UNIVERZITET U SARAJEVU

FAKULTET POLITIČKIH NAUKA

ODSJEK SIGURNOSNE I MIROVNE STUDIJE

ZAVRŠNI RAD

STUXNET I IZAZOVI DIGITALNOG DRUŠTVA U 21. STOLJEĆU

Mentor:

prof. dr. Azinović Vlado

Student:

Hajdarević Ena

Broj indexa: **1035/II-SPS**

Sarajevo, 2024. godina

I UVOD

Svijet je zakoračio u novu fazu razvoja- fazu digitalnog društva. Digitalno društvo je društvo u kojem internet ima glavnu ulogu u oblikovanju socijalnih, političkih, ekonomskih i drugih oblika interakcije koja se odvija između ljudi. Digitalizacija je omogućila izuzetan razvoj i napredak, koji se u svakodnevnom društvu manifestuje kroz upotrebu digitalnih tehnologija, kao što su internet, pametni telefoni itd.

Zbog toga se mehanizmi i prakse, kao i oprema i tehnologije mijenjaju i razvijaju, te ostvaruju sve veći napredak. Međutim, sa razvijanjem i napretkom, pored svih pozitivnih stvari koje se koriste kako bi se ljudima olakša svakodnevnica i pružio bolji kvalitet života, pojavljuju se i izazovi sa kojima se treba na pravi način i adekvatno suočiti. Sa nastankom i razvojem digitalnog društva, nastaje i cyber prostor, kao i cyber prijetnje, kojima su državne infrastrukrute i građani izloženi svakodnevno. Jedan od najistaknutijih primjera, koji je pokazao kako se tehnologija može koristiti kao opasna prijetnja i tako da se izazove velika šteta po neku državu jeste slučaj Stuxnet. Vjeruje se da je Izrael uz pomoć Sjedinjenih Američkih Država pokušao uništiti Iran, koji je vidio kao prijetnju zbog razvoja i proizvodnje u nukelarnim postrojenjima, te je zbog toga i nastao Stuxnet.

Stuxnet je bio prvi cyber napad koji se dešavao 2010. godine,u potpunoj tajnosti, te je uzrokovao ogromnu štetu bez dokaza u datom trenutku. Stuxnet je cyber crv, napravljen tako da je njegov zadatak bio da napada iranske industrijske sustave u nuklearnim postrojenjima. Softverski sistemi koji su bili pogođeni Stuxnet napadom, bili su zaduženi za kontrolu ferkvencijskih pretvarača, koji kontrolišu brzinu centrifuga u programu. Ovaj cyber napad je učinio da se ubrzaju komande softwer sistema do mjere da se centrifuge same unište. Stuxnet je tako ukazao na potrebu za razvojem cyber sigurnosti i promijenio perspektivu svijeta kada je u pitanju sigurnost digitalnog durštva i zaštita kritičnih infrastruktura država. Slučaj Stuxnet je pokazao i važnost za dominacijom u cyber prostoru, što do tada nije bio slučaj, jer se uglavnom radilo o konvencionalmim prijetnjama i konvencialnim ratovima, međutim sa razvojem tehnologije, dolazi i do pojave cyber prijetnji i cyber ratovanja.

Stuxnet je jedan od primjera izazova sa kojim se suočava digitalno društvo u 21. stoljeću, uz širok spektar “novonastalih” prijetnji, kao što su cyber ratovanja, krađa identiteta, internet prevare, privatnost podataka, cyber criminal, umjetna inteligencija itd. Sve navedeno nam ukazuje da

izazovi digitalnog društva postaju sve kompleksniji te zahtijevaju saradnju sudionika svih nivoa u državi, uključujući aktere na globalnom niovu, pojedinačno države pa na kraju i same pojedince, kako bi se adekvatno i uspješno odgovorilo na savremene digitalne izazove.

1.PROBLEM I PREDMET ISTRAŽIVANJA

1.1 Problem istraživanja

Problem ovog istraživanja predstavlja promjena stanja sigurnosti u cyber svijetu nakon Stuxnet napada.

Poslije cyber napada koji je izazvao značajnu štetu, ključan problem je postao kako da se tako nešto više ne ponovi, što je doprinijelo razvoju cyber sigurnosti na znanto viši nivo.

1.2. Predmet istraživanja

Predmet ovog istraživanja jeste Stuxnet napad i njegove posljedice. Stuxnet je specifično napravljen sa namjerom da sabotira iranski nuklearni program, te je alarmiralo Iran i ostale države u svijetu da počnu raditi na cyber zaštiti svojih sistema i kritičnih infrastruktura.. U konačnici Stuxnet napad je postao izuzetno bitna prekretnica za razvoj prijetnji, ali i zaštite u cyber svijetu.

1.3. Činioci sadržaja predmeta

1.Uslovi: Glavni uslov je postojanje odgovarajućih sigurnosnih cyber sistema i zaštita, prvenstveno globalno, koji će adekvatno odgovoriti na cyber izazove svakodnevnice, kao što je to npr. bio slučaj Stuxnet.

2. Subjekti: Subjekte za ovo istraživanje će činiti četiri nivoa: globalni nivo, državni nivo, društvo i institucije. Globalni i državni nivoi će nastojati kroz uspostavljanje neophodnih zakonskih akata i međusobne saradnje pružiti neophodnu zaštitu od cyber napada, kao i pružati svojim građanima neophodne informatičke edukacije.

Društvo će se educirati u nastojanju prepoznavanja i odbrane od cyber napada (krađa identiteta, internet prevare itd.), kako bi adekvatno mogli prepoznati cyber prijetnju i prevenirati je.

Institucije trebaju raditi na odbrani i zaštiti cyber podataka, pružati neophodne edukacije o cyber sigurnosti svojim uposlenicima, naročito sigurnosne institucije, te raditi na međusobnoj saradnji sa ostalim subjektima.

3. Motivi, interesi i ciljevi: Glavni ciljevi su zaštita građana u cyber svijetu, kritičnih infrastruktura države koje su izložene svakodnevnim cyber napadima, uspostavljanje stanja sigurnosti u cyber prostoru, spremnost da se adekvatno odbrani od cyber napada i drugih digitalnih izazova današnjice.

4. Aktivnosti aktera: Podrazumijevaju sve aktivnosti vezane za bolje razumijevanje digtalizacije i cyber izazova kojim je svakodnevno izloženo društvo u 21. stoljeću.

5. Metode i sredstva: Upotreba metoda i sredstava, informisanja, strategija iz oblasti cyber sigurnosti koji će doprinijeti zaštiti od cyber napada.

6. Efekti djelovanja aktera: U slučaju djelovanja aktera i poduzimanja potrebnih mjera, došlo bi do postizanja većeg nivoa cyber sigurnosti, prvenstveno na globalnom, a zatim i na ostalim nivoima.

1.4. Vremensko određenje predmeta istraživanja:

Vremensko istraživanje će se odnositi na period od 2009. godine, kada se zapravo počinje sa puštanjem Stuxnet crva u kompjuterske sisteme u Iranu, pa do danas.

1.5. Prostorno određenje predmeta istraživanja:

Prostorno istraživanje će se zbog svoje specifičnosti problema prvenstveno odnositi na dešavanja u Iranu prije otkrića Stuxnet napada, a zatim na cijeli svijet.

1.6. Disciplinarno određenje predmeta istraživanja:

Ovo istraživanje je interdisciplinarno, te će se realizirati u okviru sigurnosnih studija, uz pomoć ostalih nauka.

2. CILJEVI ISTRAŽIVANJA

2.1. Naučni cilj istraživanja

Naučni ciljevi istraživanja se temelje na analizi postojećih dokumenata u okviru postojećih zapisa, naučnih članaka i drugih izvora podataka o Stuxnet napadu, kao i ostalim mnogobrojnim cyber napadima.

Naučni ciljevi su zadati nivoi naučnog saznanja, koji se namjeravaju ostavriti naučnim istraživanjem i koji će biti sadržani u rezultatima istraživanja.

Naučni cilj ovog istraživanja jeste stjecanje naučnog saznanja o predmetu istraživanja, odnosno da se dođe do relevantnih podataka koji će pomoći da napadi poput Stuxneta budu na vrijeme otkriveni i spriječeni, jer je Stuxnet napad dao inspiraciju za mnoge napade koji su uslijedili poslije njega i za koje se tek očekuje da će se desiti.

2.2. Društveni cilj

U samom fokusu društvenog cilja je dizanje svijesti svih korisnika Interneta o cyber izazovima poput Stuxneta.

Kroz Stuxnet slučaj se najbolje može vidjeti kakve posljedice mogu biti po jednu državu, počevši od ekonomije, međunarodnih odnosa i diplomatije itd,, te je zbog toga neophodna edukacija državnih službenika uposlenih u sigurnosnim institucijama, jer su oni osobe koje se prve suočavaju sa cyber napadima, njihovom detekcijom i rješavanjem.

Od iznimne važnosti je ostvariti i podizanje niova pismenosti građana u polju medijske i informacijske pismenosti, te da problem cyber sigurnosti postane dio svakodnevnice o kojoj će se govoriti, što do sada i nije zastupljeno u velikoj mjeri.

Da bi društvo bilo demokratsko, mora imati visok nivo informiranosti, pa bi svi građani trebali biti upućeni u osnovne informacije o cyber sigurnosti i cyber prijetnjama, te kako se zaštitit od istih.

3. HIPOTEZE I INDIKATORI

3.1. Generalna hipoteza

Stuxnet napad je svojim djelovanjem promijenio cyber prostor u 21. stoljeću i ukazao na potrebu povećanja kapaciteta država na polju cyber sigurnosti i njihovog kontinuiranog unaprjeđivanja.

3.2. Posebne hipoteze

1. Otkrićem Stuxnet napada, razvoj cyber sigurnosti i zaštite je postao neophodan.

2. Stuxnet napad je svojim djelovanjem onesposobio iranska nuklearna postrojenja i nanio nesagledivu ekonomsku štetu Iranu.

3. Posljedice Stuxneta su doprinijele uspostavljanju adekvatnih zakonskih okvira i primjena relevantnih mjera, koji su ključni koraci u jačanju cyber sigurnosti i zaštiti od cyber napada osiguravajući stabilno i sigurno digitalno okruženje za sve građane i organizacije.

4. Nakon otkrića Stuxneta, države sve češće počinju voditi ratove u cyber prostoru.

5. Stuxnet je dokazao ranjivost kritičnih infrastruktura jedne države, te ukazao na potrebu za razvojem i adekvatnom zaštitom istih.

6. Stuxnet je narušio međunarodne odnose i ostavio posljedice na iste, zbog vjerovanja da Iran razvija nuklearno oružje.

3.3. Indikatori

Indikatori u ovom istraživačkom radu su odgovarajući pravni dokumenti, analize međunarodnih dokumenata, strategije, naučno-istraživački radovi, publikacije, medijski sadržaji, te smjernice i regulative o cyber sigurnosti i Stuxnet napadu.

4. PRISTUP- PARADIGMA I METODE ISTRAŽIVANJA

4.1. Vrsta i tip istraživanja

Ovo istraživanje je teorijskog karaktera, dakle za prikupljanje podataka, koristit će se metod analize sadržaja. Podaci će biti prikupljeni primarno kroz literaturu korištenu za cyber sigurnost i Stuxnet napad, a sekundardno kroz ostalu literaturu koja obuhvata digitalizaciju i druge izazove digitalnog društva u 21. stoljeću.

4.2. Teorijsko-metodološki pravac

Pristup ovom istraživanju je integralno-sintetički, gdje ne favorizira niti jedan teorijsko-metodološki pravac, što predstavlja jedan opći pogled na temu istraživanja. Ovo istraživanje sprovest ćemo uz primjenu naučnih metoda.

4.3. Opće naučne metode

U ovom naučnom istraživanju će se koristiti analitičko-deduktivna metoda. Na osnovu podataka koje prikupimo putem ove metode pokušat ćemo pružiti adekvatna rješenja za zaštitu sigurnosnih sistema i građana od cyber izazova, kojima su svakodnevno izloženi i koji predstavljaju prijetnju po njihovu sigurnost.

5. NAUČNA I DRUŠTVENA OPRAVDANOST ISTRAŽIVANJA

5.1. Naučna opravdanost istraživanja

Naučna opravdanost istraživanja proizilazi iz njegovog naučnog značaja, produbljivanja i proširivanja znanja.

Ovo istraživanje omogućava usavršavanje naučnih saznanja o faktorima koji utiču na razvijanje cyber napada poput Stuxneta, cyber sigurnosti i odbrane u svijetu.

Nastojati ćemo naučni doprinos ostvariti potvrđivanjem naučno provjerenog rada, kroz prikaz postojećih dokumenata o podacima koji pokazuju rasprostranjenost cyber izazova i prijetnji sa kojima se društvo zbog toga svakodnevno suočava, te ukazati na važnost cyber sigurnosti

5.2. Društvena opravdanost istraživanja

Društvena opravdanost istraživanja može se ogledati u značaju ovog pitanja na globalnom nivou.

Obzirom da živimo u dobu “digitalizacije”, cyber sigurnost je dobila izuzetan značaj, a cyber prijetnje kao što je Stuxnet, počele su predstavljati izuzetnu opasnost za državu i njene građane. Primjena i doprinos naučnih saznanja mogu doprinijeti razvoju cyber sigurnosti i prevenciji kada su u pitanju cyber napadi.

