je SEA ukradla kritične dokumente (strateške in taktične vojaške načrte, potrebe po preskrbi) in pogovore sirske opozicije preko programa Skype. Te so obelodanili na spletu. Podatke (glej tabelo 4.11) so pridobili na zelo prefinjen način oziroma s taktiko, ki je stara že stoletja, uporabili so avatarje privlačnih in simpatičnih žensk ter na ta način zavedli nasprotnika. Ciljnim tarčam so pošiljali fotografije teh »žensk«, ki so bile okužene z vohunskim programom (uporabili znan program DarkComet RAT). Ko je oseba na drugi strani pogovora kliknila na sliko, se je program avtomatsko naložil na računalnik in omogočil napadalcu, da je dobil popoln nadzor nad računalnikom. Ti podatki niso pripadali samo opoziciji, ampak tudi novinarjem, humanitarnim delavcem in vsem, ki so podpirali sirske upornike. Koliko so ti obveščevalni podaki vplivali na bojne operacije, ni znano. Čeprav po drugi strani pa je opozicija prekinila eno od glavnih operacij ravno zaradi tega, ker so sumili da je vlada ukradla bistvene vojaške načrte (Fireyee 2015).

[35] NSA je imela izdelan kibernetski načrt na sirsko elektronsko infrastrukturo, ki bi lahko ohromila zračne obrambne sile in ogrozila napajanje električnega omrežja. Vendar Obama oziroma ameriški kongres za ta napad ni dal privolitve, ker bi lahko prišlo do stopnjevanja kibernetske vojne med ZDA in Sirijo ter njenimi zaveznicami (Haynard 2015).

Tabela 4.11: Tabela ukradenih informacij sirski opoziciji

Vojaške informacije	• Pogovori in dokumenti načrtovanja vojaških operacij • Podrobnosti o vojaški opremi in lokacijah enot na bojišču • Imena članov bojnih skupin in njihova orožja
Politične informacije	• Razprave političnih strategij • Politični manifesti in zavezništva znotraj opozicije
Humanitarne aktivnosti in financiranje	• Ocene humanitarnih potreb • Seznam materialov za gradnjo begunskih taborišč • Evidenca izplačil za humanitarno finančno pomoč
Osebni podatki beguncev	• Zahtevki za pomoč beguncev za turške oblasti • Seznami prejmkov pomoči, skenirane osebne izkaznice
Mediji in komunikacija	• Dokumenti in informacijska strategija, ki se nanašajo na objavljanje v medijih • Poročila o stanju žrtev • Informacije o zlorabah pravic

Fireeye (2015).

Začetek leta 2014 je SEA zopet zaznamovala z napadom na enega od najbolj znanih medijev v ZDA, to je CNN. Za nekaj čas je prevzela nadzor nad računi socialnih omrežij in blogi ter pustila sporočilo naj nehajo objavljati lažne novice, preimenovali so tudi ameriškega predsednika v Obamo Bin Ladna. Hkrati pa so izvedli še napad na univerzo Kolumbijo in Organizacijo za človekove pravice (Shoichet 2014).

Napade na globalne medijske organizacije (CNBC, Forbes, Reuters, Chicago Tribune, PC World, Independent, The LA Times, The Evening Standard, The Boston Globe, OK Magazine, NBC, CBC, The Sun, IBT, Femme Actuelle, La Repubblica in drugi) so tokrat v tem letu izvajali z drugačnimi metodami z razliko od prejšnjih (okuženi maili poslani zaposlenim) v letu poprej. Pri Forbsu so v nadzorno ploščo administratorja in 3 twitterjeve račune (@ForbesTech, urednikov račun @The AlexKnapp in račun, ki upravljalke financ Forbsa @SamSharf) vdrli preko WordPressa (odprtokodni blog oziroma program za objavo člankov). Stran so uporabili samo za svojo propagando in da so pridobili pozornost javnosti, druge škode ni bilo (Gilbert 2014).

Pri ostalih medijih pa je SEA vdrla preko registaracijske platforme Giggya (GoDaddy.com), ki so jo uporabili kot posrednika (niso jo napadli direktno) pri napadu, da so dostopali do ciljnih tarč. Giggya upravlja z registracijsko domeno več kot 700 vodilnih blagovnih znamk. Napadene spletne strani niso popolnoma sesuli, ampak so vse povezave samo preusmerili na svojo uradno propagandno stran. Tehnične službe medijskih organizacij so se s problemom ukvarjali več ur, preden so vzpostavili stanje v normalo. Ponekod so morali uporabniki iz varnostnih razlogov počistiti predpomnilnik brskalnika. Platforma in njeni podatki niso bili ogroženi, so pa zaradi teh napadov tehnične službe poostrile in nadgradile varnostne ukrepe (CBC News 2014). Na deseto obletnico ustanovitve socialnega omrežja Facebook so člani SEA skušali ukrasti administratorjevo registracijsko domeno (orig. »Domain registrar-MarkMonitor«). Ta podvig jim ni uspel, ker je vse skupaj zahtevalo preveč časa, ki pa ga niso imeli na razpolago. Zato so samo spremenili kontaktne podatke in preusmerili povezavo na svojo uradno stran. Kot razlog so navedli, ker je administracija Facebooka brisala račune od SEA in ker so podpirali upornike režima (Kumar 2014).

Napad na Reuters, so sirski hekerji izvedli preko oglasnega sporočila Taboola. Tako da spletne strani, ki so posedovale isti tip oglasnih sporočil (Yahoo, Fox News, BBC), so s tem postale potencialne tarče napadov Sirske elektronske armade (Payne 2014). Razlogi za napad na medijske organizacije so bili isti kot v prejšnjih primerih, zaradi sovražnih izjav do SEA in sirskega režima oziroma pisanja »lažnih« člankov o konfliktu.
Glede na to da SEA uporablja pomoč hekerjev izven ozemlja Sirije, tudi ZDA, natančneje agencija FBI uporablja pomoč hektivistične skupine Anonimni. Eden izmed hekerjev z vzdevkom Sabu (drugače Hector Xavier Monsegur) je sklenil dogovor z ameriškimi oblastmi, da v zameno za informacije in pomoč pri napadanju na tuje strani ameriških največjih nasprotnikov (v Siriji, Braziliji in Iranu) ne odsluži zaporne kazni. Monsegur je uporabil svoj vpliv znotraj skupine Anonimni in vodil ostale hekerje, da so napadli vladne sirske spletne strani – banke, ministrstva, da si je ameriška vlada posledično lahko zagotovila vpogled in dostop do sirskih sistemov (Gilbert 2014).

