UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Klemen Kovačič

Kibernetski terorizem Islamske države

Diplomsko delo

Ljubljana, 2016

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Klemen Kovačič

Mentor: izr. prof. dr. Uroš Svete

Kibernetski terorizem Islamske države

Diplomsko delo

Ljubljana, 2016

Zahvala

Ob tem trenutku bi se rad zahvalil vsem, ki ste mi v času študija stali ob strani in me moralno in materialno podpirali. Velika zahvala gre družini, prijateljem in še posebej punci, saj ste mi neizmerno pomagali v vseh pogledih in omogočili, da uspem.

Velika zahvala gre tudi mentorju dr. Urošu Svetetu, ki mi je z veliko mero strokovnih in znanstvenih nasvetov ter usmeritev pomagal pri nastanku diplomskega dela.

Kibernetski terorizem Islamske države

Informacijsko-komunikacijska tehnologija je omogočila prenos bojev iz konfliktnih območij v kibernetski prostor. Tako kot države tudi terorizem išče nove načine povečevanja učinka in uspeha v bojih in sicer tako, da se poslužuje kibernetskih napadov proti svojim sovražnikom, ki so v kibernetskem prostoru veliko bližje kot v realnem svetu. Vendar pod kibernetski terorizem ne smemo šteti le kibernetskih napadov na nasprotnikovo kritično informacijsko infrastrukturo, ampak tudi dejavnosti razširjanja propagande, rekrutiranja, načrtovanja in koordiniranja ter financiranja v kibernetskem prostoru. Prav zaradi novih načinov delovanja, ki jih omogoča kibernetski prostor, je Islamska država izoblikovala skupine, ki v njenem imenu delujejo v kibernetskem prostoru. Z dobro oblikovano mrežo propagandnih in drugih komunikacijskih poti je hitro postala najbolj poznana teroristična organizacija ter v svoje vrste privabljala vse več somišljenikov. Kibernetski napadi, ki jih izvajajo skupine Islamske države, v kibernetskem prostoru dosegajo uspehe, ki jih, podkrepljene z dobrim propagandnim mehanizmom, hitro predstavijo javnosti za večji učinek strahu.

KLJUČNE BESEDE: Islamska država, kibernetski prostor, kibernetski terorizem, informacijsko-komunikacijska tehnologija, propaganda.

Cyberterrorism of Islamic State

Information and communication technology made it possible to take fights from conflict zones to cyber space. Much like the countries, terrorism is searching for new ways to maximize effect and success in conflicts. One of such ways is with cyberattacks, because in cyberspace enemies are closer than in physical world. But cyberterrorism is not only conducting cyber-attacks, but also includes propaganda, recruitment, planning, coordination and financing in cyberspace. New communication and information technology made it possible for the Islamic state, as a new terrorist organization, to conduct its operations in cyberspace with the help of newly created cyber groups. Its success results in well-known public appearance of organization and attracts new members to join. Successful cyberattacks with good propaganda mechanism help spread the news of success and help spread fear to public with greater effect.

KEY WORDS: Islamic state, cyberspace, cyberterrorism, information and communication technology, propaganda.

Kazalo vsebine

1 Uvod

Informacijsko-komunikacijska tehnologija (IKT) je v zadnjih dvajsetih letih izvedla eno največjih revolucij pri izvajanju dejavnosti držav, družb in družbenih skupin ter posameznikov. S svojim pojavom je povzročila povezanost na lokalni, regionalni in globalni ravni. S tehnologijo so posamezniki, skupine in države pridobili novo okolje, v katerem lahko komunicirajo, sodelujejo in tekmujejo. Porast uporabe informacijsko-komunikacijske tehnologije je še dodatno podkrepil procese digitalizacije in globalizacije, saj se zaradi svoje moči povezovanja in informatiziranja prenaša na vse dejavnosti posameznikov in tudi držav.

Digitalizacija in informatizacija vseh dejavnosti predstavlja širjenje IKT v naše domove, službe, avtomobile (osebna informacijska infrastruktura) in z njimi povezana cestna omrežja, industrijske procese, javno upravo, varnostne sisteme, energetske procese, zdravstvo, zaslediti pa jo je možno še drugod (kritična informacijska infrastruktura) (Prezelj in Svete 2015). Uporaba takšne tehnologije omogoča izboljševanje učinkovitosti dejavnosti ter zmanjšuje čakalne vrste in stroške ter omogoča uporabnikom prijazno uporabo.

S tem se odpira povsem novo poglavje v delovanju držav, saj te poskušajo uporabiti IKT za izvajanje nalog in dejavnosti, svoje sisteme pa so tako prisiljene tudi ustrezno zaščititi pred namernimi ali nenamernimi grožnjami (Svete 2005, 108).

Kljub vse večji povezanosti se geopolitično in geostrateško okolje ni veliko spremenilo. Po razpadu Varšavskega pakta je prišlo do razdrobitve nekdanjega vzhodnega zavezništva. Nove suverene države so bile prisiljene iskati nove zaveznike, ki so jih velikokrat našle na zahodu. Integracije v Severno Atlantsko zavezništvo oziroma NATO in Evropsko Unijo so predstavljale dodaten razdor na tehnici razmerja moči med vzhodnimi in zahodnimi državami. Poljska in Baltske države so iskale zaveznike na zahodu zaradi strahu pred Rusko federacijo, ta pa se poskuša ponovno vzpostaviti kot globalna velesila. Ruski strah pred NATO-m na eni ter ruski geostrateški interes na drugi strani predstavljata razcep v iskanju novih poti za zagotavljanje lastnih interesov, obenem pa Rusijo prisiljujeta v izogibanje neposrednim konfrontacijam z zahodom. Poleg Ruske federacije je prišlo do ekonomskega razcveta in razvoja Kitajske in drugih vse močnejših držav, ki poskušajo prehiteti zahodne države na vseh področjih.

Tako globalne velesile kot tudi manjše države so z razvojem lastnih in z analizo tujih IKT spoznale potencial digitaliziranega prostora za tekmovanje in vodenje vojne v kibernetskem prostoru. Države so pričele z razvojem orožij za informacijsko bojevanje, s katerim bi nasprotnikom onemogočili dostop do nujnih informacij ali jim uničili informacijsko infrastrukturo. Prvi poskusi tega so se zgodili s kibernetskim napadom na Estonijo leta 2007 in z razvojem računalniškega zlonamernega programa Stuxnet, ki je izvedel napad na iranski jedrski program. Poleg teh napadov so bili izvedeni še drugi, vendar niso dosegli tolikšne medijske publicitete ali bili tako odmevni.

Vendar države niso edini uporabnik informacijskih ali kibernetskih orožij. Teh se vse več poslužujejo tudi kibernetski kriminalci, hektivisti in kibernetski teroristi (Baldi in drugi 2003, 17–18). Kibernetski kriminalci uporabljajo digitalna oziroma kibernetska orožja z namenom izvedbe kriminalnih dejanj ter zaslužka. Hektivisti so aktivistična gibanja, ki poskušajo prisiliti državne organe ali posameznike v spremembo politik, ki škodijo ljudstvu ali družbeni skupini, kar počnejo z osramotitvijo na spletu. Kibernetski terorizem je uporaba kibernetskih orodij in sistemov z namenom zastraševanja, razširjanja propagande, rekrutacije, izvedbe kibernetskih napadov in indoktrinacije ter marsičesa drugega (Baldi in drugi 2003, 17–18). Kibernetski terorizem ni nova oblika delovanja terorističnih skupin. V preteklosti smo lahko opazovali uporabo kibernetskega prostora za propagandne aktivnosti. A danes je sofisticiranost kibernetskega terorizma prerasla enostavno propagandno dejavnost (Olmstead in Siraj 2009). V primeru sodobnega kibernetskega terorizma lahko govorimo o celotnem obsegu informacijskega bojevanja, saj imajo teroristične skupine, kakršna je Islamska država, izoblikovane specializirane enote, ki so namenjene izvedbi kibernetskih terorističnih dejanj.

Uspešnost kibernetskega terorizma Islamske države je izredno zaskrbljujoča. Uspešna izvedba kibernetskih napadov na informacijske sisteme, uporabniške račune pomembnih politikov ali znanih oseb ter propagandna dejavnost govorijo o sposobnostih Islamske države, kot jih teroristične skupine še niso imele. Še bolj zaskrbljujoči so procesi radikalizacije, ki se dogajajo vse hitreje in istočasno z ostalimi dejavnostmi ter lahko pripeljejo izvedbo terorističnih napadov na prag katerekoli države.

2 Metodološko-hipotetični okvir

2.1 Relevantnost in namen vsebine

V svoji diplomski nalogi želim raziskati delovanje in sposobnosti kibernetskega terorizma Islamske države. Namen naloge je ugotoviti načine, na katere poskuša Islamska država izvajati kibernetsko vojno in terorizem, razširjati sporočila ter propagandne ideje. Nameravam tudi analizirati načine in poskuse rekrutacije, financiranja in mobiliziranja posameznikov s pomočjo družbenih omrežij in temu namenjenih spletnih strani. Podrobnejša analiza kibernetskih napadov na informacijske sisteme bo predstavila taktike in sposobnosti izvajanja kompleksnejših kibernetskih terorističnih napadov. Islamska država se v medijih velikokrat pojavlja s krutimi propagandnimi filmi, s katerimi poskuša izzvati strah med prebivalci zahodnih držav ter mobilizirati mogoče podpornike. Vendar ima Islamska država tudi druge sposobnosti, ki se odvijajo skrito pred očmi javnosti. Kibernetski terorizem ne zajema le razširjanja propagandnih posnetkov in slik, ampak tudi izvajanje napadov na informacijsko infrastrukturo.

Slovenija je leta 2016 izoblikovala strategijo Digitalne Slovenije 2020 (MIZŠ 2016), s čemer želi uporabo informacijsko-komunikacijske tehnologije prenesti na vse ravni delovanja države. S tem se odpira razširjeno (digitalno) okolje, v katerem lahko tuje države kot tudi skupine kibernetskih kriminalcev, hektivistov in teroristov izvajajo aktivnosti, usmerjene proti Republiki Sloveniji.

Pomembnost razumevanja kibernetskega terorizma mora biti zato prisotno v vseh strukturah državnih in zasebnih organizacij. Analiziranje načinov in taktik, ki jih takšne teroristične skupine uporabljajo, lahko močno izboljša obrambne sposobnosti države in drugih organizacij na kibernetskem področju. Obenem lahko predstavlja tudi nepogrešljiv vir informacij za obveščevalne službe in varnostne organe o namerah in načrtih lokalnih celic ali globalnih terorističnih organizacij.

2.2 Cilj

Cilj diplomske naloge je raziskati in analizirati sposobnosti Islamske države za izvajanje kibernetskih dejavnosti. Te dejavnosti zajemajo izvajanje kibernetskih napadov, razširjanje propagande, izvajanje procesov rekrutacije in izobraževanja pripadnikov ter samega financiranja

Islamske države prek kibernetskega prostora. Analizirati nameravam komunikacijske poti, ki so uporabljene za razširjanje propagande in informacij ter komuniciranje s pripadniki Islamske države in zunanjim občinstvom, ki se želi priključiti organizaciji.

2.3 Metodološki okvir

Diplomska naloga je razdeljena na dva večja dela. Prvi del predstavlja pridobivanje in iskanje teoretične osnove, s pomočjo katere bodo zastavljeni temelji za nadaljnjo raziskovanje. Za izoblikovanje konceptualne in teoretične osnove bodo uporabljeni primarni in sekundarni viri, katerih avtorji so kredibilni in strokovni ter znanstveni. Uporaba kredibilnih in strokovnih virov mi bo omogočila primerno in pravilno definiranje terorizma, kibernetskega prostora in kibernetskega terorizma, saj se bo drugi del diplomske naloge navezoval na te definicije. Drugi del diplomske naloge bom razdelil na več poglavij, ki bodo zajemale propagando, rekrutacijo, kibernetske napade in financiranje Islamske države. Za raziskovanje tem bom uporabil primarne in sekundarne vire, s čimer si bom postavil jasne temelje za izvedbo podrobnejše analize samih dejavnosti, povezanih s kibernetskim terorizmom. Zbiranje podatkov in virov za analizo samih kibernetskih dejavnosti Islamske države bom opravil s pomočjo virov, ki jih bom našel na indeksiranem, globokem in temnem spletu, njihovi avtorji pa so pripadniki ali podporniki Islamske države.

Indeksiran splet, na katerem bom primarno iskal podatke, pomeni splet, ki je dostopen brez posebne programske opreme. Do teh strani se lahko dostopa s pomočjo spletnih iskalnikov, kot so Google, Bing, Yahoo in drugi, ki s pomočjo spletnih pajkov (angleško: crawlers) preiščejo spletne vsebine in jih indeksirajo v podatkovne baze, ki so namenjene lažjemu dostopanju do internetnih strani. Na indeksiranem spletu se bom osredotočil na družbena omrežja, spletne strani podpornikov in pripadnikov Islamske države, strani strokovnih analiz kibernetskega terorizma in vsebin medijskih hiš. Zbiranje podatkov in virov mi bo omogočilo lažjo analizo sposobnosti in razsežnosti kibernetskega terorizma Islamske države.

Temen in globoki splet predstavlja splet, do katerega ni mogoče dostopati brez posebne programske opreme. Programska oprema, kot na primer I2P, Freenet in Tor, omogoča anonimno brskanje po spletu zaradi povezave, ki poteka skozi soležnike. Programska oprema dostopa do

spletnih strani, ki so bile odstranjene iz indeksiranega spleta ali uporabljajo strežnike po meri, ki omogočajo ohranjanje anonimnosti. Na temnem in globokem spletu bom iskal spletna mesta, ki niso dostopna na indeksiranem spletu in so povezana z Islamsko državo ali njenimi kibernetskimi terorističnimi skupinami. Namen iskanja na temnem in globokem spletu je zbrati dodatne podatke, ki bi mi omogočili dopolnjevanje analize sposobnosti in razsežnosti kibernetskega terorizma Islamske države na področjih, ki jih bom obravnaval.

2.4 Hipoteze

Za lažje raziskovanje in analizo problema kibernetskega terorizma Islamske države si bom postavil več raziskovalnih vprašanj in trditev.

Hipoteza 1: *Islamska država ima sposobnost za izvajanje kibernetskih napadov*.

Hipoteza 2: *Sposobnosti kibernetskega terorizma Islamske države so napredno strukturirane*.

Hipoteza 3: *Islamska država uporablja kibernetski terorizem primarno za razširjanje propagandnih vsebin.*

2.5 Opredelitev temeljnih pojmov

2.5.1 Terorizem

Terorizem se v medijih predstavlja kot nov način vodenja vojne. To ni res, saj lahko prve teroristične napade zasledimo že v času rimskega imperija na ozemljih današnje Palestine. Tamkajšnje ekstremne skupine so z akti političnega nasilja poskušale odvrniti lokalno prebivalstvo od sodelovanja z Rimljani (Chaliand 2007, 56).

Skozi celotno zgodovino so se pojavljale podobne zgodbe z ekstremnimi skupinami, ki so poskušale z nasiljem in s političnim ozadjem vplivati na politiko vladarjev ali držav. Do največjega preskoka v delovanju terorizma pa je prišlo z mediatizacijo vojn in konfliktov. Hiter prenos podatkov po radiu in kasneje televiziji je pripeljal takšen način bojevanja v ospredje (Udupa 2009). Velike in močne države so se v času od druge svetovne vojne do leta 1991 konstantno srečevale s takšno strategijo sovražnega delovanja. Strategija terorizma je omogočala

majhnim in slabše oboroženim silam, da se zoperstavijo veliko močnejšemu nasprotniku, obenem pa odvračala lokalno prebivalstvo od sodelovanja.

Med leti 1991 in 2001 so se teroristične akcije in skupine veliko bolje organizirale in razširile po celem svetu. Pričele so delovati ofenzivno proti velesilam na Bližnjem vzhodu, Kavkazu in Rusiji, Združenih državah Amerike in drugod. Kulminacija terorističnega delovanja je bila izvedena 11. septembra 2001 z napadi na ameriški Pentagon in dvojčka Svetovnega trgovinskega centra. Odziv, ki je sledil zaradi 3000 smrtnih žrtev, je bil izjemno oster. Izoblikovala se je koalicija za boj proti terorizmu in države so pričele z vojno proti terorizmu (Mccormic 2014). Z vzponom novih terorističnih celic, gibanj in skupin pa se vojna proti terorizmu ni zaključila in se danes nadaljuje tudi proti Islamski državi.

