Vojni sukobi u virtualnom prostoru

Marasović, Bruno

SVEUČILIŠTE U RIJECI
Fakultet za menadžment u turizmu i ugostiteljstvu
Sveučilišni preddiplomski studij

BRUNO MARASOVIĆ

Vojni sukobi u virtualnom prostoru

Military Conflicts in Virtual Space

Završni rad

Opatija, rujan 2023.

SVEUČILIŠTE U RIJECI
Fakultet za menadžment u turizmu i ugostiteljstvu
Sveučilišni preddiplomski studij
Poslovna ekonomija u turizmu i ugostiteljstvu
Studijski smjer: Menadžment u hotelijerstvu

Vojni sukobi u virtualnom prostoru

Military Conflicts in Virtual Space

Završni rad

Kolegij:	**Informatika**	Student:	**Bruno MARASOVIĆ**
Mentor:	Izv. prof. dr. sc. **Ljubica Pilepić Stifanich**	Matični broj:	**23363/15**

Opatija, rujan 2023.

SVEUČILIŠTE U RIJECI UNIVERSITY OF RIJEKA
FAKULTET ZA MENADŽMENT U TURIZMU I UGOSTITELJSTVU
FACULTY OF TOURISM AND HOSPITALITY MANAGEMENT
OPATIJA, HRVATSKA CROATIA

IZJAVA O AUTORSTVU RADA I O JAVNOJ OBJAVI OBRANJENOG ZAVRŠNOG RADA

Bruno Marasović	**23363/**
(ime i prezime studenta)	(matični broj studenta)

Vojni sukobi u virtualnom prostoru
(naslov rada)

Izjavljujem da sam ovaj rad samostalno izradila/o, te da su svi dijelovi rada, nalazi ili ideje koje su u radu citirane ili se temelje na drugim izvorima, bilo da su u pitanju knjige, znanstveni ili stručni članci, Internet stranice, zakoni i sl. u radu jasno označeni kao takvi, te navedeni u popisu literature.

Izjavljujem da kao student–autor završnog rada, dozvoljavam Fakultetu za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci da ga trajno javno objavi i besplatno učini dostupnim javnosti u cjelovitom tekstu u mrežnom digitalnom repozitoriju Fakulteta za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci.

U svrhu podržavanja otvorenog pristupa završnim radovima trajno objavljenim u javno dostupnom digitalnom repozitoriju Fakulteta za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci, ovom izjavom dajem neisključivo imovinsko pravo iskorištavanja bez sadržajnog, vremenskog i prostornog mog završnog rada kao autorskog djela pod uvjetima *Creative Commons* licence CC BY Imenovanje, prema opisu dostupnom na http://creativecommons.org/liceses/.

U Opatiji, rujan 2023._____

Bruno Marasović
Potpis studenta

Sažetak

Tema vojnih sukoba u virtualnom prostoru predstavlja izazovnu i kompleksnu sferu suvremenih međunarodnih odnosa. U ovom radu tema virtualnih sukoba predstavit će se široj javnosti i pružiti osnovno razumijevanje ključnih aspekata virtualnog svijeta i sukoba unutar njega. Čitatelji će biti uvedeni u osnovne pojmove i koncepte koji se tiču ove domene, uključujući virtualni svijet i prirodu virtualnih konflikata. Također ćemo razmotriti alate, tehnike i strategije koje se koriste u kibernetičkim operacijama. Povijest virtualnih sukoba ima bogat i raznolik kontekst koji će biti obuhvaćen u ovom radu. Istražit će se ključni trenuci i događaji koji su oblikovali razvoj kibernetičkog ratovanja, uključujući početke računalnih mreža i prve znakove kibernetičkih napada. Razumijevanje povijesti virtualnih sukoba bitno je za prepoznavanje budućih obrazaca ponašanja. Posljedice virtualnih sukoba nisu ograničene samo na digitalni svijet. Osim što utječu na informacijsku sigurnost, oni mogu imati stvarne implikacije na gospodarstvo, nacionalnu sigurnost i privatnost građana. U radu će se analizirati štetne posljedice kibernetičkih napada i kako one oblikuju današnji svijet. Nadalje, osvrnut ćemo se prema budućnosti virtualnih sukoba i izazovima koji nas očekuju. Digitalna sfera neprestano napreduje, pa je razumijevanje trendova i budućih prijetnji ključno za pripremu i zaštitu društva od potencijalnih rizika. Ovaj rad ima za cilj olakšati razumijevanje teme vojnih sukoba u virtualnom prostoru, istražujući ključne aspekte, povijest, posljedice i budućnost. Ovo je važno jer nam omogućava bolje suočavanje sa svakodnevnim izazovima koji proizlaze iz ove kompleksne i dinamičke domene.

Ključni pojmovi: Vojni sukobi, Virtualni prostor; Kibernetički napadi; Zlođudni softver.

Sadržaj

Uvod

U današnjem digitalnom dobu, virtualni prostor postao je sve važnijom arenom za međunarodne sukobe i konflikte. Ovaj prostor, poznat i kao kibernetički prostor, predstavlja kompleksno okruženje u kojem države, organizacije i pojedinci izvode različite operacije kako bi ostvarili svoje ciljeve. Razumijevanje ovog prostora i njegovih karakteristika ključno je za analizu i suočavanje s rastućim izazovima kibernetičkog ratovanja.

"*War. War never changes. The Romans waged war to gather slaves and wealth. Spain built an empire from its lust for gold and territory. Hitler shaped a battered Germany into an economic superpower. But war never changes. In the 21st century, war was still waged over the resources that could be acquired...*" [1] Ovaj dijalog na samom početku kultne igre Fallout 1 iz 1997. godine govori nam ukratko o povijesti ratovanja i nastavlja dalje s pričom o nuklearnom ratu i nuklearnoj pustoši koja je ostala nakon njega. Srećom u stvarnom svijetu takvo nešto se još nije dogodilo, međutim, iako se svrha ratovanja nije puno promijenila, promijenila se tehnologija, tako da smo od mačeva došli do virtualnih oružja kakva su donedavno bila samo znanstvena fantastika.

Predmet i svrha ovog rada je istraživanje raznih aspekata vojnih sukoba u virtualnom prostoru. Počet ćemo definiranjem virtualnog okruženja i otkrivanjem njegovih karakteristika, postavljajući temelje za dubinsku analizu.

Zatim će se fokusirati na povijesnu putanju virtualnog ratovanja, prateći njegove korijene, evoluciju i ključne trenutke koji su oblikovali suvremeni kibernetički pejzaž. Od njegovih početaka, kroz doba Hladnog rata, pojavu računalnih virusa, pojavu svijesti o kibernetičkom prostoru 1980-ih, do prvih državnih kibernetičkih napada 1990-ih, navigirat ćemo kroz prošlost virtualnog ratovanja.

Nakon toga, preći ćemo na ključne elemente kibernetičkog sukoba, istražujući ciljeve koje se nastoji postići, arsenal alata koji se koriste i strategije koje se izvode u kibernetičkom ratovanju. Rasvijetliti ćemo motive iza virtualnih sukoba, analizirati složene tehnološke uređaje koji se koriste, i istražiti kompleksne strategije koje leže u osnovi ovog novog doba ratovanja.

Slijedi analiza glavnih aktera uključenih u virtualne sukobe, osvjetljavajući uloge koje igraju nacije, vlade i ne-državni entiteti u oblikovanju suvremenog kibernetičkog teatra. Njihovi motivi, kapaciteti i značaj u sve dinamičnijem krajoliku kibernetičkog ratovanja bit će podvrgnuti analizi.

[1] Videoigra Fallout 1, Intro, 1997.

Okrećući svoj pogled prema skorijoj povijesti, krenut ćemo na putovanje kroz neke od najzanimljivijih i najutjecajnijih kibernetičkih napada suvremenog doba. Od ruskih kibernetičkih kampanja, Stuxnet crva koji je prekretnica u virtualnim sukobima, napada na električnu mrežu Ukrajine, hakiranja Sonyja, miješanja u američke izbore 2016., epidemije ransomwarea NotPetya, globalnog haranja WannaCryja, kompromitacije SolarWinds lanca opskrbe, pa sve do nedavnog kibernetičkog napada na vladu Kostarike, ovi studijski slučajevi pružit će vrijedne uvide u raznovrsne prijetnje s kojima se suočavamo u kibernetičkom prostoru.

Također ćemo baciti kritički pogled na opipljive posljedice koje proizlaze iz virtualnih sukoba. Društvene, ekonomske i nacionalne sigurnosne posljedice ovih sukoba bit će ispitane kako bi se naglasio njihov utjecaj u stvarnom svijetu.

Na kraju, naše putovanje će kulminirati perspektivom prema budućnosti, razmatranjem tijeka sukoba u virtualnom prostoru. Razmotrit ćemo izazove i prilike koje leže pred nama, razmišljajući o dinamici kibernetičkog ratovanja i njenim implikacijama za međunarodne odnose i sigurnost.

Metode korištene u ovom radu uključuju: Induktivnu i deduktivnu metodu, metodu generalizacije, metodu kompilacije, analiza i sinteza podataka, metoda generalizacije.

Završni rad podijeljen je na 7 poglavlja. Prvo poglavlje definirat će virtualni prostor i njegove karakteristike, drugo poglavlje sadži pregled ključnih događaja kroz povijest. U trećem poglavlju predstavljeni su ciljevi, alati i strategije korištene u virtalnim sukobima. Četvrto poglavlje odnosi se na različite aktere u virtualnom svijetu, a peto poglavlje je kronološki pregled nekih od najvećih i najznačajnijih kibernetičkih napada u 21. stoljeću. U šestom poglavlju analizirat ćemo neke od posljedica virtualnih sukoba, dok zadnje poglavlje nosi pogled u budućnost.

1. Što je virtualni prostor?

1.1. Virtualni prostor

Virtualni prostor je koncept koji je u suvremenim vojnim sukobima postao bitan jednako kao i stvarni prostor. Ovaj pojam označava prostor koji se ne nalazi fizički, već je digitalni, elektronički odnosno kibernetički. Virtualni prostor igra ključnu ulogu u suvremenim vojnim operacijama i može biti kritički faktor za uspjeh ili neuspjeh u vojnim konfliktima.

U kontekstu kibernetičkog ratovanja, odnosi se na apstraktno područje gdje se vode sukobi i operacije u virtualnom svijetu. Obuhvaća globalnu mrežu međusobno povezanh računala i server, routera i drugih komunikacijskih sistema.[2] To je mjesto gdje se razmjenjuju informacije, pohranjuju podaci i odvijaju digitalne komunikacije. Taj virtualni prostor također je bojište za razne aktivnosti kibernetičkog ratovanja, kao što su hakiranje, špijunaža, sabotaža i manipulacija digitalnim informacijama.