Rezultati istraživanja će biti društveno korisni, tako što će se na osnovu njih moći poduzeti konkretne akcije na poboljšanju stanja cyber sigurnosti i spremnosti da se zaštiti od cyber napada kao što je to bio Stuxnet, te upoznavanju i edukaciji društva podizanjem svijesti o digitalnim izazovima i nesigurnosti koja nastaje zbog istih.

6. KATEGORIJALNI POJMOVI

SIGURNOST - „Podrazumijeva općenito stepen zaštićenosti ljudi od različitih oblika ugrožavanja, zaštitu materijalnih i kulturnih dobara u ličnoj i društvenoj svojini, zaštitu društva i njegovih vrijednosti, cjelovitu zaštitu naroda, nacije, države.., svjetske zajednice, od svih vidova ugrožavanja, a naposlijetku, sigurnost podrazumijeva stepen zaštićenosti od ugrožavanja na kozmičkom i planetarnom nivou života općenito, ljudskoga roda u cjelini.“ (Beridan, 2008)

CYBER SIGURNOST- „Cyber sigurnost je 95 posto informacijske sigurnosti“ (Košutić, 2012.). Kao jedinu razliku između njih, Košutić (2012.) navodi činjenicu da informacijska sigurnost uključuje sigurnost informacija i po pitanju nedigitalnih medija (papira), odnosno, sigurnost informacija u tradicionalnom obliku. S druge strane, cyber sigurnost fokusira se isključivo na sigurnost informacija u digitalnom obliku.”

CYBER KRIMINAL- „Kriminal koji se odnosi na bilo koji oblik kriminala koji se može izvršavati sa kompjuterskim sistemom i mrežama, u kompjuterskim sistemima i mrežama ili protiv kompjuterskih sistema i mreža(Porobić i Bajraktarević, 2012.)“

DIGITALIZACIJA - digitalizacija (engl. digitalization, od digit: znamenka), u najširem smislu, prevođenje analognog signala u digitalni oblik (analogno-digitalno pretvaranje). U užem smislu, pretvaranje teksta, slike, zvuka, pokretnih slika (filmova i videa) ili trodimenzijskog oblika nekog objekta u digitalni oblik, u pravilu binaran kôd zapisan kao računalna datoteka sa sažimanjem podataka ili bez sažimanja podataka, koji se može obrađivati,pohranjivati ili prenositi računarima i računarskim sistemima. Postupci digitalizacije, kao I uređaji kojima se ona obavlja (analogno-digitalni pretvarači), ovise o vrsti gradiva koje se digitalizira. (Hrvatska enciklopedija, 2021.)

II NAUČNA I DRUGA SAZNANJA O PREDMETU ISTRAŽIVANJA

1.2. Polazna saznanja od predmetu istraživanja

Proces digitalizacije uz sve prednosti, sa sobom nosi i mane. Države i društvo su sve izloženiji cyber napadima, a vrste cyber prijetnji postaju sve brojnije. Stuxnet napad, kao jedan od prvih cyber napada sa velikim posljedicama, ukazuje na potrebu konstantnog razvijanja cyber sigurnosti i zaštite.

Prema Vajzović (2019) postoje tri ključna elementa cyber sigurnosti, potrebna za sveobuhvatno poimanje a to su: tehnologija, procedure i ljudski resursi. Cyber sigurnost je izazov za međunarodno (humanitarno) pravo, međunarodne organizacije, multinacionalne korporacije i pojedinačne države i pojedince. Iz toga proizilazi da je koncept cyber sigurnosti i značaj osnaživanja te vrste sigurnosnih pitanja kroz medijsku i informacijsku pismenost važno i nužno razumijevati i pratiti na tri nivoa: individualnom, institucionalnom te državnom i međunarodnom nivou.

2.2. Fundamentalna pitanja koja proizilaze iz predmeta istraživanja

-Kako je Stuxnet napad promijenio percepciju i strategiju razvoja cyber napada?

-Kako se mogu poboljšati odgovori na cyber napade?

-Koliki je doprinos slučaja Stuxnet u razvoju cyber napada?

-Koliki je doprinos slučaja Stuxnet u razvoju cyber sigurnosti?

-Šta se može očekivati u budućnosti u pogledu cyber izazova i cyber sigurnosti?

-Kako je Iran postupio nakon Stuxnet napada, u vidu jačanja i razvoja cyber sigurnosti itd.?

2.3. Koncepti mogućih odgovora

Proces digitalizacije značajno je povećao složenost cyber izazova s kojima se društvo susreće u 21. stoljeću. Stuxnet napad promijenio je percepciju i strategiju u borbi protiv cyber napada, zbog potrebe za složenijim i zahtjevnijim pristupima cyber sigurnosti.

Slučaj Stuxnet je doprinio razvoju cyber napada, pokazavši kakve su štete moguće na kritičnim infrastrukturama kroz djelovanje cyber napada, što je do Stuxnet slučaja bilo nepoznanica. Također, Stuxnet je omogućio i razvoj cyber sigurnosti, jer je ukazao na hitnu potrebu za unapređenjem zaštitnih mjera i međunarodnom suradnjom. U budućnosti se očekuje da će cyber izazovi postati još kompleksniji, što će zahtijevati kontinuirano poboljšanje sigurnosnih tehnologija i strategija. Nakon Stuxnet napada, Iran, kao I mnoge države su pristupile puno ozbiljnije cyber sigurnosti i zaštiti kritičnih infrastruktura, te su uspostavile nove zakonske regulative i inicijative za jačanje cyber sigurnosti i za odbranu od cyber napada.

Procesom digitalizacije, neminovno je da će se cyber prijetnje svakodnevno razvijati i postajati sve opasnije, samim tim je potrebno pronaći adekvatna rješenja za odbranu od istih, što će pretpostavljamo biti glavni cilj u skorijoj budućnosti, jer je nemoguće da cyber napadi nestanu u potpunosti.

III CYBER SIGURNOST I CYBER RATOVANJE

3.1. Cyber sigurnost

U eri "digitalnog svijeta", gdje su informacije od izuzetne važnosti, cyber sigurnost ima veliki značaj. Tehnologiju koristimo svakodnevno, kako bi obavljali sve vrste poslova, za komunikaciju sa dragim ljudima, odlazak kod doktora, rješavanje neophodne papriologije, dokumentacije, pohranu i čuvanje novca, itd. Cyber sigurnost ima ulogu da štiti sve navedeno i svakodnevno nam omogućava normalan i nesmetan tok života.

Jedan od najvažnijih primjera značaja adekvatne cyber sigurnosti jeste Stuxnet napad. Posljedice Stuxnet napada su ukazale na potrebu razvoja cyber sigurnosti, kako ne bi ključne infrastrukture, kao što je to bilo slučaj sa iranskim nukleranim postrojenjima, pale u ruke ljudi koji će to katastrofalno iskoristit npr. teroristi koji će napraviti i upotrijebiti nuklearno oružje.

Rendulić (2021) navodi da je cyber sigurnost specifična vrsta informacione sigurnosti koja se odnosi na način na koji organizacije štite digitalne informacije, kao što su mreže, programi, uređaji, serveri i drugi digitalni podaci. Iako je ovo samo jedan aspekt informacione sigurnosti, njemu se posvećuje najviše pažnje jer su cyber prijetnje zastupljenije od fizičkih prijetnji.

Cyber prijetnje su postale dio svakodnevnice, te jedan od lakših načina da se nanese šteta drugoj državi ili individui, bez pretjeranog zamaranja i sa različitih krajeva svijeta. To su neki od mnogih razloga zašto su cyber prijetnje jako brzo postale zastupljenije i rasprostranjenije od fizičkih prijetnji. Za njih nije potrebno sjediti u istoj prostoriji, biti blizu svome cilju kako bi izvršio napad i ono što je možda i najzabrinjavajuće jeste da uz pristup Internetu, cyber napad može izvesti bilo ko, dakle uopšte ne mora biti neko ko je upoznat sa cyber industrijom, npr. maloljetnik iz Hrvatske je uspio provaliti u Pentagonovu bazu podataka i tražiti otkupninu.

Autori Spremić i Šimunić (2018) ističu da se svakodnevno bilježi porast cyber napada na kritične infrastrukture. Prethodno se smatralo da je rizik ovih napada na kritične infrastrukture nizak zbog potrebe za specijalističkim znanjem i zbog nepostojanja odgovarajućih internetskih veza. Međusobna povezanost mnogih digitalnih tehnologija i važnih ili kritičnih infrastrukturnih sustava dovela je do stvaranja novih ranjivosti s dalekosežnim posljedicama .

Heijden, R., Dietzel, S., Leinmuller, T. i Kargl, F. (2019) smatraju da poznavanje definicije cyber sigurnosti nije dovoljno bez detaljnijeg razumijevanja različitih vrsta napada. Napadi se mogu podijeliti u tri logične cjeline, a to su:

- cyber kriminal (fokusiran na ekonomsku dobit),
- cyber napad (prvenstveno politički) i
- cyber terorizam.

Dok prema Agenciji Europske unije za cyber sigurnost (2021) postoji devet glavnih skupina prijetnji:

1. Ucjenjivački softver (eng. ransomware) – nakon neovlaštenoga upada u računar, najčešće djelovanjem računalnoga virusa kojega je pokrenuo neoprezni korisnik, šifriraju se podaci koji su u njemu pohranjeni, a koji su neophodni za nastavak rada ili poslovanja, pri čemu računalni kriminalci traže odštetu (najčešće u bitcoinima) za njihovo dešifriranje (Spremić,2017).

2. Zlonamjerno rudarenje kriptovalute (eng. cryptojacking) – neovlašteno korištenje tuđih računalnih resursa za rudarenje kriptovalute (Chickowski, 2022).

3. Prijetnje podacima – objavljivanje osjetljivih, povjerljivih ili zaštićenih podataka u nepouzdano okruženje.

4. Zlonamjerni računalni programi (eng. malware) – računalni virusi i ostali zlonamjerni računalni kodovi napisani i distribuirani s namjerom da naprave štetu nad računalnim i ostalim resursima (Spremić, 2017).

5. Dezinformacija – širenje pogrešnih informacija kako bi se smanjilo povjerenje.

6. Nezlonamjerne prijetnje –ljudske pogreške i pogrešne konfiguracije sustava.

7. Prijetnje dostupnosti i integritetu – napadi koji sprječavaju korisnike sustava u pristupu njihovim podacima uzrokujući smanjenje performansi, gubitak podataka i prekide usluga.

8. Prijetnje povezane s e-poštom – cilj je manipulirati ljudima putem e-pošte.

9. Prijetnje lancu opskrbe – npr. napad na pružatelja usluga, kako bi se dobio pristup podacima kupca.

Procesom digitalizacije i svakodnevnim korištenjem tehnologije, dolazi i potreba za većom cyber sigurnošću, a samim tim nastaju i cyber prijenje koje je pokušavaju narušiti. Sa pojavom cyber sigurnosti i slučajem Stuxnet, očekivano je bilo da dođe i do ratovanja u cyber prostoru, i borbe država za moć i prevlast u istom. Cyber prijetnje su uvijek prisutne i nije ih moguće u potpunosti spriječiti, te je potrebno dobro ih poznaviti i educirati uposlenike u sigurnosnom sektoru i građane o cyber napadima, kako bi ih prepoznali i eventualno spriječili ili ublažili moguće posljedice.

3.2. Cyber ratovanje

Cyber ratovanje, kakvim ga danas poznajemo, nije uvijek bilo razvijeno u ovolikoj mjeri. Jedna od najvećih zasluga i prekretnica za razvijanje cyber sigurnosti i cyber ratovanja jeste Stuxnet napad. Stuxnet napad je kroz svoje djelovanje doprinio tome da države vojne sukobe počinju sve češće voditi u sajber prostoru.

Mladenović (2016) ističe da je cyber ratovanje, ratovanje u cyber prostoru, zasnovano na primjeni informacionokomunikacionih tehnologija. Ono predstavlja specifičan oblik međunarodnih sukoba, koji se od tradicionalnih formi ratovanja razlikuje po sredstvima, metodama i učesnicima. Cyber ratovanje se primjenjuje nezavisno od perioda rata i mira. Po tehnikama, metodi i procesu napada, ono se tehnološki značajno ne razlikuje od kriminalnih, špijunskih ili terorističkih aktivnosti. Potencijal ovog, tehnološki zasnovanog oblika sukoba, raste sa zastupljenošću i uticajem informacionih tehnologija na nacionalnom i globalnom nivou. Međunarodna praksa sukoba u cyber prostoru je stvarna i dinamična. Države izdvajaju rastuća budžetska sredstva za vođenje sukoba u cyber prostoru, razvijaju kapacitete i organizacione strukture za preduzimanje operacija u sajber prostoru i usvajaju doktrine i strategije njihove primene i razvoja. Pojedine države su proglasile cyber prostor petim područjem izvođenja vojnih dejstava, ravnopravan sa kopnom, morem, vazduhom i svemirom.