A vendar; kako lahko definiramo Islamsko državo kot teroristično skupino oziroma organizacijo? Enotne definicije za terorizem ni, saj se s problemom terorizma srečuje veliko držav in vsaka od njih želi definirati pojem tako, da bo v skladu z njihovimi potrebami in njihovimi notranjimi zakoni in da bo lažje sodno preganjala izvajalce in simpatizerje.

Severno Atlantsko zavezništvo NATO definira terorizem kot nezakonito uporabo sile ali grožnje s silo proti posamezniku ali njegovi lastnini z namenom prisiljevanja ali ustrahovanja vlade in družbe za doseganje političnega, verskega ali ideološkega cilja (NATO Glossary 2014).

Evropska unija definira terorizem kot akt, ki povzroči škodo državi ali mednarodni organizaciji, z namenom ustrahovanja družbe, prisiljevanja ciljne vlade v izvajanje ali neizvajanje dejanj ali z napadi povzročijo destabilizacijo ter uničenje temeljnih političnih, ustavnih, ekonomskih, družbenih struktur ciljne države ali mednarodne organizacije (Council of the European Union 2002).

Prezlj definira terorizem kot »izvajanje in podpiranje nasilnih dejavnosti ali groženj z nasilnimi dejanji, ki so načrtovana in organizirana. Usmerjene so proti civilistom in nedolžnim ciljem z namenom doseganja političnih ciljev. Z vplivanjem na vlado poskušajo prisiliti v izvedbo ali neizvedbo njihovih dejanj in ukrepov« (Prezelj 2006, 177-178).

Pri naštetih definicijah lahko opazimo veliko skupnega. Kot prvo: terorizem uporablja nasilna dejanja ali grožnjo s silo. Napadi so usmerjeni proti posameznikom z namenom ustrahovanja družbe in s tem doseganja političnih ciljev na državni ravni, ko se prisili vlado ali druge organe v izvajanje ali neizvajanje dejanj ali ukrepov. Kljub temu, da si definicije niso identične, je očitno, da si ne nasprotujejo. Vsaka definicija dodaja nekaj, kar druge ne vsebujejo.

V diplomski nalogi bom uporabljal definicijo Evropske unije, saj menim, da je najbolj obsežna, ker zajema poleg povzročene škode državam tudi škodo, povzročeno mednarodnim organizacijam, ter definira tip škode, ki nastaja. Po definiciji Evropske unije lahko Islamsko državo definiramo kot organizacijo, ki izvaja nasilna dejanja v Evropi, Združenih državah Amerike, na Bližnjem vzhodu in drugod po svetu. Namen takšnih napadov je ustrahovanje družbe in posameznikov ter prisiljevanje vlad v izvajanje ali neizvajanje politik. S svojimi napadi Islamska država povzroča največjo škodo in destabilizacijo držav na Bližnjem vzhodu. Napadi povzročajo politične krize, spodkopavajo ustavne pravice in pravice državljanov, povzročajo veliko ekonomsko škodo in ustrahujejo ciljno družbo. Za razumevanje njenega načina delovanja in načina širjenja strahu pa bom dodatno definiral še novo okolje, v katerem je pričela z izvajanjem svojih psiholoških in kibernetskih operacij.

2.5.2 Kibernetski prostor

Novo okolje, v katerem teroristične organizacije delujejo, je kibernetski prostor (imenujemo ga lahko tudi digitalni prostor, kiberprostor in kibernetični prostor). Islamska država je izredno hitro spoznala prednosti novega okolja in ga sebi v prid uporabila na lokalnem in regionalnem območju.

Kibernetski prostor je v najosnovnejši definiciji fiktiven prostor, kjer poteka komunikacija med informacijsko-komunikacijskimi sistemi (Oxford Dictionary 2016). Vendar zaradi fenomena digitalnega prostora prihaja do velikega števila raziskav iz različnih področij, ki uporabljajo različne definicije, te pa sovpadajo z njihovimi znanstvenimi področji. V moji diplomski nalogi bom uporabljal politično in varnostno-obrambno definicijo, saj je z mojo temo najbolj povezana.

Po definiciji ameriškega ministrstva za obrambo je kibernetski prostor »globalna domena delovanja v informacijskem okolju. Informacijsko okolje je sestavljeno iz med seboj povezanih in soodvisnih sistemov in omrežij informacijske infrastrukture. Informacijska infrastruktura vključuje internet, telekomunikacijska omrežja in računalniške sisteme« (Evans in Carey v Bernik in Prislan 2012, 41).

Kibernetski prostor ima zaradi povezanosti omrežij in sistemov informacijske infrastrukture sposobnosti hitrega prenosa pomembnih informacij čez velike geografske razdalje in ovire. Število teh informacij ima edino omejitev v IKT kanalih, ki povezujejo računalniške sisteme. S tem se lahko skozi kibernetski prostor prenaša veliko količino informacij, ki so regulirane redko ali sploh ne. Kibernetski prostor ima zaradi hitrega premeščanja geografskih razlik in možnosti prenosa velikega, nereguliranega števila informacij, veliko sposobnost pri mobilizaciji uporabnikov IKT (Manjikian v Bernik in Prislan 2012, 42–43).

To naredi kibernetski prostor privlačen za teroristične organizacije, saj imajo skozi njega možnost hitrega prenosa velike količine nereguliranih informacij kamorkoli po svetu. Vendar pa je potrebno za nadaljnjo analizo kibernetskega terorizma Islamske države definirati prav posebno obliko terorizma, ki se lahko odvija v takšnem prostoru.

2.5.3 Kibernetski terorizem

Informacijsko-komunikacijska tehnologija se je z digitalno revolucijo prenesla na vse ravni družbe. Ena od pomembnejših ravni je tista, ki skrbi za varnost in obrambo posameznikov, družbe in države. Zato mora biti država sposobna zagotoviti varnost in obrambo pred nenamernimi grožnjami IKT in namernimi kibernetskimi napadi kibernetskih kriminalcev in teroristov.

Najbolj razširjena definicija kibernetskega terorizma predstavlja združevanje definicij terorizma in kibernetskega prostora. Kibernetski terorizem je razumljen kot nezakonit napad ali grožnja z napadom proti računalnikom, omrežjem in informacijam, shranjenih na njih, z namenom ustrahovanja ali prisiljevanja vladnih organov ali ljudi v dejanja za doseganje političnih ali družbenih ciljev teroristične organizacije. Napad na informacijsko infrastrukturo mora povzročiti

škodo ali nasilje, ki vodi v strah, poškodbe ali smrtne žrtve. Kibernetski napadi, ki so usmerjeni proti kritični infrastrukturi države, so lahko klasificirani kot kibernetski terorizem, vendar morajo doseči dovolj močan vpliv na družbo ali vladne organe. A ta definicija se nanaša le na čisti kibernetski terorizem, ki je popolnoma izoliran od samih fizičnih aktivnosti terorističnih organizacij (Gordon in Ford 2003).

Pri delovanju Islamske države ne moremo govoriti zgolj o čistem kibernetskem terorizmu, saj se domeni fizičnega in kibernetskega prepletata. Zato bom uporabil definicijo, ki je bolj primerna za hibridno delovanje terorizma (lahko ga poimenujemo tudi nov terorizem), ki uporablja IKT kot enega od svojih orožij za doseganje ciljev (Gordon in Ford 2003).

Bernik in Prislan definirata kibernetski terorizem kot načrtovano politično dejavnost, ki uporablja informacijsko-komunikacijsko tehnologijo v kibernetskem prostoru za izvajanje napadov na druge informacijsko-komunikacijske sisteme. Informacijsko-komunikacijske sisteme definirata kot računalniške ali informacijske sisteme ter njihovo programsko opremo in podatke. Kibernetski teroristi uporabljajo IKT za napad na cilje, ki se ne zoperstavljajo napadu. Cilj kibernetskega terorizma je zato povzročiti strah in paniko ter večjo medijsko odzivnost in prepoznavnost same skupine. V najslabšem primeru pa lahko kibernetski napadi povzročijo poškodbe ali smrtne žrtve (Bernik in Prislan 2012, 123–124).

Definicija, ki sta jo zapisala Bernik in Prislan, omogoča veliko boljšo analizo kibernetskega terorizma Islamske države, saj obsega napade na IKT vključno z informacijami. Namen je povzročiti strah, paniko in večjo medijsko prepoznavnost skupine, katero lahko uporabi za nadaljnjo širjenje lastnih sporočil in propagande.

Želja po razširitvi sposobnosti in povečanju učinkovitosti v vojni proti svojim nasprotnikom je teroristične skupine, kot je Islamska država, pripeljala do tega, da poleg fizičnih napadov v svoje delovanje vključijo tudi kibernetsko sposobnost. Tako Islamska država ne želi napadati svojih sovražnikov le skozi kibernetski prostor, ampak tega tudi uporabiti za izvajanje drugih, prikritih aktivnosti.

Za najbolj pogoste in prepoznavne oblike kibernetskega terorizma lahko razumemo napade na sisteme IKT, s katerimi želijo spremeniti ali uničiti njihovo vsebino. Uničenje ali sprememba vsebine takšnih sistemov je lahko usmerjena tudi na kritično informacijsko infrastrukturo, kjer je tarča stabilnost IKT z namenom uničenja podatkov na njih ali celotnih informacijskih sistemov. To dolgoročno onesposobi dostopnost do podatkov na računalniških in drugih sistemih, ob tem pa lahko povzroči veliko ekonomsko škodo ter nevarnost za ljudi. Tretja oblika kibernetskega terorizma je namenjena načrtovanju fizičnih terorističnih napadov. V tem primeru gre za organizacijo celice ali posameznika, ki uporabi IKT za dostopanje do informacij, ki so potrebne za izvršitev takšnih dejanj. Četrta oblika kibernetskega terorizma zajema pridobitno dejavnost, pri kateri poskuša teroristična organizacija zbirati finančna sredstva za izvedbo terorističnih dejanj in napadov, ki so politično motivirani, ter za posredovanje in objavljanje ekstremistične ideologije ter propagande (Ballard in drugi 2004, 58–59). Zaradi vse bolj sofisticiranih kibernetskih napadov bi bilo potrebno dopolniti prvo in drugo obliko kibernetskega terorizma. V današnjem času prihaja do vse večje uporabe napadov za zavrnitev sistema, ki onemogoči dostop do vsebine na IKT. Ob tem ne prihaja do uničenja ali spremembe podatkov na informacijskih sistemih, le dostop do njih je onemogočen.

Oblike kibernetskega terorizma predstavljajo napade in delovanje terorističnih skupin v kibernetskem prostoru, vendar morajo za to imeti motiv, ki je skupen s teroristično organizacijo ali se z njo identificirajo. V primeru, da za napadom posameznika ne bi bilo motivacije, ki izhaja iz teroristične organizacije, bi bilo dejanje akt kibernetske kriminalitete. Motivacija posameznika mora prihajati iz ciljev teroristične organizacije in povzročiti strah in paniko v družbi ter vplivati na vladne organe (Veerasamy 2010).

Sposobnosti terorističnih organizacij na področju kibernetskega terorizma se močno razlikujejo. Nekatere skupine se specializirajo za čisti kibernetski terorizem, druge pa uporabljajo kibernetsko dimenzijo le kot dodatek k tradicionalnim metodam. Zato lahko opazimo razkorak med sofistikacijo in sposobnostjo izvedbe kibernetskih terorističnih napadov. Kategorizacijo sposobnosti najbolje definira Center za preučevanje terorizma in iregularnega vojskovanja na Mornariški podiplomski šoli v Kalifornijskem Montereyu, ZDA.

S svojim poročilom *Kibernetski terorizem: vidiki in implikacije* (*Cyberterror – Prospects and Implications*) je Monterejska skupina definirala tri ravni sposobnosti kibernetskega terorizma. Razdelila jih je na:

- Enostavne in nestrukturirane
- Napredno strukturirane
- Kompleksno strukturirane (Nelson in drugi 1999, 13–17)

Enostavne in nestrukturirane sposobnosti predstavljajo izvajanje kibernetskih napadov na individualne računalniške sisteme. Za izvedbo takšnih napadov se uporabljajo orodja, ki so prosto dostopna na spletu in so od katerih so skupine odvisne. Napadi s takšnimi orodji so izvedeni proti najbolj ranljivim računalniškim sistemom, ki nimajo taktične ali strateške pomembnosti. Takšni napadi predstavljajo nezmožnost podrobnejše analize tarč in pomanjkanje znanja ali sredstev za napad na sisteme z boljšo zaščito. Teroristične organizacije s takšno sposobnostjo izkazujejo nesposobnost integracije enot in strokovnjakov v aktivnosti, pomanjkanje nadzora nad njimi ter slabe učne sposobnosti organizacije na področju izvedbe kibernetskih napadov (Nelson in drugi 1999, 13–14).

Napredno strukturirane sposobnosti predstavljajo uspešnejše in bolj sofisticirane napade na več računalniških sistemov ali omrežij z namenom povzročanja željenega učinka. Teroristična organizacija izkaže sposobnost programiranja osnovnih orodij in reprogramiranja javno dostopnih orodij za kibernetske napade. Organiziranost takšne skupine izkazuje osnovno hierarhično strukturo in omogoča zaporedne napade iz enotne lokacije. Organizacija je sposobna analizirati tarčne računalniške sisteme in spremeniti osnovne pristope k napadom. Takšna teroristična organizacija izkazuje učne sposobnosti in zna prenašati to znanje do novih članov (Nelson in drugi 1999, 16).

Kompleksno strukturirane sposobnosti kibernetskih teroristov pa zajemajo zmožnosti za izvajanje več koordiniranih sofisticiranih napadov, ki povzročijo velike prekinitve v delovanju IKT ali dostopu do njih iz različnih lokacij. Sposobnosti takšne organizacije zajemajo podrobno analizo ranljivosti, izvedbo vdorov v zaščitene računalniške sisteme in programiranjem orodij za kibernetske napade. Takšne organizacije imajo dobro razdelano hierarhijo poveljevanja in

nadzora. Organizacijska učna sposobnost predstavlja sposobnost hitre adaptacije na novo tehnologijo, spremljanje sprememb v kibernetskem prostoru, pojavu ranljivosti in spremembi delovanja same organizacije za optimalnejšo delovanje (Nelson in drugi 1999, 16–17).

Kompleksno strukturirane sposobnosti se zaradi svoje obsežnosti razvijajo v dveh smereh. Prva razvija popolnoma integrirano kibernetsko teroristično podporo tradicionalnim terorističnim napadom in dejavnostim. Druga smer pa predstavlja grožnjo čistega kibernetskega terorizma. Kompleksnost kibernetske teroristične dejavnosti in sposobnost, da koordinirajo in izvedejo napad na eno ali več omrežnih infrastruktur iz več lokacij in z različnimi sistemi, različnih sistemskih arhitektur ter programskih jezikov, kar povzroči omrežno preobremenjenost in onesposabljanje varnostnih mehanizmov. Celosten napad omogoči rahljanje varnostnih protokolov, kar omogoči dostopanje do informacij in podatkov, ali pa popolnoma onesposobi omrežno infrastrukturo, kot v primeru napada za zavrnitev storitev DOS ali DDOS. Izvedba takšnih napadov predstavlja visoko organiziranost organizacije ter poglobljeno in strokovno znanje informacijsko-komunikacijske tehnologije (Nelson in drugi 1999, 16–17).

Poleg izredno sofisticiranih kibernetskih napadov na informacijsko-komunikacijsko tehnologijo uporabljajo teroristične skupine informacijske in računalniške sisteme tudi v manj kompleksne namene. Za izvedbo zgoraj opisanih napadov morajo imeti teroristične organizacije veliko mero strokovnega in tehničnega znanja, zato se organizacije poslužujejo internetnih aktivnosti za načrtovanje, koordiniranje, financiranje, politične akcije, rekrutiranje, propagando in prikazovanje moči (Cohen 2002).