Unutar kibernetičkog prostora virtualna okolina obuhvaća različite mreže, sustave i uređaje koji su meta ili se iskorištavaju tijekom kibernetičkih operacija. To može uključivati mreže vlada, sustave kritične infrastrukture (npr. elektroenergetske mreže, sustave prijevoza), vojne komunikacijske sustave, privatne kompanije i drugo.

Virtualni prostor uključuje ogromnu količinu podataka i informacija koje se prenose, pohranjuju i manipuliraju. Ovi podaci mogu varirati od osjetljivih vladinih dokumenata do osobnih informacija i intelektualnog vlasništva.

Virtualno okruženje obuhvaća mjesta gdje kibernetički napadači implementiraju zlonamjerni softver i druga kibernetička oružja kako bi kompromitirali, oštetili ili poremetili mete. Uključuje viruse, crve, ransomware i drugi zlonamjerni kod. S druge strabe postoje obrambene mjere i alati za kibernetičku sigurnost koje koriste vlade, organizacije i pojedinci kako bi se zaštitili od kibernetičkih prijetnji. To uključuje vatrozide, sustave za otkrivanje provala, antivirusni softver i drugo. Koristi se šifriranje i protokoli za zaštitu podataka i komunikacija. Tehnologije šifriranja igraju ključnu ulogu u osiguranju osjetljivih informacija od presretanja ili manipulacije.

[2] Janczewski, Lech J. i Colarik, Andrew M. Cyber Warfare and Cyber Terrorism, SAD, 2008.

1.2. Karakteristike virtualnog prostora:

Virtualni prostor, u kojem se odvijaju kibernetički napadi, posjeduje nekoliko karakterističnih svojstava koje su različite od uobičajenih fizičkih sukoba:

- Digitalna prisutnost: Digitalna prisutnost omogućava sudionicima da komuniciraju i djeluju putem interneta i računalnih mreža. Ovo se koristi za izvođenje napada, širenje propagande i obavljanje špijunaže. Uz to, digitalni tragovi ostavljeni u virtualnom okruženju omogućuju analitičarima praćenje aktivnosti i prikupljanje dokaza o kibernetičkim incidentima.
- Anonimnost: Anonimnost u virtualnom okruženju olakšava napadačima da prikriju svoj identitet i izbjegnu otkrivanje. To može otežati utvrđivanje odgovornosti i izazvati zbunjenost u situacijama kada države negiraju svoje umiješanosti. Razvoj tehnologije za deanonimizaciju postaje ključan za identifikaciju aktera u kibernetičkim napadima.
- Neprekidan sukob: Sukobi u virtualnom prostoru često su neprestani i dinamični, jer se prijetnje neprestano prilagođavaju i traže ranjivosti u digitalnom okruženju.
- Kibernetički napadi: Kibernetički napadi dolaze u različitim oblicima, uključujući DDoS napade, ransomware, krađu podataka i napade na infrastrukturu. Države ih mogu koristiti za ostvarivanje svojih ciljeva, uključujući ekonomske štete, oslabljivanje obrambenih sposobnosti i ometanje protivnika.
- Automatizacija: Kibernetički napadi često koriste automatizaciju i botove, što omogućuje napadačima da povećaju obim svojih operacija i izvode napade s minimalnim ljudskim intervencijama.
- Špijunaža: Kibernetička špijunaža obuhvaća prikupljanje obavještajnih podataka putem napada na računalne sustave i komunikacije. Države koriste ove informacije za donošenje strategijskih odluka i prikupljanje obavještajnih podataka o protivnicima. Takvi napadi često zahtijevaju sofisticirane tehničke vještine i resurse.
- Propaganda i psihološki rat: Korištenje virtualnog prostora za širenje propagande i dezinformacija postalo je sveprisutno u međunarodnim sukobima. Države mogu stvarati lažne vijesti, poticati polarizaciju i manipulirati javnim mnijenjem kako bi ostvarile svoje ciljeve. Ovaj oblik sukoba često se naziva "hibridnim ratom."
- Društveni mediji: Društveni mediji igraju ključnu ulogu u oblikovanju javnog mnijenja i političkog dijaloga. Povećana pažnja na društvenim medijima čini ih idealnim kanalom za širenje propagande i dezinformacija, ali i za organiziranje prosvjeda i aktivizma.

- Sukobi za prostor: Kontrola nad ključnim internetskim resursima, kao što su domene i IP adrese, može se koristiti za uskraćivanje pristupa protivniku ili za ometanje komunikacije. Ova vrsta sukoba posebno je izražena u situacijama gdje je pristup internetu reguliran ili cenzuriran.
- Međunarodno pravo i norme: Međunarodno pravo koje se primjenjuje na kibernetičke sukobe još je u razvoju, ali postoje napori za uspostavu jasnih normi i pravila. Pitanja vezana uz suverenitet, pravo na samoobranu i odgovornost u virtualnom prostoru postaju sve važnija.
- Protu-kibernetičke obrambene mjere: Države razvijaju složene sustave zaštite kako bi se obranile od virtualnih napada. Ovo uključuje učinkovite sustave za otkrivanje prijetnji, vatrozide i edukaciju osoblja o sigurnosnim praksama.
- Međunarodna dimenzija: Kibernetički napadi često prelaze nacionalne granice, što čini međunarodnu suradnju ključnom. Države surađuju kako bi razmijenile informacije o prijetnjama i napadima, razvile zajedničke strategije obrane i radile na uspostavi međunarodnih standarda u kibernetičkom prostoru. Ovakvi sukobi često imaju međunarodne posljedice i mogu pojačati diplomatske napetosti između država.
- Informacije kao oružje: Informacijske i dezinformacijske kampanje ključne su za kibernetičko ratovanje, gdje lažne narative i propaganda mogu biti jednako štetni kao i tradicionalni kibernetički napadi.
- Sveprisutnost: Virtualni prostor nije ograničen geografskim granicama i može se koristiti za napade iz bilo kojeg dijela svijeta.
- Kontinuirano učenje i prilagodba: Akteri u virtualnom prostoru neprestano razvijaju nove tehnike i alate te se prilagođavaju promjenama u kibernetičkom okruženju.
- Ekonomski utjecaj: Napadi na virtualni prostor mogu prouzročiti značajnu ekonomsku štetu, uključujući gubitak podataka i poremećaj poslovnih operacija.
- Evoluirajući pejzaž: Virtualni prostor neprestano se razvija, s novim tehnologijama, prijetnjama i oblicima napada koji se redovito pojavljuju. Obrana u kibernetičkom prostoru mora se konstantno prilagođavati ovom evoluirajućem svijetu.

Ove karakteristike ilustriraju kompleksnost kibernetičkih sukoba i naglašavaju potrebu za multidisciplinarnim pristupom i suradnjom kako bi se očuvala sigurnost i stabilnost u virtualnom okruženju.[3][4][5]

[3] Even, Shmuel i David Siman-Tov. Cyber Warfare: Concepts and Strategic Trends, Izrael, 2012.

[4] Yuchong Li, Qinghui Liu. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments; https://www.sciencedirect.com/science/article/pii/S2352484721007289?via%3Dihub (posjećeno 2023.)

[5] Tabansky, Lior. Basic Concepts in Cyber Warfare, SAD, 2011.

2. Povijest virtualnog ratovanja

Virtualno ratovanje, ili ratovanje u kibernetičkom prostoru, označava upotrebu računalnih sustava i mreža za provođenje napada, špijunažu, sabotažu i obranu. Povijest kibernetičkog ratovanja obuhvaća razdoblje od pionirskih eksperimenata s računalima do sveprisutnih prijetnji u digitalnom dobu. Razvoj kibernetičkog ratovanja kroz povijest:

2.1. Rani korijeni (1940-1960)

Počeci kibernetičkog ratovanja sežu unatrag do Drugog svjetskog rat. Tijekom rata, vojske su koristile računalne sustave za kriptoanalizu, dešifriranje šifriranih poruka i razmjenu vojnih informacija. Početkom 1940-ih, nacistička Njemačka koristila je Enigma stroj za šifriranje komunikacije, a britanski znanstvenik Alan Turing razvio je "Colossus," prvo računalo namijenjeno za razbijanje Enigminih šifri.

Nakon Rata, tehnološki napredak u računalima omogućio je razvoj vojnih sustava i kompjuterskih mreža. Američka vojska razvila je sustav "SAGE" (Semi-Automatic Ground Environment) za rano upozoravanje na zračne napade, što se može smatrati ranim oblikom kibernetičke obrane.

2.2. Hladni rat (1960-1980)

Tijekom Hladnog rata, SAD i Sovjetski Savez su se natjecali u razvoju računalnih tehnologija i kibernetičkih kapaciteta. Obje strane su razvijale sustave za nadzor i obranu protiv nuklearnih prijetnji, a to je uključivalo i računalnu obranu.

U ovom razdoblju počeli su se razvijati koncepti kibernetičkog napada, ali su većinom ostali u eksperimentalnoj fazi. Vojni analitičari razmišljali su o mogućim scenarijima kibernetičkog ratovanja, uključujući isključivanje neprijateljskih komunikacijskih mreža.

2.3. Prvi kompjuterski virusi (1970-1980)

Prvi računalni virusi počeli su se pojavljivati 1970-ih godina. Jedan od najranijih primjera je "Creeper" virus, koji je 1971. godine inficirao ARPANET, prethodnika interneta. Iako "Creeper" nije nanosio štetu, predstavljao je početak fenomena računalnih virusa.

Uskoro su slijedili drugi virusi poput "Elk Cloner" i "Brain," a programeri su eksperimentirali s širenjem tih virusa putem disketa. Ovo je bilo prije pojave interneta kakvog ga mi poznajemo.

2.4. Razvijanje svijesti (1980-1990)

1980-ih godina, računalne mreže su postajale sveprisutne, ali se sigurnosna svijest tek razvijala. Haktivističke skupine poput "Chaos Computer Club" u Njemačkoj počele su ukazivati na ranjivosti u računalnim sustavima i sigurnosnim propustima.

Incident "Morris Worm" iz 1988. godine označio je prvi veliki računalni crv koji je paralizirao tadašnji internet. Autor crva, Robert Tappan Morris, kasnije je tvrdio da nije imao zlonamjerne namjere, ali je incident izazvao zabrinutost u vezi kompjuerske sigurnosti.

2.5. Prvi državni kibernetički napadi (1990-2000)

Tijekom 90-ih godina, telekomunikacijski sustavi postali su česta meta cyber napada. Napadači su često ciljali telefonske centrale i druge infrastrukture kako bi prouzrokovali prekide u komunikacijama. Sukobi tijekom raspada bivše Jugoslavije vidjeli su rane primjere kibernetičkog ratovanja. Hrvatska i Srbija suočile su se s kibernetičkim napadima usmjerenim na ometanje komunikacijskih sustava.