Cyber ratovanje se najčešće vodi protiv vladinih i vojnih mreža kako bi se spriječilo, ometalo ili spriječilo njihovo korištenje. Cyber ratovanje ne treba poistovijetiti sa terorističkom eksploatacijom cyber prostora, cyber špijunažom i cyber kriminalom. (Sheldon, 2024).

Stuxnet je tako postao prvi poznati primjer cyber napada, koji je pokazao da se cyber napadi mogu koristiti kao oružje za cyber ratovanje, te da se nanese velika šteta nekoj državi bez upotrebe fizičke aktivnosti, pa se postavlja pitanje kako je zapravo Stuxnet razvijen i infiltriran u sisteme bez da ga nadležni organi uspiju primjetiti i spriječiti na vrijeme? Stuxnet je bio inspiracija za svoje nasljednike i zapravo početak cyber ratovanja, kakvim ga danas poznajemo. Države su počele ulagati znatna sredstva u razvoj cyber oružja i za vođenje cyber ratova. Razvoju cyber ratovanja pogodovao je i Korona virus, jer je na par mjeseci vođenje normalnog života stalo i sve je prešlo u cyber prostor, što je pogodovalo izvođenju cyber napada.

3.3. Oblici cyber ratovanja

Šipek (2022) navodi oblike cyber ratovanja:

- Špijunaža – koristi se u svrhu nadziranja drugih, suprotstavljenih država i krađe povjerljivih ili značajnih državnih tajni i informacija. To često uključuje korištenja botnet-ova i phishinga kako bi se kompromitirali računalni sustavi prije same krađe osjetljivih informacija.
- Sabotaža – korišteno od strane terorističkih organizacija u svrhu krađe i/ili uništenja osjetljivih informacija.

- DdoS napadi (denial-of-service) – opstrukcija pristupu važnim web stranicama koje koriste građani, vojska, znanstvenici i drugi tako da opterećuje poslužitelja velikim brojem lažno stvorenih zahtjeva koji potom toliko opterete web stranicu da ga korisnici više ne mogu koristiti. Najčešće se izvode putem botneta.
- Electrical Power Grid – cyber napadi na električne mreže gradova ili čak regija, u kojem hakeri uspostavljaju potpunu kontrolu nad električnom opskrbom stanovništva. Najčešće traže velike otkupnine kako bi vratili kontrolu vlastima.

- Propaganda – pokušaji kontroliranja mišljenja ljudi putem širenja privatnih tajni i lažnih vijesti prema javnosti. Jedno do najupješnijh propaganda je bila u SAD-u 2014. godine u političke svrhe. Pawn Storm, poznata grupacija za cyber špijunažu je targetirala

demokratsku stranku DNC putem phishing napada. Ciljali su na utjecajne članove stranke, kompromitirali su web stranicu stranke i nudili ukradene podatke medijima kako bi utjecali na mišljenje javnosti.

- Ekonomska disrupcija – napadači ciljaju mreže ekonomskih ustanova kao što su burze i banke kako bi ukrali novac ili blokirali pristup ljudima na svoj novac. Rezultat za poduzeća i institucije je katastrofalan jer se širi panika među korisnicima te naglo pada sigurnost i kredibilitet takvih ustanova. Oporavak od takvih cyber napada može trajati mjesecima ili godinama.
- Iznenadni napadi – cyber napad slične taktike kao vojni napadi na Pear Harbour i 9/11. Cilj iznenadnih cyber napada je unazaditi ili uništiti nespremnu cyber obranu institucije ili države. Često se koristi u hibridnom ratu (zajedničko korištenje cyber i fizičkog ratovanja).

S obzirom na prethodno navedeno, možemo uočiti da postoje raznovrsni oblici cyber ratovanja, sa ciljem da se nanese šteta drugim državama i njihovim kritičnim infrastrukturama, kako bi se vjerovatno ostvario politički cilj i stekla određena nadmoć u geopolitčkim odnosima.

3.4. Najpoznatiji primjeri cyber ratovanja

- Cyber napadi na Gruziju (2008): Tokom rusko-gruzijskog rata u augustu 2008. godine, Gruzija je postala meta masovnih cyber napada. Napadi su ciljali ključne web stranice i komunikacijske sustave, uzrokujući prekide u komunikaciji i destabilizaciju infrastrukture. Iako se nije direktno potvrdila ruska vlada, većina stručnjaka sugeriše na njenu povezanost s napadima. (Andress i Winterfeld. 2013).
- Stuxnet (2010): Stuxnet je visoko sofisticiran kompjuterski crv koji je otkriven 2010. Godine i specijalno je ciljao iranska nuklerarna postrojenja, postavši tako prvi znani digitalni virus, koji je uzrokovao fizičku destrukciju kritične infrastrukture sistema. On je bio dizajniran tako da precizno utječe samo na određene ciljeve i da uzrokuje minimalnu štetu tamo gdje nema cilja. (Gemserv, 2019).
- NotPetya (2017): Napad se izrazito brzo širi mrežom, a svi podaci na pogođenim računalima su šifrirani, zbog čega korisnici efektivno gube pristup podacima i kontrolu nad računalom. Zaraženo računalo korisniku prikazuje ucjenjivačku poruku koja traži korisnika

da napadaču plati određeni novčani iznos. Ovaj virus je prvo pogodio Ukrajinu, a zatim se širio dalje Rusijom, Evropom itd. (Fischer, 2019).

- BlackEnergy (2015): 2015. godine, 2 dana prije Božića, oko 225.000 Ukrajinaca ostalo je bez napajanja strujom. To je trajalo oko 6 sati i poslije se saznalo da je u pitanju cyber napad na kritičnu infrastrukturu koju su izveli Rusi.

Iz navedenog, ali i mnogih drugih primjera cyber ratovanja se može zaključiti, da se nekada konvencionalni ratovi, počinju odvijati u cyber prostoru, kao cyber ratovi. Stuxnet je imao doprinos tome da cyber prostor postaje prostor za izvođenje vojnih dejstava i države se počinju boriti za moć u cbyer prostoru. Ukazujući na ove činjenice, ne čudi da cyber napadi postaju sve učestaliji i opasniji za kritične infrastrukure država, ali i same građane. Najsvježiji primjer cyber raovanja može se vidjeti na napadu Rusije na Ukrajinu.

IV RAZVOJ I DJELOVANJE STUXNET VIRUSA

4.1. Značaj operacije Olimpijske igre za nastanak Stuxneta

Kamiński (2020) navodi da je pod šifrom pod nazivom "Olimpijske igre", započet je pokušaj izbjegavanja izravnog sukoba s Iranom. Olimpijske igre bile su suradnja (još uvijek nepriznata) između američkih i izraelskih obavještajnih službi i bile su dio većeg napora da se infiltrira i ometa Iran pod nazivom "Nitro Zeus". Iz ove operacije nastao je malware poznat kao Stuxnet (kombinacija ključnih riječi .stub & mrxnet.sys).

Operacija Olimpijske igre bila je poznata samo malom uskom krugu vojno-obavještajnih dužnosnika SAD-a. Osim onesposobljavanja Iranskog nuklearnog programa na duže vrijeme, bilo je potrebno privoljeti Izrael da ne bombardira Natanz postrojenje planiranim avionskim napadom već da zajedno provedu kibernetički napad. Ovo je prvi ofanzivni kibernetički napad izveden na jednu državu od strane američka agencije NSA[1] i izraelskog pandana Unit 8200.

[1] NSA-Nacionalna sigurnosna agencija

Operacija je trajala nekoliko godina i odvijala se u nekoliko faza dok u konačnici zlonamjerni program kojeg danas poznajemo pod nazivom Stuxnet nije ubačen u postrojenje. Napad je izveden kombinacijom nekoliko različitih vrsta napada, socijalni inženjeringom, izradom ciljanog zlonamjernog koda, uključenjem špijunskih agencija, otimanjem i mučenjem odgovornih pojedinaca s ciljem otkrivanja vrijednih informacija i sl.

4.2. Razvoj Stuxnet virusa

Prema Gemserv (2019), Stuxnet je visoko sofisticiran kompjuterski crv koji je otkriven 2010. godine i specijalno je ciljao iranska nuklearna postrojenja, postavši tako prvi znani digitalni virus, koji je uzrokovao fizičku destrukciju kritične infrastrukture sistema. On je bio dizajniran tako da precizno utječe samo na određene ciljeve i da uzrokuje minimalnu štetu tamo gdje nema cilja.

Povod za sami nastanak Stuxnet crva, bilo je vjerovanje da početkom 2000ih godina Iran razvija nuklearno oružje u svom postrojenju za obogaćivanje urana u Natanzu. Iranska nuklearna postrojenja su bila zračno odvojena, što znači da nisu bila direktno povezana sa Internetom ili bilo kojim drugim kompjuterom koji je bio konektovan na Internet iz sigurnosnih razloga.

Stuxnet je zapravo počeo kontrolirati industrijske kontrolne sustave još 2007. godine, međutim o njemu se nije počelo govoriti sve do ljeta 2010. Godine, kada je izdato upozorenje od strane Cyber Emergency Response Team-a za industrijske kontrolne sustave (ICS-CERT).

Stuxnet je vrlo sofisticiran dio softvera. Procjenjuje se da je multinacionalnom timu kodera trebalo do tri godine da razvije crva. To je, naravno, uključivalo povratne informacije, što je timu omogućilo fino podešavanje i razvoj drugačije metode napada. Ključ napada bila je sposobnost crva da prati i bilježi normalne podatke o radu. Operater je vidio ono što je izgledalo kao normalni radni parametri na zaslonu sučelja čovjek-stroj (HMI) dok je centrifuga radila nepovoljno.

Crv je tiho radio u pozadini, bilježio operativne podatke i spremao ih u skrivene datoteke koji su preuzeti i zatim poslani nazad programerskom timu. Ovi podaci su analizirani, I u skladu s podacima prikupljenim iz operativnih centrifuga u Oak Ridgeu i Izraelu, dizajniran je vektor napada i modificiran kod.

Vjeruje se da je Stuxnet unsen preko USB-a, koji su unijeli agenti unutar nukleranih postrojenja, jer je bilo koji drugi način bio nemoguć, zbog sigurnosnih mjera koje izoluju kompjutere ili mreže i sprječavaju ih da ostvare vanjsku konekciju.

Kao što se može zaključiti, operativna okruženja su često odvojena od poslovnih, kako bi se osigurala najveća moguća sigurnost, te da bi se ta prepreka uspješno zaobišla, crv se replicirao u sustave i prijenosne medije kako bi se dalje uspješno širio.

Ako nakon određenog broja prijenosa malware[2] nije stigao do svog konačnog cilja (kontrolnih PLC-ova), prestao bi se širiti kako bi izbjegao pokretanje sigurnosnih kontrola. Još jedna od posebnosti ovog malwarea jeste sposobnost komunikacije sa poslužiteljima za zapovijedanje i kontrolu, pa čak i bez pristupa Internetu. Malware je komunicirao putem kompjutera i sustava, koja je već kompromitirao u mreži, pronalazeći put do interneta i prosljeđujući informacije nazad, omogućujući napadačima da modificiraju svoj kod čak i unutar postrojenja, što je značilo veliku prednost za napadače. (Kaspersky, 2018).

Još jedna, a možda i najbitnija prednost za napadače, jeste što za razliku od ranijih cyber napada koji su se dešavali, Stuxnet je iskoristio nekoliko prethodno nepoznatih ranjivosti u Windows sustavu, tzv. zero-day ranjivosti.

Kaspersky (2019), nagalašava da je Zero-day ranjivost softverska ranjivost koju napadači otkriju prije nego što proizvođač postane svjestan da ona postoji. Budući da proizvođači nisu svjesni tih ranjivosti, ne postoji zaštita od tih napada, što čini napade uglavnom vrlo uspješnima. Nekada mogu proći dani, pa čak i mjeseci prije nego što programeri identificiraju ranjivost koja je dovela do napada. Stuxnet je bio opremljen s ukupno četiri zero-day ranjivosti. Ranjivosti nultog dana vrlo su vrijedne hakerima, pa je korištenje njih četiri bilo neobično, ako ne i bez presedana.

Kaspersky (2019) ističe da se pored Zero-day ranjivosti, Stuxnet sastojao od tri dijela:

- Crva koji je obavljao većinu posla,
- Povezničke datoteke koja je automatizirala izvođenje kopija crva,

[2] Malver (eng. malware) je reč izvedena od dve reči – "Malicious Software", i predstavlja svaki softver koji je napisan u maliciozne svrhe, odnosno koji ima cilj da nanese štetu računarskim sistemima ili mrežama. Preuzeto sa: https://www.it-klinika.rs/blog/sta-je-malver-i-kako-se-odbraniti

- Rootkita koji je skrivao datoteke od otkrivanja.

Zero-day ranjivost je bila nepoznanica do slučaja Stuxnet, te je zapravo i jedan od glavnih razloga zašto je trebalo dugo vremena da se otkrije da su sistemi zaraženi virusom. Hakeri koristeći zero-day ranjivosti odmah steknu prednost, jer znaju da ih proizvođači neće biti u mogućnosti vidjeti određeni vremenski period, u kojem će već biti nanesena znatna šteta. To je zapravo i najveća prednost zero-day ranjivosti.

