Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

CYBER TERORIZAM KAO NOVI OBLIK RATOVANJA: SEKUNDARNA ANALIZA SLUČAJA „STUXNET“ I TEORETSKI OKVIRI CYBER TERORIZMA

CYBER TERRORISM AS NEW WAY OF WARFARE: SECONDARY CASE ANALYSIS OF “STUXNET” AND THEORETICAL APPROACH TO CYBER TERRORISM

Stručni rad

Emir Muhić[172]

SAŽETAK

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Dolaskom u novu eru rapidnog razvoja informacionih sistema i tehnologija i neokolonijalnih težnji i borbe za resurse dolazi do evolucije terorizma koji poprima nove nenasilne ali jednako ubilačke oblike. Napadi i diverzije na informacione sisteme vlada ili nuklearnih istraživačkih centara (primjer Irana) predstavljaju novi oblik ratovanja koji zamjenjuje konvencionalno oružje i seli se iz prirodnog u digitalno okruženje. Novi frontovi pomjeraju granice društvene etičnosti i otvaraju vrata novim malicoznim oblicima ljudskog ponašanja.

Ciljevi rada (naučni i/ili društveni): Rad pruža uvid u oblike i načine gerilske i paravojne borbe protiv uspostavljenih državnih i nacionalnih sistema. Rat protiv teorizma nije dobijen, on je promijenio samo formu, ali je suština ostala ista te kao takav još uvijek predstavlja značajnu prijetnju društvu. Rezultati mogu poslužiti kao smjernice i uvidi u događanja u skorijoj budućnosti koja će postati tehnološki naprednija, samim time i ranjivija.

Metodologija/Dizajn: Istraživanje je deskriptivno te će predstavljati sekundarnu analizu i pregled događaja koji su klasifikovani kao rad obavještajnih agencija i pojedinaca u domeni elektronskog ratovanja i uspostavljanja političkih pritisaka na druge regionalne i globalne aktere.

Ograničenja istraživanja/rada: Sam terorizam predstavlja dinamičnu kategoriju čiji se elementi kreću na političkom spektru od borbe za slobodu do opravdanog preventivnog napada. Jasna i tačna klasifikacija svakog od događaja ima notu favorizovanja i osuđivanja aktera što može ući u domen političke korektnosti i nacionalne favorizacije određenih subjekata. Rad predstavlja hipotetički okvir događaja koji se mogu desiti, ali nisu uslovljeni niti direktno vezani za trenutnu političku klimu.

Rezultati/Nalazi: Rezultati prezentirani u radu predstavljaju predviđanje budućih događaja koji nastaju kao rezultat anarhije cyber prostora i međusobnog obavještajnog rata državnih i paradržavnih aktera u borbi za dominaciju nad globalnom politikom. Multipolaritet i neravnomjerna raspodjela snaga i moći bilo državnih ili paradržavnih

[172] Student FKKSS, emirmuhic@fkn.unsa.ba

aktera predstavlja značajnu opasnost za narušavanje krhkog mira i relativne sigurnosti zemalja prvog svijeta koje kao kolonizatori porobljavaju ostatak zemaljske kugle sigurni da neće doći do retribucije.
Generalni zaključak: Ranjivost cyber prostora omogućava različitim akterima da djeluju protiv nacionalnih i državnih sistema kao primarnih meta koje omogućavaju brz i efikasan povrat informacija o uspješnosti napada. Pritisci nastali od strane terorističkih organizacija i njihovog obavještajnog sistema na države ili vlade imaju poguban karakter jer se u pitanje dovodi nacionalni opstanak. Promijenjen je samo front djelovanja, od postavljanja bombi u tržne centre u postavljanje virusa i malware programa u nuklearna postrojenja, hidrocentrale i finansijske sisteme.
Opravdanost istraživanja/rada: Radom su prikazani mogući elementi i načini izvršenja terorističkih aktivnosti koji mijenjaju modus operandi i prelaze na društveno i nacionalno opasnije akte poput rušenja berzi, diverzija električne mreže, uništenja nuklearnih reaktora i pristupa tajnim informacijama na primjeru napada na iranska nuklearna postrojenja.

Ključne riječi
cyber napadi, cyber terorizam, rat, teroristička organizacije, zastrašivanje

ABSTRACT
Reason for writing and research problem (s): New age of rapid evolution of information systems and technology and neocolonial aspirations and struggle for resources leads to the evolution of terroirsm that takes new form, non-violent but equally deadly. Attacks and diversions in government information systems or nuclear research centers (eg Iran) represent a new form of warfare that replaces conventional weapons and moves from a natural to a digital environment. New fronts are pushing the boundaries of social ethics and opening the door to new malicious forms of human behavior.
Aims of the paper (scientific and/or social): The paper provides insights into new ways of guerrilla and paramilitary struggle against established state and national systems, the war against terrorism was not won, it changed only form but the essence remained same, and as even more represents a significant threat society. The results can serve as guidelines and insights into what will happen in the near future, which will become more technologicaly advanced, but in same time more vulnerable.
Methodology/Design: The research is descriptive and will present a secondary analysis of events that are classified as a work of intelligence agencys and subjects in the domain of electronic warfare and the establishment of political pressures on other regional and global actors.
Research/Paper limitation: Terrorism itself represents a dynamic category of all elements that move on the political spectrum from struggle for freedom to a justified preventive attack. The clear and accurate classification of each individual act has favoritizations and judgments of actors that can enter into the domain of political correctness and national favoritisation of certain subjects. The paper presents a hypothetical framework of acts that can happen but are not conditioned or directly related to the current political climate.
Results/Findings: The results presented in the paper shows future events that can arise as a result of the anarchy of cyber space and the mutual intelligence wars of the state and paramilitary actors in the struggle for domination of global politics. Multipolarity and uneven distribution of power of state or parastatal actors, poses a significant risk

of disturbing the fragile peace and relative security of the countries of the first world, which, as colonizers, enslaved the rest of the world while not anticipating retribution.
General Conclusion: The vulnerability of cyber space allows different actors to act against national and state systems as primary targets that enable fast and efficient return of informations on the success of the attack. The pressures incurred by terrorist organizations and their intelligence systems on hostage states or governments have a devastating character because national survival is in question. Only weapons have been changed, from planting bombs at shopping malls to setting up viruses and malware programs to nuclear plants, hydroelectric power stations and financial systems.
Research/Paper Validity: The paper presents possible elements and ways of committing terrorist acts that change modus operandi and switch to socially and nationally dangerous acts such as destroying stock exchanges, electricity diversion, destruction of nuclear reactors and access to classified information shown as example on Iranians nuclear plants.