Leto 2015 je SEA začela z napadi na evropski celini, na francoski spletni časopis Le Monde. Z uporabo so metode okuženega maila, jim je uspelo vdreti le v twitterjev račun, kjer so objavili sporočilo, da obsojajo teroristične napade v Parizu in hkrati še francosko vlado, da podpira terorizem. Do glavne strani časopisa niso mogli dostopati zaradi dobre varnostne zaščite, preko katere se niso mogli prebiti. Uspelo se jim je prebiti le do orodja za objavljanje

člankov, nato pa so iz obupa izvedli DDoS napade in spletno stran poplavili z ogromno količino podatkov, da je stran počasneje delovala. Francija je bila v istem tednu ko se je ta napad zgodil, pogosta tarča kibernetskih napadov še s strani radikalnih islamističnih skupin. Zato je napovedala da bo ustanovila »kibernetske patrulje«, ki je napadalcem sledila in hkrati opozarjala na nevarnost islamske indokrinacije na spletu (Samuel 2015). SEA se je lotila tudi turške vlade in vdrla v številne njihove e-maile (Pultarova 2015).

Poleti istega leta je izvedla napad na twitterjev račun Ameriške vojske (preko omrežja Limelight je dobila dostop do nadzorne plošče računa urada za javne odnose) in preden je račun vojska začasno odstranila s spleta, jo je SEA sprva uporabila za objavljanje svojih propagandnih sporočil (da ameriški poveljniki usposabljajo teroriste, navezava na IS) nato pa še uporabila metodo DDoS napadov (glej sliko 4.12) (Lawler 2015).

Slika 4.12: Napad na Ameriško vojsko

Gallagher (2015).

Ista propagandna sporočila je pustila tudi na strani Washington Posta, da je ZDA podpirala teroriste v Siriji (IS) (Price 2016).

V jeseni 2015 je Vladimir Putin poslal rusko vojsko na sirsko ozemlje in začel izvajati letalske napade na IS. ZDA s koalicijo so na položaje IS izvajale letalske napade že dobro leto poprej. Rusija je svojo vlogo vojaških vdorov v druge države tudi nadgradila s kibernetskimi bojevanjem. Sestavljen je iz dveh splošnih faz, ki se lahko kronološko prekrivajo v sami izvedbi:

- *Prva faza*: Rusija izvaja veliko število kibernetskih napadov na ciljno državo, da upočasni ali onemogoči komunikacijski sistem in ovira usklajevanje obrambnih sil nasprotnika ter zamaskira prihod ruskih sil na ozemlje.
- *Druga faza*: prodor ruskih sil v ciljno državo, kibernetski napadi se lahko še vedno izvajajo kot podpora pri vzpostavitvi ruskih vojaških sil znotraj države nasprotnika (Givens 2015).

Obe fazi napadov je ruska vojska uporabila pri vdoru v Gruzijo, v pokrajino Abhazijo in Ukrajino (Krim) (Givens 2015). Konec 2015 in v začetku leta 2016 so bili ruski hekerji vpleteni v kibernetsko vohunjenje[36] v Siriji. Tarče napadov so bile opozicija, dobrodelene organizacije in Sirski obzervatorij za človekove pravice ter delujoče skupine izven sirijskega ozemlja (predvsem v Turčiji). Napadi so trajali 4 dni, metodo DDoS pa so uporabili na 400.000 turških spletnih strani, ki so imele v naslovu .tr domeno (TheNewArab 2016).

V letih 2015 in 2016 je svetovno medijsko pozornost na spletu bolj dobila IS kot SEA, zato je v primerjavi s prejšnjimi leti, v teh letih ni bilo toliko zabeleženih napadov. So pa v letu 2016 ZDA obtožile 4 člane SEA računalniškega hekanja in potegavščine. Ahmad Umar Agha (starost 22 let) znan pod vzdevkom »Profesionalec« in Firas Dardar (starost 27 let) z vzdevkom »Senca« sta obtožena kriminalne zarote proti ZDA:

- zaradi potegavščine glede terorističnega napada in poskusa upora ameriških OS,
- goljufivega dostopa do naprav, nepooblaščen dostop in poškodovanje računalniške opreme in nezakonit dostop do shranjenih komunikacij,
- nedovoljeno posedovanje funkcije za preverjanje pristnosti

in še Dardar in Peter Romar sta posebej obtožena zaradi večih zarot:

- nepooblaščen dostop do in poškodovanjem računalnikov in s tem povezane oderuške dejavnosti,
- prejemanje prihodkov od izsiljevanja,
- pranje denarja,
- kršitve predpisov ameriških sankcij proti Siriji,
- nezakonite meddržavne komunikacije

[36] Ruski vohunski programi so zasnovani tako, da lahko izbrišejo podatke, širijo napačne informacije iz uradnih računov socialnih omrežij, omogočajo dostop do sistemov in stikov ter do občutljivih podatkov (TheNewArab 2016).

FBI agencija ponuja razpisano nagrado 100.000 dolarjev za kakršno koli informacijo o teh 4 članih SEA (Price 2016).

Glede na to kaj vse lahko pridobimo s kibernetskimi napadi (informacije in občutljive podatke, promoviranje lastne propagande, pridobivanje in ukinjanje denarnih sredstev, onemogočanje delovanja spletnih strani in računov ipd.) je pomembno poudariti, da je nujno potrebna varnostna zaščita računalnikov in mobilnih telefonov, ki hekerjem ne dovoljuje enostavnega vdora v naprave. To načelo velja tudi za vojaške kibernetske enote in hektivistične skupine, ki so primorane z napredovanjem tehnologije razvijati obrambni vidik kibernetskega bojevanja. Mnoge korporacije Google, Twitter so začele svojim strankam ponujati dvojni korak preverjanja identitete uporabnika, kar pomeni da varnostni mehanizem deluje četudi nekdo ukrade geslo. Uporabnik se normalno prijavi v račun, kjer mora nato še odtipkati kodo, ki jo dobi preko sms sporočila. Na ta način se še enkrat preveri uporabnikova identiteta. S tem načinom so malce otežili hekerjem prevzemanje računov, ki so jih poprej pridobili z lahkoto.