Tijekom istog razdoblja, Kina je izvela napade na Tajvan, dok je grupa tinejdžera “upala” u sustav Pentagona, NASA-e i drugih organizacija Sjedinjenih država. S porastom državnih kibernetičkih aktivnosti, međunarodna zajednica počela je razmatrati potrebu za međunarodnim pravilima koja bi regulirala kibernetičko ratovanje. 1998. godine, Ujedinjeni narodi su osnovali Odbor za mirno korištenje virtualnog prostora i informacijskih tehnologija kako bi razmotrio smjernice za ponašanje u virtualnom prostoru.

Povijest virtualnog ratovanja do početka 21. stoljeća svjedoči o postupnom razvoju kibernetičkih kapaciteta i prijetnji. U tom razdoblju, kibernetičko ratovanje nije bilo dominantan oblik konflikta, ali su se postavili temelji za budući razvoj u virtualnom prostoru.

2.6. Početak 21. stoljeća: Eskalacija napada (2000-2010)

Početkom 21. stoljeća, kibernetičko ratovanje postalo je ključnom komponentom suvremenih sukoba i međunarodnih odnosa. Razvoj informacijske tehnologije i sveprisutnost interneta transformirali su način na koji nacije, organizacije i pojedinci komuniciraju, posluju i ratuju.

Kibernetičko ratovanje doživjelo je dramatičan porast u broju i složenosti napada. Sve više organizacija i država prepoznalo je potencijal kibernetičkih operacija kao sredstva za postizanje svojih ciljeva.

Estonija je postala prva žrtva masovnog kibernetičkog napada. Ovaj incident uključivao je DDoS napade (napadi uskraćivanja usluge) na estonske web stranice, financijske sustave i infrastrukturu. Napad je uslijedio nakon kontroverzi oko premještanja sovjetskog vojnog spomenika. Iako nije bilo dokaza o umješanosti Ruske države, napad su izveli hakeri sponzorirani od strane vlade ili ruski simpatizeri. Napad je izazvao međunarodnu zabrinutost i potaknuo razgovore o kibernetičkoj sigurnosti.[6]

"Stuxnet" (2010): "Stuxnet" napad označio je novu eru u kibernetičkom ratovanju. Ovaj izuzetno sofisticirani kompjutorski crv ciljao je iranski nuklearni program. Napad je uspješno oštetio iranske centrifuge za obogaćivanje urana, pokazujući sposobnost državnih aktera za provođenje naprednih kibernetičkih operacija s fizičkim posljedicama.

Haktivističke skupine kao što su Anonymous i LulzSec proveli su niz napada na vlade, korporacije i organizacije koje su smatrali neetičnima. Ovi napadi često su uključivali krađu i objavljivanje osjetljivih informacija, te su privukli veliku medijsku pažnju.

Wikileaks, platforma za objavljivanje tajnih informacija, objavila je ogroman broj povjerljivih dokumenata koji su izazvali kontroverze diljem svijeta. Hakeri su često surađivali s Wikileaksom kako bi osigurali i anonimno dostavili dokumente.

2.7. Širenje kibernetičkih napada (2010-2020)

U drugom desetljeću 21. stoljeća, haktivističke grupe i pojedinci postali su vidljivi igrači u kibernetičkom ratovanju. Njihovi ciljevi često su uključivali izlaganje korupcije, kršenja privatnosti ili političke agende. Državni akteri, poput Kine i Rusije, intenzivno provode kibernetičke špijunske operacije s ciljem prikupljanja obavještajnih podataka i tajnih

[6] Andress, Jason; Winterfeld, Steve - Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, SAD, 2013.

informacija, a kibernetički napadi postali su sveprisutni i široko rasprostranjeni. Ciljaju različite sektore, a mete uključuju državne agencije, vojnu industriju i korporacije, energetiku, financije, zdravstvo i infrastrukturne sustave. Nacije i organizacije shvatile su ozbiljnost kibernetičke prijetnje.

Ransomware napadi postali su učestali, pri čemu hakeri šifriraju podatke organizacija i zahtijevaju otkupninu za njihovo vraćanje. Napadi poput "WannaCry" i "NotPetya" nanijeli su značajnu štetu globalnim organizacijama.

Virtualni prostor postao je platforma za političke sukobe i dezinformacijske kampanje. Rusija je optužena za miješanje u izborne procese u nekoliko zemalja i federacija (Gruzija, Ukrajina, SAD, Njemačka, EU, itd.) putem kibernetičkih operacija.

S porastom kibernetičkih prijetnji, međunarodna zajednica počela je djelovati kako bi razvila međunarodne norme i pravila za kibernetičko ratovanje. Ujedinjeni Narodi su osnovali skupine eksperata koji razmatraju pitanja kibernetičke sigurnosti i razvoj međunarodnih smjernica za kibernetičko ponašanje. Osim toga, niz regionalnih i bilateralnih sporazuma dogovoren je kako bi se ograničila eskalacija kibernetičkih konflikata.

3. Ciljevi, alati i strategije

3.1. Ciljevi virtualnih sukoba

Ciljevi kibernetičkog ratovanja mogu varirati ovisno o motivaciji i namjerama napadača. Međutim, postoje neki zajednički ciljevi kibernetičkog ratovanja koji se često pojavljuju:

- Moć i geopolitička prednost: Države koriste kibernetičko ratovanje kako bi povećale svoju prijetnju drugim zemljama i postigle prednost u međunarodnim odnosima. To može uključivati prijetnje i demonstracije moći kako bi se postigao politički utjecaj ili iznudili ustupci.Špijunaža i prikupljanje obavještajnih podataka: Jedan od osnovnih ciljeva kibernetičkog ratovanja je dobivanje pristupa osjetljivim informacijama i obavještajnim podacima. Napadači mogu ciljati državne agencije, vojne organizacije, korporacije ili nevladine organizacije kako bi prikupili obavještajne podatke o vojnim strategijama, političkim odlukama, ekonomskim planovima i slično.
- Sabotaža kritične infrastrukture: Napadi na kritičnu infrastrukturu, poput energetskih mreža, vodoopskrbe ili prometnih sustava, mogu imati ozbiljne posljedice. Cilj može biti izazivanje prekida u opskrbi, poremećaja u komunikaciji ili stvaranje ekonomske štete.
- Širenje dezinformacija i laži: Kibernetički napadi mogu se koristiti za širenje lažnih informacija ili dezinformacija kako bi se utjecalo na javno mnijenje, izbore ili političke procese. Cilj je često stvaranje konfuzije, polarizacije ili destabilizacije društava.
- Krađa intelektualnog vlasništva: Kibernetički napadi često ciljaju korporacije kako bi se ukrala intelektualna svojina, patenti ili poslovne tajne. Ovo može rezultirati ekonomskim gubicima i ometanjem konkurencije.
- Vojne operacije i rat: U slučajevima otvorenog sukoba, kibernetičko ratovanje može se koristiti za potporu konvencionalnim vojnim operacijama. Cilj može biti onesposobljavanje protivničke komunikacije, nadzora nad vojnim sustavima ili stvaranje dezinformacija kako bi se protivniku nanijela šteta.

Ciljevi virtualnih sukoba u vidu međunarodnih operacija slični su već uobičajenim ciljevima svakog fizičkog sukoba odnosno rata koji se dosad odvio. Ljudi odnosno nacije sukobljavaju se zbog ekonomske moći i geopolitičke prednosti, a akcije koje provide su špijuniranje, sabotaža infrastrukture te krađa podataka, a u slučaju fizičkog sukoba, virtualni sukob je također neizbježan.

3.2. Alati korišteni u virtualnim sukobima

Napadači koriste različite alate za izvođenje kibernetičkih napada, pri čemu svaki alat ima svoje specifične svrhe u kibernetičkom prijetnjama. Ti alati variraju po složenosti, sposobnostima i namjerama. Nekoliko uobičajenih kategorija alata koji se koriste za kibernetičke napade:

- Virusi: Računalni virusi su zlonamjerni programi koji se kopiraju i šire u drugim datotekama i računalima. Mogu uništavati podatke ili širiti štetne funkcije.
- Crvi: Crvi su vrsta malvera koji se sami repliciraju i šire putem računalnih mreža. Često se koriste za brzo širenje u velikim mrežama.
- Trojanski konji: Trojanski konji su skriveni unutar legitimnih programa i obično omogućuju udaljeni pristup napadaču na ciljano računalo.
- Ransomware (Otkupnina): Ransomware je zlonamjerni softver koji šifrira podatke na žrtvinom računalu i zahtijeva otkupninu za dešifriranje. Ovo je postalo posebno problematično u posljednjem desetljeću.
- Phishing (Ribarenje): Phishing je tehnika koja se koristi za prevare korisnike da otkriju osobne informacije poput lozinki i kreditnih kartica. Napadači često koriste lažne e-pošte ili web stranice kako bi izgledali autentično.
- Password attack (napadi na lozinke): Napadi na lozinke predstavljaju pokušaje neovlaštenog pristupa računalnim ili internetskim računima tako da se pogađaju, otkriju ili dešifriraju lozinke korisnika.
- Distributed Denial of Service (DDoS) (Napadi na uskraćivanje usluge): DDoS napadi su usmjereni na preopterećenje ciljane mreže ili usluge velikim brojem zahtjeva, čime se onemogućava pristup legitimnim korisnicima.
- Zero-Day Exploits (Eksploatacije nultog dana): Zero-day eksploatacije su ranjivosti u softveru koje napadači iskorištavaju prije nego što izdavatelj softvera objavi zakrpu. To omogućava napadačima pristup sustavima dok programeri još nisu svjesni propusta.
- Botnets (Bot mreže): Botnets su mreže kompromitiranih računala koja kontrolira napadač. Ovi botovi mogu se koristiti za izvođenje različitih vrsta napada, uključujući DDoS napade.
- Backdoors (Stražnja vrata): Backdoors su skriveni načini pristupa računalnom sustavu koji omogućuju napadačima kontrolu nad sustavom bez znanja vlasnika.
- Cyber Weapon Systems (Sustavi kibernetičkog oružja): Države i vojske razvijaju specijalizirane kibernetičke alate i sustave za vojne operacije. Primjer je Stuxnet, koji je korišten za napad na iranske nuklearne instalacije.

- Kibernetička obavještajna zajednica: Radi na analitičkim alatima koji se koriste za prikupljanje, analizu i tumačenje kibernetičkih podataka radi otkrivanja prijetnji i potencijalnih napada.
- Sigurnosni softver: Upotreba antivirusnih programa, firewalla i sigurnosnih paketa može pomoći u otkrivanju i blokiranju zlonamjernih aktivnosti.
- Skripte: Napadači često koriste različite skripte za automatizaciju napada i olakšavanje izvođenja napada.