4.3. Djelovanje Stuxnet virusa

Prema Capano (2021), napadi zlonamjernim programima na računalno upravljana industrijska postrojenja postali su novi oblik ofanzivnog ratovanja. Specijalizirani zlonamjerni programi dizajnirani su u svrhu sabotaže i napada na programibilne logičke kontrolere (programmable logic controllers - PCL) kako bi ih onesposobili ili natjerali da rade izvan predviđenih parametara.

Stuxnet je prvobitno pokrenut već u junu 2009. godine, a njegov tvorac ga je ažurirao i usavršavao tokom vremena, objavljujući tri različite verzije. Jedan od pokazatelja koliko su bili odlučni da ostanu anonimni bilo je to što je jedna od datoteka drajvera virusa koristila validni potpisani certifikat ukraden od RealTek Semiconductor, proizvođača hardvera u Tajvanu, kako bi prevarila sisteme da misle da je malver pouzdan program od RealTek-a. (Rosenberg, 2017).

Središte operacije bio je laboratorij Natanz smješten usred pustinje oko 33 km od civilizacije. Postrojenje, tehnički poznato kao "postrojenje za obogaćivanje goriva", jedno je od 17 drugih iranskih nuklearnih postrojenja. Koristi centrifuge za koncentriranje i odvajanje U-235 od plina uran heksafluorida. U objektu je otprilike radilo 19.000 centrifuga.

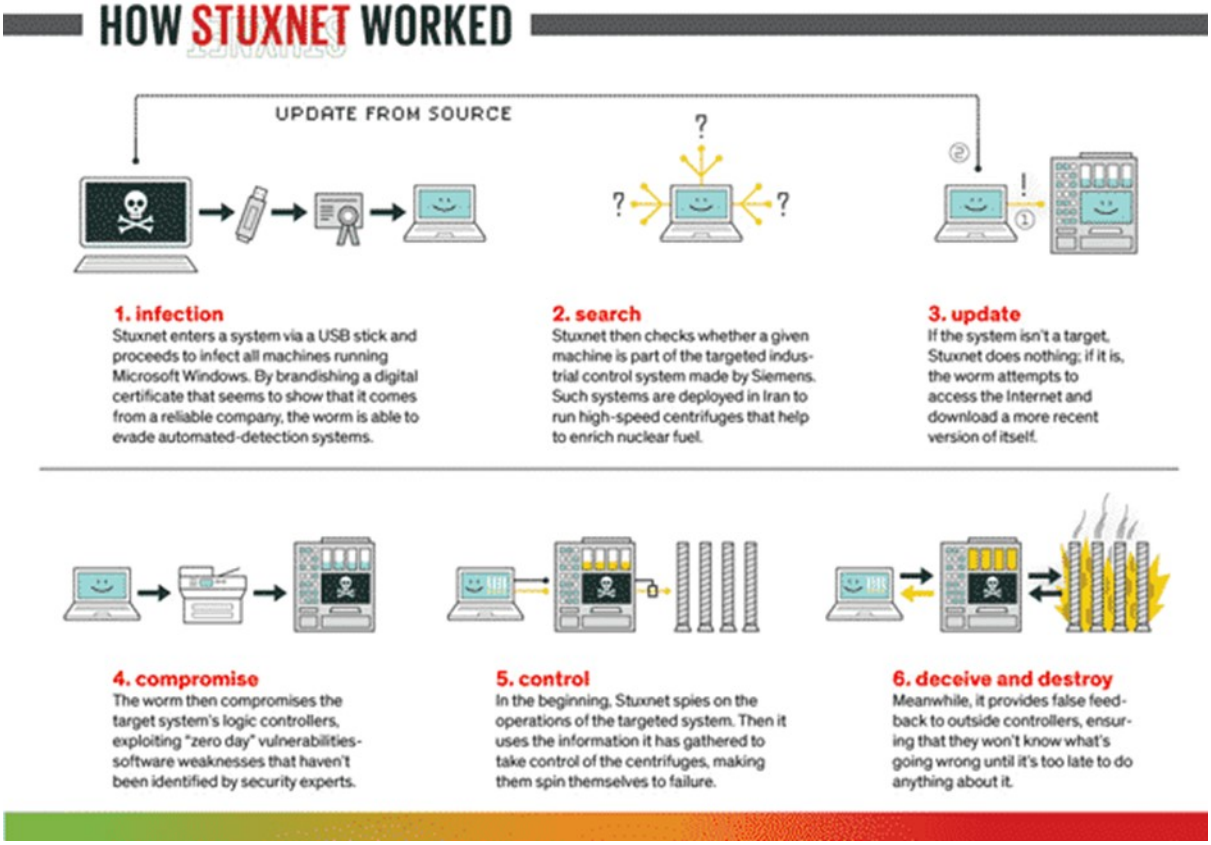
Natanz ima zračni otvor, jer je izoliran od vanjskog svijeta. Podzemno postrojenje za preradu je jako utvrđeno, prekriveno je sa 22 metra zemlje i projektirano je da bude neosvojivo, kako fizički tako i elektronički.

Prije napada Stuxnet, operativna okruženja i sustavi kritične nacionalne infrastrukture (CNI) smatrani su dovoljno izoliranim, nepovezanim i skrivenim da bi bili zaštićeni od cyber napada.

Stuxnet je bio skup za izradu. Procjenjuje se da je bilo potrebno 8 do 10 ljudi šest mjeseci da ga napišu. Tu je i postavljanje laboratorija—svakako bi bilo koja organizacija koja ulaže toliko truda

testirala stvar prije nego što je pusti—i prikupljanje obavještajnih podataka kako bi se tačno znalo kako ga ciljati. Osim toga, zero-day eksploiti su vrijedni. Teško ih je pronaći, a mogu se koristiti samo jednom. Onaj ko je napisao Stuxnet bio je spreman potrošiti mnogo novca kako bi osigurao da se zadatak za koji je bio namijenjen uspješno obaviti.

Dakle, Stuxnet ne djeluje kao kriminalni crv, ne širi se neselektivno, ne krade podatke o kreditnim karticama niti pristupne vjerodajnice računa, ne okuplja zaražena računala u botnet, te koristi višestruke zero-day ranjivosti. Kriminalna grupa bi pametnije napravila različite varijante crva i koristila po jednu u svakoj od njih. Stuxnet provodi sabotažu. Ne prijeti sabotažom, kao što bi mogla kriminalna organizacija koja želi iznuditi novac.



Slika 1. Prikaz Stuxnet napada (Dostupno na: https://gemserv.com/our-thoughts/stuxnet-the-first-cyber-weapon/)

Prvi korak operacije bilo je snimanje postrojenja i izrada tzv. Blueprinta.[3] U tu svrhu proizveden je zlonamjerni kod Beacon koji je ubačen sa ciljem mapiranja cijelog Natanz postrojenja, otkrivanja kako kontroliraju centrifuge, kako se odvija dnevna rutina i sl. Najbitnija informacija je kako su centrifuge povezane sa PLC-ovima (programmable logic controllers)?

Rotori kao najvažniji dijelovi centrifuge, okreću se na velikoj brzini i svaka centrifuga u nizu proizvodi čišću verziju Urana 235 od prethodne. Brzina na kojoj se okreće centrifuga je vitalna i ukoliko bi se brzina značajno povećala prijetila je raspadom sustava.

Ukoliko bi se sustav naglo zaustavio, također postaje nestabilan i ponaša se kao metalni tornado uništavajući sve u blizini uključujući i ljude koji rade u postrojenju. Upravo su ovo efekti koje je operacija "Olimpijske igre" trebala proizvesti.

PLC-ovi su računala koja upravljaju svim aspektima rada centrifuga i u to vrijeme su bili potpuno nezaštićeni. Podizanje takozvane "air gap1" zaštite podrazumijevalo se sigurnim od bilo kakvih zlonamjernih programa ili napada. Zaobilaženje „air gap" zaštite bio je prvi operativni problem tj. ubacivanje Beacona u sustav. U tu svrhu iskorišteni su djelatnici Siemensa koji su redovito servisirali PLC-ove, a koji nisu ni znali za operaciju tj. da su njihova računala nosioci Beacona.

Nakon nekoliko mjeseci rezultati tj. blueprints svih direktorija, elektroničkih komunikacija i što je najvažnije konfiguracija centrifuga stigle su u stožer operacije Olympic Games. NSA i Unit 8200 imali su materijal za početak rada na računalnom virusu kojeg su nazvali „bug". Nakon razvoja Bug je trebalo testirati na istim centrifugama koje je imao Iran, oznake P-1.

Iste centrifuge preko nekoliko ruku SAD je kupio od Muammera Qaddafia nakon što je 2003. odustao od nuklearnog programa. Nakon niza testova na nekoliko centrifuga Bug se pokazao vrlo uspješnim i akcija je mogla započeti. Kad je izveden prvi napad 2008. godine, inženjeri u Natanz postrojenju nisu bili ni svjesni napada već su mislili da se radi o grešci sustava. Od ukupno 5.000 centrifuga onesposobljeno je njih 984 i cijeli program je zaustavljen.

Jednom ubačen, kod je koristio druge ranjivosti za repliciranje i širenje kroz industrijske upravljačke sustave (ICS) koji nadziru i kontroliraju rad centrifuge. Crv je instalirao rootkite,

[3] Blueprint- fotografskim procesom dobiveni otisak tehničkog nacrta na posebnom papiru; nacrt, predložak- Dostupno na: https://jezikoslovac.com/word/x9ii

omogućujući potpunu kontrolu rada; Stuxnet je prva poznata upotreba programabilnog logičkog kontrolera (PLC) rootkita.

Zapovijedanje i kontrola nad crvom obavljali su se putem dvije web stranica smještenih u Danskoj i Maleziji, iako one nisu korištene nakon početnih faza operacije. Crv je također koristio ukradene digitalne certifikate za mnoge upravljačke programe kako bi se pokazao legitimnim.

Bio je sposoban inficirati računala bazirana na Windows operativnom sustavu, pokrivajući četiri generacije od Windows-a 2000 do Windows-a 7/Server 2008R2. Primarni cilj Stuxnet malwer-a, bio je sustav koji se sastoji od Siemens SIMATIC WinCC i PCS7 softvera, zajedno sa specifičnim modelima S7 PLC-ova koji koriste PROFIBUS protokol za komunikaciju s dva specifična dobavljača pogona s promjenjivom frekvencijom (VFD). Pogoni sa promjenjivom ferkvencijom su korišteni za kontrolu centrifuga, koje su se koristile u procesu obogaćivanja urana. (Wolf, 2015).

Kada se Stuxnet malware infiltrirao u sisteme, pretraživao je sve zaražene kompjutere u potrazi za Siemens Step 7 Softverima koji se koriste za automatizaciju i nadzor elektromagnetske opreme. Kada bi Stuxnet pronašao neophodni softver počeo bi ažurirati svoj kod i slati destruktivne upute kompjuterima. U isto vrijeme, Stuxnet bi ljudima koji kontrolišu i upravljaju sistemima, slao povratne informacije da je sve uredu sa sistemima, što znači da kontroleri ne bi shvatili do samog kraja da nešto nije uredu, tačnije dok se oprema ne bi sama uništila, što je izazivalo izrazitu konfuziju i nemogućnost da se brže otkrije Stuxnet. (Kaspersky, 2018).

Prema Rosenberg (2017), od prvobitnih 38.000 zaraženih sistema, oko 22.000 je bilo u ciljanom zemlji. Sljedeća najzaraženija zemlja bila je na dalekom drugom mjestu, sa oko 6700 infekcija, a treća po redu imala je oko 3700 infekcija. Sjedinjene Američke Države su imale manje od 400

U suštini, Stuxnet je manipulirao ventilima koji su pumpali plin urana u centrifuge u reaktorima u Natanzu. Povećavao je volumen plina i preopterećivao centrifuge koje su se vrtjele, uzrokujući njihovo pregrijavanje i samouništenje. Međutim, za iranske znanstvenike koji su promatrali ekrane kompjutera, sve je izgledalo normalno

Capano (2021) ističe da iranski operateri nisu mogli vidjeti šta se događa unatoč onome što su vidjeli na svojim ekranima. Centrifuge koje se okreću svojim nazivnim brzinama imaju karakterističan šum. Pri 59 000 okretaja u minuti centrifuga zvuči drugačije od one koja radi pri 84 000 okretaja u minuti. Svako ko je proveo vrijeme u postrojenju s velikom rotirajućom

opremom bilo koje vrijeme može čuti radi li mašina ispravno. Iskusni tehničari mogu čuti pokvareni ležaj ili druge mehaničke anomalije jednostavnim slušanjem. Nagađa se da je to glavni razlog zašto je Stuxnet imao ograničen učinak. Nakon brojnih kvarova, tehničko osoblje je moralo napraviti dijagnostički program za novinare na cijelom terenu koji je uključivao sva sredstva detekcije i rješavanja problema. To bi također uključivalo cjelovitu reviziju softvera za kontrolu.

Iako se ovo može činiti očiglednim u 2021., godini, to su bile neistražene vode u 2010. godini. Treba napomenuti da se nije očekivalo da će neko koristiti ofanzivno cyber oružje u bilo koju svrhu. Cyber oružje je do tada postojalo samo u konceptu, ili se tako barem samo mislilo.