4.3 Primerjava kibernetske oblike bojevanja Iraka in Sirije

Obe državi imata izkušnje z avtoritativnim režimom, kar pomeni da so državljani bili in so še (Sirija, kjer takšen režim še vedno obstaja z razliko v Iraku) zatirani s strani vlade oziroma predsednika države. Mediji in telekomunikacije so v takšnem primeru pod nadzorom vlade, ni svobodnega izražanja in vsak, ki to počne, je zakonsko preganjan. In ravno ti dogodki so povzročili revolucijo v obeh državah, ko so se ljudje naveličali represije in zatiranja s strani vlade. Obdobje v času Husseina in Bašarjevega očeta, je prineslo to, da državi nista vlagali v razvoj IKT in s tem je bilo posledično slaba dostopnost do internetne in mobilne povezave. Ponavadi je bila ta dosegljiva le v večjih mestih in le politični in vojaški eliti. V Iraku je imelo dostop do interneta le približno 12.000 ljudi kar je zelo majhno število glede na število prebivalstva. V Siriji ni bilo nič drugače, pred letom 2000 je imelo dostop do interneta le 30.000 Sircev. Informacijska infrastruktura je bila v obeh državah zastarela, nerazvita v oddaljenih mestnih območij. Zunanjih ponudnikov interneta ni bilo, vse je bilo centralizirano in monopolizirano s strani države. Po ameriški vojaški invaziji v Iraku in s prihodom na oblast Bašarja al-Assada (navdušenega računalničarja) so se razmere glede IKT začele izboljševati (povečalo se je število ponudnikov interneta in mobilnih komunikacij, povezljivost infrastrukture se je razširila na ruralna območja). Dostop do interneta in mobilnih

komunikacij so dobili vsi državljani obeh držav. Številke uporabnikov le-teh so se z leti povečevale: 17% celotne populacije v Iraku uporablja internet, v Siriji 30% (CIA World Factbook 2016). Ampak državljanska vojna, ki se je razvila v obeh državah, je marsikje uničila infrastrukturo, tako da so bile občasno povezave motene oziroma prekinjene. V Siriji je sirska vlada namerno izklapljala mobilno in internetno povezavo, da sirski uporniki ne bi več objavljali video posnetkov in slik dogajanja v državi, to je vladnega nasilja nad civilisti. Prva kibernetska vojna na spletu, ki se je odvijala med uporniki in državo se je začela v Siriji, ko so revolucionarji dvignili socialna omrežja na novo drugo raven. Prvotno namembnost socialnih omrežij (povezovanje in komuniciranje na lokalni in globalni ravni) so spremenili v propagandni namen, namreč revolucionarjem so socialna omrežja postala ena od glavnih orožij v uporu. Z objavo posnetkov in slik so vršili pritisk mednarodne javnosti na predsednika Assada in njegovo vlado. V Iraku je razvoj kibernetskega bojevanja sovpadalo z čedalje večjim vplivom IS, tako ozemeljskim (zavzemanje področij v severnem Iraku in deloma v Siriji) kot političnim (več milijonov ljudi je padlo pod nadzor IS). Glavni napadalki, ki sta izvajali redne kibernetske napade na zahodne države in njihove organizacije sta bili IS (ki je začela z letom 2014) in SEA (že od samega začetka revolucije – 2011). Glavni razlog začetka kibernetskega bojevanja na spletu, je bil vmeševanje zahodnih držav v politiko in ozemeljsko celovitost Bližnjega vzhoda (v Iraku zaradi vojaške okupacije države s strani ZDA in njene koalicije). In pa seveda, ker so zahodne države imele vojaško premoč na terenu, se je kibernetsko bojevanje izkazalo za pravo rešitev upornikov, da so jim vsaj malo povzročili škode. Le-te v primerjavi z Irakom in Sirijo imajo zelo razvejano in razvito IKT, zato je lažje napasti tarče in povzročiti škodo. Uporniki se zavedajo tega, da četudi bi velesile izvedle povračilne ukrepe, za njih ne bi bilo bistvene razlike, saj je državljanska vojna v teh letih v veliki meri na območjih napadov uničila IKT. Uporniki režimov so se kljub temu znašli in prišli do globalne povezave s spletom. Uporabljali so proxy modeme (v Iraku), povezave na klic (v Siriji), satelitske telefone in mednarodne SIM kartice (predvsem sosednjih držav). Tako so bili kibernetsko bitko na spletu še naprej, kljub oviram ki sta jih postavljali državi. Oba akterja IS in SEA kategoriziramo kot nedržavna akterja. IS ima na spletu svoje podpornike, ki so večinoma civilisti (prostovoljci, privrženci ali plačanci), ki v njihovem imenu vršijo kibernetske napade. Medtem pa Sirski elektronski armadi uradno ni bilo dokazano, da je državna enota kljub temu da ima registrirano domeno, ki je povezana z državo in v imenu sirskega predsednika ter vlade bije bitko na spletu. Zato lahko zaradi vpletenosti nedržavnih akterjev trdim, da gre za družbeni konflikt nizke intenzivnosti.

Metode, ki sta jih obe skupini uporabljali pri svojih napadih so večinoma iste:

- DDoS napadi na spletne strani in socialna omrežja,
- ribarjenje (okužen mail poslan tarči napada) - prevzemanje računov socialnih omrežij in preko njih objava propagandnega materiala in puščanje grozilnih sporočil,
- uporaba zlonamerne programske opreme (Njrat Bitfrost, DarkComet) za pridobivanje obveščevalnih podatkov, brisanje ali spreminjanje podakov, pridobitev popolnega nadzora nad računalnikom ali strežniki tarče napada

Člani SEA so v primerjavi s hekerji IS (ti v praksi pogosteje uporabljajo osnovne metode kibernetskih napadov - opisani zgoraj) bolje računalniško izobraženi, kar se je izkazalo tudi v praksi. Ti občasno izvajajo sofisticirane napade, ki zahtevajo več znanja in strokovnosti (napad na AP, napadi preko oglasnih sporočil, spreminjanje registrskih domen spletnih strani). IS za izvedbo težjih napadov, plača hekerske storitve na črnem trgu. IS bije kibernetsko vojno proti državnim akterjem (proti iraški kibernetski enoti in vojaškim kibernetskim enotam ZDA) in nedržavnemu akterju (hektivistični skupini Anonimni, ki je napovedala spletno vojno takoj po terorističnih napadih v Franciji).