Svaki od navedenih alata koristi se u sukobima na virtualnom polju, često se kombiniraju jedni s drugima, pogotovo kad su u pitanju veliki napadi na industrijska postrojenja, javnu opskrbu i velike kompanije. [7][8]

3.3. Strategije u kibernetičkom ratovanju

Strategije korištene u kibernetičkom ratovanju obuhvaćaju različite pristupe i taktike koje koriste državni i nadržavni akteri kako bi ostvarili svoje ciljeve u digitalnom prostoru. Evo nekoliko uobičajenih strategija:

- Advanced Persistent Threats (APT)(Napredne dugotrajne prijetnje): APT je strategija koja uključuje dugotrajno i ciljano prodiranje u računalne mreže ciljane organizacije ili države. Napadači koriste sofisticirane metode kako bi ostali neprimjetni, prikupljali informacije i izbjegavali otkrivanje.
- Ransomware: Ova strategija uključuje inficiranje računalnih sustava zlonamjernim softverom koji kriptira podatke. Napadači zatim traže otkupninu za dekripciju podataka. Ransomware je često usmjeren na korporacije i organizacije.
- Social Engineering: Ova strategija se oslanja na manipulaciju ljudskim ponašanjem. Napadači koriste psihološke trikove kako bi prevarili ljude da otkriju povjerljive informacije, kao što su lozinke ili podaci za prijavu.
- Supply Chain Attacks: Napadači ciljaju ranjivosti u opskrbnom lancu organizacija, često napadajući manje zaštićene dobavljače kako bi se infiltrirali u sustav ciljane organizacije. To može uključivati unošenje zlonamjernih komponenata u hardver ili softver.
- Phishing: Phishing je tehnika u kojoj se koriste lažne e-pošte ili web stranice kako bi se prevarili korisnici da otkriju osjetljive informacije, poput lozinki ili brojeva kreditnih kartica.

[7] TechTarget.com 13 Common Types of Cyber Attacks and How to Prevent Them (posjećeno 2023.)
[8] Andress, J., Winterfeld, S. The Basics of Cyber Warfare in Theory and Practice, SAD, 2012.

- Spear Phishing: Ova tehnika je naprednija verzija phishinga, u kojoj se napadači ciljano usmjeravaju prema određenim osobama ili organizacijama. E-pošta i poruke su prilagođene kako bi izgledale autentično.
- Man-in-the-Middle (MitM) Attacks: U MitM napadima, napadač se pozicionira između komunikacijskog toka između dviju strana i može presretati, mijenjati ili čak kontrolirati komunikaciju.
- Tuneliranje prometa: Napadači često koriste virtualne privatne mreže (VPN) ili proxy servere kako bi preusmjerili svoj promet i ostali anonimni.
- Korištenje bot mreža: Bot mreže sastoje se od zaraženih računala koja se koriste za izvođenje masovnih napada, kao što su DDoS napadi, ili za širenje spam e-pošte.
- Zloupotreba legitimnih alata: Napadači često koriste legitimne administrativne alate i skripte kako bi izbjegli detekciju, kao što su PowerShell skripte ili Windows Management Instrumentation (WMI).
- Obrazovanje i osposobljavanje: Osoblje i korisnici trebaju biti educirani o potencijalnim prijetnjama, prepoznavanju phishing napada i sigurnim praksama na internetu.
- Redovito ažuriranje sustava: Redovita ažuriranja operativnih sustava i aplikacija mogu zakrpati ranjivosti koje bi napadači mogli iskoristiti.
- Mrežna segmentacija: Razdvajanje mreže na segmente može ograničiti širenje napada unutar sustava.
- Dvostruka autentifikacija: Upotreba dvostruke autentifikacije može otežati pristup računalnim sustavima, čak i ako napadač zna korisničko ime i lozinku.
- Analiza prometa: Praćenje i analiza mrežnog prometa može pomoći u otkrivanju neobičnih aktivnosti ili znakova napada.
- Incident Response Plan: Razvijanje plana za reagiranje na sigurnosne incidente može pomoći organizacijama da brzo i učinkovito reagiraju na napade.
- Suradnja: Organizacije i države često surađuju kako bi dijelile informacije o prijetnjama i razmjenjivale najbolje prakse za obranu od kibernetičkih napada.

Kibernetičko ratovanje ostaje dinamično područje koje se brzo razvija. Napadači stalno pronalaze nove strategije, alate i tehnike, stoga je ključno da organizacije i države ostanu u tijeku s najnovijim prijetnjama i stalno poboljšavaju svoje sigurnosne mjere. Ova neprestana evolucija čini kibernetičko ratovanje izazovnim i zahtjevnim područjem sigurnosti, te zahtijeva

suradnju i koordinaciju na globalnoj razini kako bi se zaštitila sigurnost i stabilnost digitalnog svijeta. [9]

[9] Andress, J., Winterfeld, S. The Basics of Cyber Warfare in Theory and Practice, SAD, 2012

4. Akteri sukoba u virtualnom prostoru

Sukobi u virtualnom prostoru uključuju raznolik niz aktera, od država i vladinih agencija do nevladinih aktera, kriminalnih organizacija i haktivističkih grupa. U ova dva potpoglavlja pregledat ćemo neke on najvećih aktera u virtualnim sukobima.

4.1. Države i vlade

Praktički sve države i vlade svijeta danas imaju svoj trag na virtualnom prostoru, a u ovom teksu pregledat ćemo one koje su dosad ostavile najveći trag na polju virtualnih sukoba:

- Sjedinjene američke države se smatraju jednim od najvećih aktera u kibernetičkom prostoru. Imaju razvijene kibernetičke vojne jedinice i obavještajne agencije koje se bave špijunažom, obranom i izvođenjem kibernetičkih operacija. SAD su također poznate po upotrebi kibernetičkog oružja u međunarodnim konfliktima.
- Rusija se široko smatra jednim od najaktivnijih nacionalnih državnih aktera u kibernetičkom ratovanju. Povezana je s brojnim kibernetičkim operacijama, uključujući miješanje u strane izbore, kibernetičku špijunažu i napade s razaranjem. Poznate ruske državno sponzorirane hakerske grupe su APT29 (Cozy Bear) i APT28 (Fancy Bear).
- Kina ima dugu povijest sudjelovanja u kibernetičkim operacijama kako bi prikupljala obavještajne informacije i postizala strateške ciljeve. Grupama poput APT10 i APT41 pripisuju se kibernetičke aktivnosti sponzorirane od strane Kine. Kina je povezana s kampanjama kibernetičke špijunaže koje ciljaju vlade, korporacije i kritičnu infrastrukturu.
- Sjeverna Koreja je poznata po svojim državno sponzoriranim hakerskim grupama, uključujući Glavni odjel za izviđanje (RGB). RGB je odgovoran za provođenje kibernetičkih operacija u ime sjevernokorejskog režima. Druge sjevernokorejske hakerske grupe uključuju Lazarus grupu (poznatu i kao Hidden Cobra), APT38 (podgrupu Lazarus grupe) i Bluenoroff. Osim špijunaže i sabotaže, poznati su i po ciljanju financijskih institucija.
- Estonija je poznata po svojem proaktivnom pristupu kibernetičkoj sigurnosti i kibernetičkim operacijama. Nakon što je doživjela masivni kibernetički napad 2007. godine, koji se vjeruje da je bio pokrenut iz Rusije, Estonija je postala lider u razvoju snažnih kibernetičkih obrana. Ujedno je pokretač NATO-ovog centra za kooperaciju među članicama kada je u pitanju obrana od napada: NATO Cooperative Cyber Defence of Excellence.

- Iran je također aktivan u kibernetičkom prostoru, posebno u regiji Bliskog istoka. Razvoj kibernetičkog sektora Grupe APT33 i AT34 povezane su s iranskom vladom poznate su po napadima na energetske sektore, vojnu infrastrukturu i druge ciljeve.
- Izrael je poznat po razvijanju naprednih kibernetičkih kapaciteta i njihovoj upotrebi za vojne operacije i obranu. Grupa poput Unit 8200 smatra se jednom od najnaprednijih obavještajnih jedinica u kibernetičkom svijetu.
- Francuska ima svoje kibernetičke vojne jedinice i aktivno sudjeluje u kibernetičkim operacijama za obranu i izviđanje. Također su poznati po svojim naporima za zaštitu europske kibernetičke infrastrukture.
- Ujedinjeno Kraljevstvo, putem svoje Agencije za komunikacije vlade (GCHQ), sudjelovalo je u kibernetičkim operacijama, uglavnom u području prikupljanja obavještajnih informacija i kibernetičke sigurnosti.
- Njemačka aktivno razvija svoje kibernetičke kapacitete za obranu i napade. Njemačka Federalna služba za obavještajne poslove (BND) sudjeluje u prikupljanju kibernetičkih obavještajnih informacija, a zemlja se također obvezuje na jačanje kibernetičke sigurnosti unutar Europske unije.
- EU ima svoje kibernetičke sigurnosne agencije i strategije za zaštitu svojih članica od kibernetičkih prijetnji. Također su usmjereni na promicanje kibernetičke sigurnosti na globalnoj razini.
- NATO je razvio kibernetičke sposobnosti i strategije za kolektivnu obranu članica. Organizacija je pokazala posvećenost obrani od kibernetičkih prijetnji i izvođenju protu-kibernetičkih operacija.
- Nekoliko zemalja Bliskog istoka, uključujući Saudijsku Arabiju i Ujedinjene Arapske Emirate, razvilo je kibernetičke sposobnosti za špijunažu i regionalni utjecaj.[10]

4.2. Ne-državni akteri

U području kibernetičkog ratovanja, ne-državni akteri odnose se na grupe ili entitete koji nisu izravno povezani s vladom, ali se bave kibernetičkim operacijama iz različitih razloga, uključujući akcije iz političkih ili ideoloških motiva, kibernetički kriminal ili promicanje

[10] Andress, Jason. Winterfeld, Steve - Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, SAD, 2013.

ideoloških ili političkih ciljeva. Neki od najvećih ne-državnih aktera u području kibernetičkog ratovanja uključuju:

- Hacktivističke grupe: To su obično politički ili ideološki motivirane grupe koje koriste hakiranje kao sredstvo za promicanje svojih ciljeva. Anonymous i LulzSec su jedni od najpoznatijih kolektiva takvih haktivista i sudjelovali su u raznim kibernetičkim operacijama i prosvjedima.
- Kriminalne organizacije: To su grupe ili pojedinci koji su prvenstveno motivirani financijskim dobitkom. Bave se aktivnostima kao što su napadi ransomwareom, krađa podataka i krađa identiteta. Primjeri uključuju ransomware grupe poput REvil i DarkTequila.
- Plaćenici: Neke privatne grupe nude usluge kibernetičkog ratovanja za najam. Mogu raditi u ime vlada, korporacija ili drugih entiteta kako bi provodili kibernetičku špijunažu, sabotažu ili druge ofenzivne operacije. Poznata je NSO grupa koja radi na razvoju alata za virtualno ratovanje.
- Kibernetički posrednici s potporom države: Iako su tehnički povezani s vladama, ovi entiteti djeluju s nekom razinom autonomije i ponekad se smatraju ne-državnim akterima. Primjeri uključuju kibernetičke kriminalce koji surađuju s državno podržanim hakerima ili privatne grupe hakera koje koriste vlade kako bi provodile kibernetičke operacije.
- Terorističke organizacije: Terortističke organizacije poput Al-Qaedae i ISIS-a su pokazali rastući interes za uporabu tehnika kibernetičkog ratovanja kako bi ostvarili svoje ciljeve. Iako im možda nedostaje sofisticiranost državnih aktera, i dalje mogu predstavljati prijetnje kritičnoj infrastrukturi i sigurnosti podataka.
- White Hat udruge: Neki pojedinci ili grupe unutar šire kibernetičke zajednice bave se odgovornim hakiranjem, testiranjem penetracije i istraživanjem ranjivosti. White Hat hacker je naziv za osobe koje rade na otkrivanju propusta u suradnji s vladama i korporacijama. Iako im namjere obično nisu zlonamjerne, njihovi postupci mogu neizravno utjecati na dinamiku kibernetičkog ratovanja.
- Prijetnje iznutra: Osobe s unutarnjim pristupom organizacijama, poput nezadovoljnih zaposlenika ili izvođača radova, mogu predstavljati značajne kibernetičke prijetnje. Oni mogu otkrivati osjetljive informacije, provoditi sabotažu ili kompromitirati sigurnost iznutra. Najpoznatije ime u ovom kontekstu je Edward Snowden koji je “procurio” dotad neviđene količine povjerljivih informacija, želeći javnosti ukazati na špijunaže građana koje je pokrenula američka Nacionalna agencija za sigurnost (NSA).
- Tvrtke za kibernetičku sigurnost: Tvrtke specijalizirane za virtualni svijet poput CrowdStrike, FireEye i Palo Alto Networks igraju značajnu ulogu u kibernetičkoj obrani

pružanjem obavještajnih informacija o prijetnjama, odgovora na incidente i sigurnosnih rješenja koja štite organizacije od kibernetičkih napada.

- Tajne grupacije: Osim poznatih aktera, postoji mnogo tajnih ili manje poznatih kibernetičkih grupacija koje se bave špijunažom, vojnim operacijama i napadima na različite ciljeve.
- Međunarodne kriminalne organizacije: Međunarodne kriminalne organizacije, često smještene u istočnoj Europi, bave se kibernetičkim kriminalom poput prijevara s kreditnim karticama, krađom identiteta i online iznudama, predstavljajući financijske i sigurnosne prijetnje širom svijeta.[11]

Ne-državni akteri često djeluju izvan tradicionalnih okvira međunarodnog ratovanja i velik su izazov za virtualnu sigurnost. Njihove akcije su vođene osobnim uvjerenjima, motivima i ciljevima i ne moraju nužno biti u skladu s ciljevima vlada država u kojima žive. Tu su granice nedefinirane, i države će često koristiti ovakve udruge ili pojedince za ispunjenje svojih agendi dok u isto vrijeme negiraju upletenost. S druge strane, pojedinci poput Edwarda Snowdena mogu napraviti veliku štetu svojim državama objavljivanjem tajnih podataka široj javnosti.

[11] Andress, Jason. Winterfeld, Steve - Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, SAD, 2013.

5. Pregled najzanimljivijih napada modernog doba

Od početka 21. stoljeća dogodile su se tisuće manjih i većih napada na razne organizacije, države, privatne i javne kompanije. U ovom pregledu pokušat ću pobliže pojasniti neke od njih i po čemu su specifični.

5.1. Ruski napadi

Napad na estonske web stranice: U travnju 2007. godine, estonske web stranice, uključujući web stranice vlade i banaka, postale su metom masovnih distribuiranih napada odbijanja usluge (DDoS). Iako nije izravno povezan s ruskim vlastima, napad je uslijedio nakon micanja Sovjetskog ratnog spomenika. Napad je izazvao poremećaje u estonskim internetskim uslugama i ilustrirao potencijalnu ranjivost država na kibernetičke prijetnje. [12]

Napad na Gruziju: Tijekom rusko-gruzijskog rata u kolovozu 2008. godine, Gruzija je postala meta masovnih kibernetičkih 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 sugerira na njezinu povezanost s napadima.[13]

Napadi na Ukrajinu: Nakon ruske aneksije Krima 2014. godine, Ukrajina je postala žarište intenzivnih kibernetičkih napada. Napadi su uključivali DDoS napade na web stranice vlade, širenje štetnih malvera poput "BlackEnergy" i "NotPetya" te pokušaje infiltracije u kritičnu infrastrukturu, uključujući energetske mreže. Većina tih napada povezana je s ruskim napadačkim skupinama. Osim napada na infrastrukturu, napadaju se i vojne jedinice, državne agencije, postrojenja i slično. [14]

5.2. Stuxnet (2010.)

[12] Andress, Jason. Winterfeld, Steve: Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, SAD, 2013.
[13] Andress, Jason. Winterfeld, Steve: Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, SAD, 2013.
[14] Wired.com https://www.wired.com/story/russian-hackers-attack-ukraine/ (posjećeno 2023.)

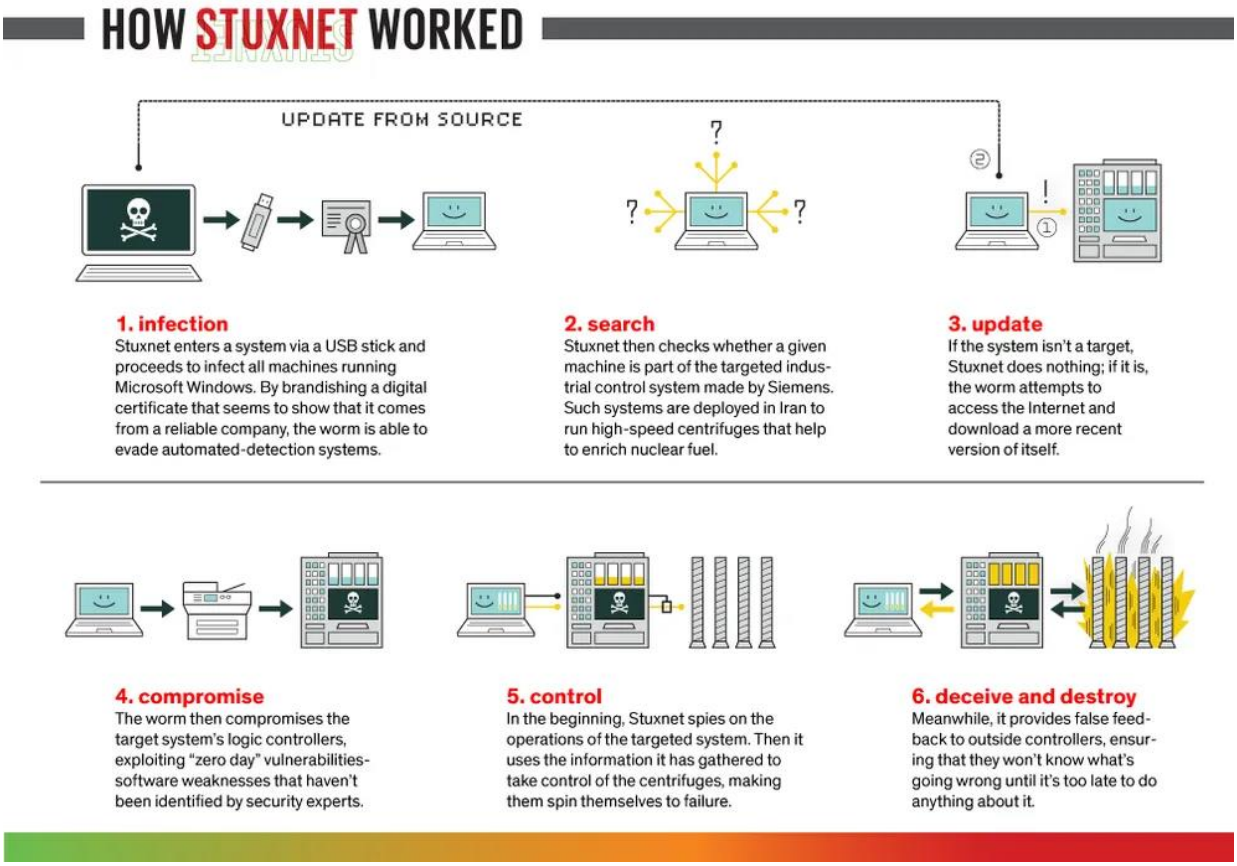
Iran je tijekom godina pokušavao razviti vlastiti nuklearni program, što je izazvalo ozbiljne zabrinutosti međunarodne zajednice. Ciljano je postrojenje za obogaćivanje urana locirano u nukleranom postrojenju Natanz. Stuxnet je bio dio šireg napora da se zaustavi iranski nuklearni program, a posebno centrifuge koje su ključne za obogaćivanje urana.

Jedna od iznimnih karakteristika Stuxneta bila je upotreba tzv. zero-day ranjivosti u Microsoft Windows operativnom sustavu. Dotad neviđeno, Stuxnet je iskoristio 4 zero-day ranjivosti. Ove ranjivosti nisu bile poznate i nisu bile zakrpane u trenutku napada, što je ukazivalo na veliko znanje i resurse iza napadača. Iskorištavanje nultih dana omogućilo je Stuxnetu da se neprimjetno infiltrira u ciljane sustave. Stuxnet je dodatno povećao svoju vjerodostojnost korištenjem digitalnih certifikata dviju tajvanskih tvrtki koje su bile ugledne i pouzdane. Ovo je otežalo otkrivanje i zaobilaženje antivirusnih programa jer su se digitalni potpisi činili legitimnima.[15]

Najzanimljivija karakteristika Stuxneta bila je njegova sposobnost precizne sabotaže. Malware je ciljao programabilne logičke kontrolere (PLC-ove), koji su bili odgovorni za kontrolu brzine vrtnje centrifuga. Manipulacijom brzinom vrtnje, Stuxnet je postupno uzrokovao mehaničke probleme u centrifugama, uzrokujući velike oscilacije u vrtnji i konačno njihovo uništavanje. Ovaj nivo preciznosti bio je bez presedana u svijetu kibernetičkog napada i naglašavao je duboku stručnost napadača.