Dakle, glavni cilj napada Stuxnet bio je kontrolisati centrfigue u pogonu, odnosno ubrzavati ih, kako bi se na kraju uništile i spriječile proces obogaćivanjem urana. Zato su se ciljali isključivo Siemens softveri, dok ostali nisu bili od interesa za napad.

Stvarni učinak napada Stuxnet pomalo je običan u usporedbi s popularnim percepcijama napada. Stuxnet nije rezultirao eksplozijama u postrojenju niti je bio brz proces. Razvoj i implementacija napada zahtijevali su značajno vrijeme i resurse. Utjecaj je bio polagano uzrokovanje štete na više od 1000 centrifuga u nuklearnom postrojenju u Natanzu, prilagođavanjem načina na koji su radile. Nije ponuđeno objašnjenje za operativno zaustavljanje, ali se sumnja da je to bilo kako bi se pregledale kontrole i sustavi pogođeni nakon otkrića malwarea.

Nedavno je otkriveno da su postojale čak i starije verzije Stuxnet-a koje su ostale neotkrivene niz godina. Prva je ciljala gasne ventile u nuklearnim reaktorima, a druga je ciljala jezgre reaktora. (Rosenberg, 2017).

Napad Stuxnet je bio evolucionaran za cyber sigurnost i cyber ratovanje. Zbog svoje sofisticiranosti i kompleksnosti, ali i vremena koje je bilo potrebno za izradu, smatra se prekretnicom za cyber ratovanje. Koristeći zero-day ranjivosti, odnosno mogućnost nevidljivosti izazvao je štetu na preko 1000 centrifuga u Natanz postrojenju, za koje se smatralo da je izuzetno čuvano i osigurano. To je zapravo bio početak odvijanja ratova u cyber prostoru i pokazatelj koliko cyber napadi mogu narušiti sigurnost jedne zemlje, a samim tim i okolnih zemalja, te nanijeti ekonomsku i druge oblike štete.

4.4. Misterija širenja Stuxneta

Uvijek je postojao određeni misterij iza toga kako je crv raspoređen u Natanzu. Prevladavajuća teorija je bila da su zaraženi USB pogoni postavljeni na mjestima koja je često posjećivalo tehničko osoblje Natanza, budući da je jedna od ranjivosti nultog dana dopuštala učitavanje zlonamjernog softvera s USB pogona bez obavijesti ili interakcije s operativnim sustavom nakon umetanja. Ova metoda je korištena kasnije u operaciji, ali na drugačiji način.

U početku je nizozemska obavještajna služba, AIVD, u suradnji s izraelskom obavještajnom službom, Mossadom, koristila etablirane krtice i paravan-kompaniju u Iranu za ubacivanje zlonamjernog softvera u sustave bez zraka na licu mjesta. To je bio rezultat nekoliko godina prikupljanja obavještajnih podataka u objektu.

Njemačka je također dostavila tehničke podatke o ICS-ovima koji kontroliraju rad centrifuge. Osim toga, SAD je zaplijenio pošiljku centrifuga, identičnu onima koje se koriste u Natanzu, na putu za Libiju. Te su centrifuge ponovno sastavljene u Oak Ridgeu u Izraelu – a potom su uništene ranim prototipom Stuxneta. Dijelovi uništene centrifuge bačeni su na konferencijski stol u prostoriji Bijele kuće kao dokaz koncepta njihovog plana, što im je dalo zeleno svjetlo za nastavak.

Crv je prvobitno dizajniran za zatvaranje ispusnih ventila centrifuga kako bi se stvorio pretjerani pritisak i otpadni plin – centrifuge rade u vakuumu, a plin se skrućuje pri niskom pritisku – trenutno uništavajući centrifugu. Ova metoda nije bila previše učinkovita; Iranci su pronašli zaobilazno rješenje i šteta je bila ograničena. Ova verzija crva ažurirana je na licu mjesta nekoliko puta kako je krtica promatrala više operativnih podataka i izvijestila ih konzorciju.

U ovom trenutku, izgubljen je pristup objektu iz nepoznatih razloga; također je moguće da više nije trebao pristup. Paralelno s operacijama ubrizgavanja na licu mjesta, nekoliko iranskih izvođača radova koji su izvodili radove u postrojenju bilo je kompromitirano ili su njihova računala bila zaražena drugom verzijom crva.

Vjerojatno su noviju verziju crva isporučili zaposlenici koristeći metodu podmetnutog USB pogona; međutim, bilo bi lakše zaraziti interne mreže izvođača. Crv ne napada računala, već je dizajniran za napad na softver za nadzornu kontrolu i prikupljanje podataka (SCADA) i PLC-ove.

Došlo je do problema: kako bi se osiguralo učinkovito širenje crva, napisan je kod za iskorištavanje prednosti nekoliko metoda širenja, što ga je učinilo promiskuitetnim i uzrokovalo da izmakne kontroli. Proširilo se na nekoliko drugih izvođačevih klijenata, a potom i na svijet. Nažalost, nekoliko ugovornih zaposlenika uhapšeno je i pogubljeno zbog unošenja crva u Natanz.

Promjene koje je uveo ovaj zlonamjerno uvedeni funkcijski blok bile su izuzetno male. Promjena je povećala brzinu okretanja centrifuga na Hz na 15 minuta, nakon čega su se centrifuge usporile na 50 minuta. Nakon tog razdoblja, vraćale su se na normalan rad dok je zlonamjerni kod ostao uspavan 27 dana. Ova izmjena kroz duže vremensko razdoblje uzrokovala je dovoljno fizičke štete centrifugama, tako da su se morale kontinuirano zamjenjivati.

Iako je napad imao izravan utjecaj na operacije iranskog postrojenja za obogaćivanje urana, Stuxnet je zaslužan za prikazivanje sposobnosti cyber napada da imaju izravan utjecaj na fizičke sustave i procese. (Kopfstein, 2012).

Iz navedenih činjenica, može se zaključiti koliko je zapravo bila kompleksna i zahtjevna operacija širenja Stuxnet crva u iranskom postrojenju Natanz. Za to je bila potrebna suradnja više obavještajnih službi, kako bi cilj bio ostvaren. Napad je pokazao da cyber napadi sada mogu imati uticaj na kritične infrastrukture i izazivati štetu na njima, što je do Stuxnet slučaja bilo nepoznanica.

4.6. Reakcija Irana nakon Stuxnet napada

Prema Capano (2021)., Iranci su brzo secirali kod i s razumnom sigurnošću utvrdili da SAD i njegovi saveznici stoje iza cyber napada. Širenje Stuxneta omogućilo je nekoliko tvrtki, ponajprije Symantecu, da izvrše reverzni inženjering koda i izvijeste o svojim pronalascima. Sjedinjene Američke Države i Izrael odmah su identificirani kao počinitelji, ali to nikada nije potvrdila ni jedna ni druga država. Prijavljeno je da su umiješane strane Agencija za nacionalnu sigurnost (NSA), Središnja obavještajna agencija (CIA) i Mossad, točnije Jedinica 8200, njihov ogranak signalne obavještajne službe (SIGINT).

Nakon otkrića napada Stuxneta i pripisivanja, Iran je krenuo u agresivan protunapad koji je uključivao firme i kritičnu infrastrukturu u obje zemlje i pokrenuo napade na koje se sumnjalo da su objekti u savezničkim zemljama. Na primjer, ARAMCO rafinerije bile su pogođene virusom Shamoon koji je izbrisao podatke s 30.000 računala. Osumnjičeni iranski hakeri ukrali su intelektualno vlasništvo (IP) brojnim firmama i univerzitetima.

Možda je najbolji primjer odlučnih aktera prijetnje bio iranski napad na kritičnu infrastrukturu koji nije bio samo najava onoga što će doći, već je također pružio neko olakšanje. Iranska Revolucionarna garda koristila je uobičajeno dostupne alate za traženje ranjive kritične infrastrukture. Njihov napad slijedio je klasične korake izviđanja, procjene i raspoređivanja. Njihovo izviđanje koristilo se Googleom. Postoji nekoliko tehnika pretraživanja i sintakse koje se nazivaju "Google Dorking". Pretvaraju Google iz jednostavne tražilice u moćan istraživački alat.

Sljedeći alat u njihovom arsenalu je Shodan, specijalizirana tražilica koja traži ICS-ove spojene na internet. Shodan se neprestano ažurira SCADA-om okrenutom prema internetu i samostalnim sustavima upravljanja.

Drugi vrlo koristan alat bili su društveni mediji. Na stranicama poput Facebooka i LinkedIna postoji riznica osobnih i profesionalnih podataka koje treba iskopati. Konačno, korišteni su i uobičajeni IT i alati za reviziju kao što su ICMP i SNMP.

Ono što su Iranci umjesto toga napali je brana Bowman Avenue u Rye Brooku, New York. Brana Bowman Avenue visoka je 20 stopa i široka 50 stopa, blokirajući poplavnu fazu Blind Brooka. Iranski tim pronašao je nezaštićeni bežični modem koji bi se koristio za daljinsko upravljanje

kliznim vratima brane (nije bio povezan s kontrolnim sustavom vrata). Nagađa se da je to bio vektor napada za branu Arthur Bowman; vrata brane bila bi otvorena ili zatvorena da izazovu poplavu ili preplavljivanje – bilo što bi predstavljalo problem, iako gubitak života nije vjerojatan.

Prema njihovoj procjeni, zanemarili su izviđanje terena. To je za njih dovelo do neuspjeha visokog profila, ali je ipak poslužilo kao poziv na uzbunu. Pokazalo je da svaki objekt može biti napadnut. Ovo je bio početak cyber rata.

Stuxnet je kao izuzetno kompleksna operacija i napad nanio izrazitu štetu Iranu i podstakao Iran, ali i ostale države na neopohodni razvoj cyber sigurnosti. Pokazao je i dokazao, da bez obzira koliko su zaštićene kritične infrastrukture, moguće je doći do njih i izazvati štetu. Kroz ovaj slučaj Iran je na svojoj koži naučio da se virus može i fizički unijeti, te ukazao i na potrebu za fizičkom zaštitom kritičnih infrastruktura i konstantnom kontrolom. Stuxnet napad je doprinio tome i da Iran počinje kao svoje oružje koristiti cyber napade, pa je tako kao odgovor na Stuxnet, napao branu Bowman Avenue u New Yorku, kako bi pokazao da nije bezopasan protivnik u cyber ratovanju.

4.7. Posljedice Stuxnet napada na Iran

Prema Centru za sigurnosne studije, ETH Zürich (2017) posljedice Stuxnet napada na Iran se ogledaju u :

- Socijalne i političke posljedice- Na domaćoj političkoj sceni, cyber napad je diskreditirao iransku vladu, jer iranske vlasti nisu bile u stanju zaštititi svoje nuklearne postrojenja od stranog cyber napada. Iranska vlada je izgledala neodlučno u vezi s time kako službeno reagirati na vijest da bi računarski crv mogao zaraziti njihova nuklearna postrojenja. Stuxnet nije imao gotovo nikakve izravne posljedice na iransko stanovništvo ili društvo. On je bio dizajniran tako da izbjegne kolateralnu štetu (Rosenbaum, 2012). Najveći utjecaj Stuxneta na društvo vjerojatno je bio osjećaj nesigurnosti, jer se upad u privatnu sferu nikada ne shvaća olako, pa se može pretpostaviti da su se Iranci osjećali izdano zbog neučinkovitih mjera cyber sigurnosti zemlje i njenog slabog stava prema počiniteljima.

Infekcija iranskih mreža pokazala je da, iako su mreže odvojene od interneta obično sigurnije od drugih mreža, ne mogu se smatrati dovoljno sigurnima (Zetter, 2014).