Kar se tiče financiranja skupin, SEA ima podporo sirske vlade, zato ji glede tega ni potrebno skrbeti, medtem ko se IS financira preko prodaje nafte in plina na črnem trgu, uporablja pa tudi nezakonite zvijače na spletu – ustanavlja humanitarne neprofitne spletne organizacije preko katerih potem zbira denarna sredstva, ki jih nakažejo donatorji. SEA uporablja splet predvsem za politični in propagandni namen, medtem ko IS uporablja internet tudi za druge namene: rekrutacijo borcev po vsem svetu, psihološko ustrahovanje nasprotnikov in ljudi, ki jih imajo pod nadzorom s prikazovanjem brutalnih video posnetkov obglavljanj in mučenj, širjenje kalifata (verski vidik), zbiranje denarnih sredstev, poročanje v živo iz bojišča. Zato je pomembno dejstvo, da se vpliv IS lahko zmanjša tako, da se čim bolj onemogoči prodaja nafte in plina na črnem trgu (ker ima IS od tega največji zaslužek), fizično uniči transportno in komunikacijsko strukturo in na dnevni bazi redno ukinja račune socialnih omrežij preko katerih širijo svojo ideologijo. Slednja je pravzaprav najtežja, kajti ko administracija socialnih omrežij ukine en račun, se pod drugim imenom pojavi že 10 novih. Isti problem imajo tudi s SEA, ki ji tudi redno brišejo račune. Ker kibernetski prostor ni fizično omejen prostor, je izredno težko biti kibernetsko vojno proti radikalnim verskim skupinam. Zato bodo v prihodnosti države lahko samo omejile delovanje teh skupin v kibernetskem prostoru, ne bodo pa jih mogle onemogočiti in izkoreniniti.

Poudariti pa je treba še pomembnost varnostnega vidika sistemov globalnih in državnih organizacij, ki so nenehna tarča napadov s strani IS in SEA. Ni dovolj, da organizacije samo denarno vlagajo v redno posodabljanje varnostnih sistemov in opreme, po mojem mnenju je kjučen vidik še izobraževanje zaposlenih o varnostnih kibernetskih ukrepih. Saj so v mnogih primerih pripadniki IS in SEA prišli do podatkov in dostopa sistemov ravno zaradi nespametnega ravnanja zaposlenih, ki so odpirali okužene maile in priponke. Seveda pa ne smemo pozabiti na profesionalno izobražen kader bodisi v organizacijah (tehnična računalniška služba) ali vojski (enote za kibernetsko obrambo), ki imajo znanje in sposobnosti, da odvračajo takšne napade. Tudi ti so eden od ključnih elementov kibernetske obrambe. Torej, redno izobraževanje zaposlenih in dober varnostni sistem morata sovpadati, da lahko organizacije preprečijo čim večje število kibernetskih napadov.

5 SKLEP

Kibernetski napadi niso več grožnja v glavah pisateljev znanstvene fantastike in teoretikov zarot, temveč je resnična, zdaj in tukaj. Napadi v ZDA se na vladna ali privatna omrežja dogajajo vsaki dve sekundi. (Kindamo 2015, 51). Kibernetsko bojevanje predstavlja 5. domeno vojskovanja, poleg ostalih štirih, ki so zemlja, zrak, morje in vesolje (Mahon 2016, 68).

Kibernetska oblika bojevanja postavlja danes oboroženim silam nove izzive, in sicer nasprotnik je anonimen, neotipljiv, deluje lahko od kjerkoli in za svoje delo uporablja orodja, ki so dostopna vsakomur. Boj z njo zahteva sodelovanje tako znotraj države, kjer je pomembno sodelovanje obveščevalnih agencij, civilne gospodarske strukture, ki razvija IKT in oboroženimi vojaškimi silami. Za boj proti zunanjemu sovražniku pa je pomembno sodelovanje med državami na vladni in vojaški ravni, da bi tako dosegle čim večji uspeh in učinkovitost kibernetskega bojevanja.

Glede postavljenih hipotez na začetku svojega dela, sem med pisanjem diplomske naloge, ugotovila naslednje. Prva hipoteza se je glasila, da je kibernetsko bojevanje del informacijskega vojskovanja. O tem je med prvimi pisal Martin Libicki, ki je dejansko zastavil splošne okvire informacijskega vojskovanja za nadaljnje analize in razprave drugih avtorjev. Navedbe definicij umestitve kibernetskega bojevanja, ki sem jih navedla v poglavju 3.2 potrjujejo mojo prvo hipotezo.

Druga hipoteza se je glasila, da kibernetsko bojevanje uporabljajo izključno samo vojaške OS in da so tarče samo vojaške. To ne drži, namreč zaradi prepletenosti civilne in vojaške strukture, je težko točno določiti vojaški cilj, ne da bi pri tem bile posledice za civilni del prebivalstva. Že iz vidika kolateralne škode, ki se lahko zgodi med napadom ne morem potrditi, da so tarče napadov samo vojaške, v teoriji lahko potrdim, v praksi pa to ni izvedljivo. Na primer vojaški objekti, bolnice, elektrarne, transport, bančni sistemi si delijo isto električno in komunikacijsko omrežje. Prvotno je bilo mišljeno, da bi to obliko bojevanja uporabljale samo OS (ker imajo za to potrebna vsa sredstva v obliki financ, razvoja tehnologije in opreme) ob podpori vojaškega posredovanja. Ampak s pojavom hektivističnih (v mojem primeru skupina Anonimni, SEA) in radikalnih islamističnih skupin (IS) na spletu, so se meje kibernetskega bojevanja prestavile izven državnih okvirjev, zatorej zopet ne morem potrditi, da je kibernetsko bojevanje zgolj domena vojskovanja OS.