3 Islamska država

3.1 Nastanek Islamske države

Islamska država ima svoje korenine v Organizaciji za monoteizem in džihad, ki je bila ustvarjena leta 1999. Skozi leta delovanja jo je najbolj spodbudila invazija na Irak leta 2003, kjer je postala ena od aktivnejših terorističnih organizacij v Iraku. Delovala je proti koalicijskim silam z namenom odvračanja civilnega prebivalstva od sodelovanja z njimi in poskušala odstaviti vmesno vlado. Islam je igral pomembno vlogo v ideologiji organizacije, saj je za utemeljevanje lastnega delovanja in mobilizacijo podpornikov uporabljala vero in Koran. Leta 2004 se je organizacija integrirala v širšo mrežo Al Kaide in v njenem imenu delovala na območju Iraka. Bila je znana po svojem krutem in neselektivnem delovanju tako proti koalicijskim silam kot tudi civilistom. Leta 2006 je prišlo do preimenovanja skupine v Islamsko državo v Iraku (ISI), vendar večje reorganizacije iz časov Al Kaide v Iraku ni bilo zaznati (Hashim 2014). Z umikanjem ZDA in zaveznic iz mest ter predajanja nalog Iraškim varnostnim silam pa je Islamska država v Iraku ponovno pridobila možnost za nadaljevanje svojih aktivnosti (Laub 2016). Organizacijske spremembe, ki jih je v času od 2010 do 2013 izvedel Abu Bakr al-Baghdadi, so povzročile večjo učinkovitost na bojišču in tudi doseganje veliko večjih uspehov pri implementaciji načrtov. Spremenila se je tudi strategija pristopa k boju, saj je prišlo do večje selektivnosti pri izbiri ciljev in zmanjševanja ugleda krute organizacije. Močna propagandna in informacijska dejavnost je dodatno izboljšala ugled in privabila veliko število novih podpornikov tako v Iraku kot tudi drugod po svetu (Hashim 2014). Marec 2011 je predstavljal novo priložnost za delovanje in širjenje ISI v Sirijo. Sirska državljanska vojna je oslabila vlado sirskega predsednika Basharja al-Assada, kar je Islamska država v začetnih stopnjah izrabila za izoblikovanje skupine Jabhat al-Nusra kot svoj podaljšek v Siriji (Hashim 2014). Kljub neuspešni združitvi s to skupino je Islamska država leta 2014 pričela z vojaškimi akcijami v Siriji in Iraku ter zajela velik del teritorija. Po uspehih se je ISI preoblikovala v Islamska državo v Siriji in Iraku, po nekaj mesecih pa se je oklicala za Islamsko državo oziroma kalifat z kalifom Bakrom al-Baghdadijem (BBC 2015). Nasprotovanje Islamske države državam, ki sodelujejo v konfliktu, se je stopnjevalo do te mere, da je Islamska država napovedala vojno proti "intervencionističnim" državam in prešla v uporabo strategije ofenzivnega džihada. S tem je pričela z izvajanjem terorističnih akcij izven

svojega ozemlja in izpeljala serijo terorističnih napadov, ki so povzročili več kot tisoč smrtnih žrtev (Tomkiw 2016).

3.2 Islamska država in kibernetski terorizem

Preplet terorizma in kibernetske kriminalitete postaja vse bolj kompleksen. Nov terorizem, kot so ga poimenovali nekateri, uporablja tradicionalne metode delovanja, ki jim dodaja tudi nove načine izvajanja napadov. Kibernetski prostor ponuja okolje, kjer je malo regulacije in zaradi tega omogoča anonimno ter nemoteno delovanje terorističnih organizacij.

Islamska država je pokazala, da razume pomen kibernetskega bojevanja. S svojo upravno organiziranostjo je izoblikovala oddelek za informiranje, ki deluje po celotnem okupiranem ozemlju. Uprava je razdeljena na več upravnih območij oziroma provinc (wiliyat), kjer delujejo časopisni, radijski in televizijski mediji, namenjeni informiranju in zabavi prebivalstva. Ti mediji imajo močno prisotnost tudi v kibernetskem prostoru, saj je možno do njih dostopati prek notranjega interneta, vzpostavljenega na ozemljih pod nadzorom Islamske države (Jihad Intel 2016).

Poleg informacijske dejavnosti so se v kibernetskem prostoru izoblikovale tudi specializirane skupine, ki so namenjene zagotavljanju varnosti informacijske infrastrukture in izvedbo napadov na internetne in kibernetske tarče Islamske države.

3.2.1 Caliphate Cyber Army

Caliphate Cyber Army (Vojska kibernetskega kalifata ali CCA) je pridobila prepoznavnost po razglasitvi Islamske države za kalifat 29. juniju 2014. CCA je deloval pod vodstvom Junaida Hussaina z vzdevkom TriCk ali fame (v hekerskem kolektivu TeaMp0isoN). Hussain je pobegnil iz Velike Britanije v Raqqo, Sirija leta 2013, ko je odslužil zaporno kazen za dejanja kibernetske kriminalitete. V Siriji se je pridružil Islamski državi in zaradi svojega tehničnega znanja in izkušenj pridobil možnost za vzpostavitev hekerske skupine Kibernetskega kalifata (Cyber Caliphate). Kljub svojemu znanju in izkušnjam Hussain ni mogel vzpostaviti bolj uspešne skupine zaradi pomanjkanja podpore širše hekerske skupnosti (Alkhouri in drugi 2016, 3–5).

Po Hussainovi smrti avgusta 2015 se je delovanje CCA nekoliko upočasnilo. Pomanjkanje vodstva je povzročilo velike spremembe v sami skupini, a to je dodatno spodbudilo pripravljenost in izvajanje kibernetskih napadov. Hussaina je na vodstveni funkciji zamenjal Siful Haque Sujan, 31-letni britanski računalniški strokovnjak bangladeških korenin. Štiri mesece po smrti Hussaina so Združene države Amerike izvedle napad z brezpilotnim letalom na novo vodstvo CCA in ubile tudi Sujana (Alkhouri in drugi 2016, 4).

3.2.2 Islamic State Hacking Devision

Islamic State Hacking Devision (ISHD) je pridobil na prepoznavnosti v začetku leta 2015. Struktura hekerskega oddelka je dobila idejo po CCA, z njo pa je imela veliko povezav. Junaid Hussain je v obeh skupinah igral pomembno vodstveno vlogo, kar pojasni povezanost med ISHD in CCA (Alkhouri in drugi 2016, 6–8).

ISHD so prvi pričeli z aktivno integracijo tujih računalniških strokovnjakov v svoje vrste, čeprav niso bili na ozemlji Islamske države. Uspehi in širjenje informacij med hekerji ter prevzemanje odgovornosti Islamske države ali ISHD so povzročili prve pravne postopke proti hekerjem izven območja Islamske države. Za primer lahko vzamemo kosovskega hekerja Th3Dir3ctorY, Ardita Ferizija, ki je sodeloval pri kibernetskih napadih in podatke predal ISHD (Alkhouri in drugi 2016, 7).

3.2.3 Islamic Cyber Army

Islamic Cyber Army (ICA) je pridobila prepoznavo 10. septembra 2015 s svojo prvo uradno objavo na družbenem omrežju Twitter. Sporočili so, da hekerski podporniki mudžahedinov (Islamske države) delujejo pod imenom Islamic Cyber Army in izvajajo e-džihad proti ZDA in njenim zaveznikom (Alkhouri in drugi 2016, 9–11).

Sposobnosti ICA so bile takrat pomanjkljive, saj so napadali informacijske sisteme s šibko varnostjo. Strateškega ali taktičnega cilja ni bilo, v veliko primerih pa so bili napadi izvršeni na spletne strani, ki niso bile povezane z ZDA ali njenimi zaveznicami, vendar so na njih pustili njim namenjena sporočila (Alkhouri in drugi 2016, 11).

3.2.4 Sons of Caliphate Army

Sons of Caliphate Army (SCA) je hekerska skupina, ki je pridobila prepoznavnost januarja 2016 v zasebni skupini CCA v aplikaciji Telegram. Povezave in sodelovanje med CCA in SCA so bile zelo razširjene, saj sta si skupini medsebojno delili podatke, informacije, uradne izjave ter kreditirali prevzeme odgovornosti za kibernetske napade. Iz tega sodelovanja lahko razberemo, da je bila strukturna sestava in koordinacija med obema skupinama veliko boljša kot pri ostalih skupinah (Alkhouri in drugi 2016, 15–16).

3.2.5 AnonGhost Caliphate

AnonGhost so pro-palestinska kibernetska teroristična organizacija, ki je pričela delovati januarja 2014. AnonGhost nekateri strokovnjaki povezujejo tudi z Anonymous Tunizija in je organizacija, ki se bori proti izraelski okupaciji Palestine in Gaze. Njihovo delovanje v kibernetskem prostoru je usmerjeno proti izraelskim spletnim stranem in stranem njihovih podpornikov. Zaradi obsežnih kibernetskih napadov v sklopu operacij delovanja proti Izraelu OPisrael in OPisraelBirthday so si prislužili naziv kibernetskih teroristov (TRAC 2016).

V sklopu obeh večjih operacij je organizacija izvedla 11,000 napadov na spletne strani z napadi razobličenja spletnega mesta in napadi za zavrnitev storitve (Distributed Denial Of Service). Zaradi močnega nasprotovanja judovstvu in njegovim zaveznikom (TRAC 2016) je Islamska država hitro opazila potencial, ki ga AnonGhost predstavlja, in ga poskusila pridobiti v svoje vrste.

Del AnonGhost skupine se je januarja 2016 preimenoval v AnonGhost Caliphate, ob tem pa objavil slikovno in video vsebino, v katerem uradno izkazujejo pripadnost Islamski državi in predvajajo njeno propagando (Mirror 2016).

3.2.6 Kalachnikov.TN

Kalachnikov.TN (poznan tudi kot Kalachnikov e-security team ali Fallaga.TN) je tunizijska hekerska skupina, ki je aktivna v kibernetskem prostoru vse od sredine leta 2013 (Kalachnikov.TN 2013). Kalachnikov.TN izvaja svoje aktivnosti z namenom izboljšanja življenj

Arabcev po vsem svetu. Med primarnimi fokusi skupine so kibernetski boji proti izraelski okupaciji Palestine in Gaze, proti medetničnemu konfliktu v Burmi ter proti indijski okupaciji Kašmirja (Kalachnikov.TN 2013). Aktivnosti Kalachnikov.TN skupine so izobraževanje džihadistov o računalniški in informacijski dejavnosti, širjenje informacij, vključno z propagando, aktivnostmi za privabljanje novih kadrov in izvajanje kibernetskih napadov (MEMRI 2016c).

Skupini AnonGhost Caliphate in Kalachnikov.TN imata povezave z lokalno hektivistično skupino Anonymous iz Tunizije, kar predstavlja možnost lokalnega sodelovanja in koordiniranja skupin ter širjenja informacij o ciljih (Kalachnikov.TN 2016b). Zaradi izvedbe kibernetskih napadov in širjenja propagande skozi razobličene spletne strani si je tudi skupina Kalachnikov.TN pridobila naziv kibernetske teroristične skupine.

3.2.7 United Cyber Caliphate

Štiri od zgoraj opisanih podpornikov, konkretno CCA, SCA, Kalachnikov.TN in AnonGhost Caliphate, so se 4. aprila 2016 združile v enotno skupino oziroma organizacijo United Cyber Caliphat. Uradno sporočilo o združitvi je bilo poslano prek CCA-jevega zasebnega kanala v aplikaciji Telegram. V sporočilu je objavljena povezava do družbenega omrežja Twitter, na katerem so člani CCA ugrabili enega od osebnih računov ter prek njega sporočili informacijo o integraciji štirih skupin v enotno organizacijo UCC. Sporočilo je bilo poslano v štirih jezikih: angleščini, arabščini, francoščini in ruščini. S tem so poskušali zajeti čim večjo javnost in spodbuditi mobilizacijo mogočih podpornikov (Alkhouri in drugi 2016, 17–19).

Namen združitve je bil povečanje zmogljivosti izvajanja kibernetskih aktivnosti in boljšo koordinacijo v boju s nasprotniki Islamske države ter izobraževanje na področju informacijske varnosti in zaščite (Alkhouri in drugi 2016, 17–19). Vendar kljub združenju skupin v enotno krovno organizacijo, ki se identificira z Islamsko državo, vsaka od teh skupin še nadaljnjo izvaja aktivnosti v lastnem interesu. Primer sta skupini AnonGhost Caliphate in Kalachnikov.TN, ki nadaljujeta s svojim bojem proti izraelski okupaciji Palestine in Gaze, vendar na razobličenih spletnih straneh ne zapišeta povezav z Islamsko državo (Priloga Č.1).

3.2.8 Rabitat Al-Ansar

Rabitat Al-Ansar (z angleškim prevodom League of Supporters) je islamističen medij, ki spada pod Globalno islamistično medijsko fronto. S pojavom Islamske države je Rabitat Al-Ansar sprva deloval kot džihadističen medij za promocijo Islamske države in širjenje njene propagande, kasneje pa je s porastom uporabe informacijskih sistemov za prenos informacij in propagande posegel tudi v uporabo kibernetskega prostora za izvajanje napadov. Izoblikovana je bila posebna skupina znotraj Združenja podpornikov, imenovana Hacker Aldmar. Združenje podpornikov je z izvedbo napadov in uradnim prevzemom odgovornosti zanje opozorilo na svoje sposobnosti in bilo zaradi povezav z Islamsko državo obtoženo kibernetskega terorizma (Alkhouri in drugi 2016, 12–14).

3.2.9 Problematika raziskovanja kibernetskih skupin

Kibernetski prostor daje možnost za anonimno delovanje hekerskih skupin. Ravno ta anonimnost predstavlja veliko problem za raziskovanje vseh možnih skupin, ki delujejo v imenu Islamske države. Te skupine imajo na medmrežju možnost hitrega spreminjanja imen, kar vodi v različna poimenovanja istih skupin ali neenoten zapis imen skupin in članov teh skupin. In ravno ta različna poimenovanja, skupaj z anonimnostjo ter različnimi prevodi istih skupin in organizacij, vodijo do tega, da se v veliko primerih prikazujejo kot različne organizacije. Lep primer tega je skupina Kalachnikov e-security, ki je v preteklosti in še danes uporablja več različnih imen. Skupina Kalachnikov e-security je poznana tudi kot Kalachnikov.TN ali Fallaga.TN, kot sem že omenil. Podobno je tudi z imeni oziroma vzdevki posameznikov, ki v teh skupinah delujejo. Vzdevki omogočajo ohranjanje anonimne identitete, obenem pa sprememba identitete omogoča občutek, da v skupinah deluje večje število računalniških strokovnjakov ali hekerjev.

Zgoraj omenjene skupine največkrat prevzamejo odgovornost za kibernetske napade prek družbenih omrežij ali spletnih strani, katere ugrabijo ali razobličijo. S takšnim delovanjem preusmerijo pozornost nase in stran od drugih možnih akterjev v kibernetskem prostoru. Na temnem internetu je možno najeti hekerske skupine, ki izvedejo kibernetski napad in niso motivirane zaradi pripadnosti, ampak zaradi denarja. Vendar je dokazovanje takšnih povezav med kibernetskimi kriminalci in kibernetskimi teroristi izredno težko. Poleg kibernetskih

kriminalcev so na temnem internetu tudi arhivi informacij in podatkov iz prejšnjih kibernetskih napadov, ki jih hektivistične ali kibernetske kriminalne skupine ponudijo v odkup. Te velikokrat vsebujejo osebne podatke, podatke o kritični infrastrukturi in podatke o informacijskih sistemih (Paganini 2015).

4 Analiza kibernetskega terorizma

4.1 Kibernetski napadi

Kibernetske skupine terorističnih organizacij so vse bolj aktivne v kibernetskem prostoru, saj prepoznavajo njegov potencial. Nasprotnik oziroma njegova infrastruktura (tudi kritična) je le nekaj klikov stran in omogoča kibernetskim teroristom izvajanje dejavnosti, ki jih ne bi bili sposobni v fizičnem okolju.

V svojem diplomskem delu nisem pokril vseh napadov, saj bi bilo to zaradi obsežnosti raznolikih napadov praktično nemogoče. Zaradi tega je v tem poglavju mogoče najti opise zgolj najpomembnejših napadov, pri čemer sem kot kriterij uporabljal medijsko odmevnost in strateško pomembnost ciljev.

Islamska država je s svojo združeno skupino UCC pridobila sposobnosti, ki jih v preteklosti ni imela še nobena druga teroristična skupina. Vendar pa ne smemo gledati le na UCC kot osrednje izvajalce kibernetskih napadov znotraj Islamske države. Obstajajo tudi druge hekerske skupine, ki opravljajo takšne napade v imenu Islamske države. Primer takšne skupine je Hacker Aldmar v skupini Rabitat Al-Ansar, opisani v prejšnjem poglavju (Alkhouri in drugi 2016, 12–14).

Kibernetske napade lahko definiramo kot napade na informacijske sisteme in kritične informacijske infrastrukture z namenom preprečevanja dostopa do podatkov, spremembo ali uničenjem elektronske vsebine, vdora in prenosa informacij, poškodovanja ali uničenja računalniških in drugih informacijskih sistemov. Kibernetski napadi so usmerjeni proti programski kot tudi proti strojni opremi (Ballard in drugi 2004, 58–59).

Kibernetski oddelki Islamske države so skozi svojo mrežo računov na družbenih omrežjih od začetka delovanja prevzemali odgovornost za izvedene napade. Njihova prepoznavnost v kibernetskem prostoru je odvisna od dosežkov in vsebin, ki jih generirajo. Zato lahko velikokrat opazimo njihove predstavitvene vsebine in slikovno gradivo na socialnih omrežjih in spletnih straneh, ki so jih ugrabili ali razobličili.