- Ekonomske posljedice- Ovaj napad također je imao izravne ekonomske posljedice za Iran. Budući da je Iran podložan međunarodnim embargom, nema pristup međunarodnim tržištima za kupovinu materijala povezanih s nuklearnim programom. Konkretno, ne može kupovati centrifuge, pa ih stoga izrađuje sam. Biti pod embargom također znači da Iran ima vrlo ograničene resurse, a kvar gotovo 1.000 centrifuga dodatno je povećao pritisak na zalihe materijala i proračune. S gledišta omjera troškova i koristi, loši rezultati u pogledu produktivnosti nuklearnog postrojenja u Natanzu mogli su dodatno opteretiti državne financije, jer je obogaćeni uran trebao biti kupljen iz drugih zemalja. Cyber napad također je imao dugoročne ekonomske posljedice za Iran jer je morao upravljati kašnjenjima u proizvodnji nisko obogaćenog urana. Uvođenje novih sigurnosnih i cyber mjera u nuklearnim postrojenjima kako bi se spriječilo ponavljanje napada poput Stuxneta također bi zahtijevalo značajnu financijsku investiciju. Na primjer, Iran je 2011. godine stvorio novu cyber jedinicu unutar Revolucionarne garde kako bi se nosila s cyber napadima (Fogarty, 2011).
- Tehnološke posljedice- Stuxnet napad je također direktno utjecao na tehnološki sektor. Kompanije koje su razvile softver sa ranjivostima koje su iskorištene za infekciju i kontrolu računara u Iranu bile su primorane da reaguju kako bi obuzdale crv. Dugoročne tehnološke posljedice Stuxneta su evidentne u tome što Iranci s većim stepenom nepovjerenja pristupaju tehničkim kvarovima u svojim postrojenjima, jer svaki bug ili kvar može izazvati sumnju na još jedan kibernetički napad na iranske sisteme.
- Međunarodne posljedice- Na međunarodnom nivou, cyber napad je uspio da odgodi iranski program obogaćivanja urana na kratak period i tako donekle smanji povezane međunarodne tenzije. Čini se da su kašnjenja u programu dovoljna da umire Izrael, tako da ne bi rizikovao pokretanje vazdušnog udara kako bi fizički zaustavio obogaćivanje. Na međunarodnom nivou, kreator Stuxneta, iako njegova identitet ostaje neizvjestan, pokazao je da je moguće izgraditi visoko sofisticiran ofanzivni cyber alat, te da počinitelji imaju resurse za ostvarivanje takvog napada. Štaviše, ovaj slučaj pokazuje da odvajanje kritične infrastrukture od interneta više ne može biti smatrano adekvatnom sigurnosnom mjerom. Države su shvatile da moraju preduzeti mjere kako bi izbjegle postati žrtve napada ovog

tipa. Nekoliko država, uključujući Iran, naknadno je investiralo u cyber sigurnost ili osnovalo vojne cyber jedinice i/ili centre kako bi ojačali svoje sposobnosti u slučaju nadolazećeg cyber rata. Neke države su također počele preispitivati i ažurirati svoje cyber strategije kako bi obuhvatile kritičnu infrastrukturu i ojačale svoju sposobnost da pravno odgovore na cyber napade. Druga posljedica Stuxnet cyber napada bila je činjenica da je crv iscurio i proširio se na druge računare van Irana. Imati malware u javnoj upotrebi značilo je da bi bilo ko s pravim kompetencijama mogao da ga analizuje, modificira za druge svrhe, proda ili upotrijebi.

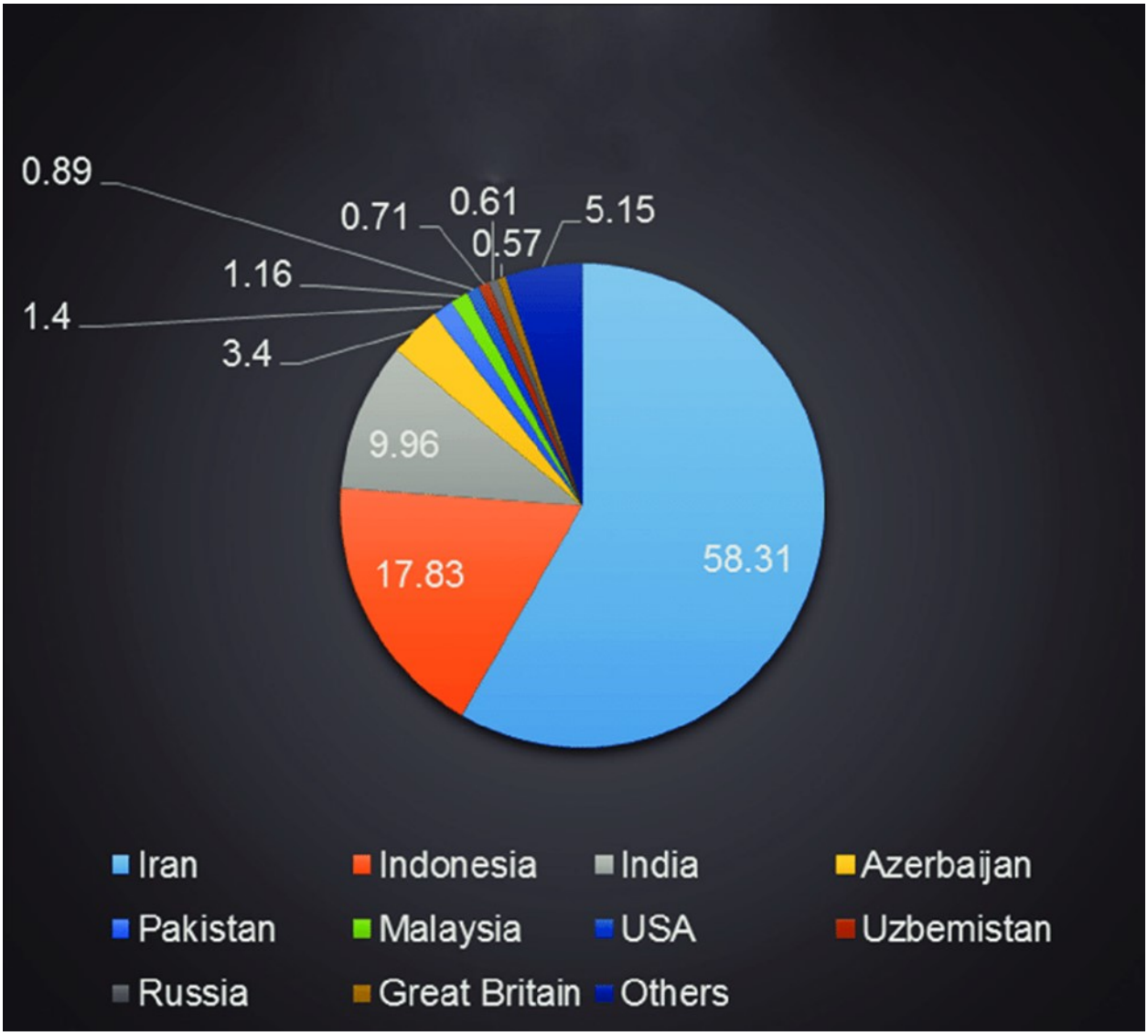
Navedene posljedice nam ukazuju da cyber napad ne ostavlja samo ekonomske posljedice, nego doseže mnogo širi spektar posljedica sa kojima se države moraju suočavati. Potrebno je sanirati načinjenu štetu, ulagati u cyber sigurnosne sisteme, poslati sliku svijetu da je Iran država koja je zapravo sposobna da adekvatno odgovori na cyber prijetnje i pruži svojim građanima neophodni osjećaj sigurnosti. Na međunarodnom planu je potrebna saradnja svih država, jer ukoliko bi se desilo da crv procuri, nema veze koja je država napadnuta, može se proširiti i nanijeti štetu svim ostalim državama. Globalizacija je doprinijela tome da se problem koji se dešava u jednoj zemlji, osjeti i na durgim zemljama, te su ozbiljne stvari poput cyber napada postali globalni problem, koji iziskuje rješenja prvenstveno na međunarodnom nivou.

V CYBER SVIJET NAKON STUXNETA

Kompanije koje se bave zaštitom informacijskih sustava, otkrile su vektore napada i vremenom su došle do vrlo zanimljivih informacija pa je osim Stuxneta otkriveno još nekoliko zlonamjernih programa koji su također proizvedeni u cilju napada na računalno upravljane proizvodne sustave i infrastrukturu određenih zemalja.

Stuxnet je otkriven u mnogim zemljama, kao što se vidi na slici br. 2., u julu 2010. godine, Stuxnet je otkriven osim Irana u Maleziji i Indiji. Navedeni primjer pokazuje cijeli niz propusta u sigurnosnom sustavu i politici sigurnosti, za koju možemo zaključiti ili da je nije bilo ili je se nisu pridržavali. Kako se radilo o visokorizičnom industrijskom postrojenju u svakom pogledu, začuđuje količina propusta u sigurnosnom sustavu:

- Potpuno nepravilno rukovanje korisničkim imenima i šiframa – Ne korištenje nikakvog mehanizma zaštite na korisničkom nivou (pametne kartice, kriptografija i sl.)
- Održavanje sustava nije rađeno
- Serviseri računara nisu provjeravani, te nije provjeravana njihova oprema
- Spajanje na mrežu vanjskim računarima i prijenosnim diskovima
- Upravljanje s podatkovnim medijima
- Uvjerenje da je “air-gap” zaštita dovoljna
- Upravljanje podacima i zaštita podataka
- Pristup mrežnim resursima iako su dijelovi mreže segmentirani
- Međusobno povezivanje segmenata mreže nije odrađeno na siguran način
- Zaštita od zlouporabe očito nije postojala i evidencija o zlouporabi nije postojala
- Kompletna politika upravljanja kontinuitetom poslovanja nije postojala
- Neadekvatna politika fizičke sigurnosti ili ne pridržavanje iste
- Neadekvatna politika zaštite osoblja i događanja ili ne pridržavanje iste
- Politika internih istraga – prve naznake nepravilnosti rada nisu dovele do aktiviranja



Slika 2. Rasprostranjenost Stuxneta po državama

(Dostupno na: https://www.researchgate.net/figure/Stuxnet-infection-geographic-distribution-Murchu-2011_fig2_321028312)

Cyber ratovanje je sada preferirani način vođenja sukoba između nacionalnih država. Dok su Stuxnet i njegovi rođaci uveli u eru cyber ratovanja, ovu veliku promjenu u međunarodnim odnosima zasjenio je nedavni val napada ransomwarea koji su ciljali kritičnu infrastrukturu. Jedna pojava dogodila se na Floridi u februaru, gdje je spriječen napad na postrojenje za pročišćavanje vode; ovaj napad je bio sličan napadu na izraelsko postrojenje za obradu vode.

Kako se paradigma međunarodnih odnosa pomiče s otvorenog, fizičkog sukoba na virtualni rat, imperativ je da počnemo prepoznavati da smo svi odgovorni ne samo za vlastitu sigurnost, već i za institucije na koje se oslanjamo u svom načinu života. (Capano, 2021).

Žagar (2016), navodi da se razvojem digitalnih tehnologija i sveobuhvatnom povezanosti kao i porastom znanja i sposobnosti korisnika, za očekivati je nove načine i vještine za provedbu napadačkih digitalnih strategija. Budući ratovi mogli bi se voditi i pobjeđivati bez ispaljenog metka. Napadač može pritiskom gumba zatvoriti cjelokupnu nacionalnu infrastrukturu napadnute strane te kompletno kontrolirati ili uništiti njegovu infrastrukturu, postrojenja, komunikacijske mreže i sl.

Drugim riječima čak i država bez sposobnosti izvršavanja konvencionalnog napada može pokrenuti kibernetički napad. Ovakve prijetnje zahtijevaju razvoj i implementaciju novih Internet arhitektura otpornijih na cyber ratovanje. To bi podrazumijevalo kodiranje sa snažnim sigurnosnim elementima, znatno snažniji sustav kontrole upada, razvoj sigurnijih operacijskih sustava te izradu i striktno primjenjivanje politika sigurnosti.

U pogledu cyber ratovanja Stuxnet predstavlja dosad najsloženije i najopasnije digitalno oružje ikad izrađeno. Prije otkrivanja Stuxneta, zlonamjerni programi koristili su se u svrhe hakiranja računala, ostvarivanja nelegalne zarade, dolaska do povjerljivih informacija ili iz razloga dokazivanja i sl. Ima primjera korištenja zlonamjernih programa tj. cyber napada od strane država na druge države, poput Rusije na Gruziju ili Čečeniju, Izraela na Palestinu i sl., ali ne u ovako kompleksnim operacijama.

Stuxnet je pokazao kako se zlonamjerni računalni program može koristiti kao ofanzivno cyber oružje i time je vjerojatno otvorena Pandorina kutija u pogledu mogućih terorističkih napada na ciljeve koji koriste SCADA ili slične sustave. U prilog tomu ide i izjava bivšeg ministra obrane Velike Britanije kako su nuklearne podmornice Trident ranjive na cyber napade.

Nakon Stuxnet napada, lideri zemalja su počeli shvatati ozbiljnije cyber sigurnost i adekvatnosti fizičke sigurnosti u nuklearnim postrojenjima suočenim s prijetnjama terorizma. Kao rezultat toga, zemlje su poduzele važne korake za jačanje nuklearne sigurnosti na domaćem planu, a mnoge međunarodne organizacije—Međunarodna agencija za atomsku energiju (IAEA), Svjetski institut za nuklearnu sigurnost (WINS), Ujedinjeni narodi i Nuklearni sigurnosni samiti, među ostalima—pokrenule su napore za poboljšanje međunarodne pripreme, prevencije i odgovora. (Van Dine, 2017).

Van Dine (2017) ističe da je posljednjih desetljeća došlo do proliferacije digitalnih tehnologija u nuklearnoj industriji. Ove tehnologije donose stvarne prednosti u smislu sigurnosti i fizičke zaštite; međutim, one također stvaraju cyber ranjivosti koje često ostaju neanalizirane ili čak neprimijećene. Više digitalizacije znači više iskoristivih slabosti, čime se stvara dinamična i sveprisutna prijetnja koja opterećuje nacionalne i međunarodne vlasti podjednako.

Štaviše, terorističke organizacije poput al Qaede i Islamske države Iraka i Levanta (ISIL) nastoje steći radiološke i nuklearne sposobnosti i naglašavaju napade koji maksimalno povećavaju paniku i uništenje. Cyber ranjivosti bi se mogle iskoristiti u postizanju tih ciljeva.