Iako nije bilo službeno potvrđeno, napad Stuxneta stručnjaci pripisuju zajedničkom naporu Sjedinjenih Američkih Država i Izraela (Unit 8200).

[15] Wired.com https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (posjećeno 2023.)



Slika 5.1. Kako se odvio Stuxnet napad [16]

5.3. Napad na električnu mrežu Ukrajine (2015.)

Napad je počeo isključenjem električne energije u nekoliko regija zapadne Ukrajine, uključujući Ivano-Frankivsk, Lviv i Ternopil. Ovaj incident doveo je do prekida u opskrbi električnom energijom tijekom hladne zime, stvarajući ozbiljne poteškoće za građane i tvrtke. Napad se dogodio tijekom vrhunca ukrajinskog sukoba s proruskim separatistima na istoku zemlje, što je pojačalo sumnje u rusku povezanost.

Stručnjaci kažu da je malware poznat kao "Industroyer" ili "Crash Override" drugi takav u svijetu, nakon Stuxneta. Zajedničko im je da uzrokuju fizičku štetu na postrojenjima.

Analize nakon napada otkrile su da su napadači koristili malware kako bi se infiltrirali u računalne sustave energetskih kompanija i preuzeli kontrolu nad kritičnim komponentama električne mreže. Nakon što su preuzeli kontrolu, napadači su udaljeno isključivali sklopke i prekidače, uzrokujući prekide u opskrbi električnom energijom.

[16] IEEE Spectrum The Real Story of Stuxnet - IEEE Spectrum (posjećeno 2023.)

Iako se napad brzo sanirao, a električna energija ponovno uspostavljena, ovaj incident postao je upozorenje svijetu o mogućnostima kibernetičkih napada na kritičnu infrastrukturu. Osim toga, napad na ukrajinsku električnu mrežu ilustrira kako se kibernetičko ratovanje koristi kao sredstvo izvan vojnog sukoba za postizanje političkih ciljeva i stvaranje dezinformacija. [17]

5.4. Sony (2014.)

Napad na Sony dogodio se u studenom 2014. godine i predstavljao je jedan od najznačajnijih i najmedijski eksponiranih kibernetičkih napada u povijesti. Ovaj napad ciljao je Sony Pictures Entertainment, filmsku i televizijsku podružnicu japanskog multinacionalnog konglomerata Sony Corporation. Prouzročio je velike štete tvrtki, uključujući krađu osjetljivih podataka, curenje e-pošte poznatih osoba i prijetnje terorističkim napadima.

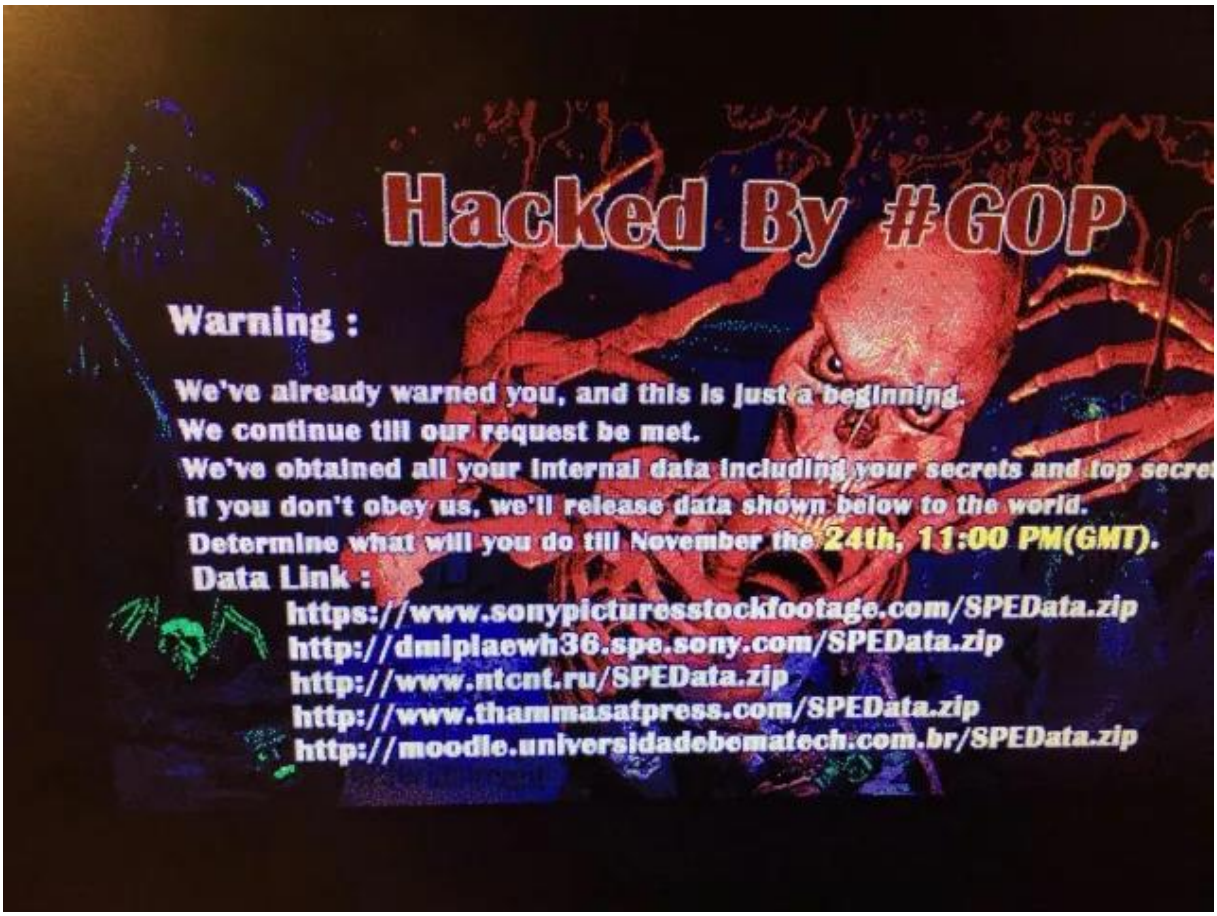
Autori ovog napada nisu bili neposredno poznati na početku, ali su se kasnije identificirali kao grupa nazvana "Guardians of Peace" ili skraćeno GOP. Iako su tvrdili da djeluju iz ideoloških razloga i u ime pravde, mnogi stručnjaci i američke vlasti sugerirali su da bi iza napada mogla stajati Sjeverna Koreja. No, važno je napomenuti da službena potvrda o izvoru napada nije postojala.

Napad je započeo u studenom 2014. godine, kada su zlonamjerne aktivnosti prvi put primijećene u mreži Sony Pictures Entertainment. Napadači su se postupno infiltrirali u mrežu i prikupljali podatke tijekom razdoblja od nekoliko tjedana. Prvi znakovi napada postali su vidljivi kada su interni dokumenti i e-poruke zaposlenika procurili na javne internetske platforme u prosincu iste godine. Napad je bio vrlo sofisticiran i raznovrstan. Napadači su koristili različite tehnike društvenog inženjeringa, phishing, tehnike zaobilaženja sigurnosnih sustava i šifriranih komunikacija kako bi se infiltrirali u mrežu tvrtke. Ključni trenutak bio je kada su napadači uspjeli preuzeti kontrolu nad glavnim poslužiteljem i serverima Sony Pictures Entertainmenta.

Nakon infiltracije, napadači su počeli krađu i šifriranje velikih količina osjetljivih podataka, uključujući interne dokumente, financijske informacije, e-poruke zaposlenika i, najpoznatije, niz neobjavljenih filmova studija. Također su prijetili terorističkim napadima na kina koje bi prikazivala film "The Interview," komediju koja je parodirala sjevernokorejskog lidera Kim Jong-una. “The Interview” je navodno bio i razlog napada na Sony. [18]

[17] Wired.com https://www.wired.com/story/crash-override-malware/ (posjećeno 2023.)
[18] Cinemagic: The Sony Picures hack explained The Sony Pictures Hack Explained (posjećeno 2023.)

Reakcija na napad bila je brza i snažna. FBI je preuzeo istragu, a američka vlada uvela sankcije protiv Sjeverne Koreje kao odgovor na sumnje o njihovoj povezanosti s napadom. Sony Pictures Entertainment donio je odluku o povlačenju filma "The Interview" iz nekoliko kina, ali ga je kasnije izdao digitalno. Također su pojačali sigurnosne mjere i revidirali svoje postupke zaštite podataka. [19]



Slika 5.2. Ekran računala hakiranog u napadu

5.5. Američki izbori 2016.

Napad na američke izbore 2016. godine bio je iznimno značajan događaj u svijetu kibernetičkog ratovanja. Ovaj napad bio je usmjeren na američki politički sustav i posebno na demokratski proces tijekom predsjedničkih izbora. Iako nema nedvojbenih dokaza o upletenosti ruske vlade, mnogi stručnjaci i obavještajne agencije sugerirali su da su ruski akteri bili umiješani u ovaj napad.

[19] Wired.com https://www.wired.com/2014/12/sony-hack-what-we-know/ (posjećeno 2023.)

Virtualni napad na izbore 2016. godine dogodio se tijekom predsjedničke kampanje u Sjedinjenim Američkim Državama. Napadi su počeli ranije u kampanji, a kulminirali su tijekom ljeta i jeseni 2016. godine, u tjednima koji su prethodili izborima održanim 8. studenog 2016. godine. Početkom 2016. godine, hakiranje je izvršeno na računalne sustave Demokratske nacionalne komisije (DNC), glavnog odbora Demokratske stranke SAD-a. Hakeri su provalili u sustav DNC-a i krađom e-poruka i dokumenata izazvali veliki skandal kada su te informacije objavili putem WikiLeaks-a. Prikazane informacije izazvale su kontroverze unutar stranke i naškodile kampanji Hillary Clinton.

Ruski akteri su također izveli ciljane phishing kampanje, pokušavajući prevariti pojedince povezane s izbornom kampanjom, uključujući osoblje Clintonove kampanje. Cilj ovih napada bio je prikupljanje pristupnih podataka i osjetljivih informacija.

Postojali su i napadi na biračke sustave nekoliko država u SAD-u. Iako nije došlo do masovnog hakiranja samih izbornih rezultata, napadi su uzrokovali zabrinutost zbog ranjivosti izbornog sustava. [20]

Osim moguće državne uključenosti, postoje i indicije da su pojedinačni ruski hakeri bili motivirani željom za širenjem dezinformacija, stvaranjem nereda u američkom političkom sustavu i poticanjem podjela.