Prvi kibernetski napadi so bili v imenu Islamske države izvedeni že decembra 2014. CCA, ki je te napade izvedla, je napadala predvsem spletna mesta s šibko obrambo in jim spremenila vsebine ali jih ugrabila za lastne potrebe. Njihova prisotnost na družbenih omrežjih je bila vzpostavljena ob začetkih delovanja organizacije, predvsem z namenom informiranja javnosti o uspelih kibernetskih napadih in privabljanja istomiselnih hekerjev v svoje vrste (Alkhouri in drugi 2016, 3–5).

Sposobnosti CCA so bile izjemno šibke in nestrukturirane. Posamezni uspehi na področju razobličenja spletnih mest so predstavljali slabo organiziranost, neznanje pri iskanju in analizi tarč ter nesposobnost izoblikovanja sofisticiranih orodij za izvedbo vdorov ali napadov za zavrnitev storitev (Alkhouri in drugi 2016, 5).

8. aprila 2015 je skupina prevzela odgovornost za napad na francosko televizijsko postajo Monde Tv5. V napadu naj bi uspela prevzeti nadzor nad računalniškim sistemom, ki je odgovoren za oddajanje, in ga ustaviti za tri ure. Ob tem napadu so pripadniki skupine tudi uspeli prevzeti nadzor nad uporabniškimi računi družbenih omrežij, na katerih so objavili propagandno vsebino in osebne podatke pripadnikov francoskih organov, ki sodelujejo v boju proti Islamski državi. Vendar je francoski preiskovalni organ analiziral napade in ugotovil, da za izvedbo napada najverjetneje stoji ruska hekerska skupina APT28. Zaradi tega se pojavljajo dvomi, da so kibernetski oddelki Islamske države izvedli napad, čeprav so odgovornost zanj prevzeli (Paganini 2015b).

Med letoma 2014 in 2016 je prišlo do izboljšanja sposobnosti CCA, saj je z vdorom v strežnike ali račune elektronske pošte prišla do tajnih podatkov, ki so zajemali osebne podatke zaposlenih. Primer je dostop do osebnih podatkov pripadnikov newyorške tranzitne policije in policije zvezne države Minnesote, ki je prikazal uspešnost novejših taktik. Izoblikovane in urejene osebne podatke so poimenovali Kill List oziroma sezname za uboj, ki so jih nato javno objavili prek svojih družbenih omrežij. Pozvali so ameriške doma radikalizirane pripadnike Islamske države, da na njih in njihove družine izvedejo napade (SITE 2016).

ICA je kot ena od podpornih skupin izvajala napade leta 2015 v okviru svoje akcije America Under Attack (napad na Ameriko). S sofisticiranim kibernetskim napadom je vdrla v strežnike

Bele hiše in prenesla osebne podatke zaposlenih in imena osebja, zaposlenega v zakonodajnih institucijah ZDA. Te podatke je javno objavila s podobnim pozivom kot CCA. Drugi kibernetski napad je bil usmerjen proti zaposlenim FBI (Zveznega preiskovalnega urada) in je zajemal 300 računov elektronske pošte in osebnih podatkov. Flashpoint, organizacija za preučevanje temnega spleta in kibernetskih aktivnosti, je analizirala 300 objavljenih računov elektronske pošte in ugotovila, da je seznam le kopija LulzSec-ovega seznama, ki je bil objavljen leta 2012. Tako tega vdora ne smemo pripisati ICA, saj so le kopirali arhive prejšnjih vdorov in jih javno objavili. Nadaljnji vdori so prikazali pomankanje sofisticiranosti in znanja, saj se je ICA usmerila le v napade spletnih mest s šibko obrambo. Primer tega je serija napadov oktobra 2015, kjer so napadli več spletnih mest brez povezav z ZDA, vendar so na razobličenih spletnih straneh pustili sporočilo s propagandno vsebino, namenjeno ZDA (Alkhouri in drugi 2016, 9–11).

Rabitat Al-Ansar je leta 2015 izvedla napade na strežnike ameriških in drugih organizacij z namenom pridobivanja osebnih podatkov. Pripadniki hekerske veje Rabitat Al-Ansarja so pridobili dostop do imen, naslovov in telefonskih številk več kot 2000 posameznikov, večina katerih je bila Američanov. Nadaljevanje svojih operacij v kibernetskem prostoru je bilo zaznati maja 2015, ko je skupina izvedla napade na ameriške in avstralske spletne strani, ki so jih razobličili in napolnili s propagandnimi sporočili. Skupina je z napadom na spletne trgovine dosegla dostop do podatkov o kreditnih karticah American VISA in Mastercard. Te so javno objavili in pozvali podpornike, naj jih uporabijo v lastne namene. Flashpoint je analiziral objavo in podatke kreditnih kartic in ugotovil, da so ti podatki najverjetneje prišli iz spletne trgovine Scarfaze hack store, ki se ukvarja s preprodajo ukradenih kreditnih kartic. Dostop do teh kreditnih kartic za to ne smemo pripisati Rabita tal-Ansarju, saj so ti podatki bili pridobljeni s strani drugih hekerskih skupin (Alkhouri in drugi 2016, 13–14).

Sons of Caliphate Army je s svojim delovanjem v letu 2016 dosegla veliko uspehov pri vdorih v uporabniške račune družbenih omrežij Twitter in Facebook. Skupina je v svojem video gradivu prikazala več ugrabljenih uporabniških računov, celotno število ugrabljenih računov pa naj bi bilo 15,150 (10,000 Facebook računov in 150 skupin ter 5,000 Twitter računov). Nadaljevanje napadov proti družbenemu omrežju Twitter se je nadaljevalo 4. februarja, ko so pripadniki SCA

izvedli napad za zavrnitev storitve DDOS. Spletna stran družbenega omrežja je bila zato nedosegljiva za 2 uri (Alkhouri in drugi 2016, 15–16).

Hekerski oddelek Islamske države je pričel s svojim delovanjem leta 2015. Takrat je prevzel odgovornost za vdor v ameriški strežnik in iz njega prenesel osebne podatke okoli 1,500 zaposlenih v državni upravi in oboroženih silah ZDA. Podatki so zajemali ime in priimek, oddelek zaposlitve, naslove elektronske pošte, telefonske številke, gesla in lokacijo ali naslove. Poleg teh podatkov so bili pridobljeni tudi podatki o kreditnih karticah, družinskih članih in elektronskih pogovorih (SITE 2016, 7). Junija 2015 je hekerski oddelek Islamske države pridobil dostop do italijanskih vojaških strežnikov in osebnih podatkov 10 vojaških častnikov, ki so zajemali ime, naslov in telefonske številke. Nova objava osebnih podatkov je sledila na obletnico 11. septembra, ko je hekerski oddelek Islamske države objavil dodaten seznam z osebnimi podatki 100 vojaških uslužbencev. Vse sezname je ISHD objavil javno prek svojih družbenih omrežij in pozval doma radikalizirane džihadiste v izvedbo napadov na objavljene osebe (Alkhouri in drugi 2016, 6–8; SITE 2016, 7).

Hekerski skupini Anonghost Caliphate in Kalachnikov.TN sta pred svojo podreditvijo Islamski državi izvajali kibernetske napade na spletna mesta držav in organizacij, za katere sta menili, da povzročajo krivico in zatirajo muslimane. Skupini sta izvajali napade za razobličenje spletnih mest, potem pa so na njih pustili sporočila, ki so imela propagandne vsebine in vzdevke ter ime napadalcev. S tem so prevzeli odgovornost za izveden napad in razširjali propagando (Priloga Č). Napadi, ki so bili izvedeni po uradni razglasitvi pripadnosti Islamski državi, so bili redki, vendar so nadaljevali s podobnim načinom izvajanja terorističnih akcij. Posebnost Kalachnikov.TN skupine, ki deluje v imenu Islamske države, je močna prisotnost na družbenih medijih, prek katerih razširja uporabne vsebine za posameznike, ki bi radi izvajali kibernetske napade. S tem izobražujejo in novačijo nove pripadnike za lastno skupino in za druge, ki delujejo v imenu Islamske države (Russon in Murdock 2016).

Kalachnikov skupina je 4. marca izvedla napade na italijanske strežnike. Z uspešnimi vdori se je dokopala do osebnih podatkov vendar jih niso javno objavili, kot so to počele druge skupine. Nekaj dni kasneje, 8. marca, so na svojih družbenih omrežjih objavili seznam uspešnih vdorov v

strežnike spletnih strani. Seznam obsega 32 spletnih mest, ki so večinoma zahodna in katerih vsebine so zamenjali z lastnimi propagandnimi temami, kontakti in vzdevki napadalcev. 9. marca so nadaljevali z objavami uspehov kibernetskih napadov in sestavili seznam zdajšnjih in prejšnjih uslužbencev Banke Zveznih rezerv ZDA, objavili njihove osebne ter kontaktne podatke in naslove. V okviru akcije proti Savdski Arabiji je Kalachnikov.TN izvedel več napadov z namenom prisiljevanja vlade v prenehanje izvajanja vojaških aktivnosti v Jemnu. Napadi na Banko Zveznih rezerv in spletna mesta v Savdski Arabiji so bili izvedeni s pomočjo džihadistične hekerske skupine CyberTeam Rox, ki je veljala za avtonomno hekersko skupino brez povezav z Islamsko državo (MEMRI 2016l).

AnonGhost Caliphate je po javni objavi pripadnosti Islamski državi nadaljeval izvajanje kibernetskih napadov za razobličenje spletnih mest. Pri njih je mogoče opaziti posebnost, saj kljub uradni pripadnosti hekerji na razobličenih straneh ne pustijo propagandnih ali drugih vsebin Islamske države, ampak le vzdevke sodelujočih hekerjev in sporočilo za osvoboditev Palestine.

Združen kibernetski kalifat je s svojimi kibernetskimi akcijami začel takoj po razglasitvi združitve na novem računu družbenega omrežja Twitter in Telegram. 5. aprila 2016 je UCC prevzel odgovornost za razobličenje spletnega mesta indonezijskega veleposlaništva v Franciji. Na spremenjeni spletni strani so objavili tekstovno in slikovno propagandno vsebino v skladu s propagandnimi napori Islamske države (SITE 2016). Sposobnosti UCC-ja so se po združitvi močno izboljšale.

Kibernetski napadi so se močno razširili po 15. aprilu, ko so napadli avstralske strežnike in razobličili več spletnih strani (MEMRI 2016e). 25. aprila je prišlo do vdora v strežnike ameriškega državnega urada, iz katerega so ukradli osebne podatke (SITE 2016, 6). Vdori, ki so sledili, so zajemali različne tarče, med njimi ameriška podjetja, vladne organizacije, ameriške oborožene sile in politične stranke (MEMRI 2016c, MEMRI 2016č, MEMRI 2016k). Poleg ameriških organizacij so pripadniki skupin izvajali tudi napade na evropske strežnike in strežnike Savdske Arabije (MEMRI 2016l).

Oblikovanje in objavljanje seznamov za usmrtitve (Kill Lists) se je pričelo 22. aprila, ko so pripadniki UCC objavili imena in osebne podatke 3,000 uglednejših prebivalcev New Yorka in Brooklyna (SITE 2016). Objava osebnih podatkov iz vdora v strežnike Državnega urada ZDA 25. aprila je bila objavljena naslednji dan, zajemala pa je okoli 100 zaposlenih (MEMRI 2016j). Nove objave takšnih seznamov so se zgodile še 27. maja z napadom na knjižnico v Arkansasu (MEMRI 2016c), 13. julija z objavo osebnih podatkov 22 zaposlenih v Državnem uradu ZDA (MEMRI 2016b), 16. in 17. julija z napadom na strežnike izvršilnih organov ZDA, ko so objavili večje število osebnih podatkov zaposlenih (MEMRI 2016f), 20., 25. julija in 3. avgusta pa so pripadniki UCC iz neznanih strežnikov ukradli informacije več kot 1000 pripadnikov ameriških oboroženih sil (MEMRI 2016g, MEMRI 2016i, MEMRI 2016j). 21. julija je prišlo do objave osebnih podatkov 2,700 prebivalcev New Yorka (MEMRI 2016a; MEMRI 2016h), 11. avgusta pa do objave osebnih podatkov 362 zaposlenih v ameriški vojski (SITE 2016, 8–16). Vsi javno objavljeni seznami so bili namenjeni doma radikaliziranim pripadnikom Islamske države, ki so jih v svojih sporočili poskušali spodbuditi v izvajanje terorističnih aktivnosti proti objavljenim osebam (SITE 2016, 8–16).

Pripadniki UCC so zelo aktivni na družbenih medijih. Družbene medije uporabljajo za širjenje propagandnih vsebin, prevzemanje odgovornosti za kibernetske napade in iskanje tarč. Primer tega je ugrabljanje uporabniških računov na Twitterju in Facebooku, ko prevzamejo nadzor nad njimi in jih uporabijo v lastne namene. V najnovejših napadih so pripadniki UCC pridobili nadzor nad vsemi uporabniškimi računi ameriškega CENTCOM-a oziroma Centralnega poveljstva ZDA, ki je odgovorno za informiranje o dogajanju na območju severne Afrike, centralne Azije in Bližnjega vzhoda (Alkhouri in drugi 2016, 18).

Sofistikacija in obseg napadov kibernetskih skupin Islamske države sta se v zadnjem letu močno povečali. Uspehi pri izvedbi kibernetskih napadov so pokazali, da so kibernetske teroristične skupine Islamske države takšne napade sposobne izvajati in povzročiti škodo vsaj na programskem delu IKT.

Orodja, ki jih te skupine uporabljajo, so težko dokazljiva, vendar jih lahko uvrstimo v dve kategoriji. Prva kategorija so orodja za vdore, druga pa zavzemajo zlonamerno programsko

vsebino, ki omogoča lažje dostope do kompromitiranih sistemov (Alkhouri in drugi 2016, 21–22).

Orodja za vdore lahko Islamska država pridobiva iz javno dostopnih spletnih strani na indeksiranih spletnih straneh ali temnem in globokem spletu (Alkhouri in drugi 2016, 22). To predstavlja uporabo orodij, ki so jih naredile druge hekerske skupine ali organizacije in so že testirana oprema, ki je lažja za uporabo, saj ne potrebuje toliko tehnično strokovnega znanja kot programiranje novih, zasebnih orodij. Zaradi pomanjkanja tehničnega in strokovnega znanja je najbolj verjetno, da skupine Islamske države uporabljajo prosto dostopna orodja, saj je izvedba bolj naprednih napadov proti sistemom z dobro obrambo zaenkrat še neizvedena. Uporabnost zasebno programiranih orodij bi bila verjetno preveč kompleksna za uporabo manj izkušenim hekerjem, ki so se pridružili skupinam.

Za razliko od orodij pa je verjetnost uporabe po meri oblikovanih zlonamernih programov veliko večja. Pripadnikom hekerskih skupin je veliko lažje programirati nov program, ki bo izrabljal ranljivosti sistemov in ostal neodkrit s strani varnostnih sistemov na računalnikih (antivirus, požarni zid in drugi) (Alkhouri in drugi 2016, 22). Vendar do zdaj še ni bilo zaznanih posebnih zlonamernih programov, ki bi bili sprogramirani s strani skupin Islamske države.

Cilje, ki jih napadajo kibernetske teroristične skupine Islamske države, lahko razdelimo v dve kategoriji. Prva so tisti cilji s šibko varnostjo sistemov, ki hitro postanejo nov uspeh skupin, medtem ko drugi zajemajo kompleksne tarče, ki vsebujejo vladno, ekonomsko ali družbeno pomembne sisteme z bolj sofisticirano obrambo. Zaradi delovanja tujih držav v sirskem in iraškem konfliktu hekerske skupine usmerjajo napade proti večjim akterjem, ki aktivno delujejo v konfliktu. V primeru Islamske države so glavni cilji informacijska infrastruktura ZDA, Velike Britanije, Francije, Italije, Avstralije, Savdske Arabije in tudi Ruske federacije, odkar so Rusi posredovali v Siriji (Alkhouri in drugi 2016, 23; SITE 2016).

5.2 Propaganda

Psihološko bojevanje spada v koncept informacijskega bojevanja, vendar lahko močno posega v območje kibernetskega terorizma, saj je ena od osrednjih dejavnosti terorističnih organizacij

uporaba internetne propagande za upravičevanje svojih dejavnosti, medtem ko prikazuje nasprotnika kot nelegitimnega in nemoralnega. Preplet področij delovanja informacijskega bojevanja postane v dobi IKT še bolj kompleksen.