Keywords
cyber attacks, cyber terrorism, war, terrorist organizations, intimidation

1. UVOD

Terorizam u novom milenijumu je svakodnevno prisutan, te u jednu ruku postaje svakodnevnica. Teroristički napadi postaju novi način izražavanja političkih stavova i vrijednosti svih ekstremnih skupina, lijevih i desnih, religioznih i kriminalnih. Za vrijeme hladnog rata i bipolariteta svijet je strahovao od napada ICBM-ovima sa nuklearnim bojevim glavama. Novo, cyber doba je zamijenilo barbarske i „prljave" nuklearne projektile sa dosta sofisticiranijim i perfidnijim načinima borbe u kojima je napadač anoniman, djeluje bez emocija i za novčanu naknadu.

Cyber kao pojam se pojavljuje ekspanzijom kompjutera i označava kompjuterske mreže ili virtuelni prostor. Dominacija cyber prostora u novom milenijumu je označila početak nove silikonske ere, ere čiji frontovi se ne nalaze u poljima, ravnicama ili šumama, nego u novom neopipljivom i metafizičkom svijetu- svijetu 0 i 1.

Prema definiciji FBI-a terorizam se definiše kao nezakonita upotreba sile ili nasilja nad osobama ili vlasništvom, kako bi se zastrašila ili na nešto prinudila vlast, civilno stanovništvo ili neki njihovi segmenti radi postizanja političkih ili socijalnih ciljeva (Coady & O´Keefe, 2004). Način zastrašivanja u novom dobu je putem virusa i malware programa koji vrše pritisak na određene dijelove društva kako bi ih potčinili i nametnuli svoju volju. Prema Šmitu (1983) terorizam je metod ponovljenih akcija, nasilja koji podstiče uznemirenost; koriste ga polutajni pojedinci, grupe ili državni činioci, zbog idiosinkrazijskih, kriminalnih ili političkih razloga, gdje nasuprot atentatu neposredni ciljevi nasilja nisu i glavni ciljevi. Tomaševski (1983) navodi da se pod pojmom terorizma obuhvataju različiti akti nasilja i ugrožavanja ljudskih prava i ljudskih života, kao i javnih, odnosno zajedničkih, individualnih dobara. Shodno tome, nasilje i prijetnje po ljudski život pronalaze svoje

mjesto i u cyber domeni, koja uticajem na određene bitne objekte i faktore društva ugrožava živote ljudi.

Kada govorimo o novoj eri terorizma i razvoju informacionih tehnologija moramo pomenuti ekstenzivnu evoluciju interneta te razvoj industrijskih kapaciteta i kritične infrastrukture širom svijeta. Internet kao čudo 20. stoljeća je sada poprimio novi oblik, oblik svakodnevnice kako u privatnom tako i u javnom sektoru, a ubrzani razvoj tehnologija i industrije uporedo prati i razvoj interneta. Korelacija između intrerneta i kritične infrastrukture zasniva se na stvaranju, prijemu i protoku informacija koja je neophodna za funkcionisanje kritične infrastrukture koja koristi kompjuterske sisteme spojene na internet (Catrantzos, 2009). Osjetljivost podataka i ranjivost samog sistema kojeg koriste subjekti kritične infrastrukture predstavljaju ključni faktor zaštite od cyber napada od strane terorističkih organizacija. Evolucija terorističkih organizacija u domenu elektronskog ratovanja predstavlja značajnu prijetnju nacionalnoj sigurnosti bilo koje države i nacije. Sama kritična infrastruktura predstavlja stvar nacionalne i javne sigurnosti i ekonomske stabilnosti koja proizilazi iz njenog funkcionisanja. Krah u domenu kritične infrastrukture predstavlja značajnu pogubnost za samu državu i uspostavlja hijerarhijsku strukturu između države i terorističke organizacije koja je izvela napad i stvara stanje opće panike koja je multiplicirana prestankom rada elemenata kritične infrastrukture. Loša prevencija i zaštita kritične infrastrukture od malicioznih antisocijalnih elemenata može prouzrokovati novi elektronski 11. septembar gdje bi cyber napadom posebni elementi industrije ili infrastruktura bili neutralizovani i uništeni, a društvom bi zavladao strah, histerija i panika. Slučaj iz Irana 2010. godine i moć Stuxnet virusa, ali i drugih malicioznih programa predstavlja sve bližu i bližu budućnost za svijet koji je potresen stalnim ratovima i krizama koje su vjerovatna uvertira za treći svjetski rat između azijskih, evropskih i američkih aktera koji su u trenutnom trgovinskom i ekonomskom ratu potpomognuti industrijskom špijunažom.

Cyber terorizam kao novo moćno oružje u rukama svjetskih aktera predstavlja novi oblik političke prinude i oblik proxy ratovanja. Nekonvencionalni oblici ratovanja predstavljaju efikasniji način vođenja borbe između suprostavljenih strana. Ekonomski, cyber ili drugi vidovi ratovanja omogućavaju zaraćenim stranama da prikažu prividno stanje mira i spriječe socijalne kolapse dok se iza kulisa odigravaju presudne bitke za opstanak nacija i država.

2. Analiza Stuxnet napada na iranska nuklearna postrojenja

Proxy ratovi vođeni između Irana i ostatka pro-zapadno orjentiranih država koje su stale uz SAD su kulminirali slučajom Stuxnet. Malware koji je pogodio iranska nuklearna postrojenja je otovorio vrata novog fronta koji za razliku od konvencionalnog ratovanja ne koristi „primitivnu tehniku" poput tenkova, aviona i pješadije nego kompjuterske kodove. Specijalno dizajnirani programi omogućavaju napadaču da elektronskim putem izvršava napade na kritičnu infrastrukturu udaljenu hiljadama kilometara i obezbjeđenu svim mogućim fizičkim oblicima zaštite. To se upravo i desilo iranskom postrojenju u Natanzu koje

je bilo „žrtva" takovog jednog programa nazvanog Stuxnet koji usporio iranski nuklearni program i odgodio planove za obogaćivanje uranijuma namjenjenog za vojne svrhe.