Tretja hipoteza se glasi, da se je kibernetsko bojevanje v Iraku izvajalo v okviru informacijskih operacij v prvi fazi vojaškega posredovanja. To drži, namreč ameriška vojska ima v Skupni kibernetski doktrini (JP3-13) opredeljeno, da se kibernetsko bojevanje, ki je del informacijskih operacij, izvaja kot podpora vojaškim operacijam na terenu oziroma najbolj v praksi sovpada z letalskimi napadi, ki so del prve faze vojaškega posredovanja. V primeru Iraka so se kibernetski napadi izvajali že pred samo Operacijo Iraška svoboda (napad na spletno stran predsednika Husseina) in med samo operacijo v obliki pošiljanja sms sporočil in e-pošte vojaškim poveljnikom in ter gospodarski in politični eliti, naj ne podpirajo več režima Husseina. Tisti glavni kibernetski napad, ki naj bi se zgodil na finančni sistem iraškega predsednika pa se ni uresničil, ravno iz razloga globalne prepletenosti civilnih sistemov. Kajti iraški finančni sistem je povezan s francoskim in če bi se Američani odločili za ta napad, bi čutila posledice vsa Evropa in posledično tudi druge države sveta. Na kratko povedano zgodil bi se domino efekt na celotni globalni ravni. Irak ni izvajal povračilnih ukrepov proti ZDA vse do 2014, ko je IS razširila svoj vpliv tako na spletu kot na iraškem ozemlju. Sirija je izvajala povračilne ukrepe oziroma podpornica režima SEA. Uspešni sta bili obe skupini v smislu političnega in psihološkega vidika. S kibernetskimi napadi na zahodne in arabske medije ter organizacije sta povzročali gospodarsko škodo za tisti čas, ko so bili računi in strani nedejavne. Namreč mediji služijo preko oglasnih sporočil, ki se pojavljajo samo v primeru čim večjega števila sledilcev na profilih socialnih omrežij in po tem koliko so obiskane njihove strani. In v primeru globalno poznanih medijih kot so New York Times, Global Post, The Wall Street Journal, The Sun, NBC, Reuters in drugi štejemo številke v milijonih. Zato sta skupini izvajali napade ravno na te medije, ker je pozornost svetovne javnosti velik pa čeprav samo za časa napada.

Razvoj orožja za kibernetsko bojevanje (napad in obrambo) bo v prihodnosti vroča točka za zapravljanje denarja v tej smeri. Namreč vse kaže na to, da bodo države glede na razmah in pogostost kibernetskih napadov na njihove sisteme, vse več sredstev namenjale za 5. domeno vojskovanja. Še vedno pa bo potekala nadaljna razprava o tem ali naj se kibernetska orožja vedno uporabijo v primerih vojaškega posredovanja, ali samo občasno ko bodo vojske imele dostopne tarče napada. Kibernetsko bojevanje lahko primerjamo z učinki UMO, namreč posledice, ki jih lahko prinesejo neprekinjeni kibernetski napadi neke države na drugo, ima lahko katastrofalne učinke (uničenje civilne in vojaške strukture). Če bi razneslo IKT največjih sil ZDA, Rusije, Kitajske bi posledice občutil ves svet. Zato pa lahko trenutno stanje primerjamo z elementi hladne vojne (popuščanje napetosti), ker nobena izmed sil ne želi

izvesti uničujoče kibernetske napade, čeprav imajo vsa sredstva in tehnologijo. Zaradi globalne povezanosti sistemov, še vedno omejujejo oziroma skrbno načrtujejo uporabo kibernetskih napadov na nasprotnika.
Kombinacija tehnologije in informacijske prevlade v kibernetskem prostoru, bi v prihodnosti zagotovila, da bi bila sodobna vojna hitra in enostavna in brez večjih žrtev na obeh straneh vključenih akterjev. Saj v primeru kibernetskega bojevanja ne prihaja do neposrednega fizičnega stika na bojišču, ker se vse odvija na virtualni ravni preko IKT (Rezk 2010).

Zavedati pa se moramo, da pri informacijski revoluciji in tehnološkem napredku, je še vedno pomemben človeški faktor. Namreč gre za obliko bojevanja, ki vključuje usposobljene hekerje in je podprta z elektronsko in človeško inteligenco, da bi prekinili tuja (nasprotnikova) računalniška omrežja ter informacijske sisteme (Gertz 2016). Pri vsem tem ne smemo pozabiti na vse večjo medsebojno povezavo tehnologije in človeka, saj ljudem vsak dan te informacijsko-komunikacijske naprave olajšujejo življenje tako v poslovanju, komuniciranju, druženju in navsezadnje vojskovanju. Zato je tudi IKT postala nepogrešljiva oprema sodobnih vojaških sistemov in vsakega vojaka sodobnih oboroženih sil.

6 LITERATURA

1. Abbas, Mohammed. 2012. Syria activists using U.S. tech to beat curbs. *Reuters*, 21. junij. Dostopno prek: http//: www.reuters.com/article/us-syria-us-technology-idUSBRE85K14C20120621 (10. maj 2016).
2. AFP. 2015. IS hacker take down Syria war monitor site. *Security week*, 8. julij. Dostopno prek: http//: www.securityweek.com/hackers-take-down-syria-war-monitor-site (10. maj 2016).
3. --- 2016. US military conducting cyber attacs on Daesh. *Gulf wars*, 27. april. Dostopno prek: http//: gulfnews.com/news/mena/iraq/us-military-conducting-cyber-attacks-on-daesh-1.1813240 (10. maj 2016).
4. Andress, Jason in Steve Winterfeld. 2014. *Cyber Warfare.* Second edition. Waltham: Elsvier, Inc.
5. Aršič, Stanko. 2013. Kibernetsko vojskovanje. *Revija Obramba* 45 (november): 32–34.
6. Arquilla, John in David F. Ronfeldt. 1997. *In Athena's Camp: Preparing for conflict in the information age*. Washington D.C.: RAND.
7. BBC News. 2003. *US hackers told to leave Iraq alone*. Dostopno prek: http//: www.news.bbc.co.uk./2/hi/technology/2760899.stm (10. maj 2016).
8. --- 2016. *Islamic State group: Crisis in seven charts*. Dostopno prek: http//: www. bbc.com/news/world-middle-east-27838034 (5. junij 2016).
9. Beaumont, Peter. 2010. US appoints first cyber warfare general. *The Guardian*, 23. maj. Dostopno prek: http//: www.theguardian.com/world/2010/may/23/US-appoints-cyber-warfare-general (25. maj 2016).
10. Berginc, Tim. 2014. *Vojna v Siriji-lokalni spopad med globalnimi akterji*. Diplomsko delo. Ljubljana: Fakulteta za družbene vede.
11. Berton, Beatrice in Patryk Pawlak. 2015. Cyber jihadists and their web. *European Union Institute for Security Studies*. Dostopno prek: http//: www.iss.europa.eu/ uploads/media/Brief_2_cyber_jihad.pdf (2. maj 2016).
12. Boni, William in Gerald L. Kovacich. 2000. *Netspionage, the global threat to information*. Woburn: Butterworth-Heinemann.
13. Buncombe, Andrew. 2003. Iraqi leaders are sent private e-mails and phone messages as information war begins. *Independent*, 25. februar. Dostopno prek: http//:

http://www.independent.co.uk/news/world/politics/iraqi-leaders-are-sent-private-e-mails-and-phone-messages-as-information-war-begins-120353.html (10. maj 2016).