Propagando lahko umestimo tudi v kibernetski terorizem, kljub temu, da ima svoje področje delovanja v informacijskem bojevanju. Definicija propagande Daughertyja in Janowitza govori o propagandi kot »o načrtovanem razširjanju novic in informacij ciljnemu občinstvu. Namen razširjanja informacij je sprememba ali vplivanje na razmišljanje občinstva, njihovo verovanje ali delovanje« (Daugherty in Janowitz v Malešič 1994, 32).

Terorizem uporablja načrtovano informiranje in razširjanje novic ciljnemu občinstvu, ki ga lahko razdelimo v dve skupini. Prva skupina so podporniki, na katere mora sporočilo vplivati pozitivno ali mobilizacijsko, s čemer pripomore k naporom bojevanja na tleh in v mislih prvega tarčnega občinstva. Na drugo skupino pa mora vplivati negativno tako, da povzroči strah in paniko ter neželjo po delovanju proti terorizmu.

Kibernetski terorizem in z njim povezana propaganda zajemata vzpostavljanje spletnih strani (Cohen v Bernik in Prislan 2012, 132), uporabniških računov na družbenih omrežjih in oblikovanje pisnega, slikovnega, glasovnega ali video gradiva, ki ga prek teh načinov razširjajo. Z njimi poskušajo vplivati na razmišljanje tarčnega občinstva ter ohranjajo moč nad kanali komunikacije, s čimer lahko spreminjajo, selekcionirajo in enostavno izbrišejo informacije.

Islamska država daje velik poudarek informacijskemu in psihološkemu bojevanju že od samih začetkov Organizacije za monoteizem in džihad (Hashim 2014). Informiranje javnosti jim omogoča razširjati njihovo interpretacijo sveta in njihovo resnico (Cohen v Bernik in Prislan 2012, 132), obenem pa jim omogoča odgovor na in zanikanje nasprotnikove propagande.

Propagandni sistem Islamske države je strukturno zelo razvejan in specializiran geografsko ali medijsko. To omogoča doseganje večjega občinstva zaradi preferenc starostnih skupin in medijske razpoložljivosti. V preteklosti je bila teroristična propaganda močno vezana na osrednje medijske sisteme zaradi širše nerazpoložljivosti internetnih kanalov. Takrat je bil osrednji

poudarek na časopisnih, radijskih in televizijskih medijih. S pojavom IKT se je njihov pomen zmanjšal, saj lahko posamezniki le z nekaj kliki dostopajo do vsebin kjerkoli in kadarkoli.

Delovanje terorizma se je zato v zadnjih 20 letih preusmerilo na globalni splet, saj omogoča hitrejše širjenje specializiranih informacij. Teroristične skupine so pričele z vzpostavljanjem spletnih forumov in klepetalnic, ki so bile dostopne tistim, ki so imeli geslo (Winter 2015, 11). Takšni forumi so omogočali širjenje propagandne in izobraževalne vsebine, vendar so predstavljali varnostno pomanjkljivost zaradi hekerskih aktivnosti. Nekdo, ki je znal obiti varnostne nastavitve, je lahko prosto dostopal do informacij, jih spreminjal ali brisal. Z naprednimi in sofisticiranimi napadi so javno dostopne spletne strani postale tarča obveščevalnih, hektivističnih in drugih organizacij. Napadi za zavrnitev storitev so onemogočali dostop do spletnih vsebin in nadaljevanje aktivnosti na terorističnih spletnih straneh.

S pojavom družbenih omrežij so takšne spletne strani in forumi postajali nepotrebni, saj se je večina uporabnikov preusmerila na družbena omrežja, ki so jim omogočala anonimno delovanje in komuniciranje s preostalimi somišljeniki. Možnost javnega ali zasebnega komuniciranja je omogočila delovanje terorističnih skupin v kibernetskem prostoru, saj so se informacije iz vseh področij teroristične organizacije znašle na enem mestu. Tako so teroristične skupine pričele uporabljati družbene medije za načrtovanje in koordiniranje akcij, razširjanje propagande in informativnih vsebin ter rekrutiranje novih kadrov in iskanje sponzorjev.

Vendar so tudi na družbenih omrežjih nastale prepreke za necenzurirano in anonimno delovanje. Administratorji in novi načini indeksiranja vsebin so pričeli z odstranjevanjem terorističnih skupin, posameznikov in vsebin, kar je prisililo kibernetske teroriste v iskanje novih načinov komuniciranja (Kensworthy 2016). Primer takšnih so družbena omrežja, ki temeljijo na izmenjavi podatkov skozi souporabnike ali soležnike (peer to peer) in ne skozi strežnike, kot se to dogaja tradicionalnih družbenih omrežjih. Takšni komunikacijski programi so Kik, Surespot in Telegram (Winter 2015, 11). Povezava, ki poteka skozi druge uporabnike, omogoča večjo anonimnost in varnost na internetu, v povezavi s šifriranjem in zaklepanjem kanalov pa omogoča izoblikovanje zasebnih komunikacijskih poti. Lastnik takšnih kanalov ima moč urejati, objavljati

in selekcionirati informacije, ki potujejo po komunikacijskih poteh in zagotavlja čimbolj optimalno propagandno dejavnost.

Fundacija Quilliam je ena od prvih organizacij, ki se ukvarja z preučevanjem skupin z ekstremno ideologijo. V svoji javno dostopni analizi *Documenting Virtual Caliphate* so analizirali propagandne vsebine Islamske države na internetu. Analizo propagande so opravili tematsko, prostorsko in na način prenosa, časovno obdobje pa je bilo od 17. julija do 15. avgusta 2015 (Winter 2015, 10).

Ugotovili so, da sta Twitter in Facebook najbolj razširjeni spletni strani, prek katerih se širi propaganda. Veliko število uporabnikov lahko hitro generira in prenaša vsebine, namenjene v propagandne namene. Število edinstvenih propagandnih sporočil, ki so bili poslani prek ključnih besed Twitterja, je bilo kar 1,146. To predstavlja dnevno 36 vsebin, ki se kopirajo in širijo naprej (Winter 2015, 12–13).

Tolikšno število vsebin pomeni dobro organiziranost razširjanja propagande po enem samem družbenem omrežju. Različni računi, ki so bili uporabljeni v te namene, so dnevno generirali novo vsebino in poročali iz posameznih geografskih lokacij. Quilliam je analiziral geografsko lokacijo dnevno generirane vsebine, kadar je bilo to mogoče. Največ objav je prišlo iz Sirije (301) in Iraka (380), sledila je severna Afrika (140). V Libiji in Egiptu je bilo ustvarjenih 56 vsebin, medtem ko so bile v Jemnu in Afganistanu ustvarjene 4. Alžirija, Savdska Arabija in zahodna Afrika pa so ustvarile vsaka po 2 vsebini (Winter 2015, 12).

Po formatu propagandne vsebine je bilo največ slikovnega gradiva, ki je predstavljalo 78 odstotkov celotne vsebine. Napisanih ali natipkanih propagandnih sporočil je bilo 11 odstotkov vsebine. Avdio in video gradivo pa sta predstavljali po 4 in 7 odstotkov (Winter 2015, 13).

Tematsko je Quilliam fundacija razporedila propagando v 6 različnih kategorij: utopijo, vojaško propagando, usmiljenje in pomoč, prikaz Islamske države in prebivalcev kot žrtve, kruto propagando in pripadnost. Največji delež je predstavljala utopija, ki je zajemala 52,57 odstotka (Winter 2015, 30–37). Sledila ji je vojaška propaganda, ki je zajemala 37,12 odstotka (Winter 2015, 24–29). Prikaz žrtev prebivalcev in Islamske države, ki so jih povzročile nasprotne sile, je

bilo 6,84 odstotkov (Winter 2015, 22–24). Kruta propaganda je predstavljala 2,13 odstotka vseh vsebin (Winter 2015, 21). Pripadnost Islamski državi in Islamu je predstavljalo 0,89 odstotka vsebin (Winter 2015, 19). Prikaz usmiljenosti borcev na bojišču in pomoči ogroženim skupinam pa je zajemal 0,45 odstotka vseh vsebin (Winter 2015, 8).

Analiza Quilliam fundacije je zelo nazorno razporedila propagandne vsebine in odstotek, ki ga zajemajo. Islamska država ohranja takšen način tematskega predstavljanja in informiranja, saj ji prinese največ koristi. Vendar je Islamska država v zadnjem letu spremenila način razširjanja propagande zaradi vse ostrejših omejitev za objavljanje takšne vsebine na družbenih omrežjih (Kenworthy 2016). Prestavili so se na druga družbena omrežja, kot je ruski VK, ki manj omejuje delovanje teh skupin (Lokot 2014). Uporabljajo tudi nove družbene aplikacije, ki delujejo na principu soležnikov, kot na primer aplikacija Telegram in Surespot ali aplikacije medijske agencije Amaq, ki so posebej oblikovane s strani pripadnikov Islamske države.

Telegram je aplikacija, ki za izboljšanje varnosti in anonimnosti uporabnikov ponuja komunikacijske poti, ki potekajo skozi več soležnikov. Dodatna možnost šifrirane povezave omogoča še večjo stopnjo zaščite, ki jo skušajo teroristične organizacije izpopolniti. Aplikacija Telegram omogoča vzpostavitev skupinskega komunikacijskega kanala, ki je zaščiten z geslom. Le administratorji skupine imajo možnost sprejemati nove uporabnike, s čemer še dodatno izboljšajo zaščito (Khayat 2015) . Prek teh skupin potuje slikovno, tekstovno in video gradivo, ki ga lahko v večini primerov umestimo v kategorijo propagande. Primeri kanalov, ki jih uporablja Islamska država v aplikaciji Telegram, so Elite Section Of IS (Khayat 2015), namenjen zagotavljanju informacijske varnosti pripadnikov in propagandiranja uspehov kibernetskih skupin, Online Dawah Operations (Russon in Murdock 2016), ki je namenjen za rekrutacijo, koordinacijo spletnega medijskega delovanja in prenosa propagande, Did you know? (Russon in Murdock 2016), namenjen reinterpretaciji zgodovine, saj objavlja popularne vsebine iz zahoda, ki jih poveže z ekstremno interpretacijo Islama in Islamske države, KhilafahNews (Russon in Murdock 2016), namenjen propagandiranju o uspehu vojske Islamske države, in Nashir ali Nasher, namenjen prenašanju vseh novic, povezanih z Islamsko državo (Khayat 2015).

Medijska agencija Amaq je množični medij, ki uporablja internet za razširjanje informacij in propagandnih vsebin (Asharq al-Awsat 2016). Pripadniki te organizacije so izoblikovali šifrirano aplikacijo za uporabo na računalnikih in pametnih telefonih android, predvsem z namenom lažjega in širšega doseganja občinstva, saj so večino njihovih internetnih komunikacijskih kanalov onemogočile kibernetske enote vlad ali haktivistične skupine. Aplikacija prenaša sporočila v štirih jezikih, kar še dodatno prikazuje prepoznavo pomembnosti širšega občinstva. Amaq prek svoje aplikacije pošilja vsebine v arabskem, angleškem, francoskem in ruskem jeziku (Katz 2016).

Pomembne strani za prenašanje propagande so tudi spletne strani in forumi, ki so bili ustvarjeni s tem namenom. Takšne spletne strani delujejo še danes (Priloga A). Primer takšne spletne strani na indeksiranem spletu je ansarukhilafah.wordpress.com. Ta spletna stran ponuja informacije, novice, propagandno vsebino in članke o kalifatu (Islamski državi) (AnsaruKhilafah 2016). Jezik spletne strani je angleški, kar omogoča dostopanje zahodnega in globalnega občinstva. V večini objavljenih člankov opazimo uporabo in navezovanje na Koran pri argumentaciji družbenih statusov, izvajanju osebnega džihada, politični ureditvi, zakonih in verovanju.

Vse večja pa je migracija spletnih strani terorističnih skupin na temen in globoki splet. Uporaba soležniških omrežij za zagotavljanje anonimnosti in ohranjanju nevidnosti spletnih mest na indeksiranem spletu omogoča Islamski državi uporabo povsem necenzuriranega, nereguliranega okolja in delovanja. Prek teh spletnih mest se razširjajo prej omenjene propagandne vsebine in uporabne informacije. Primer takšnih spletnih strani sta Khilafah in Issues of Islamic state (objave Islamske države) (Priloga D). Ti spletni strani delujeta kot osrednji spletni mesti za širjenje propagandnih vsebin, saj je na njunih strežnikih mogoče najti propagandne vsebine tudi izpred 3 let. Vsebine zajemajo tekstovno, glasovno, slikovno in video gradivo, ki je namenjeno zastraševanju nasprotnika in rekrutaciji novih kadrov.

Delovanje Islamske države in njenih kibernetskih enot pa je možno zaslediti tudi na spletnih mestih, ki so namenjeni svobodi govora, kot na primer Reddit in na neindeksiranem spletu 8chan. Moderatorji Reddita so pričeli v zadnjem letu vse bolj aktivno regulirati vsebine, ki so se na njem objavljale, zaradi spremembe politike pa so regulirali tudi podpoglavje Islamske države.

V tem delu je bilo objavljeno več propagandnih vsebin, kar so moderatorji opazili in popolnoma onemogočili dostop do teh podpoglavij (Reddit 2016) (Priloga B.1). 8chan (poznan tudi kot infinitechan) je skupnost, ki deluje na temnem oziroma globokem delu spleta. Namenjen je popolni svobodi govora in zelo redko prihaja do regulacije vsebin. Pod poglavjem religije in Islamske države se je izoblikovala skupnost, ki jo lahko pripišemo naprednim muslimanom, vendar znotraj skupnosti delujejo tudi ekstremne in džihadistične skupine. Z razširitvijo delovanja Islamske države v kibernetskem prostoru so pričeli ti posamezniki objavljati propagandne in kontaktne vsebine tudi v te podskupine. Tako je tam mogoče najti povezave na druge spletne strani Islamske države na temnem spletu in stopiti v kontakt z moderatorji, ki lahko pošljejo vabila za dostop do zasebnih kanalov Islamske države v aplikaciji Telegram (Priloga B.2).

Spletne teroristične dejavnosti so se delno preusmerile tudi v objavljanje propagandnih vsebin v obliki tiskanih ali spletnih revij, kot sta Dabiq in Kybernetiq. Islamska država je pričela z izdajanjem spletne revije Dabiq 5. julija 2014. Od leta 2014 do avgusta 2016 je bilo izdanih 15 številk spletne revije. Namen revije je prenašati propagandne in informacijske revije v zahodne države in tudi po arabskem svetu. Zato je revija Dabiq izdana v štirih jezikih: arabščini, angleščini, nemščini in francoščini. Ukvarja se s temami enotnosti, iskanja verske resnice, migracij, džihada in družbe, katere argumentira s pomočjo salafistične interpretacije Korana. Za vsako temo so napisani kvalitetni članki, tako v arabskem kot drugih jezikih, kar kaže na dobro organizacijo in znanje izdajatelja. Revija daje močan poudarek na vero in džihad ter prikazuje potrebo vsakega muslimana, da se pridruži Islamski državi (Clarion Project 2016). Kybernetiq za razliko Dabiq-a ni povezan z Islamsko državo, vendar velja za nemško džihadistično revijo, ki daje nasvete o informacijsko-komunikacijski tehnologiji. Nekateri avtorji so zaradi uporabe in razširjanja Kybernetiq-a na družbenih omrežjih pripisali povezave s hekerskimi terorističnimi skupinami, kot so Kalachnikov.TN, SCA in UCC ter posledično tudi z Islamsko državo. Prevedeni deli spletne revije so pogosto uporabljeni za dopolnjevanje islamističnih revij ali specializiranih revij, ki govorijo o informacijski varnosti Al Kaide in Islamske države (Paganini 2016).

Ogromno propagande generirajo tudi hekerske skupine, ki delujejo znotraj Islamske države. Te prevzemajo odgovornost za izvedene kibernetske napade prek svojih družbenih medijev in razobličenih spletnih mest ali ugrabljenih uporabniških računov (Priloga E). Na njih pustijo propagandno vsebino v obliki besedil, slik ali video gradiv, s katerimi izkazujejo moč Islamske države v kibernetskem prostoru in zmožnosti hekerskih skupin. Pomemben del propagande so tudi video in slikovna gradiva, ki jih skupine, kot so UCC, SCA in drugi, objavljajo prek svojih družbenih omrežij. V njih prikažejo moč, sposobnosti in uspehe skupin, obenem pa grozijo svojim nasprotnikom in nasprotnikom Islamske države, kot se je zgodilo v primeru SCA, ko so grozili ustanoviteljema Twitterja in Facebooka (Hamersma 2016).