Vladine vlasti, nacionalni regulatori, nuklearna industrija i međunarodne organizacije prepoznale su cyber prijetnju nuklearnim postrojenjima i poduzimaju korake za razvoj i implementaciju rješenja. Na primjer, u Sjedinjenim Državama, Nuklearna regulatorna komisija (NRC) i Ministarstvo domovinske sigurnosti (DHS) definirali su uloge u prevenciji i odgovoru na mogući cyber napad na nuklearno postrojenje.

Međunarodne organizacije također su preuzele svoju ulogu, pri čemu IAEA posebno naporno radi na pružanju mogućnosti obuke za regulatore i osoblje postrojenja širom svijeta, razvijanju i distribuciji smjernica te olakšavanju međunarodnog dijaloga o toj temi. Nuklearna industrija također je bila lider u ovom području, s Nuklearnim industrijskim summitom koji okuplja međunarodnu radnu grupu predstavnika industrije kako bi razmotrili prijetnju, razvili rješenja i skrenuli pozornost na cyber sigurnost na visokoj razini. Činjenica da će ova grupa nastaviti sastanke, čak i u nedostatku nastavka Nuklearnih sigurnosnih summita, pokazuje predanost industrije ublažavanju ove prijetnje.

Iako su svi ovi napori korisni i nužni za poboljšanje globalne cyber-nuklearne sigurnosti, svijet je i dalje nedovoljno pripremljen za suočavanje s ovom dinamičnom prijetnjom. Trenutni pristup nije u stanju kretati se tako brzo i fleksibilno kao cyber prijetnja i neravnomjerno se primjenjuje geografski. Previše zemalja s nuklearnim materijalima ili visokorizičnim nuklearnim postrojenjima nema odgovarajuće pravne i regulatorne okvire u ovom području. Ograničeni ljudski kapacitet koji postoji na spoju cyber i nuklearne sigurnosti je snažno koncentriran u Sjevernoj Americi, Europi i Rusiji, što znači da mnoge zemlje s novim ili proširujućim nuklearnim programima nemaju potrebnu tehničku stručnost.

VI ZNAČAJ STUXNET NAPADA ZA CYBER SIGURNOST

Stuxnet je jedan od najvažnijih i najznačajnijih događaja, koji je u potpunosti promijenio pogled na cyber sigurnost, uz izuzetan doprinos razvoju cyber sigurnosti. Prije Stuxnet napada cyber sigurnost se uglavnom svodila na zaštitu podataka, zaštitu od krađe identiteta, Internet prevara i slično, dok je Stuxnet svojom sofisticiranošću i složenošću pokazao da se mora puno ozbiljnije pristupiti cyber sigurnosti. Danas, ako postoji prijetnja koja dolazi od Stuxneta, onda je to ona koja proizlazi od njegovih nasljednika.

Kao što smo već napomenuli, postoje druge porodice malwarea koje izgleda imaju funkcionalnost izvedenu iz Stuxneta; one mogu potjecati iz iste obavještajne agencije, ili mogu predstavljati freelance hakere koji su uspjeli reverzno inženjerirati dio Stuxnetove moći.

Istraživači sigurnosti i dalje se oslanjaju na Stuxnet kako bi otkrili nove tehnike napada. Ali osim specifičnih tehnologija, Stuxnet je značajan jer je predstavljao prvo široko prepoznato ubacivanje kompjuterskog koda u svijet međunarodnih sukoba U desetljeću koje je nakon toga uslijedilo, posebno u sukobu između Rusije i Ukrajine, cyber napadi su postali prihvaćeni dio ratnog arsenala. Dakle, možemo zaključiti da je Stuxnet podstakao mnoge novonastale tehnike cyber napada, ali i izuzetno doprinio da cyber napadi postanu svakodnevnica i koriste se čak i u konvencionalnim ratovima, kako bi se oslabio neprijatelj.

Stuxnet virus je ostavio značajne posljedice na Iran, ali i svijet nakon što je otkriven i nakon posljedica koje su nastale zbog njegove sofisticiranosti i učinka. On nije imao samo posljedice po ključnu infrastrukturu i razvoj potencijalnih budućih oružja za sajber napade, već je pokazao i značaj za nukleranu sigurnost, kao i teroriste. Stuxnet napad je pokazao da se vrlo lahko može doći do sistema koji se koriste za pravljenje oružja za masovno uništenje i preuzeti se kontrola nad njima, dok se ljudima koji provjeravaju i kontrolišu sisteme, čini da je sve u najboljem redu, a posljedice u tom slučaju bi bile katastrofalne.

Ono što je možda i najveći problem jeste što je Stuxnet kod dostupan online i pitanje je vremena prije nego što se sličan napad opet desi, te je iz tih razloga neophodno ulagati u cyber sigurnost, iako mnoge države to ne shvataju ozbiljno, koliko bi trebale.

6.1. Preporuke za budućnost nakon Stuxneta

Naoružani Stuxnetovim lekcijama, čelnici danas mogu poboljšati globalnu spremnost i konstruirati učinkovite obrane. Sljedeće preporuke zahtijevaju kontinuirano ulaganje resursa, financija, intelektualnih resursa i drugih, te oni također predstavljaju prijeko potreban napredak prema sveobuhvatnoj sigurnosti koju svijet treba.

- Trenutačni pristup cyber sigurnosti u nuklearnim postrojenjima mora biti iz temelja promišljena. Nova strategija, utemeljena na tehnički ispravnoj i okrenutoj budućnosti načela, moraju se razviti kako bi se odgovorilo na ovu dinamičku prijetnju.

Unatoč stalnim naporima Međunarodne agencije za atomsku energiju, Svjetskog instituta za nuklearnu sigurnost, Ujedinjenih naroda, i raznih nacionalnih inicijativa posljednjih su se godina vidjeli primjeri za primjerima uspješne infiltracija u nuklearne objekte zlonamjernim softverom, ciljano ili na drugi način. Ovi slučajevi sami pokazuju nedostatak adekvatnog pristupa kada su u pitanju cyber prijetnje. Kako bi se adekvatno odbranili od dobro financiranih, ciljanih cyber napada na postrojenja koji bi mogli uzrokovati značajnu štetu, potreban je svjež pogled na ono što je potrebno za odbranu od istih.

U slučaju Stuxnet, malware se uspio infiltrirati u objekt iz dva ključna razloga. Prvo, organizacijsko pretjerano oslanjanje na zračne praznine za zaštitu mreža od napada, stvorilo je lažni osjećaj sigurnosti, a napadači su to mogli iskoristiti u svoju korist. Drugo, digitalni sustavi korišteni za održavanje i rad iranskih centrifuga IR-1 bili su vrlo složeni i stoga vrlo ranjivi. Nova strategija cyber sigurnosti u nuklearnim postrojenjima mora se pozabaviti sa oba ova faktora.

- Treba se fokusirati na smanjenje upotrebe digitalnih tehnologija u kritičnim infrastrukturama objetka, te smanjenje kompleksnosti u najvažnijim sustavima. Uklanjanje ovih poznatih multiplikatora ranjivosti iz objekata, bio bi važan korak prema višem stanju sigurnosti.
- Države moraju ulagati u sposobnosti odgovora u zemlji i na međunarodnom nivou. Čak i ako bi savršena sigurnosna politika mogla biti napisana sutra, još uvijek će trebati nekoliko godina da se provede. Tokom svog tog vremena, mogućnost cyber napada s ozbiljnim fizičkim posljedicama i dalje bi postojala.

- Svaka zemlja mora imati jasno artikuliran plan brzog odgovora, sa svim odredbama potrebnim za olakšavanje međunarodne suradnje. Štaviše, one zemlje koje imaju koristi od većeg broja cyber-nuklearnih stručnjaka trebale bi raditi na tome da razviju načine za dijeljenje ove stručnosti sa zemljama kojima je potrebna za prevenciju ili odgovor na cyber incidente.

Što se tiče prevencije, stručnjaci bi se mogli konsultirati s upraviteljima objekata na tome koji su to koraci, koji se mogu odmah poduzeti za poboljšanje zaštite od cyber napada. Ako se cyber napad odvija u trenutku, ti isti ljudi mogli bi se staviti na raspolaganje kako bi pomogli odgovoriti ili, barem za pomoć u analizi nakon incidenta. Nuklearna bi industrija mogla igrati važnu ulogu za olakšavanje tih veza.

- Međunarodna zajednica mora raditi na izgradnji globalnih ljudskih kapaciteta u ovom području. Postizanje održive strategija za ublažavanje ove prijetnje zahtijeva dovoljno talenta za razvoj i provedbu. Ovaj se cilj može postići jačanjem globalne cyber-nuklearne zajednice i olakšavanjem veze preko granica, tražeći prilike za potporu ili poticanje obrazovanja programa koji su usmjereni na cyber-nuklearne edukacije, te financiranje i podrška programima obuke u zemlji i na međunarodnom nivou radi poboljšanja i izgradnje stručnosti u ovom području. (Van Dine, 2017).

Stuxnet napad je otvorio oči i ukazao na potrebu za jačanjem cyber sigurnosti. Međunarodna zajednica sa liderima zemalja mora razvijati strategije koje će biti adekvatne za odgovor na cyber napade. Uposlenicima u sigurnosnim institucijama, ali i samim građanima mora biti pružena adekvatna edukcija za cyber sigurnost i cyber prijetnje. Cyber prijetnje i cyber ratovi tek doživaljavaju svoj razvoj, te smatramo da će se u godinama koje dolaze ratovi voditi isključivo u cyber prostorima. Vrlo je bitno prepoznati prijetnju na vrijeme, dok nije napravila nesrazmjernu štetu, te se mora konstantno raditi na povećanju kapaciteta cyber stručnjaka.

Svaka zemlja bi trebala imati plan šta da uradi konkretno, ako bi došlo do cyber napada, jer prva reakcija je možda i najvažnija kako bi se spriječila šteta. Ono što je možda i najvažnije, jeste da se oprezno radi sa digitalnim sistemima na mjestima koja su izuzetno osjetljiva npr. nuklearna postrojenja. Tu treba obratiti posebnu pažnju na računalne sustave i smanjiti najviše moguće sve digitalne pristupe u takvim postrojenjima, jer ukoliko bi došle određene informacije u ruke ljudi u koje ne smiju doći npr. terorista, moglo bi završiti katastrofalno.

ZAKLJUČAK

Kao rezultat ovog istraživanja, može se potrvditi glavna hipoteza u radu, tačnije da je Stuxnet napad zaista svojim djelovanjem promijenio cyber prostor u 21. stoljeću i ukazao na potrebu povećanja kapaciteta država na polju cyber sigurnosti i njihovog kontinuiranog unaprjeđivanja. Pored toga, dokazane su i posebne hipoteze, dakle da je Stuxnet napad je promijenio pogled na cyber sigurnost i cyber ratovanje i druge.

Uz svoju efektivnost I posljedice koje je ostavio na iranska nuklerana postrojenja, te uz razvoj digitalnih tehnologija, koje su postale svakodnevnica ljudskog života, ukazao je na izrčitu potrebu za jačanjem cyber sigurnosti i insipirsao je mnoge cyber ratove. Cyber ratovi se danas biraju umjesto konvecnionalnih ratova, te napadači mogu napraviti štete kritičnim infrastrukturama država, sa drugog kraja svijeta, što se u prošlosti nije moglo ni zamisliti. Države koje nisu vojno jake i konkurente, mogu biti izuzetno spremne za cyber napade, te se u cyber prostoru mogu očekivati cyber napadi i od slabije opremljenih država, pojedinaca i sl.

Stuxnet napad je pokazao da ne postoji nikakva prepreka i potupno efektna zaštita, kada je ovako opasan virus mogao bit unesen u izuzetno zaštićeno mjesto i kada danima nije primjećena šteta koju Stuxnet pravi, jer je prilikom kontrola sistema sve izgledalo potpuno normalno. Međutim, kroz primjer Stuxneta se može vidjeti koliko je zapravo osjetljiva kritična infrastuktura, koja je od izuzetne važnosti za svaku državu. Prije Stuxnet napada, cyber napadi su se uglavnom odnosili na hakiranje računara, krađu podataka, za prodaju informacija koje se skupe kako bi se stekao određeni profit, ali specifičnost i važnost Stuxneta jeste upravo u tome, što je on pokazao koliko je zapravo opasan i da se virusi poput njega mogu koristiti i za cyber ratovanje, čemu države postaju sve više naklonjene i cyber prostor postaje peti prostor za izvođenje vojnih dejstava.

Obzirom da se cyber prijetnje razvijaju i napreduju svakodnevno, potrebna je saradnja međunarodne zajednice kako bi se adekvatno odgovorilo na cyber napade i pokušala smanjiti nanesena šteta. Stuxnet je pokazao da osim ekonomske štete, ovako opasan napad može narušiti i međunarodne odnose i diplomatiju, ali sa druge strane može protivnicima obezbjediti veliku prednost i nanijeti nesagledivu štetu, te sa tim ostvariti svoj cilj napada.

Na samom kraju, možemo zaključiti da je cyber sigurnost danas postala jedan od najvažnijih aspekata funkcionisanja državnih struktura, te zbog toga je neophodno da se razvija, da države

osim obuka uposlenika koji su zaduženi za cyber sigurnost, obučavaju i građane kako da prepoznaju kada su ugroženi od mogućeg napada i kako da se zaštite. Cyber prijetnje su postale svakodnevnica i nemoguće ih je u potpunosti spriječiti, ali uz adekvatne obuke i inovacije, te međunarodnu saradnju, moguće ih je prevenirati ili ublažiti.