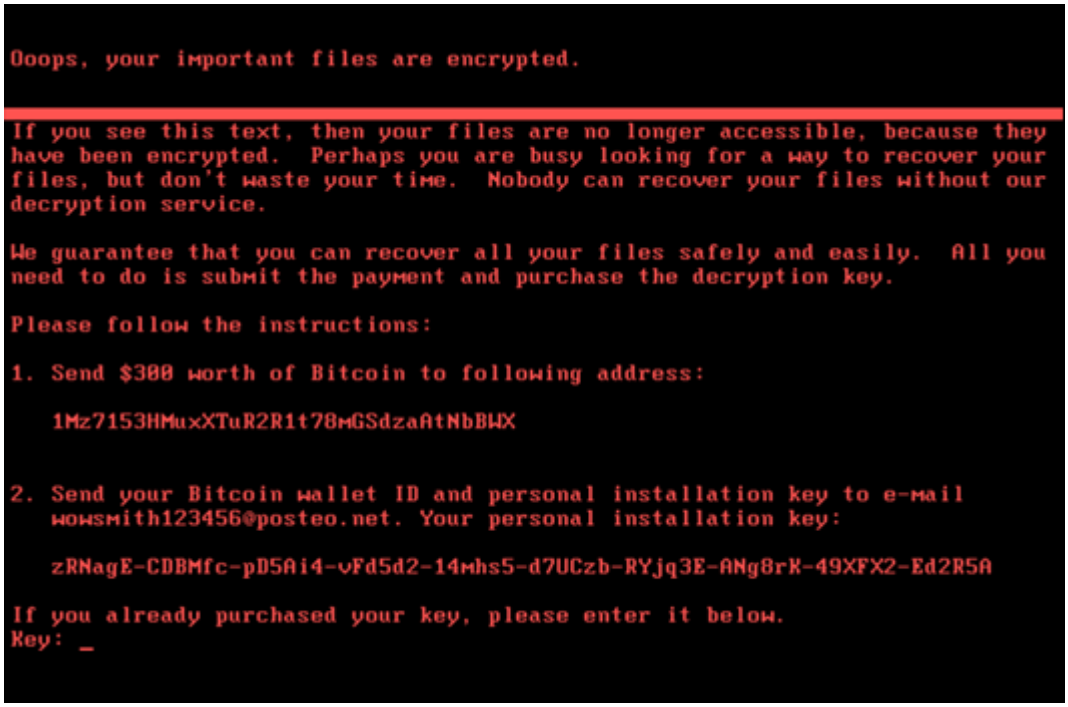
Napad se dogodio u vrijeme napetih odnosa između Sjedinjenih Američkih Država i Rusije, uključujući sankcije protiv Rusije i napetosti u Ukrajini. Neki analitičari sugeriraju da bi napadi mogli biti povezani s geopolitičkim interesima Rusije i tadašnjim ruskim vojnim djelovanjima u Europi, Aziji i Africi. Napadi su također ukazali na ranjivost američkog izbornog sustava i potrebu za poboljšanjem kibernetičke sigurnosti u procesu glasanja.

5.6. NotPetya (2017.)

Napad NotPetya, poznat i kao Petya, predstavlja jedan od najdestruktivnijih i najsofisticiranijih kibernetičkih napada u povijesti, a dogodio se u lipnju 2017. godine. Iako se napad činio kao ransomware, brzo se ispostavilo da je imao mnogo dublje i ozbiljnije posljedice. Ovaj napad prvenstveno je ciljao Ukrajinu, ali je brzo eskalirao i zahvatio tisuće računala širom svijeta, uzrokujući ozbiljne gospodarske i sigurnosne posljedice.

[20] Time magazin, https://time.com/5565991/russia-influence-2016-election/ (posjećeno 2023.)

NotPetya je prvi put otkriven u Ukrajini i širio se putem zlonamjernog ažuriranja računalnih programa. Ispričavao se kao ažuriranje računalnih sustava, ali umjesto toga, inficirao bi računala s malwareom. Ovaj malware iskorištavao je poznate ranjivosti u Windows operativnom sustavu kako bi se proširio i infiltrirao računala.[21]



Slika 5.3. Prikaz ekrana zaraženog računala

Ono što je napad NotPetya činilo posebno razornim bila je njegova sposobnost brze lateralne kretnje kroz zaraženu mrežu, što je rezultiralo brzim širenjem i zarazom drugih računala u istoj mreži. Jednom kad bi se računalo zarazilo, malware bi se pokušao širiti unutar mreže i inficirati druge uređaje, što je prouzročilo kaskadni efekt širenja napada.

NotPetya je šifrirao podatke na zaraženim računalima. Nakon infekcije korisnici bi vidjeli poruku o otkupnini koja traži plaćanje u Bitcoinima kako bi dešifrirali svoje podatke. Međutim, čak i nakon što bi žrtve platile otkupninu, njihovi podaci nisu bili vraćeni, jer su napadači uništavali ključeve za dešifriranje.[22]

Iako su prve naznake ukazivale na to da je riječ o običnom ransomware napadu, brzo se ispostavilo da su motivi napadača bili mnogo dublji. Istražitelji su otkrili da je cilj napadača bio uzrokovati kaos i štetu, umjesto ostvarenja financijske dobiti putem otkupnine. Mnogi su sumnjali u ruski izvor napada, iako službena potvrda nije postojala. [23]

---

[21] Wired.com https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (posjećeno 2023.)

[22] DarkNet Diaries https://darknetdiaries.com/episode/54/ (posjećeno 2023.)

[23] Deutsche Welle Documentary: Drones, hackers and mercenaries - The future of warfare https://www.youtube.com/watch?v=MZ60UDys_ZE (posjećeno 2023.)

5.7. WannaCry (2017.)

Napad ransomwarea poznat pod nazivom "WannaCry" dogodio se u svibnju 2017. godine i postao je jedan od najpoznatijih i najrazornijih kibernetičkih napada u povijesti. WannaCry je izazvao globalnu zabrinutost zbog svoje sposobnosti brzog širenja i ozbiljnih posljedica po računalne sustave širom svijeta.

Napad WannaCry koristio je zlonamjerni program koji je iskorištavao ranjivost u Microsoft Windows operativnom sustavu pod nazivom "EternalBlue" (originalno razvijen od strane Nacionalne agencije za sigurnost - NSA). Ranjivost je bila poznata vlastima, ali mnogi korisnici nisu instalirali zakrpu koju je Microsoft izdao kako bi je ispravio. To je omogućilo napadačima da brzo šire ransomware putem mreže, posebno u korporativnim okruženjima.

Na zaraženim računalima, WannaCry bi šifrirao podatke na disku i prikazao otkupninu koja traži plaćanje u Bitcoinima kako bi žrtve dobile ključ za dešifriranje svojih podataka. Napad se proširio širom svijeta, zarazio stotine tisuća računala u više od 150 zemalja te uzrokovao velike gubitke i prekide u poslovanju.

Napad WannaCry brzo je postao globalna prijetnja, a žrtve su uključivale velike korporacije, bolnice, vlade i obične korisnike. Jedna od najpoznatijih žrtava bila je britanska Nacionalna zdravstvena služba (NHS), što je dovelo do otkazivanja tisuća operacija i pregleda. [24]

Iako se autori napada nikada nisu potpuno identificirali, neki su sugerirali da je napad mogao potjecati iz Sjeverne Koreje ili iz kriminalnih skupina koje su pokušavale profitirati od ranjivosti u sigurnosti računalnih sustava. Napad WannaCry ostaje podsjetnik na to koliko je važno ozbiljno shvatiti kibernetičku sigurnost i uložiti napore kako bi se zaštitili računalni sustavi i podaci.

[24] DarkNet Diaries https://darknetdiaries.com/episode/73/ (posjećeno 2023.)

Slika 5.4. Prikaz WannaCry ransomwarea

5.8. Solarwinds (2020.)

SolarWinds kibernetički napad bio je ogroman napad na opskrbni lanac koji je kompromitirao softverske nadogradnje SolarWindsa, istaknute tvrtke za upravljanje i nadzor IT sustava. Napadači su ubacili zlonamjerni kod u SolarWinds-ov softver poznat kao Orion.

SolarWinds-ova platforma Orion široko se koristi u mnogim organizacijama, uključujući vladine agencije i Fortune 500 tvrtke, kako bi upravljale i nadzirale svoju IT infrastrukturu.

Američke obavještajne agencije i stručnjaci za kibernetičku sigurnost brzo su povezali napad s grupom APT29 ili Cozy Bear. Cozy Bear ima povijest sofisticiranih kibernetičkih kampanja. Napadači su održavali visoku razinu skrivene aktivnosti i sofisticiranosti tijekom operacije, što je otežavalo otkrivanje i direktno povezivanje napada s određenim akterima. Iskoristili su ranjivost u procesu softverskog ažuriranja, ubacujući "Sunburst" u SolarWinds-ov softver Orion. Kada su korisnici instalirali ova kompromitirana ažuriranja, napadačima je omogućen pristup sustavima.

Nakon što su ušli u kompromitirane mreže, napadači su se kretali neprimjetno, ostajući neotkriveni mjesecima i pristupajući osjetljivim podacima i sustavima. Proveli su špijunažu, eksfiltrirali podatke i potencijalno prikupili kritične informacije.

Šteta uzrokovana napadom SolarWinds bila je značajna. Napadači su mogli pristupiti mrežama organizacija, špijunirati komunikaciju i krađom podataka ugroziti sigurnost i povjerljivost informacija. Važno je napomenuti da se napad nekoliko mjeseci nije otkrio, što je omogućilo napadačima da dugotrajno djeluju u kompromitiranim sustavima.[25]

5.9. Napad na vladu Kostarike (2022)

Napad na vladu Kostarike dogodio se za vrijeme predsjedničkih izbora u toj državi. Kriminalna organizacija Conti, poznata po svojoj pro-ruskoj ideologiji, napala je 30 različitih državnih institucija. Osim ransomware napada, ukradeni su podaci građana, emailovi i srušene su web stranice. Vlada je morala ugasiti svoje kompjuetske sisteme što je uzrokovalu štetu u desecima milijuna dolara.

Grupa Conti poznata je po svom ransomwareu kojeg su koristili u ovom napadu. Za povrat podataka tražili su 10 milijuna dolara, no vlada Kostarike nije pristala na zahtjeve. Po završetku izbora, predsjednik je proglasio ratno stanje u državi, nazivajući napade terorističkima. Ovaj napad je prouzročio tromjesečni kaos, zbog nefunkcioniranja vladinih sustava, narod je protestirao. [26][27]

[25] CNBC The SolarWinds Hack And The Future Of Cyber Espionage The SolarWinds Hack And The Future Of Cyber Espionage (posjećeno 2023.)
[26] Wired.com https://www.wired.com/story/costa-rica-ransomware-conti/ (posjećeno 2023.)
[27] Americas Quarterly The Dramatic Cyberattack That Put Latin America on Alert (posjećeno 2023.)