4.3 Rekrutacija in izobraževanje

Rekrutacija novih borcev in mobilizacija sta pomembni za vse oborožene sile. Za Islamsko državo je to še veliko bolj bistveno, saj se srečuje z pomanjkanjem strokovnega in tehničnega kadra. Poleg pomanjkanja specializiranih kadrov pa potrebujejo nove borce za ohranjanje ali povečevanje števila pripadnikov, kar jim omogoča nadaljevanje vojaških in terorističnih akcij. Ker je Islamska država tarča dveh koalicij (rusko-sirske in zahodne), je pridobivanje novih pripadnikov še toliko bolj pomembno.

Islamska država svoj kader išče tudi izven okupiranega ozemlja. Tuji borci, ki delijo skupne vrednote in vero z Islamsko državo, so tako vabljeni, da pripomorejo k izoblikovanju kalifata in sodelujejo v oboroženih bojih. V Siriji in Iraku pridobijo znanje in izkušnje za izvajanje oboroženih in terorističnih akcij. Tuje borce se izučene in izkušene pošlje nazaj v matične države, kjer naj bi izvedli lastne teroristične napade in s tem pripomogli k širjenju kalifata (Engel 2015).

Nova oblika rekrutacije pa zajema rekrutacijo tujih borcev, ki so že od začetka usmerjeni v izvajanje terorističnih napadov. Islamska država poziva vse muslimane ekstremne ideologije, ki ne živijo v Siriji in Iraku, v izvajanje samotarskih terorističnih napadov v državah, iz katerih izvirajo (Engel 2015). Ob pozivih jim pomagajo tudi z informacijami, ki so potrebne za izvedbo napada. Te zajemajo sezname usmrtitev z osebnimi podatki, informacije in podatke o uporabi in

izgradnji orožij, eksplozivov in drugih sredstev za izvedbo napada ter motivacijsko podporo (Khayat 2015).

Proces radikalizacije posameznika, ki se odloči za izvedbo napadov, je izredno kompleksen in brez uporabe IKT ne bi bil mogoč. Kibernetski prostor omogoča anonimno delovanje, ki je nujno potrebno za takšne procese in predstavlja prvi stik posameznika z organizacijo. Poleg prvega stika z organizacijo pride v stik tudi s spletno skupnostjo somišljenikov, ki ga podpirajo, mu pomagajo in svetujejo ter z njim soorganizirajo napade.

Rekrutacija, ki jo izvaja Islamska država, poteka fizično na terenu in v kibernetskem prostoru. Rekrutacija, ki poteka prek interneta in vseh kanalov, ki jih Islamska država uporablja v kibernetskem prostoru, predstavlja največjo nevarnost za prebivalce zahodnih držav kot tudi drugih koalicij, ki se bojujejo proti Islamski državi. Novi kader Islamske države gre skozi procese radikalizacije na svetovnem spletu, kjer najde vse potrebne informacije za priključitev organizaciji in potovanje v Sirijo ali Irak. Tam je priključen oboroženim silam ali terorističnim skupinam, ki delujejo v imenu Islamske države. Tuji borci se po nekaj mesecih vrnejo iz Iraka in Sirije v matične države. Pridobljeno znanje in izkušnje iz Sirije lahko uporabijo za izvedbo terorističnih napadov v matičnih državah. Nova strategija rekrutacije obsega spletno radikalizacijo in pozive podpornikom po ostanku v matičnih državah, v njih pa načrtujejo in izvedejo teroristično napad ali podpirajo teroristično organizacijo.

Telegramovi kanali omogočajo širjenje vsebine, ki je nujno potrebna za doma radikalizirane pripadnike teroristične organizacije. Vsebine, ki so jim na voljo, obsegajo izdelave orožij in eksplozivov, ki so uporabljeni za takšne napade ter napotke, kako ohranjati informacijsko varnost. Primer takšnega kanala je Inspire Muslims, ki dnevno ponudi več različnih navodil za domačo izdelavo eksploziva in orožja (Russon in Murdock 2016).

Rekrutacija kibernetskih borcev Islamske države poteka s pomočjo vseh prej opisanih kanalov in predstavlja možnost iskanja novih kadrov, ki ne rabijo potovati na ozemlje Islamske države. Z možnostjo izvajanja kibernetskih napadov skozi kibernetski prostor to predstavlja novo grožnjo, ki izvira iz lokalnega okolja držav, vendar se države same tega le redko zavedajo.

Primeri rekrutacije kibernetskih teroristov se dogajajo skozi propagando (Kybernetiq), ki mobilizira posameznika, aplikacije (Telegram) in spletne klepetalnice (Khilafah), kjer stopi posameznik v kontakt s pripadniki kibernetskih skupin ter ima dostop do učbenikov za izvajanje kibernetskih napadov. Primer tega so Telegram kanali Kalachnikov.TN skupine (Russon in Murdock 2016), ki posreduje informacije in podatke o načinu izvedbe napadov, ter spletnih revij, kot je Kybernetiq, ki deluje kot izobraževalna revija za izvedbe takšnih napadov (Paganini 2016).

Izobraževanja in usposabljanja so zelo različna. Zaradi razširjenosti in nemogoče regulacije trga hekerskih orodij je dostop do teh zelo enostaven. Na indeksiranem spletu obstajajo hekerske skupine, ki ponujajo programe za izrabo ranljivosti sistema in tudi same informacijske sisteme, ki so uporabljeni za etično vdiranje. Poučevanje o njihovi uporabi poteka prek spletnih učbenikov ter video vsebin, ki so javno dostopne na portalih Youtube in specializiranih hekerskih portalih (Kalachnikov.TN 2016a). Na temnem spletu cveti trg hekerskih orodij in ponudnikov hekerskih dejavnosti, prek katerih lahko takšne skupine dostopajo do sofisticiranih orodij in znanj (Paganini 2015a).

4.4 Financiranje

Teroristične organizacije potrebujejo sredstva za delovanje. Konstantno iščejo nove načine pridobivanja finančnih in drugih sredstev, s čimer bi si zagotovili delovanje. Financiranje lahko poteka na tradicionalne načine, ki so kraje, trgovina z orožjem, drogami, umetninami in ljudmi, prodaja nafte in plina, izsiljevanje prebivalstva in gospodarskih družb, ugrabljanje ljudi za odkupnino in donacije (FATF 2015, 12–23; Shatz 2014).

Novi načini financiranja skozi kibernetski prostor pa zajemajo še crowdfunding (kampanja za zbiranje denarja) in spletne donacije prek paysafe-a, paypal-a, internetnih bančnih nakazil, predplačniških kreditnih kartic (FATF 2015, 24–25) in kripto valute Bitcoin (Flashpoint 2015).

Crowdfunding je bil najbolj razširjen pred letom 2013, saj je takrat teroristična organizacija šele pridobila na prepoznavnosti. Uporabniški računi na družbenih omrežjih Twitter in Facebook so zbirali denar z nakazili podpornikov. Računi, na katere so nakazovali denar, so bili ustvarjeni v

Iraku ali Siriji, kamor so se sredstva tudi stekala. Vendar so bili tudi primeri, kjer so posamezniki uporabljali podobno metodo v zahodnih državah. Obstaja primer iz ZDA, ko je eden od podpornikov Islamske države na družbenih omrežjih zbiral denar in prosil za nakazila do vrednosti 5,000 dolarjev. Svoja dejanja je utemeljeval s pomočjo Korana, saj je argumentiral finančno podporo kot del džihada (FATF 2015, 24–25).

Novi načini preprečevanja financiranja terorističnih organizacij so takšna dejanja preprečili in prisilili podpornike v iskanje novih načinov financiranja. Primer tega so predplačniške kartice Paysafe ter spletnega računa Paypal. Prek teh lahko posamezniki prek komunikacijskih kanalov prenesejo vse za izvršitev transakcije potrebne informacije (FATF 2015, 24–25).

Najnovejši in najbolj anonimen način financiranja pa je s kripto valuto Bitcoin. Podporniki so si ustvarili spletne denarnice za kripto valuto, pripadniki Islamske države in kibernetskih enot pa objavljajo naslove za prenos Bitcoinov na svojih družbenih medijev ali v posebej oblikovanih spletnih straneh na indeksiranem in temnem oziroma globokem spletu. Primer za financiranje z Bitcoini sta spletni strani na neindeksiranem spletu oz3vngabfrasvf3i.onion in mmgkmmtzleydpc4x.onion (priloga C).

5 Sklep

Islamska država je pokazala sposobnosti prilagoditve pri izvajanju svojega ofenzivnega in defenzivnega delovanja z izoblikovanjem kibernetskih propagandnih in hekerskih struktur. Njene vsakodnevne aktivnosti v kibernetskem prostoru obsegajo širok spekter nalog, ki jih teroristična organizacija mora izvajati za ohranjanje svoje moči in vpliva na ljudstvo.

Potencial kibernetskega terorizma je izredno visok, vendar tudi tehnično zahteven. Potrebe po znanju in sredstvih so v primerjavi s tradicionalnimi napadi veliko bolj zahtevne. Po definiciji kibernetskega terorizma lahko kibernetske skupine Islamske države umestimo v to kategorijo. Kibernetske skupine uporabljajo IKT za izvajanje svojih napadov na cilje, ki so strateško pomembni. Seveda vsi cilji skupin nimajo takšne pomembnosti, ampak predstavljajo raznolikost tarč in slabo informacijsko varnost. Spletna mesta, ki niso pomembna, postanejo propagandna vsebina, usmerjena proti nasprotnikom Islamske države, pri čemer se jim pomembnost nekoliko poviša. Napadi na spletna mesta in informacijsko infrastrukturo povzročajo medijsko prepoznavnost skupin, ob tem pa med uporabniki spleta povzročajo strah in paniko. Toliko bolj pomemben del pri povzročanju strahu predstavljajo objavljeni seznami za uboje, ki ciljajo na točno določenega posameznika. Strah pred tradicionalnim napadom na te posameznike je še toliko večji ob uporabi propagandnih dejavnosti, ki pozivajo napade volkov samotarjev. Zaradi uspehov kibernetskih teroristov Islamske države sem tako lahko potrdil mojo prvo hipotezo, ki je predpostavljala, da ima Islamska država sposobnosti izvajanja kibernetskih napadov.

Vendar je sofistikacija napadov kljub dosegom v kibernetskem prostoru še vedno močno omejena. Po uporabi kriterija, ki ga je postavil Center za preučevanje terorizma in iregularnega vojskovanja na Mornariški podiplomski šoli v Montereyu iz Kalifornije, lahko definiramo sofisticiranost kibernetskih skupin po združitvi v UCC kot napredno strukturiranega. Uspešnost v izvedbi napadov na več računalniških sistemov in omrežij je pokazala sposobnosti skupin. Čeprav ni jasnih dokazov o sposobnostih programiranja novih ali specializiranih orodij za pridobivanje dostopa do strežnikov in računalnikov, pa lahko predpostavljamo, da so določeni programi spremenjeni za učinkovitejše pridobivanje dostopa. Sposobnosti analize so bile prikazane z bolj sofisticiranimi napadi na strežnike ameriških, britanskih, avstralskih in drugih

državnih organov, pri čemer so pridobili dostop do osebnih podatkov. Učne sposobnosti skupine so močno narasle z združitvijo v UCC, saj so se določene hekerske skupine (Kalachnikov.TN) usmerile v izobraževanje novih kadrov in širjenje znanj po spletu. S tem, ko sem apliciral analizo na kriterij sofistikacije kibernetskih teroristov, sem lahko potrdil hipotezo, ki je govorila, da ima Islamska država oziroma njene kibernetske skupine sposobnosti napredno strukturirane kibernetske teroristične organizacije.

Vendar kibernetski terorizem ne obsega le kibernetskih napadov. Obsega tudi uporabo informacijsko-komunikacijske tehnologije v bolj tradicionalne namene. Po definiciji Cohena lahko kibernetski teroristi izvajajo tudi spletno dejavnost na področju načrtovanja, koordiniranja, financiranja, izvajanja političnih akcij, rekrutacije, prenašanja propagande in prikazovanja moči (Cohen 2002). V diplomski nalogi sem se usmeril predvsem v raziskavo kibernetskih napadov, propagande, rekrutacije in financiranja. Podatki o skupnem načrtovanju in koordinaciji pripadnikov Islamske držav niso javno objavljeni na spletu, saj se izvajajo znotraj šifriranih soležniških aplikacij, do katerih je dostop omejen. Politične akcije so zelo redko predstavljene na spletu ali pa so predstavljene v propagandni vsebini.

V analizi kibernetskega terorizma sem združil področji delovanja propagande in prikazovanja moči, saj se močno navezujeta ena na drugo. Kljub temu, da sta propaganda in prikaz moči del psihološkega bojevanja, sem ga umestil v kibernetski terorizem zaradi Cohenove definicije (Cohen 2002) in zaradi uporabe IKT za razširjanje takšnih vsebin. Mehanizem Islamske države je konstantno aktiven in predstavlja eno od osrednjih dejavnosti organizacije in kibernetskih terorističnih podskupin. Razširjanje propagande je zaradi razumevanja pomembnosti eno od primarnih orožij Islamske države na svetovnem spletu. Zaradi velike količine dnevno generiranih vsebin in široke mreže za njihovo distribucijo jo lahko umestimo v primarno funkcijo kibernetskega terorizma. S tem sem tudi potrdil hipotezo, ki sem si jo zastavil v metodološkem okvirju, saj je propaganda lahko samostojna, lahko pa je tudi uporabljena v primeru kibernetičnih napadov za razobličenja, kjer se pusti propagandno vsebino na razobličenem spletnem mestu.

Propaganda in prikaz moči sta usmerjeni proti vsem nasprotnikom Islamske države z namenom zastraševanja, povzročanja panike in prisiljevanja vlad v spremembo politik. Obenem predstavlja

propagandna dejavnost enega od najboljših načinov za prikazovanje sposobnosti kibernetskih teroristov za prevzemanje napadov in pozivanje k izvajanju tradicionalnih napadov. Tukaj so izrednega pomena seznami za uboje, ki so jih kibernetske teroristične skupine Islamske države objavljale z namenom prikazovanja sposobnosti, povzročanja strahu, panike in obenem kot poziv doma radikaliziranih pripadnikov v izvedbo tradicionalnih napadov.

Izoblikovana mreža informacijsko-komunikacijskih programov, aplikacij in spletnih strani močno izboljšuje razširjanje zgoraj omenjenih propagandnih vsebin. Te vsebine so prenašane prek družbenih omrežij, primarno Twitter in Facebook, spletnih revij, kot Dabiq in Kybernetiq, spletnih strani na indeksiranem spletu, kot AlHayat medijski center in AnsaruKhilafah, spletnih strani na neindeksiranem spletu, kot Khilafah in Objave Islamske države, specializiranih soležniških aplikacij, kot Telegram, ter aplikacij za informiranje, katerih avtor je Islamska država (Amaq aplikacija).

Vse zgoraj opisane spletne strani, družbena omrežja in druge aplikacije omogočajo tudi rekrutiranje posameznikov za Islamsko državo ali njene kibernetske skupine. Posameznik lahko stopi v stik z teroristično organizacijo s pomočjo skoraj vseh zgoraj naštetih aplikacij. Pomembnost aplikacije Telegrama je na tej točki najvišja, saj omogoča neposreden kontakt z rekruterji in financerji Islamske države, ki ljudem omogočajo potovanje v Sirijo ali Irak, omogoča pa tudi kontakt s strokovnjaki na področju uporabe orožij in ustvarjanja eksplozivov za izvedbo tradicionalnega napada.

Za Islamsko državo je njeno lastno financiranje izrednega pomena. Vendar je po podatkih Flashpointa (Flashpoint 2015) financiranje prek interneta in drugih računalniških sistemov ena od metod, ki prinese terористični organizaciji najmanj sredstev. Ne glede na to skušajo kibernetske skupine vzpostavljati in ohranjati spletna mesta, prek katerih lahko posamezniki in druge organizacije financirajo aktivnosti. Najbolj pomembna v tem primeru je kripto valuta Bitcoin, ki omogoča posameznikom nakazila v Bitcoinih, obenem pa jim pri tem omogoči anonimnost.

Raziskovanje kibernetskega terorizma in kriminala na spletu je izredno težavno. Veliko število akterjev in njihovo poimenovanje otežuje samo zbiranje podatkov ter daje izgled večje strukturiranosti skupin. Poleg tega je na spletu veliko število zlonamernih programov in spletnih strani, ki niso povezane z iskalnim vnosom in spletne strani, ki so namenjene zbiranju informacij o uporabnikih spleta (tudi poznani kot honeypot ali honeytrap), ki se povežejo na njo, zato je pri raziskovanju teh tem pomembno še dodatno izboljšati računalniške in informacijske varnostne ukrepe. Ob iskanju informacij o kibernetskih skupinah Islamske države sem naletel na takšno stran (justpaste.it/photo1z ali justpaste.it/u7b9), ki je zabeležila moj spletni naslov in ga posredovala neznani hekerski skupini. Napad, ki ga je skupina izvedla, je onemogočila moj dostop do spleta, saj so najverjetneje z uporabo botneta (okuženega računalniškega omrežja) konstantno pošiljali zahteve za povezavo, s čimer so onemogočili dohodno povezavo z iskanih strežnikov spletnih strani zaradi preobremenjenosti povezave. V nekaj dnevih se je ta napad končal, ponovno sem dobil dostop do spleta, hitrost internetne povezave pa se je stabilizirala.