2.1. Novi cyber front

Tokom 2010. godine, po prvi put iranski inžinjeri su otkrili da su uzroci stalnih kvarova i uništenja centrifuga za obogaćivanje uranijuma rezultat kompjuterskog koda, odnosno uzrok je bio malware zvani Stuxnet. Udar na kritičnu infrastrukturu poput nuklearnih postrojenja za obogaćivanje uranijuma, elektrana ili berzi je rezultat nedovoljne zaštite i propusta u samim sistemima sigurnosti i nadzora. Propusti vezani za sistem sigurnosti iranskih postrojenja su omogućili odlaganje iranskih planova za obogaćivanje uranijuma, ne značajno, ali ipak ranjivost kritične infrastrukture je još uvijek na izrazito visokom nivou. Kritična infrastruktura u ovom slučaju je postala žrtva zlonamjernih programa koji su iskoristili dizajnerske propuste postrojenja i sigurnosne propuste koji se tiču ljudstva što direktno implicira na moć novog cyber oružja koje je u mogućnosti da djeluje bilo gdje bilo kada i nanese značajnu štetu. Žrtve ovakvih malicioznih programa mogu postati bilo koji elementi kritične infrastrukture poput termo/hidro elektrana, bankovnih sistema, telekomunikacijskih sistema, saobraćajnih sistema i mnogih drugih elemenata koji su neophodni za svakodnevno i sigurno funkcionisanje društva i prekidi u radu kritične infrastrukture bi imali značajan udar na svakodnevni život građana (US Department of Homeland Security, 2019).

2.2. Arhitektura postrojenja

Kada govorimo o industrijskim postrojenjima pažnju trebamo obratiti na sami dizajn i funkcionisanje postrojenja kroz *Industrial Control System* (ICS). ICS predstavlja kombinaciju kontrolnih komponenti koje usklađeno djeluju u ostvarivanju industrijskog zadatka (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2014). Kontrolne komponente od kojih se ICS sastoji su hardwareske i softwareske komponente, odnosno fizički elektronski uređaji i programi koji kontrolišu rad elektronskih uređaja. Uloga ICS-a u kritičnoj infrastrukturi je reguliranje struje, vode, otpadnog materijala, hemikalija, transporta materija etc (Stouffer i sur. , 2014).

U slučaju iranskih postrojenja vektor napada se sastojao iz dva dijela, kompleksnog i jednostavnog, kompleksni napad je imao za zadatak povećanje pritiska u centrifugama za obogaćenje uranijuma, dok je jednostavniji napad za zadatak imao povećanje brzine rotacije samih centrifuga (Langer, 2013). Iz navedenog zaključujemo da je Stuxnet imao dva zadataka usklađena u uništavanju centrifuga, ali na dva različita načina što možemo protumačiti kao failsafe mehanizam, ukoliko jedan napad zakaže, drugi ostaje da dovrši posao što je strategija za novi napad ukoliko bi prvi bio otkriven i zaustavljen.

Jedan od faktora uspješnosti izvršenja napada je bila i upotreba zastarjele tehnologije koju je Iran koristio u nuklearnim postrojenjima, naime upotrijebljena tehnologija datira

iz 60-ih i ranih 70-ih godina 20. vijeka koju je Iran kupio od pakistanskog nuklearnog trgovca Abdul Kadir Khana (Langer, 2013). Jedna od značajki tog zastarjelog sistema je uporeba kaskada, odnosno grupiranja centrifuga, 984 centrifuge su bile raspoređene u 6 kaskada odnosno 164 centrifuge po kaskadi (Langer, 2013). Cilj Stuxnetovog napada je bio automatska upotreba Cascade Protection System-a (CPS) koji je djelovao na dva nivoa, centrifugalnom i kaskadnom. Centrifugalni se sastojao od tri ventila za odvajanje koji su se nalazili na svakoj centrifugi, a njihova svrha je izolacija centrifuge koja ima određene probleme dok ostale rade nesmetano (Langer, 2013). Prilikom zastoja više centrifuga UF6 (Uranium hexafluoride) i stvaranja visokog pritiska prilikom čega UF6 prelazi u čvrsto stanje i oštećuje centrifugu, da bi izbjegli negativne posljedice, iranski inžinjeri su ugradili ispušne ventile čime se vrši kompenzacija za visok pritisak u centrifugama (Langer, 2013).

2.3. Modus operandi Stuxneta

Nakon što je izvršena infekcija preko mobilne memorije (USB) Stuxnet preuzeo potpunu kontrolu, a legitimna kontrola od strane inžinjera i sistema se obavljala samo koliko je to Stuxnet dozvoljavao, a u periodu mirovanja malware je dozvoljavao funkcionisanje i input i output signala inžinjera i sistema. Malware je replicirao funkciju kontrolnog operativnog sistema koji je regularno obavljao zadane funkcije, ali je isključen prilikom infekcije. Malware je obavljao funkciju *man-in-the-middle*, odnosno, kada su input i output signali slati od periferne memorije i nazad, ali preko napadnog koda koji je bio pozicioniran u „sredini". Nakon što je aktivirana napadačka sekvenca, malware preuzima kontrolu nad ispušnim ventilima te mjeri proces inputa signala 21 sekundu koju kasnije pušta u konstantu petlju prilikom napada čime prikriva prave input vrijednosti koje se očitavaju u kontrolnoj sobi, a output signali legitimne automatske kontrole nemaju efekta jer su blokirani (Langer, 2013).

2.3.1. Prva faza napada

Prilikom početka prvog procesa napada izolacijski ventili za prve i posljednje dvije faze obogaćenja se zatvaraju čime dolazi do blokade produkta, a UF6 gas se širi po zahvaćenim kaskadama. Preostale centrifuge se izoliraju osim onih koje su u fazi punjenja, te se pritisak u neizoliranim centrifugama povećava što je uzrokovano blokiranjem ispušnih ventila. Napad se okončava kada napadač odluči da je to dovoljno, te se prelazi na drugu fazu.