4. SPISAK INICIJALNE LITERATURE

1. Andress, J., & Winterfeld, S. (2012). The basics of cyber warfare: Understanding the fundamentals of cyber warfare in theory and practice. United States: Elsevier.
2. Alvarez, J. (2015). Stuxnet: The world's first cyber weapon. Stanford: Center for International Security and Cooperation. Dostupno na: https://cisac.fsi.stanford.edu/news/stuxnet, (Datum pristupa: 30. 03. 2024.)
3. Antoliš, K .(2010). Internetska forenzika i cyber terorizam, Policija i sigurnost, Zagreb.
4. Azinović, V. (2013). Terorizam-fenomenološka analiza, Demokracija i sigurnost u Jugoistočnoj Evropi. Sarajevo: Atlantska inicijativa: Udruženje za promicanje euroatlantskih integracija BiH.
5. Azinović, V. (2019). Uvod u studije terorizma, Sarajevo.
6. Babić, V. (2015). Cyber terorizam- Suvremena sigurnosna prijetnja, Novi Travnik.
7. Babić, V. (2015). Novi oblici djelovanja terorista (cyber terorizam). Zbornik radova, Zagreb: Ministarstvo unutarnjih poslova Republike Hrvatske i Policijska akademija. Dostupno na: http://bib.irb.hr/datoteka/763755.Zbornik_radova_Konferencije.pdf , (Datum pristupa: 31. 03. 2024.)
8. Babić, V. (2009).. Kompjuterski kriminal, Sarajevo: Rabic.
9. Beridan, I., (2008.) Politika i sigurnost. Sarajevo: Fakultet političkih nauka
10. Beridan, I., Tomić, M. i Kreso, M. (2001). Leksikon sigurnosti, Sarajevo: "DES".
11. Buxton, O. (2024). Stuxnet: What Is It & How Does It Work?, Dostupno na: https://www.avast.com/c-stuxnet , (Datum pristupa: 27. 03. 2024.)
12. Capano, D. E., (2021). Throwback attack: How Stuxnet changed cybersecurity. Industrial Cybersecurity Pulse.
    Dostupno na: https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-how-stuxnet-changed-cybersecurity/ . (Datum pristupa: 25.07.2024.)
13. Cluley, G. (2024). Stuxnet: The malware that cost a billion dollars to develop? Dostupno na: https://grahamcluley.com/stuxnet-the-malware-that-cost-a-billion-dollars/ (Datum pristupa: 10.08.2024.)

14. Deep, A. (2015). Hybrid War: Old Concept, New Techniques. Small Wars Journal. Dostupno na:https://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques,(Datum pristupa: 18.03. 2024.)
15. Denning, E. D. (2012). Stuxnet: What Has Changed?. Naval Postgraduate School, Monterey, USA, Department of Defense Analysis.
16. European Union Agency for Cybersecurity (2021.), ENISA Threat Landscape 2021 [epublikacija], Dostupno na: https://www.enisa.europa.eu/publications/enisathreat-landscape-2021 , (Datum pristupa: 28. 04. 2024)
17. Fischer, I. (2017). Virus koji je zarazio računala diljem svijeta zapravo je napad na Ukrajinu, nije stvoren da bi zaradio novac, stvoren je da napravi štetu: Jutarnji list. Dostupno na: https://www.jutarnji.hr/life/tehnologija/virus-koji-je-zarazio-racunala-diljem-svijeta-zapravo-je-napad-na-ukrajinu-nije-stvoren-da-bi-zaradio-novac-stvoren-je-da-napravi-stetu-6315637 , (Datum pristupa: 31. 07. 2024.)
18. Gemserv. (2019). Stuxnet – The First Cyber Weapon. Dostupno na: https://gemserv.com/our-thoughts/stuxnet-the-first-cyber-weapon/ . (Datum pristupa: 28.07.2024.)
19. Gligorević, R.(2014). Cyber kriminal. Digitalna ekonomija-Digital Economics, 163-174.
20. Heijden, R., Dietzel, S., Leinmuller, T. i Kargl, F. (2019). Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems. IEEE Communications Surveys & Tutorials 21(1)
21. Helmbrecht, U., Purser, S., Klæstrup, R., "Cyber Security: Future, challenges andopportunities". European network and information Security agency (eniSa), 2011.
22. Kamiński, M. A. (2020). Operation "Olympic Games." Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran's nuclear programme. Security and Defence Quarterly. Dostupno na: https://securityanddefence.pl/Operation-Olympic-Games-nCyber-sabotage-as-a-tool-of-American-nintelligence-aimed,121974,0,2.html . (Datum pristupa: 08. 06. 2024.)
23. Kaspersky. (2018.) "What Is Zero Day Exploit?", Dostupno na: www.kaspersky.com/resource-center/definitions/zero-day-exploit . (Datum pristupa: 21.07. 2024.)

24. Kenney, M. (2015). Cyber-Terrorism in a Post-Stuxnet World. Foreign Policy Research Institute by Elsevier Ltd.
25. Kopfstein, J. (2012). Stuxnet virus was planted by Israeli agents using USB sticks, according to new report. The Verge. Dostupno na: https://www.theverge.com/2012/4/12/2944329/stuxnet-computer-virus-planted-israeli-agent-iran . (Datum pristupa: 21. 06. 2024.)
26. Maclean, W. (2010). Stuxnet study suggests Iran enrichment aim-experts. London: Reuters. Dostupno na: https://www.reuters.com/article/security-cyber-stuxnet-idUSLDE6AF0FX20101116/, (Datum pristupa: 26. 02. 2024.)
27. Mladenović, D. (2016) "Multidisciplinarni aspekti sajber ratovanja" doktorska disertacija Beograd. Dostupno na: https://nardus.mpn.gov.rs/handle/123456789/6880 , (Datum pristupa: 19. 06. 2024.)
28. NACIONAL.HR (2020). IT PRIJETNJA: Cyber terorizam i kolaps civilizacije. Dostupno na: https://www.nacional.hr/it-prijetnja-cyber-terorizam-i-kolaps-civilizacije/ . (Datum pristupa: 15. 03. 2024.)
29. Porobić, M. i Bajraktarević, M.(2012). Cyber kriminal, pranje novca i finansijske istrage.Sarajevo
30. Rendulić, I. (2021). Informacijska sigurnost i cyber sigurnost - koje su razlike? Dostupno na: https://duplico.io/informacijska-sigurnost-i-cyber-sigurnost/ , (Datum pristupa: 01. 08. 2024.)
31. Rudeš, I., Pavelić, I. (2023). Cyber-rizik, fenomen koji postoji i ugrožava nas. Zbornik sveučilišta Libertas.
32. Sheldon, J. B. (2024). cyberwar. Encyclopedia Britannica.
33. Singer P. W. (2015). Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons. Case Western Reserve Journal of International Law. Dostupno na: https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1009&context=jil, (Datum pristupa: 27.03.2024.)
34. Spremić, M., Šimunic, A. (2018.), Cyber security challenges in digital economy, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering WCE 2018, pp. 341-347, IAENG, Hong Kong.

35. Šipek, D. (2022). Cyber ratovanje – potpuno novi oblik ratovanja. Dostupno na: https://duplico.io/cyber-ratovanje-potpuno-novi-oblik-ratovanja/ . (Datum pristupa: 03.08.2024.)
36. Termiz, Dž. (2022). Metodologija društvenih nauka: treće izmjenjeno i dopunjeno izdanje Politički fakultet Univerziteta u Sarajevu i Međunarodno udruženje metodologa društvenih nauka.
37. Termiz, Dž. & Milosavljević, S. (2018) Praktikum iz metodologije politikologije: drugo izmijenjeno, dopunjeno i prošireno izdanje. Fakultet političkih nauka Univerziteta u Sarajevu i Međunarodno udruženje metodologa društvenih nauka Beograd.
38. Termiz, Dž. (2020) Statistička obrada podataka u empirijskim društvenim istraživanjima. Fakultet političkih nauka Univerziteta u Sarajevu.
39. Termiz, Dž., Metodologija društvenih nauka- Drugo dopunjeno i prošireno izdanje,Lukavac, 2009. godina.
40. Tuitel R. (2016). Defining Cyberterrorism. Concordiam, 7(2), 10-17. Dostupno na: https://perconcordiam.com/perCon_V7N2_ENG.pdf , (Datum pristupa: 19. 03. 2024.)
41. UNODC (2019). Cybercrime Module 14 Key Issues: Cyberterrorism. Dostupno na: https://www.unodc.org/e4j/zh/cybercrime/module-14/key-issues/cyberterrorism.html, Datum pristupa: (17. 03. 2024.)
42. Vajzović, E. (2019). Medijska i informacijska pismenost u sistemu cyber sigurnosti. Kriminalističke teme, zbornik radova, godina XIX, broj 5.
43. Vajzović, E. (2020). Digitalna transformacija sigurnosti i algoritamska demokratija. Sarajevo: Fakultet političkih nauka
44. Vajzović, E. (2020). Medijska i informacijska pismenost: istraživanje i razvoj. Sarajevo: Fakultet političkih nauka. ISBN 978-9926-475-09-3. Dostupno na: https://fpn.unsa.ba/b/wpcontent/uploads/2020/12/MEDIJSKA-I-INFORMACIJSKAPISMENOSTISTRAZIVANJE-I-RAZVOJ_e-izdanje-1.pdf, (Datum pristupa 27. 03. 2024.)
45. Vajzović, E., Hibert, M., Turčilo, L., Vučetić, V., Silajdžić, L., (2021). Medijska iinformacijska pismenost: dizajn učenja za digitalno doba, Fakultet političkih nauka Univerziteta u Sarajevu, Sarajevo

46. Van Dine, A. (2017). After Stuxnet: Acknowledging the Cyber Threat to Nuclear Facilities. Project on Nuclear Issues: A Collection of Papers from the 2016 Nuclear Scholars Initiative and PONI Conference Series. Dostupno na: https://www.jstor.org/stable/resrep23162.11 , (Datum pristupa: 26. 03. 2024.)
47. Veresha, R. (2018). PREVENTIVNE MJERE PROTIV RAČUNALNOG KRIMINALA:PRIBLIŽAVANJE POJEDINCU. Informatologia, 51 (3-4)
48. Vuković, H. (2012). Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj.NATIONAL SECURITY AND THE FUTURE, 12-31.
49. Weimann, G. (2004). Cyberterrorism: How Real Is the Threat? Washington, DC: United States Institute of peace. Dostupno na: https://www.usip.org/sites/default/files/sr119.pdf , (Datum pristupa: 20. 03. 2024.)
50. Wolf, M. (2015.) "Stuxnet - an Overview | ScienceDirect Topics." Dostupno na: www.sciencedirect.com/topics/computer-science/stuxnet. (Datum pristupa: 23. 07. 2024.)
51. Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon
52. Zorz, Z. (2022). Israeli general claims Stuxnet attacks as one of his successes - Help Net Security. Help Net Security, Dostupno na: https://www.helpnetsecurity.com/2011/02/15/israeli-general-claims-stuxnet-attacks-as-one-of-his-successes/ , (Datum pristupa: 28. 03. 2024.)

UNIVERZITET U SARAJEVU – FAKULTET POLITIČKIH NAUKA

IZJAVA o autentičnosti radova

Naziv odsjeka i/ili katedre: Sigurnosne i mirovne studije

Predmet: Magistarski rad

IZJAVA O AUTENTIČNOSTI RADOVA

Ime i prezime:	Ena Hajdarević
Naslov rada:	Stuxnet i izazovi digitalnog društva u 21. stoljeću
Vrsta rada:	Završni magistarski rad
Broj stranica:	49

Potvrđujem:

- da sam pročitao/la dokumente koji se odnose na plagijarizam, kako je to definirano Statutom Univerziteta u Sarajevu, Etičkim kodeksom Univerziteta u Sarajevu i pravilima studiranja koja se odnose na I i II ciklus studija, integrirani studijski program I i II ciklusa i III ciklus studija na Univerzitetu u Sarajevu, kao i uputama o plagijarizmu navedenim na web stranici Univerziteta u Sarajevu;
- da sam svjestan/na univerzitetskih disciplinskih pravila koja se tiču plagijarizma;
- da je rad koji predajem potpuno moj, samostalni rad, osim u dijelovima gdje je to naznačeno;
- da rad nije predat, u cjelini ili djelimično, za stjecanje zvanja na Univerzitetu u Sarajevu ili nekoj drugoj visokoškolskoj ustanovi;
- da sam jasno naznačio/la prisustvo citiranog ili parafraziranog materijala i da sam se referirao/la na sve izvore;
- da sam dosljedno naveo/la korištene i citirane izvore ili bibliografiju po nekom od preporučenih stilova citiranja, sa navođenjem potpune reference koja obuhvata potpuni bibliografski opis korištenog i citiranog izvora;
- da sam odgovarajuće naznačio/la svaku pomoć koju sam dobio/la pored pomoći mentora/ice i akademskih tutora/ica.

Mjesto, datum _____

Potpis _____