6 Zaključek

Kibernetski terorizem je s pojavom Islamske države pridobil veliko večji pomen, kot ga je imel v preteklosti. Najverjetneje se bodo v prihodnosti kibernetske sposobnosti zaradi prepletenosti s preostalimi deli Islamske države še dodatno izboljšale. Nove oblike delovanja Islamske države kot teroristične organizacije bodo v prihodnosti pa vsej verjetnosti povzročile trend spreminjanja terorističnih organizacij v organizacije z vse večjo prisotnostjo na svetovnem spletu in v kibernetskem prostoru. Nastajajoče specializirane teroristične skupine in čiste kibernetske teroristične organizacije bodo lahko zaradi vse večje prepletenosti vsakdana z IKT izvajale svoje napade v kibernetskem prostoru na veliko večji stopnji, kot jih je dosegala Islamska država, in samo vprašanje časa je, kdaj se bodo pojavile prve takšne skupine.

Evolucija kibernetskih terorističnih organizacij in informacijskega bojevanja nasploh je in še bo povzročila potrebo po prestrukturiranju državnih in zasebnih organizacij za namene izboljševanja informacijske varnosti. Sposobnosti obveščevalnih služb in zasebnih podjetij se morajo dodatno izboljšati na področju zagotavljanja proaktivne varnosti in obrambe pred kibernetskimi teroristi ter njihovimi napadi in izoblikovati sisteme, ki bodo hitro zaznali takšne aktivnosti in onemogočili nadaljnjo delovanje. Novi sistemi morajo biti odporni in proaktivni, vendar morajo še vedno ohranjati spoštovanje do človekovih pravic in svoboščin.

Slovenija, ki se usmerja v hitrejši razvoj informacijsko-komunikacijske tehnologije s strategijo Digitalne Slovenije 2020, se mora močno zavedati ogroženosti kibernetskih sistemov in sposobnosti držav ter drugih organizacij na področju informacijskega bojevanja, še toliko bolj pa se mora zavedati groženj kibernetskih terorističnih organizacij, kot je Islamska država, saj lahko z razširitvijo svojih dejavnosti proti zaveznikom ZDA in zaveznikom drugih evropskih velesil ogroža tudi Slovenijo.

7. Literatura

1. AlHayat Media Center. Dostopno prek: Alhayatmedia.wordpress.com/flames-of-war/ (18. avgust 2016).
2. Alkhouri, Laith, Alex Kassirer in Allison Nixon. 2016. *Hacking for ISIS: The Emergent Cyber Threat Landscape*. Dostopno prek: https://www.flashpoint-intel.com/home/assets/Media/Flashpoint_HackingForISIS_April2016.pdf (15 . avgust 2016).
3. AnsaruKhilafah. 2016. *Everything about the Islamic State*. Dostopno prek: https://ansarukhilafah.wordpress.com (15. avgust 2016).
4. Asharq al-Awsat. 2016. *Amaq – 24/7 News Agency Run by ISIS*. Dostopno prek: http://english.aawsat.com/2016/03/article55348927/amaq-247-news-agency-run-isis (15. avgust 2016).
5. Baldi, Stefano, Eduardo Gelbstein in Jovan Kurbalija. 2003. *Hacktivism, Cyberterrorism and Cyberwar. The Activities of the Uncivil Society in Cyberspace*. Malta: DiploFoundation. Dostopno prek: http://baldi.diplomacy.edu/italy/isl/Hacktivism.pdf (20. avgust 2016).
6. Ballard, James David, Hornik, Joseph G. in Douglas Mckenzie. 2004. Technological facilitation of terrorism. V *Cyberterrorism*, ur. Alan O'Day, 39-66. Aldershot: Ashgate Publishing.
7. BBC. 2015. *What is 'Islamic State'?* 2. december. Dostopno prek: http://www.bbc.com/news/world-middle-east-29052144 (15. avgust 2016).
8. Bernik, Igor in Kaja Prislan. 2012. *Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem*. Ljubljana: Fakulteta za varnostne vede.
9. Chaliand Gerard. 2007. *The History of Terrorism: From Antiquity to al Qaeda*. Berkely: University of California Press.
10. Cohen, Fred. 2002. *Terrorism and Cyberspace*. Dostopno prek: http://all.net/Analyst/netsec/2002-05.html (15. avgust 2016).
11. Council of the European Union. 2002. *Council Framework Decision on Combating Terrorism, Art. 1. 2002*. Dostopno prek: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33168 (15. avgust 2016).

12. Engel, Pamela. 2015. *ISIS has mastered a crucial recruiting tactic no terrorist group has ever conquered*. Dostopno prek: http://www.businessinsider.com/isis-is-revolutionizing-international-terrorism-2015-5 (15. avgust 2016).
13. Financial Action Task Force. 2015. *Financing of the Terrorist Organisation Islamic State in Syria and Iraq (ISIL)*. Dostopno prek: http://www.fatf-gafi.org/documents/documents/financing-of-terrorist-organisation-isil.html (15. avgust 2016).
14. Flashpoint. 2015. *Bankrolling Terror: The Funding and Financing of ISIS*. Dostopno prek: https://www.flashpoint-intel.com/news/bankrolling-terror-the-funding-and-finance-of-isis/ (15. avgust 2016).
15. Gordon, Sarah in Richard Ford. 2003. *Cyberterrorism?* Dostopno prek: https://www.symantec.com/avcenter/reference/cyberterrorism.pdf (15. avgust 2016).
16. Hamersma, Grant. 2016. *ISIS's Raging Terror Spreads Over Facebook and Twitter*. Dostopno prek: http://www.lighthousenewsdaily.com/tag/sons-of-the-caliphate-army/ (15. avgust 2016).
17. Hashim, Ahmed S. 2014. *The Islamic State: From al-Qaeda Affiliate to Caliphate*. Dostopno prek: http://www.mepc.org/journal/middle-east-policy-archives/islamic-state-al-qaeda-affiliate-caliphate?print (15. avgust 2016).
18. Infinite Chan. Dostopno prek: 8ch.net/search/islamic-state/ (15. avgust 2016).
19. Islamic State. Dostopno prek: oz3vngabfrasvf3i.onion (15. avgust 2016).
20. Islamic State. Dostopno prek: mmgkmmtzleydpc4x.onion (15. avgust 2016).
21. Issues of Islamic State. Dostopno prek: http://isdratetp4donyfy.onion/ (18. avgust 2016).
22. Jihad Intel. 2016. *Database: Identifiers of Designated Islamic Terrorist Organization: Islamic State*. Dostopno prek: http://jihadintel.meforum.org/group/52/islamic-state-iraq-levant (15. avgust 2016).
23. *Kalachnikov.TN*. Dostopno prek: https://kalachnikovtn.wordpress.com/ (15. avgust 2016)
24. --- 2016a. *Tunisian Cracker Videos*. Dostopno prek: http://resolvedqs.com/tube/bu31ddXJ_vE/%D8%AF%D9%88%D8%B1%D8%A9-%D8%A5%D8%AE%D8%AA%D8%B1%D8%A7%D9%82-%D8%A7%D9%84%D9%85%D9%88%D8%A7%D9%82%D8%B9-

%D8%A7%D9%84%D8%AF%D8%B1%D8%B3-%D8%A7%D9%84%D8%A3%D9%88%D9%84-tunisian-cracker (18. avgust 2016).

25. --- 2016b. Dostopno prek: https://www.facebook.com/Countre.stricke (15. avgust 2016).
26. --- 2016c. Dostopno prek: amicofuoco.info/fuoco/ (18. avgust 2016).
27. --- 2016č. Dostopno prek: dms.foods.com (18. avgust 2016).
28. Katz, Rita. 2016. *ISIS's Mobile App Developers Are in Crisis Mode*. Dostopno prek: http://motherboard.vice.com/read/isis-mobile-app-developers-are-in-crisis-mode (15. avgust 2016).
29. Kenworthy, Josh. 2016. *How Twitter became a key player in the fight against ISIS*. Dostopno prek: http://www.csmonitor.com/Technology/2016/0819/How-Twitter-became-a-key-player-in-the-fight-against-ISIS (15. avgust 2016).
30. Khayat, M. 2015. *Jihadis Shift To Using Secure Communication App Telegram's Channel Service*. Dostopno prek: http://www.memrijttm.org/jihadis-shift-to-using-secure-communication-app-telegrams-channels-service.html (15. avgust 2016).
31. Khilafah. 2016. Dostopno prek: zyxfxaoguykt63nz.onion/ (18. avgust 2016).
32. *Kybernetiq*. 2015. Dostopno prek: https://ia800206.us.archive.org/0/items/kybernetiq_magazin/kybernetiq_001.pdf (15. avgust 2016).
33. Lokot, Tetyana. 2014. *The ISIS internet army has found a safe haven on Russian social network – for now*. Dostopno prek: http://www.pri.org/stories/2014-09-12/isis-internet-army-has-found-safe-haven-russian-social-networks-now (15. avgust 2016).
34. Malešič, Marjan. 1994. *Civilna obramba sodobnih držav*. Doktorska dizertacija. Ljubljana: Fakulteta za družbene vede.
35. Mccormic, Ty. 2014. *Al Qaeda Core: A short History*. Dostopno prek: http://foreignpolicy.com/2014/03/17/al-qaeda-core-a-short-history/ (15. avgust 2016).
36. MEMRI. 2016a. *Pro-ISIS Hacking Group 'Caliphate Cyber United' Leaks List Of Allegedly Prominent NYC Citizens*. Dostopno prek: http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/pro-isis-hacking-group-caliphate-cyber-united-leaks-list-of-allegedly-prominent-nyc-citizens/ (15. avgust 2016).

37. --- 2016b. *Pro-ISIS Hacking Group 'United Cyber Caliphate' Releases Personal Details Of U.S. State Department Employees.* Dostopno prek: http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/pro-isis-hacking-group-united-cyber-caliphate-releases-personal-details-of-u-s-state-department-employees/ (15. avgust 2016).
38. --- 2016c. *United Cyber Caliphate Hacks Vancouver Florist.* Dostopno prek: http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/united-cyber-caliphate-hacks-vancouver-florist/ (15. avgust 2016).
39. --- 2016č. *United Cyber Caliphate Posts On Telegram Announcement Of Hack Of 'Arkansas Library Database'.* Dostopno prek: http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/united-cyber-caliphate-posts-on-telegram-announcement-of-hack-of-arkansas-library-database/ (15. avgust 2016).
40. --- 2016d. *Pro-ISIS Hacking Group On Telegram Releases Kill List Featuring U.S. State Department Employees.* Dostopno prek: http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/pro-isis-hacking-group-on-telegram-releases-kill-list-featuring-u-s-state-department-employees/ (15. avgust 2016).
41. --- 2016e. *Pro-ISIS Hacking Group 'United Cyber Caliphate' Targets Australian Websites*. Dostopno prek: http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/memri-jttm-pro-isis-hacking-group-united-cyber-caliphate-targets-australian-websites/ (15. avgust 2016).
42. --- 2016f. *Pro-ISIS Hacking Group Releases Kill Lists Of U.S. Gov't Employees In Chicago, MI, MA, RI, Russia– And Images of U.S., Russian Military Bases.* Dostopno prek: http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/pro-isis-hacking-group-releases-kill-lists-of-u-s-govt-employees-in-chicago-mi-ma-ri-russia-and-images-of-u-s-russian-military-bases/ (15. avgust 2016).
43. --- 2016g. *Pro-ISIS Hacking Group Releases Kill List Of 289 U.S. Army Corps Of Engineers Personnel.* Dostopno prek: http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/pro-isis-hacking-group-releases-kill-list-of-289-u-s-army-corps-of-engineers-personnel/ (15. avgust 2016).
44. --- 2016h. *Pro-ISIS Hacking Group Releases Kill List With 2,461 NYC Residents' Personal Details.* Dostopno prek: http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-

activity/pro-isis-hacking-group-releases-kill-list-with-2461-nyc-residents-personal-details/ (15. avgust 2016).

45. --- 2016i. *Pro-ISIS Hacking Group Releases Kill List Of Over 700 U.S. Army Personnel.* Dostopno prek: http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/pro-isis-hacking-group-releases-kill-list-of-over-700-u-s-army-personnel/ (15. avgust 2016).
46. --- 2016j. *Pro-ISIS Hacking Group Release Kill List Featuring U.S. Air Force Personnel.* Dostopno prek: http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/pro-isis-hacking-group-release-kill-list-featuring-u-s-air-force-personnel/ (15. avgust 2016).
47. --- 2016k. *On Telegram, Caliphate Cyber Army Posts Content It Says Is From Democratic National Committee's Servers.* Dostopno prek: http://cjlab.memri.org/lab-projects/tracking-jihadi-terrorist-use-of-social-media/on-telegram-caliphate-cyber-army-posts-content-it-says-is-from-democratic-national-committees-servers/ (15. avgust 2016).
48. --- 2016l. *Kalachnikv E-Security Team Participates In #OpSaudiArabia.* Dostopno prek: http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/kalachnikv-e-security-team-participates-in-opsaudiarabia/ (15. avgust 2016).
49. Ministrstvo za izobraževanje, znanost in šport Republike Slovenije (MIZŠ). 2016. *Digitalna Slovenija 2020*. Dostopno prek: http://www.mizs.gov.si/si/delovna_podrocja/direktorat_za_informacijsko_druzbo/digitalna_slovenija_2020/ (15. avgust 2016).
50. Mirror. 2016. *Pro-ISIS hackers 'Caliphate Cyber Army' release video revealing partnership of evil with cyber terrorists AnonGhost*. Dostopno prek: http://www.mirror.co.uk/news/world-news/pro-isis-hackers-caliphate-cyber-7163124 (15. avgust 2016).
51. NATO. 2014. *Glossary of Terms and Definitions*. Dostopno prek: nso.nato.int/nso/zPublic/ap/aap6/AAP-6.pdf (18. avgust 2016).
52. Nelson, Bill, Rodney Choi, Michael Iacobucci, Mark Mitchell in Greg Gagnon. 1999. *Cyberterror – Prospects and Implications*. Dostopno prek: http://www.au.af.mil/au/awc/awcgate/nps/cyberterror_prospects.pdf (15. avgust 2016).
53. Olmstead, Summer in Siraj Ambareen. 2009. *Cyberterrorism: The Threat of Virtual Warfare*. Dostopno prek:

http://static1.1.sqspcdn.com/static/f/702523/9188710/1288393976577/200911-Olmstead.pdf?token=AM2NEe0lnc3PKun3tccZxM0VHtg%3D (15. avgust 2016).

54. Paganini, Pierluigi. 2015a. *Hacking Communities in the Deep Web*. Dostopno prek: http://resources.infosecinstitute.com/hacking-communities-in-the-deep-web/ (15. avgust 2016).
55. --- 2015b. *FireEye speculates that behind the hack of France's TV5Monde television channel there is the popular APT28 that used the pseudonymous ISIS Cyber Caliphate*. Dostopno prek: http://securityaffairs.co/wordpress/37710/hacking/apt28-hacked-tv5monde.html (15. avgust 2016)
56. --- 2016. *The Islamic State launches a new cyber war magazine for jihadists titled Kybernetiq that instructs militants about technology*. Dostopno prek: http://securityaffairs.co/wordpress/43435/hacking/kybernetiq-magazine-cyber-jihad.html (15. avgust 2016).
57. Prezelj, Iztok in Uroš Svete. 2015. Kritična Infrastruktura in IKT. V *Vitel*, ur. Mlinar Tomi, 8-12. Ljubljana: Slovensko društvo za elektronske komunikacije. Dostopno prek: http://www.drustvo-sikom.si/wp-content/uploads/2015/12/Zbornik_31.VITEL_2015.pdf (15. avgust 2016).
58. Prezelj, Iztok. 2006. Teroristično ogrožanje nacionalne varnosti Republike Slovenije. *Ujma* 20: 177-181. Dostopno prek: http://www.sos112.si/slo/tdocs/ujma/2006/prezelj.pdf (15. avgust 2016).
59. Reddit. 2016. *Islamic State search (NSFW)*. Dostopno prek: https://www.reddit.com/r/search?q=islamic+state (15. avgust 2016).
60. Russon, Mary-Ann in Jason Murdock. 2016. Welcome to the bizzare and frightening world of Islamic State channels on Telegram. *International Business Times*, 23. maj. Dostopno prek: http://www.ibtimes.co.uk/welcome-bizarre-frightening-world-islamic-state-channels-telegram-1561186 (15. avgust 2016).
61. Shatz, Howard J. 2014. *How ISIS Funds its Reign of Terror*. Dostopno prek: http://www.rand.org/blog/2014/09/how-isis-funds-its-reign-of-terror.html (15. avgust 2016).
62. SITE. 2016. *SITE Intelligence group Analyzes Kill Lists by PRO-IS Hacking Groups in New Report*. Dostopno prek: https://ent.siteintelgroup.com/Dark-Web-and-Cyber-Security/site-

intelligence-group-analyzes-kill-lists-by-pro-is-hacking-groups-in-new-report.html (15. avgust 2016).