2.3.2. Druga faza napada

Druga faza napada za cilj ima uništenje rotora centrifuga. Nova verzija virusa koja je infiltrirana na sistem preko USB-a imala je direktni utjecaj na centralni drajverski sistem (CDS). Stuxnet je postao ažuriran novim zakrpama za MS Windows propuste ali i digitalnim certifikatima koji su omogućili legitimno predstavljanje virusa kao drajverskog

softwarea kojeg je nova verzija operativnog sistema Windows prihvatila (Langer, 2013). Propusti koje je virus pronašao odnose se na kontrolu nad centrifugalnim rotorima koji postaju ranjivi prilikom prevelikog ubrzanja. Napadi u drugoj fazi mijenjali su brzinu rotora IR-1 centrifuga sa 63,000 RPM (rotations per minute) na 84,000 RPM u periodu od 15 čime su prouzrokovana određena minorna oštećenja. Kako navodi Langer (To Kill a Centrifuge, 2013) nakon toga isprobana je nova taktika naglog zaustavljanja centrifuga koje su sa 84,000 RPM spuštane na 120 RPM, nakon čega su se ponovno ubrzavale u periodu od 50 minuta pa ponovno zaustavljale što bi proizvodilo značajnija oštećenja. Zbog određenih sistema zaštite ovakvi radikalni manevri od strane Stuxneta su bili zaustavljeni automatski i načinjena šteta nije bila katastrofalna, ali je ipak odgodila završetak programa.

2.4. Razlozi ranjivosti sistema

Kako navodi Lendvay (2016), uslovi koji su trebali postojati da bi program djelovao se odnosi na tri ključna elementa ranjivosti stema, a to su: insajderska prijetnja (Stuxnet je dizajniran tako da ga je potrebno ručno spojiti na računar da bi došlo do infekcije), propusti u sigurnosnoj mreži čime je omogućena infekcija programskih logičkih kontrola i nedostatak jasnih i legitimnih cyber mjera odbrane. Ranjivost iranskih nuklearnih postrojenja se nalazi u velikom broju sabotera i insajdera koji su spremni da iz zbog nekih nepoznatih razloga zaustave razvoj nuklearnog programa. Kritična infrastruktura posjeduje element ranjivosti uzrokovan od strane insajderske prijetnje i loše kontrole i nadzora nad zaposlenim.

U slučaju iranskog postrojenja Natanz, ljudski faktor je odigrao značajnu ulogu, kontrolni sistem nije bio spojen na internet ili neku eksternu vezu, ali je ipak došlo do infekcije koja se jedino mogla desiti manualnim ubacivanjem virusa uz pomoć USB-a. Nadzor nad zaposlenicima i mogućim saboterima je ključni faktor koji je mogao da prevenira infekciju i zaustavi napad, ali nedostatak nadzora i kontrole u slučaju kritične infrastrukture ima pogubne posljedice koje se odražavaju u ekonomskim, proizvodnim i ljudskim resursima. Rudimentarnost cyber sistema zaštite kritične infrastrukture koji je trebao djelovati agresivno prema virusu je zakazao i zahtijeva konstantna unapređenja u tom polju kako bi se proces infekcije zaustavio i stavio pod kontrolu čime bi ostatak ICS-a mogao nesmetano obavljati svoje funkcije.

3. Kritična infrastruktura u cyber prostoru i terorizam

Vanredne situacije predstavljaju jedno od stalnih i učestalih situacija koje u svakom trenutku mogu da pogode kritičnu infrastrukturu te reakcija subjekata na takva stanja mora biti momentalna bilo da se radi o fizičkom ili cyber ugrožavanju te postojanje zaštite je imperativ za opstanak. Zaštita kritične infrastrukture je definisana kao strategija, politika i spremnost da se zaštiti, spriječi, a kada je potrebno i odgovori na napade na ove ključne infrastrukture i sredstva (Lewis, 2006). Kritična infrastruktura obuhvata pojedine

institucije javnog i privatnog sektora, kanale distribucije te mreže osoba i informacija koje garantuju nesmetan i kontinuiran protok ljudi, roba, servisa, usluga, što je ključno za stabilnost ekonomskog i bezbjednosnog sistema zemlje i ima direktan uticaj na nacionalnu bezbjednost, nacionalnu ekonomiju, javno zdravlje, sigurnost stanovništva i efikasnost djelovanja vlasti (Garaplija, 2018).

Simbioza KI i terorizma je od velikog značaja za nacionalnu sigurnost. Konvencionalni oblici terorističkih napada koji odnose desetine i stotine žrtava se ne mogu mjeriti sa novim cyber oblicima napada na KI gdje uspješan napad ostavlja desetine ili stotine hiljada ljudi bez pitke vode, električne energije ili dolazi do zagađenja okoliša hemijskim, nuklearnim ili drugim otpadom te uništenja finansijskog sistema države. Politički cilj koji nosi teroristički akt ogleda se u strahu i pritiscima koji nastaju ugrožavanjem KI čime dolazi do multiplikacije straha kod građana i domaća vlada se stavlja u nepovoljan položaj iz dva razloga - nemogućnost adekvatnog odgovora na napad i pucanje socijalne kohezije. Društveni nemiri potaknuti terorističkim napadima konvencionalnim sredstvima se ne mogu mjeriti sa cyber napadima iz razloga slabe detekcije istih te povjerljivosti informacija koje dolaze iz KI. U slučaju da dođe do defekata u radu KI, te se isti plasiraju kao tehnička greška u radu postrojenja, javno priznanje organizacije koja je izvela napad bi znatno oslabilo povjerenje između države i građana zbog faktora tajnosti od strane državnih tijela koja su pokušala zataškati slučaj. Nesigurnost i nepovjerenje građana bi značajno doprinijelo terorističkim organizacijama u njihovoj integraciji u javnu sferu života kroz sijanje straha čime bi postali de facto gospodari života i smrti, te oni koji formiraju socijalnu sliku društva. Takav jedan napad bi sigurno izazvao lančanu reakciju drugih napada i pojavu sabotera i insajdera koji bi pokušali da postanu pripadnici jedne takve organizacije. Socijalno isključeni pojedinci predstavljaju najbolji materijal za regrutovanje te oni kao *lone wolf* napadači bi žrtvovali i vlastiti život zarad višeg cilja.