14. Bratuša, Tomaž. 2006. *Hekerski vdori in zaščita*. Ljubljana: Založba Pasadena d.o.o.
15. Campbell, Jamie. 2015. French TV network TV5 Monde 'hacked by cyber caliphate in unprecedented attack' that revealed personal detailos of french soldiers. *The Independent*, 9. april. Dostopno prek: http//: www.independent.co.uk/news/world/europe/french-tv-network-tv5monde-hijacked-by-isis-hackers-in-unprecedented-attack-that-revealed-personal-10164285.html (2. maj 2016).
16. Carr, Jefrey. 2010. *Inside cyber warfare*. Sebastopol: O'Reilly media, Inc.
17. Chiacu, Doina. 2015. 'Cyber caliphate' hacks Newsweek Twitter account, threatens Obama. *Reuters*, 10. Februar. Dostopno prek: http//: www.reuters.com/article/us-cybersecurity-newsweek-idUSKBN0LE22Z20150210 (18. maj 2016).
18. Choney, Suzanne. 2013. New York Times hacked, Syrian Electronic Army suspected. *NBC News*, 28. avgust. Dostopno prek: http//: www.nbcnews.com/technology/new-york-times-hacked-syria-electronic-army-suspected-8C11016739 (8. maj 2016).
19. CIA. 2016. *World Factbook*. Dostopno prek: http//: www.cia.gov/library/publications/the-world-factbook/geos/us.html (10. maj 2016).
20. Cornish, Paul, David Livingston, Dave Clemente in Claire Yorke. 2010. *On cyber warfare*. London: The Royal Institute of International Affairs.
21. Coughlan, Sean. 2011. Harvard website hacked by Syria protesters. *BBC News*, 26. september. Dostopno prek: http//: www.bbc.com/news/education-15061377 (1. junij 2016).
22. Saribd. *Cyber Warfare*. Dostopno prek: http//: www.saribd.com/doc/5343005/cyberwarfare (3. april 2009).
23. CNN. 2003. *Fierce Cyber war predicted*. Dostopno prek: http//: www.cnn.com /2003/TECH/ptech/03/03/sprj.irq.info.war.ap/index.html (10. maj 2016).
24. Cox, Joseph. *Information operations in Operations Enduring Freedom and Iraqi Freedom-What went wrong?* Fort Leaven Worth: School For Advanced Military Studies.
25. Elliot, Steven. 2010. Cyber warfare and the conflict in Iraq. *InfosecIsland*, 20. avgust. Dostopno prek: http//: www.Infosecisland.com/blogview/6750-cyber-warafre-and-the-Conflict-in -iraq.html (18. april 2016).
26. Emery, Norman. 2004. Information Operations in Iraq. *Military Review* 84 (maj–junij): 11–14.

27. Fisher, Max in Jared Keller. 2011. Syria's digital counter-revolutionaries. *The Atlantic*, 31. avgust. Dostopno prek: http//: www.theatlantic.com/international/archive/2011/08/syriay-digital-counter-revolutionaries/2444382/ (1. junij 2016).
28. Foster, Peter. 2013. 'Bogus' AP tweet about explosion at the White House wipes billions of US markets. *The Telegraph*, 23. april. Dostopno prek: http//: www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-House-wipes-billions-off-US-markets.html (8. maj 2016).
29. Freedomhouse. 2012. *Syria*. Dostopno prek: http//: www.freeedomhouse.org/report/freedom-net/2012/syria (1.junij 2016).
30. Gabe, Carey. 2016. US military offers first ever annauncement of cyber attack on ISIS. *Digital trends*, 1. marec. Dostopno prek: http//: www.digitaltrends/computing/us-military-admits-to-engaging-in-cyberattacks-against-isis/#:pXmpCxKJ46HsdA (10. maj 2016).
31. Gallagher, Sean. 2015. US Army website defaced by Syrian Electronic Army (updated). *Arstechnica*, 8. junij. Dostopno prek http//: arstechnica.com/security/2015/06/us-army-website-defaced-by-syrian-electronic-army/ (8. junij 2016).
32. Gaube, Aleš. 2016. Padli slovenski borec: Gruden je moral biti avanturist. *Dnevnik*, 3. avgust. Dostopno prek http//: https://www.dnevnik.si/1042747892 (13. avgust 2016).
33. Gertz, Bill. 2016a. Pentagon wages first cyber war on ISIS. *The Washington free beacon*, 29. februar. Dostopno prek: http//: www.freebeacon.com/national-security/pentagon-wages-first-cyber-war-on-isis/ (10. maj 2016).
34. --- 2016b. The Cyber Threat: Cybercom's War on ISIS. *The Washington free beacon*, 2. maj. Dostopno prek: http//: http://freebeacon.com/national-security/cyber-threat-cybercoms-war-isis/?utm_source=Freedom+Mail&utm_campaign=bb0230ad51-WFB_Morning_Beacon_05_02_165_1_2016&utm_medium=email&utm_term=0_b5e6e0e9ea-bb0230ad51-45641965 (12. maj 2016).
35. Gilbert, David. 2014a. Forbes.com hacked by Syrian Electronic Armybecause of »Hate for Syria«. *International Buisness Times*, 14. februar. Dostopno prek: http//: www.ibtimes.co.uk/forbes-com-hacked-by-syrian-electronic-army-because-of-hate-syria-1436415 (8. maj. 2016).
36. --- 2014b. FBI informant sabu organises cyber-attack pn government websites in Iran, syria and Brazil. *International Buisness Times*, 23. april. Dostopno prek: http//: http://www.ibtimes.co.uk/fbi-informant-sabu-organises-cyber-attacks-government-websites-iran-syria-brazil-1445885 (8. maj 2016).