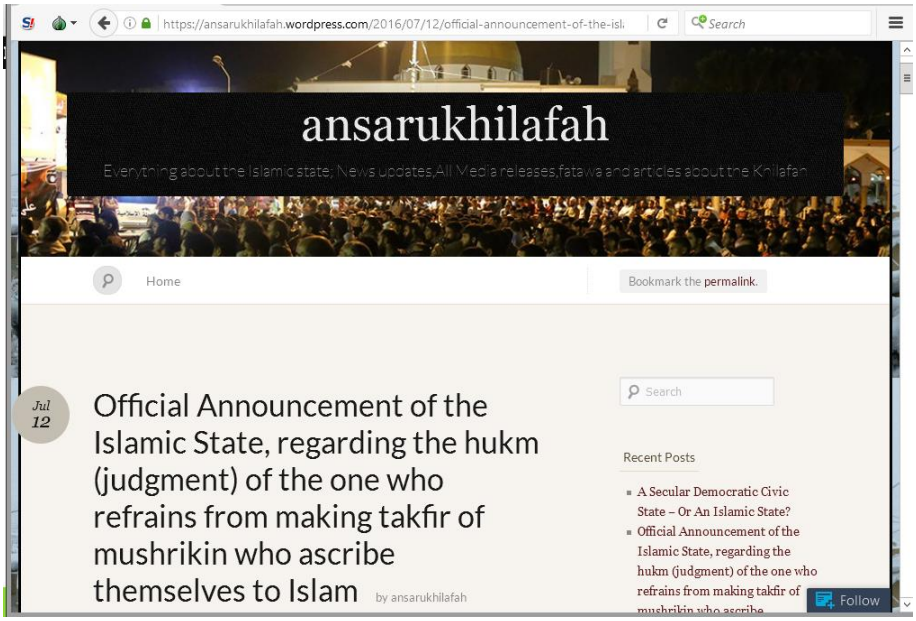
63. Svete, Uroš. 2005. *Varnost v infromacijski družbi*. Ljubljana: Fakulteta za družbene vede.
64. Terrorism Research and Analysis Consortium. 2016. *AnonGhost*. Dostopno prek: http://www.trackingterrorism.org/group/anonghost (15. avgust 2016).
65. The Clarion Project. 2016. *The Islamic State's (ISIS, ISIL) Magazine*. Dostopno prek: http://www.clarionproject.org/news/islamic-state-isis-isil-propaganda-magazine-dabiq (15. avgust 2016).
66. Tomkiw, Lydia. 2016. List of Recent ISIS Attacks: Islamic State group Hits Targets from Belgium to Syria in 2016. *International Business Time,* 29. junij. Dostopno prek: http://www.ibtimes.com/list-recent-isis-attacks-islamic-state-group-hits-targets-belgium-syria-2016-2388059 (15. avgust 2016).
67. Udupa, Sahana. 2009. *Mediatised Terror: Terror in age of Media Explosion*. Economic and Political Weekly (44). Dostopno prek: http://www.epw.in/journal/2009/09/commentary/mediatised-terror-terror-age-media-explosion.html (15. avgust. 2016).
68. United Cyber Caliphate. Dostopno prek: Twitter.com/Saaitama (29. julij 2016).
69. Veerasamy, Namosha. 2010. *Motivation for Cyberterrorism*. Dostopno prek: http://researchspace.csir.co.za/dspace/bitstream/10204/4337/1/Veerasamy_2010.pdf (15. avgust 2016).
70. Winter, Charlie. 2015. *Documenting the Virtual Caliphate*. Dostopno prek: http://www.quilliamfoundation.org/press/documenting-the-virtual-caliphate/ (15. avgust 2016).

Priloga A: Primer propagandnih spletnih strani Islamske države

Slika A.1: AlHayat Media Center.

(AlHayat 2016).

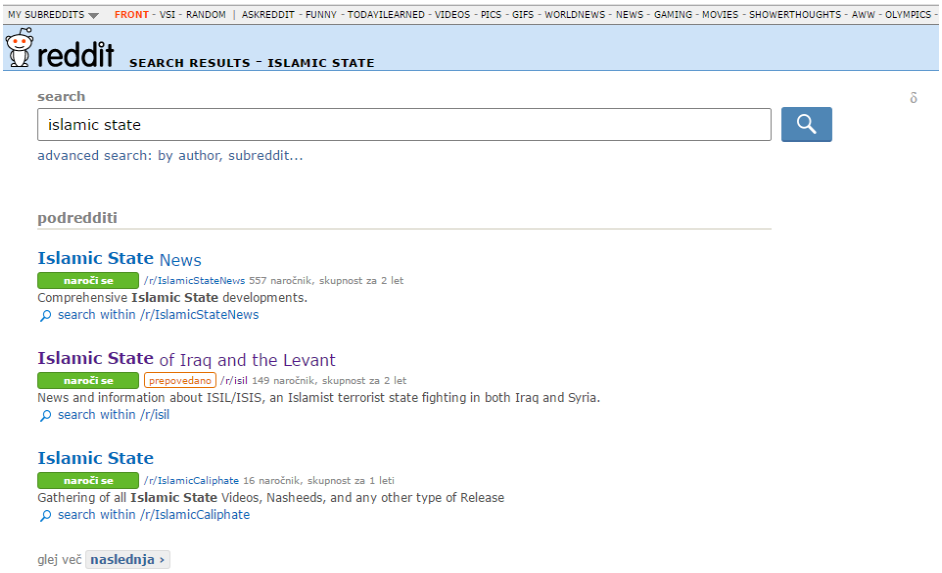
Slika A.2: Ansarukhilafah



(Ansarukhilafah 2016).

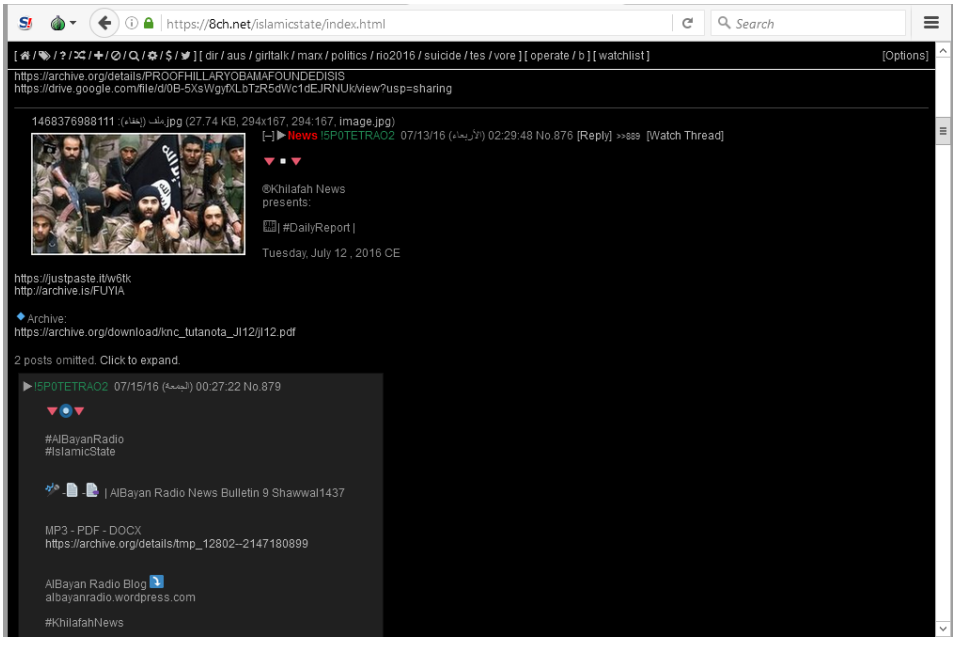
Priloga B: Portali za svobodo govora in Islamska država

Slika B.1: Reddit Islamic State



(Reddit 2016).

Slika B.2: 8chan Islamic state



(Infinite Chan 2016).

Priloga C: Financiranje Islamske države z Bitcoini

Slika C.1: Financiranje z Bitcoini.

(Islamic State 2016a).

Slika C.2: Financiranje z Bitcoini.

(Islamic state 2016b).

Priloga Č: Primeri razobličenih spletnih strani

Slika Č.1: Razobličena spletna stran.

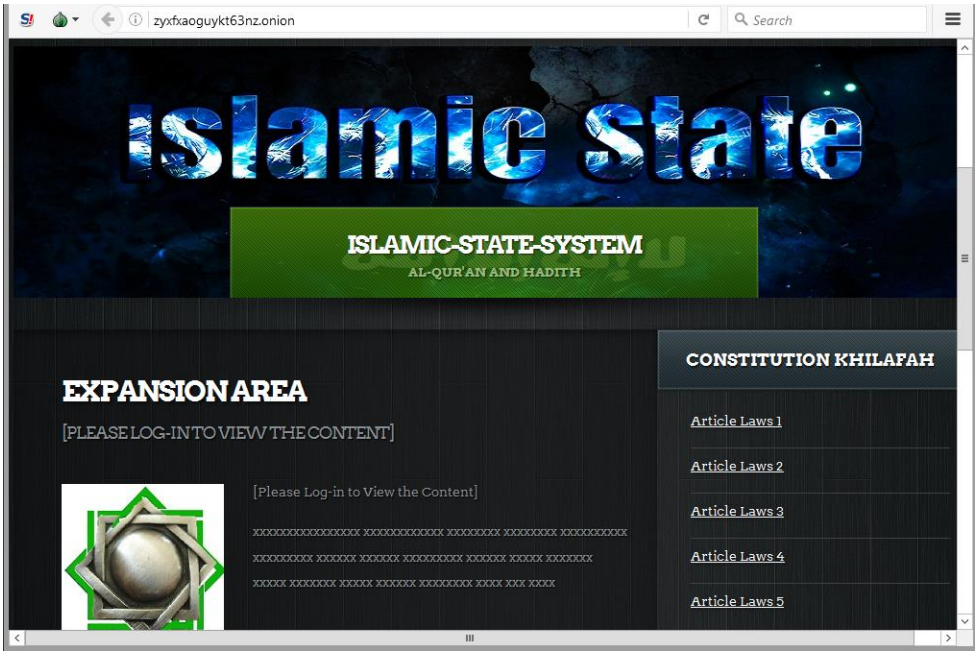
(Kalachnikov.TN 2016c).

Slika Č.2: Razobličena spletna stran s propagandno.

(Kalachnikov.TN 2016č).

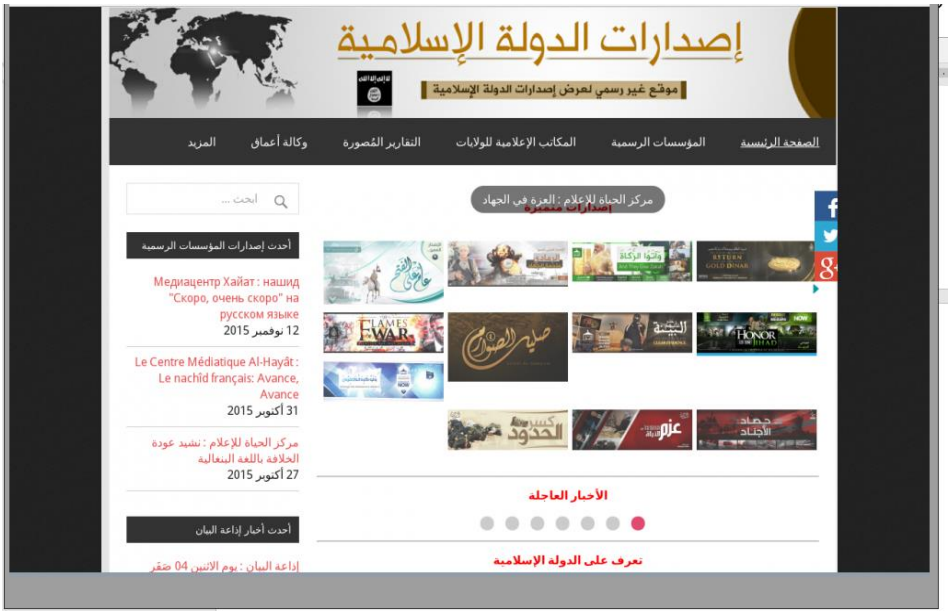
Priloga D: Propaganda Islamske države na temnem in globokem spletu

Slika D.1: Spletna stran Khilafah.



(Khilafah 2016).

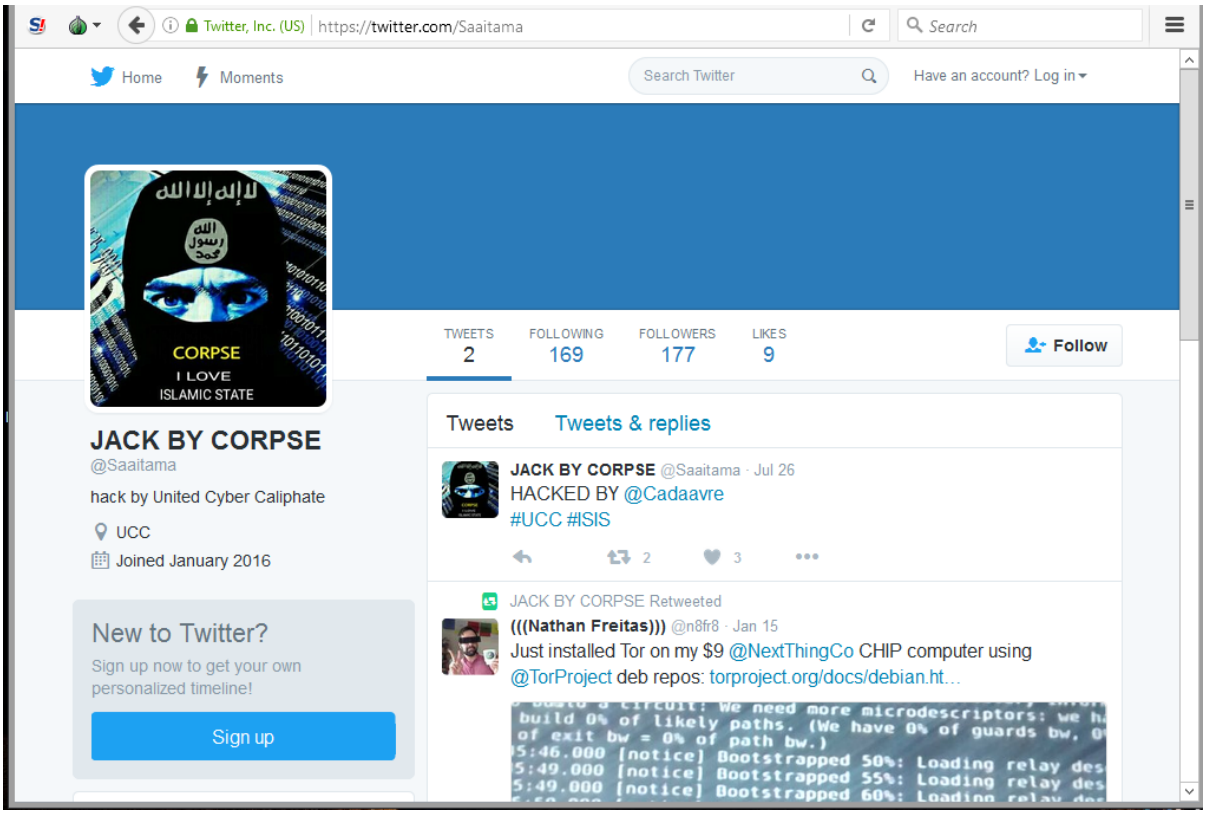
Slika D.2: Spletna stran Issues of Islamic State.



(Issues of Islamic State 2016).

Priloga E: Primer ugrabljenega uporabniškega računa Twitter

Slika E: Ugrabljen uporabniški račun Twitter.



(United Cyber Caliphate 2016).