Kada govorimo o kritičnoj infrastrukturi, istu definišemo kao infrastrukturu značajnu za određenu zajednicu, čije oštećenje ili gubitak vodi do gubitka isporuke neke usluge koje su prijeko neophodne za normalno funkcionisanje društva. U grupu kritične infrastrukture ubrajaju se telekomunikacije, elektroprivreda, skladištenje i prenos plina i nafte, bankarstvo i finansije, transport, vodosnabdjevanje, hitna služba (uključujući medicinske, policijske, vatrogasne i spasilačke službe) i druge institucije (Garaplija, 2018).

Napadi na kritičnu infrastrukturu mogu biti fizički, upotrebom određenih sredstava sile ili prinude na proizvodni proces ili virtuelni, cyber napad. I jedna i druga vrsta napada zahtijeva i ljudski angažman i djelovanje. Prilikom fizičkog i cyber napada ili ugrožavanja kritične infrastrukture, ljudski faktor igra značajnu ulogu koja se odražava kroz sabotažu, infiltriranje i djelovanje insajdera predstavlja ključni faktor uspješnosti stvaljanja van pogona infrastrukturu. Sabotažu ključnih elemenata infrastrukture obavljaju infiltratori i insajderi. Kada je riječ o infiltratorima, tada govorimo o osobama koje kao članovi neprijateljske organizacije ulaze u redove institucije i kao radnici stječu određena saznanja o ranjivostima sistema i na taj način pokušavaju da ostvare vlastiti cilj (Catrantzos, 2009). Insajderi kao osobe na visokoj hijerarhijskoj poziciji unutar institucije poznaju sve

nedostatke sistema zaštite i ključnih elemenata infrastrukture, ali ih je teže kontrolirati zbog određenih psiholoških faktora poput egocentrizma, te kod njih ne postoji lojalnost određenoj frakciji, ali i shodno tome postoji visoka šansa da planovi budu otkriveni namjerno ili njihovom nepažnjom (Catrantzos, 2009). Kao jedan od primjera insajderske prijetnje imamo cyber napad virusa Stuxnet na iranska nuklearna postrojenja u Natanzu gdje je sam virus ubačen u sistem preko USB-a, te za takvo djelovanje i pristup kontrolnom sistemu je potrebna osoba koja se nalazi visoko na hijerarhijskoj poziciji, koja posjeduje pristup svim nivoima infrastrukture bez stvaranja sumnje drugih zaposlenika.

Uloga insajdera i sabotera kao pripadnika terorističkih skupina ili kao *lone wolf* počinitelja je jedna od bitnijih sigurnosnih pitanja zaštite KI. Osobe koje imaju pristup kontrolnim tačkama i sistemima uz pomoć malicioznih programa i virusa nanose značajne štete radu KI, ali i nacionalnoj sigurnosti, te se stvara klima nepovjerenja između države i naroda.

3.1. Ranjivost kritične infrastrukture

Modernizacija industrije, ostvarena kroz globalizaciju i međunarodnu saradnju, predstavlja dobrobit za razvoj kritične infrastrukture, te se ostvaruje velika nacionalna dobrobit kroz isto, ali se pojavljuju i određeni izazovi i prijetnje u domenu sistema sigurnosti. Nacionalna ekonomska stabilnost i sigurnost ovisi o shvatanju ozbiljnosti internih i eksternih prijetnji na nivou cyber prostora. Udar na industrijski kontrolni sistem određene kritične infrastrukture predstavlja i udar na ekonomski sistem jedne države, što znači da onemogućavanje rada i proizvodnje ostvaruje posljedice i na samu ekonomsku i sigurnosnu situaciju u državi.

Uloga ICS-a u sistemu rada kritične infrastrukture je od visokog značaja, jer u samoj osnovi ICS predstavlja mozak čitave operacije proizvodnje i napad na mozak predstavlja i napad na cjelokupnu kritičnu infrastrukturu koja u tom slučaju prestaje sa proizvodnjom ili dolazi do nepoželjnih posljedica izazvanih od strane malicioznih virusa.

Napadni vektori cyber prijetnji na ICS se odražavaju u dva nivoa, prvi se odnosi na ometanje sistema komunikacija i dijeljenja informacija, a drugi na neovlaštene instrukcije, komande i spuštanje/podizanje alarmantnog praga za pojedine opasne situacije (Stouffer i sur., 2014). Neovlaštene radnje za posljedicu imaju oštećenje, onemogućenje ili gašenje opreme, oštećenje okoline ili ugrožavanje ljudskih života (Stouffer i sur., 2014). Kao primjer imamo centrifuge nuklearnog postrojenja u Nantzu koje su na osnovu neovlaštenih komandi Stuxneta rapidno ubrzavale ili usporavale rotacije ili povećavale pritisak unutar centrifuga čime dolazi do oštećenja istih. Simbioza kritične infrastrukture i ICS-a je izvršena umrežavanjem IT komponenata u postojeći sistem koji je zamjenio fizičku (ljudsku) kontrolu nad određenim mehanizmima i procesima koji se uz pomoć ICS-a obavljaju automatski samo uz ljudski vizuelni nadzor. Integrisanjem ICS-a sa mrežnim sistemima i online servisima stvara veću dostupnost samog sistema eksternim prijetnjama.

Kako navode Borau i Badita (2008) postoje 4 faktora koja doprinose eskalciji modernih prijetnji za ICS:

1. Široka upotreba standardizirane tehnologije sa poznatim ranjivostima,
2. Mrežno spajanje ICS-a sa drugim mrežama,
3. Nesigurna upotreba sistema daljinske kontrole,
4. Široka distribucija tehničkih karakterisitika o ICS-u preko interneta.

Na osnovu modernih prijetnji i jačanja cyber napada i malicioznih radnji, način zaštite kritične infrastrukture je postojanje zatvorenog sistema koji je fizički i cyber odvojen od realnog svijeta što bi kao krajnji cilj imalo stvaranje određenih problema. Problem odvojenosti sistema KI od realnog svijeta i umrežavanja na internet je nepostojanje ili nedovoljan protok informacija. Informacije koje nastaju komunikacijom sa drugim centrima KI i subjektima na terenu kao i informacije koje su potrebne za daljinsko upravljanje su neophodne za rad, te načini zaštite cyber prostora moraju da se prilagode uvjetima u kojim postoje.