37. Givens, Austen. 2015. Putin's cyber strategy in Syria: Are electronic attacks next? *The CyberDefense Review*, 17. november. Dostopno prek http:// www.cyberdefens ereview.org/2015/11/17/putins-cyber-strategy-in-syria-are-electronic-attacks-next/ (8. maj 2016).
38. Graham, Bradley. 2003. Bush orders guidelines for Cyber warfare. *Washington Post*, 7. Februar. Dostopno prek: http//: www.washingtonpost.com/archive/politics/2003/02/07/bush-orders-guideline-for-cyber-warfare/dd8b4a18-140c-4680-88a5-0041d4ce/b1c/ (12. april 2012).
39. *Google*. 1998. Ozemeljski teritorij pod nadzorom IS v letih 2014 in 2015. Dostopno prek: http//: www.google.com
40. Guin, Payton. 2015. Centcom hacking: What is US Central Command?. *The Independent*, 12. januar. Dostopno prek: http//: www.independent.co.uk/news/world/americas/centcom-hacking-what-is-us-central-command-9973699.html (2. maj 2016).
41. Hackmageddon. 2011. *AnonPlus hacked (again) by Syrian group*, 24. julij. Dostopno prek http//: www.hackmageddon.com/2011/07/24/anonplus-hacked-again-by-syrian-group/ (1. junij 2016).
42. Haynard, John. 2015. Cyber war in Syria: How Assad hacked the rebelion. *Breibart*, 2. februar. Dostopno prek: http//: http://www.breitbart.com/national-security/2015/02/02/cyber-war-in-syria-how-assad-hacked-the-rebellion/ (8. maj 2016).
43. Hildreth Steven. 2001. *CRS report for Congress*. Dostopno prek: http//: www. fas.org./sgp/crs/intel/RL30735.pdf (12. april 2012).
44. Holt, Kris. 2012. Syrian hackers take down LinkedIn's official blog. *Dailydot*, 26. april. Dostopno prek: http//: www.dailydot.com/news/syria-hackers-linked-in-blog-hack/ (1. junij 2016).
45. Chairman of the Joint Chiefs of Staff of the Armed Forces of the United States. 2006. *Joint Publication 3-13, Information operations*. Dostopno prek: http//: www.acqnotes.com/Attachments/JointPublication313InformationOperations13feb06.pdf (12. april 2012).
46. Kandamo, Brian. 2015. Cyber – the 21st Century Threat. *Military Technology* XXXIX (december): 48–51.
47. Kumar, Mohit. 2014. Facebook domain hacked by Syrian Electronic Army. *The Hacker News*, 5. februar. Dostopno prek: http//: http://thehackernews.com/2014/02/facebook-domain-hacked-by-syrian.html# (8. maj 2016).

48. Lawler, David. 2015. Syrian Electronic army hacks US Army website. *The Telegraph*, 8. junij. Dostopno prek: http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11661137/Syrian-Electronic-Army-hacks-US-Army-website.html (8. junij 2016).
49. Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts in Stephen Wolff. 2016. Brief history of Internet. *Internet Society*. Dostopno prek: http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (26. avgust.2016).
50. Libicki, Martin. 1995. *What is information warfare*. Washington D.C.: Institute for National Strategic Studies.
51. Limer, Eric. 2011. Anonymous hacks Syrian Ministry of defence. *The Mary Sue*, 8. avgust. Dostopno prek: http//: www.themarysue.com/anon-hacks-syria/#geekosystem (1. junij 2016).
52. Markhoff, John in Tom Shanker. 2009. Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk. *The New York Times*, 1. avgust. Dostopno prek: http://www.nytimes.com/2009/08/02/us/politics/02cyber.html?_r=1 (10. maj 2016).
53. Marks, Joseph. 2015. ISIL aims to launch cyber attacks on U.S. *Politico*, 29. december. Dostopno prek: http//: www.politico.com/story/2015/12/isil-terrorism-cyber-attacks-217179 (18. maj 2016).
54. Mahon, Tim. 2016. Final frontier? Or just new frontier? *Military Technology* XL (februar): 68–69.
55. Mukaram, Ahmad. 2014. Cyber threat landscape: Basic overview and attack methods. Recorded Future. *Recorded Future*, 3. junij. Dostopno prek: http//: www.recorded future.com/cyber-threat-landscape-basics/ (2. maj 2016).
56. Myers, Russel. British hacker suspected of cyber attack on Central Command Twitter account. *Mirror*, 14. januar. Dostopno prek: http://www.mirror.co.uk/news/world-news/british-hacker-suspected-cyber-attack-4974855 (18. maj 2016).
57. Nell, Grant Sebatian. 2008. *The Mongol war machine*. Dostopno prek: http//: www.grant-sebatsian-nell.suite101.com/the-mongol-war-machine-a66150 (12. april 2012).
58. Osman, Nazan. 2014. Cyberarfare on the incerase in Iraq. *SC Magazine UK*, 2. julij. Dostopno prek: http//: www.scmagazineuk.com/cyberwarfare-on-the-increase-in-iraq/article/359154/ (10. maj 2016).

59. Ovide, Shira. 2014. Social media accounts hacked by Syrian Electronic Army. *The Wall Street Journal*, 1. januar. Dostopno prek: http//: blogs.wsj.com/digits/2014/01/01/skype-social-media-accounts-hacked-by-sea (8.maj 2016).
60. Parks, Raymond C. In David P. Duggan. 2001. *Principles of Cyber-warfare*. Dostopno prek: http//: www.itoe.usma.edu/workshop/2001/Authors/Submitted_Abstracs/paperT2C1(10).pdf (12. April 2012).
61. Paul, Christopher. 2008. *Information operations, doctrine and practice*. Westport: Praeger Security International.
62. Paulson, Amanda. 2013. Syrian electronic army says it hacked Obama accounts. *The Christian Science Monitor*, 29. oktober. Dostopno prek: http//: www.csmonitor.com/USA/Politics/Decoder/2013/1029/Syrian-Electronic-Army-says-it-hacked-Obama-accounts (1. junij 206).
63. Payne, Samantha. 2014. Reuters hacked by Syrian Electronic Army via Taboola ad. *International Buisness Times*, 22. junij. Dostopno prek: http//: www.ibtimes.co.uk/reuters-hacked-by-syrian-electronic-army-via-taboola-ad-1453717 (8. maj 2016).
64. Prelc Dakič, Drago. 2013. Sporno in smrtonosno. *Revija Obramba* 45 (oktober): 19–26.
65. Price, Bob. 2016. Four members of Syrian Electronic Army charged in cyber attacks. *Breitbart*, 22. marec. Dostopno prek: http://www.breitbart.com/texas/2016/03/22/four-members-of-syrian-electronic-army-charged-in-cyber-attacks/ (8. junij 2016).
66. Pultarova, Tereza. 2015. Turkey under 'most intense' cyber attack in its history. *Engineering and Technology Magazine*, 23. december. Dostopno prek: http://eandt.theiet.org/news/2015/dec/turkey-cyber-attack.cfm (8. junij 2016).
67. Roberts, Joel. 2003. U.S. Drops »E-bomb« on Iraqi TV. *CBS News*, 25. marec. Dostopno prek: http//: www.cbsnews.com/news/US-drops-e-bomb-on-iraqi-tv/ (3. avgust 2016).
68. Rezk, Dina. 2010. The Revolution in Military Affairs and Changing Nature of Warfare in the Middle East. *LSE*. Dostopno prek: http//: www.blogs.lse.ac.uk/ideas/2010/04/the-revolution-in-military-affairs-and-the-changing-nature-od-warfare-in-the-middle-east/ (3. Avgust 2016).
69. *Slovar slovenskega knjižnega jezika*. 2000. Ljubljana: DZS
70. *Slovenski veliki leksikon (H-O)*. 2005. Ljubljana: Mladinska založba.
71. Samuel, Henry. 2015. Le Monde hacked: »Je ne suis pas Charlie« writes Syrian Army. *The Telegraph*, 21. januar. Dostopno prek: http//: http://www.telegraph.co.uk/news/