Postojanje adekvatnih cyber timova je jedan od imperativa zaštite i opstanka KI u cyber prostoru, upotreba neobrazovanog i neadekvatnog kadra u sistemu zaštite od vanjskih i unutarnjih prijetnji je jedan od otvorenih puteva za narušavanje integriteta KI, ali i društva koje ovisi o njima.

3.2. Cyber zaštita kritične infrastrukture

Kada se govori o zaštiti KI, isto se odnosi u većini slučajeva na fizičku zaštitu postrojenja uz upotrebu ljudstva i tehničkih sredstava da se osigura kontinuiran rad i otklone svi uljezi. Ono šta ja specifično za KI je to što je ista ranjivija u cyber sferi, te su štete prouzročene virusima i malwareima značajnije od fizičke štete. Šteta nastala primjenom sile je lokalizovana i izolirana te teško da u potpunosti zaustavi rad postrojenja. Također, fizička zaštita od uljeza posjeduje i preventivni vid, odnosno zastrašivanje uljeza i sabotera, dok je cyber zaštita apstraktna i nevidljiva. Sama apstraktnost i fizičko nepostojanje cyber zaštite je poziv za mnoge da pokušaju izvršiti određenu vrstu napada na KI. Postupanje pod premisom da KI nije dovoljno zaštićena u cyber sferi i da ne postoje adekvatne sigurnosne mjere može uveliko uticati na učestalost napada. U slučaju da ne postoji adekvatna cyber zaštita, da rukovodstvo štedi na zapošljavanju IT stručnjaka i kupovini nove opreme, KI postaje meta za sve one koji posjeduju dovoljno saznanja o unutarnjim propustima. Osoblje koje nema dovoljno obrazovanja u sferi cyber zaštite je daleko od optimalnog i zadovoljavajućeg stanja za preživljavanje i opstanak KI pod cyber napadima. Nesposobno osoblje također predstavlja značajnu ranjivost za samu KI koja će prvim napadom biti onesposobljena i time dolazi do ugrožavanja i prestanka normalnog funkcionisanja korisnika usluga. Kao primjer toga imamo cyber napade iz 2015. godine na električnu mrežu Ukrajine kad je bez struje ostalo 225,000 korisnika ili kada je 2016. ransomware napao US Medstar te prisilio 10 bolnica da rade bez elektronskih kartona

pacijenata i email sistema (Gallagher, 2016). U 2017. godini Wells Fargo je potvrdio postojanje DoS (denial-of-service) napada koji je 4 dana onemogućio sve online usluge (Pagliery, 2016). Cyber napadi poput onog u Ukrajni ili napada na US Medstar značajno utječu na kvalitetu života korisnika usluga, dok napadi na institucije poput Wells Fargo zadaju i značajan udarac samom finansijskom sistemu institucije, pružanja usluga, ali i postoji direktan udar na krajnjeg korisnika usluga - običnog građanina u vidu straha i nepovjerenja prema instituciji.

Kontrola fizičkih procesa može biti veoma osjetljiva na vremenska zakašnjenja (lag) koja onemogućava enkripciju ili druge sigurnosne mehanizme te kao primjer je vremenski odgovor sigurnosnih sistema u nuklearnim postrojenjima (She & Jiang, 2011). Software koji se koristi za obavljanje industrijskih procesa (ICS) je često zastario, te su njegove ranjivosti poznate napadačima, te softwarske zakrpe ne mogu biti momentalno izvršene zbog verifikacijskih procesa koje moraju biti dovršene kako bi se osiguralo da su sve kontrole nad sigurnosnim funkcijama netaknute ili će sigurnosni update uvesti nove rizike u operacije fizičkih procesa. (Babu, Ijyas, Muneer, & Varghese, 2017).

Cyber sigurnosna zaštite koje se razvijaju i postavljaju mogu ublažiti ranjivosti i prijetnje cyber-fizičkim sistemima (CPS). Odbrambeni mehanizmi kao firewall-i, antivirusni programi i sistemi prepoznavanja uljeza se implementiraju i unapređuju kako bi se onemogućio neodobreni pristutp (Nicholson, Webber, Dyer, Patel, & Janicke, 2012). Implementacija mamaca omogućava odvraćanje uljeza od pravih sistema (Disso, Jones, & Bailey, 2013). Mamci kao vid odbrane i skretanja napada su adekvatno rješenje sve dok napadač ne otkrije prevaru i usmjeri sve svoje snage na pravi sistem. Primitivni i naivni vidovi zaštite poput mamaca i slabih antivirusnih programa ne predstavljaju značajnu prepreku za cyber teroriste koji posjeduju dosta više znanja i materijalno-tehničkih sredstava za izvršenje napada.

4. Cyber terorizam i kritična infrastruktura

Kao što smo već mogli da vidimo u radu, cyber terorizam i kritična infrastruktura su u parazitskoj vezi, cyber terorizam ne bi mogao da postoji bez kritične infrastrukture koju bi iskoristio i napao, ali bez cyber terorizma kritična infrastruktura bi bila opet podložna konvencionalnim oblicima napada i opasnosti poput samoubilačkih ili bombaških napada, frontalnih napada određenih ćelija terorističkih skupina i slično. Specifičnost cyber terorizma se zasniva na podršci od stranih država i vlada koje dolaze u povoljan položaj napadom na određenu kritičnu infrastrukturu u stranoj državi (Metropuolos & Platt, 2019). Prije svega moramo postaviti pitanje koja je razlika između cyber napada i konvencionalnih oblika terorističkih djela (upotreba vatrenog ili hladnog oružja, eksplozivnih ili hemijskih sredstava)? Zašto je jedan oblik napada efikasniji od drugog i koji se ciljevi ostvaruju jednom ili drugom vrstom napada? Efikasnost i razlika između konvencionalnog i nekonvencionalnog terorističkog napada može se ogledati u nanesenoj materijalnoj šteti, izazvanom strahu i ostvarenom političkom cilju.

4.1. Proxy ratovanje

Proxy ratovi trenutno postaju novi trend vođenja globalne politike te u suštini predstavljaju indirektno učestvovanje treće strane u konfliktu koja za cilj ima nametanje vlasitih ciljeva i strategija (Rauta, 2017). Uloga državnih aktera u proxy ratovanju je značajna za izazivanje sabotaža, odnosno terorističkih napada koji služe za destabilizaciju određenih dijelova društva. U vrijeme razvijene elektronike i elektronskog poslovanja, „hakerski poduhvati" brisanje ili izmjene na raznim sajtovima, ubacivanje raznih virusa u računare itd. je sabotaža velikih dimenzija (Alispahić, 2011). Blokada određenih sradržaja na internetu, napadi na uslužne sisteme, bankarski sektor ili berze može da izazove negativne posljedice za ekonomske sisteme neke države što se direktno odražva na sve korisnike tih usluga, te na taj način izaziva socijalne nemire i strah. Cyber terorizam za razliku od konvencionalnih oblika ne upotrebljava standardna sredstva poput oružja i eksploziva za ostvarivanje cilja. Kako Alispahić (2011) navodi, „sabotaže ove vrste ostaju tajne" – niti jedna država ili institucija ne želi priznati da je bila žrtva nekog napada čime bi se kompromitirao njen status. Konvencionalnom oružju upotrijebljenom u napadu veoma lahko se može ući u trag, te se na taj način otkriti odakle oružje potiče, počinitelja, a samim time i nalogodavca, stoga takvi zastarjeli oblici napada više nisu adekvatni za postizanje određenih ciljeva. Teroristčke skupine veoma često imaju političku pozadinu i idejni tvorci takvih organizacija su dio obavještajno-sigurnosnog aparata države iz koje skupina potiče ili neke druge države koja je u „bliskom" odnosu sa državom porijeka terorističke skupine, a samim time je u cilju istim da ostanu neotkriveni. Kao takve, terorističke skupine sa direktnom vladinom pomoći mogu doći u posjed nekonvencionalnog cyber oružja kao što je Stuxnet ili sličan program koji će služiti za ostvarivanje traženih ciljeva.

4.2 Cyber terorizam

Za razliku od „primitivnih" fizičkih i brutalnih terorističkih napada, cyber terorzam ima drugačiju doktrinu i relativno „čišći" modus operandi. Cyber napadi se mogu izvršiti iz bilo kojeg dijela svijeta, potpuno anonimno i efikasno, te ne postoji mogućnost da se izvršitelji zarobe ili predaju, te da se na taj način otkrije stvarna politička pozadina i nalogodavac. Otkrivanje počinitelja cyber terorizma predstavlja komplikovan zadatak, te su izrazito visoke šanse da se počinitelji nikada ne otkriju. Primarni razlog je visoka sofisticiranost i sposobnost počinitelja da vješto sakriju tragove čime se napadi teško predviđaju, otkrivaju i sprečavaju.

Kao pretpostavku možemo imati da su cyber teroristi u najvećem slučaju vrsta paraobavještajnih službi, službi koje usko surađuju sa legitimnim državnim obavještajnim agencijama te primaju direktne naredbe od državnog vrha. U primjeru Irana, uloga državnih aktera i međunarodnih odnosa je od velikog značaja za postojanje i funkcionisanje cyber terorizma. Ono što bi izazvalo osudu međunarodne zajednice poput konvencionalnog terorističkog napada na nuklearna postrojenja, bilo je skriveno u cyber napadu. Cyber (teroristički) napadi koji su usmjereni na kritičnu infrastrukturu dosta su pogubniji kada se govori o nanesenoj šteti koja se mjeri u ljudskim životima, izgubljenoj infrastrukturi,

vremenu i finansijskim sredstvima koja su izgubljena prestankom rada infrastrukture te sredstava koja su neophodna da bi se kritična infrastruktura ponovo reparirala i stavila u pogon. Prednost takvih terorističkih cyber napada na kritičnu infrastrukturu se odražava i u tajnovitosti napada i često sama žrtva i ne zna da je bila meta napada te sami napad može biti karakterisan kao nesretan slučaj ili nepažnja prilikom rukovanja sistemima za kontrolu, ali se može pojaviti i određena organizacija koja će preuzeti krivnju kako bi se „skinula" odgovornost sa očiglednog napadača-državnog aktera. Tajnovitost takvih operacija je cilj uspješnosti u održavanju relativno dobrih odnosa sa susjednim državama i vladama, ali je i u cilju da napad ostane neprimjećen i klasifikovan kao sistemska greška čime se otklanja sumnja na neke od neprijateljski raspoloženih aktera koji bi imali koristi od takih cyber napada.

U slučaju iranskih nuklearnih postrojenja za obogaćivanje uranijuma, Iranci nisu ni bili svjesni da su žrtve cyber napada, a ne slučajnih sistemskih grešaka koje su prouzrokovale disfunkcionalnost centrifuga. Iz primjera vidimo da je bilo potrebno dugo vremena da bi se otkrili pravi uzroci kvarenja centrifuga, ali nije oktriven počinitelj ili nalogodavac, te se samo može nagađati ko stoji iza takvog napada. Efikasnost napada ogleda se u vremenu koji je potrebno da se isti otkrije te šteti koju je isti nanio. Iako šteta može biti minorna, psihološki efekat nad žrtvom (društvom) je dosta značajniji, te stvara ogromne doze nepovjerenja i paranoje unutar same napadnute strukture. Paranoja je u poptpunosti opravdana, svako može postati žrtva cyber terorista.

5. Zaključak

Kritična infrastruktura predstavlja glavnu metu novih oblika terorizma, odnosno, cyber terorizam kao svoju primarnu žrtvu ima sve oblike infrastrukture čije uništenje ili prestanak rada predstavlja opasnost po ljudski život. Primjer centra za obogaćivanje uranijuma u Iranu je jedan od niza cyber napada koji su u početku bili okarakterisani kao sistemska greška ili propust zaposlenika da bi se kasnije ispostavilo da je u pitanju sofisticirani cyber napad. Povezanost kritične infrastrukture sa „vanjskim" svijetom, odnosno internetom, predstavlja prvi i početni korak da ista postane kompromitovana i da se na taj način ostvare uvjeti za izvršenje terorističkog napada. Terorizam kao bolest pronalazi nove načine prilagođavanja okolini, te niti jedna sfera društvenog života nije sigurna od istih. Evolucija terorizma je tek započela. Nadmetanje internacionalnih aktera za dominacijom nad određenim sektorima povlači za sobom i inovacije koje su potrebne za ostvarivanje ciljeva. Cyber terorizam je novus u toj igri te u budućnosti možemo očekivati njegovu evoluciju. Ovisnost o tehnologiji pospješuje viktimizaciju kako običnog puka tako i državnih i nacionalnih sektora i oblasti te pruža plodno tlo za sijanje straha i nemira. Društvo u cjelini postaje nesigurno i zastrašeno „divljanjem" cyber terorista i disidenata, a razlog tome su vulnerabilnost ekonomije, industrije i sigurnosnog sistema koja proizilazi iz dostupnosti i povezanosti istih u cyber prostoru. Napadi na berze utiču direktno na finansijsko stanje društva, uništenje ili zaustavljanje proizvodnih kapaciteta industrije je povezano sa neprilikama ekonomske prirode i nastanka abnormalnosti u društvu, dok pad sigurnosnog sistema države karakteriše isti kao „nesposoban" te u konačnici epidemija