worldnews/europe/france/11359732/Le-Monde-hacked-Je-ne-suis-pas-Charlie-writes-Syrian-Electronic-Army.html (8. maj 2016).

72. Samuelson, Douglas. 2003. *The Netwar in Iraq*. Dostopno prek http//: www.lionhrtpub.com/orms/orms-6-03/frnetwar.html (12. julij 2007).
73. Shehabat, Ahmad. 2012. The social media cyber-war: the unfolding events in the Syrian revolution 2011. *Global media Journal Australian Edition*. Dostopno prek: http//: www.hca.westernsydney.edu.au/gmjau/archive/v6_2012_2/ahmad_shehabat%20_RA.html (5. maj 2016).
74. Smith, Charles. 2003. Cyber war against Iraq. *Newsmax,* 12. marec. Dostopno prek: http//: www.newsmax.com/archives/articles/2003/3/12/1334712.shtml (10. februar 2007).
75. Spletno uredništvo, STA. 2015. Kaj je sploh Islamska država?. *Večer,* 17. november. Dostopno prek http//: www.vecer.com/clanek/201511176158247 (12. junij 2016).
76. Svete, Uroš. 2005. *Varnost v informacijski družbi*. Ljubljana: Fakulteta za družbene vede.
77. Svete, Uroš in Anton Žabkar. 2006. Irak-poligon za preizkušanje novih vojaških doktrin. *Teorija in praksa* 43 (1–2): 285–302.
78. Theiler, Olaf. 2011. Nove grožnje: Kibernetska razsežnost. *Revija NATO*. Dostopno prek: http//: www.nato.int/docu/review/2011/11-september/Cyber-Threads/SL/index.htm (27. julij 2016).
79. The NewArab. 2016. *Russia mounts major cyber-espionage campaign against Syrian organizations*, 21. februar. Dostopno prek: http//: https://www.alaraby.co.uk/english/news/2016/2/21/russia-mounts-major-cyber-espionage-campaign-against-syrian-organisations (8. junij 2016).
80. Thompson, Loren. 1999. *Thinkexist*. Dostopno prek: http://thinkexist.com/quotes/loren_thompson/ (3. marec 2003).
81. Tisdall, Simon. 2010. Cyber warfare is 'growing threat'. *The Guardian*, 3. Februar. Dostopno prek: http//: www.guardian.co.uk/technology/2010/feb/03/cyber-warfare-growing-threat (2. april 2012).
82. Todd, Brian in Forrest Brown. 2013. Syria's cyberattack: First wave of a bigger war?. *CNN*, 30. avgust. Dostopno prek: http//: edition.cnn.com/2013/08/30/tech/syria-cyberattacks/ (1. junij 2016).
83. U.S. Marine Corps. 2001. *Information Operations*. Dostopno prek: http//: www.c4i.org/mcwp336.pdf (12.april 2012).

84. Usborne, David. 2015. Centcom hacked by ISIS supporters: US military twitter feud publishes personal information of senior officers. *The Independent*, 12. januar. Dostopno prek: http//: www.independent.co.uk/news/world/americas/us-central-command-hacked-by-islamic-state-supporters-9973615.html (2. maj 2016).
85. Zupančič, Rok. 2006. *Ameriška okupacija Iraka*. Diplomsko delo. Ljubljana: Fakulteta za družbene vede.
86. Wikipedia. 2001a. *Computer virus*. Dostopno prek: http//: https://en.wikipedia.org/wiki/Computer_virus (10.maj 2016).
87. --- 2001b. *2007 cyberattacks on Estonia*. Dostopno prek: http//: en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia (10.maj 2016).
88. --- 2001c. *Syrian electronic Army*. Dostopno prek: http//: en.wikipedia.org/wiki/Syrian_Electronic_Army (10.maj 2016).
89. --- 2001č. *2003 invasion of Iraq*. Dostopno prek: http//: http://en.wikipedia.org/wiki/2003_invasion_of_Iraq (10.maj 2016).
90. --- 2001d. *Iraqi Civil War (2014-present)*. Dostopno prek: http//: en.wikipedia.org/wiki/Iraqi_Civil_War_(2014%E2%80%93present) (10.maj 2016).
91. Žabkar, Anton. 2003. Operacija Iraška svoboda. *Vojaškošolski zbornik* 2: 63–92.
92. Žabkar Anton. 2003. Operacija Iraška svoboda. *Revija Obramba* 35 : 6–12.
93. Ward, Mark. 2014. Iraq conflict breuds cyberwar among rival factions. *BBC News*, 22. julij. Dostopno prek: http//: www.bbc.com/news/technology-28418951 (18.maj 2016).
94. Wilson, Clay. 2006. *CRS report for Congress*. Dostopno prek: http//: www.fas.org/irp/crs/RL31787.pdf (10. junij 2016).
95. Wright, Simon, Nick Dorman in Colin Cortbus. 2015. Twitter shuts down ISIS supporters and jihadists as MI5 launch anti-terror social media crackdown. *Mirror*, 24. januar. Dostopno prek: http//: www.mirror.co.uk/news/uk-news/twitter-shuts-downisis-supporters-5038305 (2. maj 2016).