straha i socijalnih nemira je prirodan slijed događaja. Cyber terorizam predstavlja novu eru terora i straha protiv koje se čovječanstvo mora boriti.

6. Literatura

A) Knjige

- Alispahić, B. (2011). Sabotaža. In B. Alispahić, Osnovi metodike rada obavještajno-sigurnosnih službi (p. 117). Sarajevo: Šahinpašić.
- Garaplija, E. (2018). Proces identifikacije, analize i evaluacije rizika kritične infrastrukture u vanrednim situacijama. Sarajevo: Institut za zaštitu od požara i eksplozije.
- Lewis, T. G. (2006). Critical Infrastructure Protection in Homeland Security-Defending a Networking Nation. New Jersey: Wiley-Interscience
- Tony Coady, Michael O´Keefe (2004). Terorizam i pravednost. T. Coady M. O' Keefee, Terorizam i pravednost. Zagreb.
- Primorac, I. (2002). Državni terorizam i protuterorizm. In I. Primorac, Državni terorizam i protuterorizm (p. 62).
- Schmidt, A. (1983). Political Terrorism. In A. P. Schmidt, Polical Terrorism. Amsterdam.
- Tomaševski, K. (1983). Terorizam u suvremenom svijetu. In K. Tomaševski, Izazov terorizma. Beograd.

B) Članci

- Gallagher, S. (2016, april 7). Maryland hospital: Ransomware success wasn't IT Department's fault. Dotupno na: https://arstechnica.com/security/2016/04/maryland-hospital-group-denies-ignored-warnings-allowed-ransomwareattack/, pristupljeno 21.06.2019
- Langer, R. (2013). To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve. Hamburg: The Langner Group. Preuzeto sa: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf Pristupljeno: 20.06.2019
- Metropuolos, E., & Platt, J. S. (2019). Global Cyber Terrorism Incidents on the Rise. Dostupno: https://www.mmc.com/insights/publications/2018/nov/global-cyber-terrorism-incidents-on-the-rise.html, Pristupljeno 13.07.2019
- Pagliery, J. (2016, maj 27). Global banking system under attack: What you need to know. Dostupno na: http://money.cnn.com/2016/05/27/technology/swift-bank-hack/ , Pristupljeno: 11.06.2019
- US Department of Homeland Security. (2019, maj 22). CISA. Retrieved from Supporting Policy and Doctrine: https://www.dhs.gov/cisa/supporting-policy-and-doctrine , Pristupljeno 22.06.2019

C) Dokumenti i izvještaji

- Babu, B., Ijyas, T., Muneer, P., & Varghese, J. (2017). Security issues in SCADA based industrial control systems. 2nd International Conference on Anti-Cyber Crimes (ICACC), (pp. 46-51). Abha, Saudi Arabia. Dostupno na: https://ieeexplore.ieee.org/document/7905261, preuzeto 21.06.2019.
- Boaru, G., & Badita, G.-I. (2008). Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems. In B. G.-I. Boaru Gheorghe. Romania. Dostupno na: http://www.codrm.eu/conferences/2008/ProQuestDocuments-2008.pdf, Preuzeto: 15.06.2019
- Catrantzos, N. (2009). No Dark Corners: Defending Against Insider Threats to Critical Infrastructure. Monterey, California: Naval Postgraduate School. Dostupno na: https://calhoun.nps.edu/handle/10945/4656 , Preuzeto 17.06
- Disso, J. P., Jones, K., & Bailey, S. (2013). A plausible solution to SCADA security honeypot systems. 2013 Eighth International national Conference on Broadband and Wireless Computing, Communication and Applications (pp. (pp. 443–448)), New York . Preuzeto sa https://ieeexplore.ieee.org/document/6690926, DOI: 10.1109/BWCCA.2013.77
- Lendvay, R. L. (2016). Shadows Of Stuxnet: Recommendations For U.S. Policy On Critical Infrastructure Cyber Defense Derived From The Stuxnet Attack. Monterey, California: Naval Postgraduate School. Preuzeto sa: https://www.hsdl.org/?view&did=792239
- National Counterintelligence and Security Center. (2018). Foreign Economic Espionage in Cyberspace. Office of the National Intelligence. Dostupno na: https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf, Pristupljeno:17.07.2019
- Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of cyber-warfare. Computers & Security, 31, 418–436. Dostupno na: https://www.researchgate.net/publication/257006726_SCADA_security_in_the_light_of_Cyber-Warfare , Pristupljeno 12.06.2019
- Rauta, V. (2017). Proxy Wars and the Contemporary Security Environment. In P. Macmillan, The Palgrave Handbook of Security, Risk and Intelligence (pp. 99-115). Basingstoke, UK: Palgrave Macmillan,dostupno na: https://www.researchgate.net/publication/318249920_Proxy_Wars_and_the_Contemporary_Security_Environment, pristupljeno: 04.08.2019
- She, J., & Jiang, J. (2011). On the speed of response of an FPGA based shutdown system in CANDU nuclear power plants. Nuclear Engineering and Design, 241, 2280–2287. Dostupno na https://www.researchgate.net/publication/232372822_On_the_speed_of_response_of_an_FPGA-based_shutdown_system_in_CANDU_nuclear_power_plants , pristupljeno: 07.07.2019

- Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2014). Guide to Industrial Control Systems Security. Gaithersburg, MD: National Institute of Standards and Technology. Dostupno na: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf , Pristupljeno: 01.08.2019