6. Posljedice virtualnih sukoba

Svaki sukob nosi određene posljedice koje imaju dublje i složenije aspekte koji se protežu kroz različite sfere društva, gospodarstva i sigurnosti. Moguće posljedice su:

- Gubitak povjerljivih informacija: Kibernetički napadi mogu rezultirati gubitkom osjetljivih informacija kao što su osobni podaci, zdravstveni dosjei, vojne tajne i poslovne strategije. Ovo ne samo da ugrožava privatnost pojedinaca nego također može dovesti do financijske štete i pravne odgovornosti za organizacije koje su odgovorne za gubitak informacija.
- Šteta ugledu: Oštećenje ugleda organizacije ili države može imati dugoročne posljedice na njezinu sposobnost privlačenja klijenata, partnera i investitora. Nakon takvih napada, organizacije moraju ulagati u obnovu svog ugleda putem transparentnih komunikacija i demonstriranja poboljšane sigurnosti.
- Ekonomske posljedice: Kibernetički napadi mogu prouzročiti velike ekonomske gubitke. Tvrtke mogu izgubiti novac zbog otkupa podataka, gubitka poslovanja ili smanjenja vrijednosti dionica. Države također moraju izdvajati sredstva za obnovu kritičnih infrastrukturnih sistema, što može opteretiti proračune.
- Uništenje infrastrukture: Napadi na kritičnu infrastrukturu mogu dovesti do poremećaja u opskrbi strujom, prometu, vodi i komunikacijama. Ovisno o razmjerima, ovi napadi mogu ugroziti živote i bezbjednost građana, te zahtijevati ozbiljne napore za ponovnu uspostavu normalnog funkcioniranja.
- Špijunaža: Špijunaža putem kibernetičkog ratovanja omogućava državama prikupljanje obavještajnih podataka o svojim protivnicima. Dok može pružiti prednosti u razumijevanju namjera drugih zemalja, takva špijunaža može dovesti do diplomatskih kriza i izazvati nepovjerenje između država.
- Eskalacija sukoba: Kibernetički napadi mogu potencijalno izazvati eskalaciju napetosti između država, jer može biti teško utvrditi tko stoji iza napada. Kako bi se izbjegli konflikti, međunarodna suradnja i postizanje sporazuma o kibernetičkoj sigurnosti postaju ključni.
- Ugroza privatnosti i život pojedinaca: Kibernetički napadi mogu ugroziti privatnost pojedinaca i dovesti do zloupotrebe njihovih osobnih podataka. Ovo ima šire implikacije jer se odnosi na pitanje kako organizacije čuvaju i obrađuju osobne podatke građana.

- Društvena nesigurnost: Kibernetički napadi koji šire dezinformacije i lažne vijesti mogu polarizirati društva i poticati socijalnu nesigurnost. U eri digitalnih medija, to može dovesti do ozbiljnih problema sa stabilnošću društva odnosno pojedinih nacija.
- Nestabilnost interneta: Kibernetički napadi koji ciljaju infrastrukturu interneta mogu rezultirati globalnom nestabilnošću u komunikaciji i ekonomiji. Ovo podcrtava važnost očuvanja struktura interneta kao ključnog dijela svjetske povezanosti.
- Zloupotreba tehnologije: Zloupotreba tehnologije za kibernetičko ratovanje može uključivati koordinirane napade na online usluge i stranice, što dovodi do nedostupnosti tih resursa. To ima široke posljedice na korisnike i kompanije koje ovise o tim online resursima.

Virtualni sukobi imaju posljedice koje se protežu daleko izvan digitalnog prostora. Mogu utjecati na ekonomiju, nacionalnu sigurnost, privatnost i svakodnevni život pojedinaca. Kibernetičkim napadima moguće je prouzročiti donedavno nezamislivu fizičku i emocionalnu štetu pojedincima ili cijelim društvima i nacijama.[28]

[28] Yuchong Li, Qinghui Liu. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments; https://www.sciencedirect.com/science/article/pii/S2352484721007289?via%3Dihub (posjećeno 2023.)

7. Budućnost sukoba u virtualnom prostoru

Budućnost kibernetičkog ratovanja nosi nove izazove i promjene u dinamici sukoba u kibernetičkom prostoru. Evo detaljnijeg pregleda ključnih aspekata budućnosti kibernetičkog ratovanja:

- Složeniji i sofisticiraniji napadi: Napadi će postati sve složeniji i sofisticiraniji. Napadači će koristiti napredne tehnike kao što su napadi s naprednim upravljanjem prijetnjama (Advanced Persistent Threats - APTs) i zero-day ranjivosti kako bi izbjegli otkrivanje.
- Socijalni inženjering i psihološko ratovanje: Kibernetički napadači mogli bi sve više koristiti psihološke manipulacije i taktike socijalnog inženjeringa kako bi iskoristili ljudske ranjivosti i pristupili kritičnim sustavima.
- Automatizacija napada i obrane: Napadači će sve više koristiti automatizaciju, posebno uz pomoć umjetne inteligencije (AI), za provođenje napada. Obrana će također koristiti AI za prepoznavanje i neutralizaciju prijetnji u stvarnom vremenu. Brza i automatska detekcija i odgovor postat će ključni za suzbijanje napada.
- Nedefinirane granice: Granica između kibernetičke špijunaže, kibernetičkog kriminala i kibernetičkog ratovanja i dalje će se zamagljivati. Hakeri pod državnom kontrolom mogu se baviti i kibernetičkom špijunažom i destruktivnim napadima, što otežava pripisivanje napada odgovornim entitetima.
- Dronovi će postati ključan element u budućem kibernetičkom ratovanju, kombinirajući kibernetičke sposobnosti s fizičkom prisutnošću. Koristit će se za napade na računalne mreže i sustave, isporuku kibernetičkih oružja te za izvid i prikupljanje obavještajnih podataka. Razvijat će se i protumjere za detekciju i obranu od neprijateljskih dronova, dok će njihova integracija s umjetnom inteligencijom omogućiti autonomnije operacije. Uz potencijalne prednosti, njihova upotreba postavlja i važna etička i sigurnosna pitanja.
- Kvantna računala: Pojava kvantnih računala nosi sa sobom prilike i prijetnje. Dok kvantni računalni mogu narušiti trenutne algoritme za šifriranje, isto tako mogu omogućiti nove, sigurnije oblike šifriranja.
- Ciljanje infrastrukture: Kritična infrastruktura, uključujući energetske mreže, telekomunikacijske, vodovodne i prometne sustave te zdravstvene ustanove postat će još atraktivniji ciljevi. Napadi na ove sustave mogu imati ozbiljne posljedice na gospodarstvo i nacionalnu sigurnost, što će povećati potrebu za njihovom zaštitom.

- Zero-trust security: Pristup sigurnosti nultog pouzdanja postat će sve šire prihvaćen, pri čemu organizacije pretpostavljaju da nijedan entitet, bilo unutar ili izvan njihove mreže, ne može biti automatski pouzdan.
- Manjak radne snage: Potražnja za stručnjacima za kibernetičku sigurnost nastavit će nadmašivati ponudu, stvarajući manjak radne snage. Organizacije i vlade morat će ulagati u obuku i edukaciju kako bi stvorile stručnu radnu snagu.
- Aktivne obrambene strategije: Proaktivne i aktivne obrambene strategije, kao što su lov na prijetnje i tehnologije obmane, dobit će na važnosti kako bi se organizacijama omogućilo rano prepoznavanje prijetnji i ometanje operacija napadača.
- Razmjena kibernetičkih alata: Države i organizacije će sve više razmjenjivati kibernetičke alate i ranjivosti kako bi podržali svoje operacije. To može dovesti do eskalacije u kibernetičkim konfliktima i povećane opasnosti od širenja napadačkih tehnika.
- Širenje kibernetičkog prostora: Kako se povećava broj uređaja povezanih na internet, uključujući pametne uređaje (Internet stvari - IoT), kibernetički prostor će se širiti. Ovo otvara nove površine za napade, uključujući i potencijalne prijetnje u sektoru zdravstva, transporta, i industrije.
- Važnost zaštite privatnosti: Kako se prikuplja i obrađuje sve više osobnih podataka, očekuje se jača regulacija i pažnja prema zaštiti privatnosti građana. Države će se suočiti s izazovima očuvanja sigurnosti dok istovremeno poštuju građanske slobode i prava.
- Širenje ofenzivnih sposobnosti: Širenje ofenzivnih kibernetičkih sposobnosti na neslužbene aktere i kibernetičke plaćenike povećat će broj potencijalnih prijetnji, čineći pejzaž složenijim.
- Međunarodna suradnja: S obzirom na globalnu prirodu kibernetičkih prijetnji, međunarodna suradnja postat će još važnija. Sklapanje međunarodnih sporazuma i protokola za suzbijanje kibernetičkog ratovanja i zaštitu kritične infrastrukture bit će ključni izazovi. Države će ostati dominantni sudionici u kibernetičkom ratovanju. Velike sile će ulagati značajne resurse u svoje kibernetičke sposobnosti, a kibernetičke operacije postat će neodvojiv dio vojnih strategija i nacionalne sigurnosti.
- Naglasak na obrazovanju i stručnosti: Stručnjaci za kibernetičku sigurnost postat će sve važniji. Obrazovanje, razvoj vještina i usavršavanje u ovom području bit će ključni za zaštitu organizacija i država od kibernetičkih prijetnji.

Budućnost kibernetičkog ratovanja obilježit će povećana složenost, dominacija državnih aktera i integracija kibernetičkih sposobnosti u vojne doktrine. Kibernetička sigurnost bit će ključna komponenta nacionalne sigurnosti, a organizacije se moraju prilagoditi mijenjajućem okruženju

prijetnji implementiranjem snažnih kibernetičkih obrana i usvajanjem proaktivnih sigurnosnih strategija. Međunarodna suradnja i razvoj normi u kibernetičkom prostoru bit će ključni u sprječavanju i ublažavanju kibernetičkih sukoba.[29]

[29] Deutsche Welle Documentary: Drones, hackers and mercenaries - The future of warfare Drones, hackers and mercenaries - The future of war | DW Documentary (posjećeno 2023.)

Zaključak

U završnom radu na temu sukoba u virtualnom prostoru istražena je tema vojnih sukoba u virtualnom prostoru. Kroz analizu povijesti, alata, tehnologije, strategija i posljedica kibernetičkog ratovanja, stečeno je dublje razumijevanje ovog izazova s kojim se suočava današnje društvo. Iako su mnogi aspekti kibernetičkog ratovanja izuzetno složeni i promjenjivi, nekoliko ključnih zaključaka moguće je izdvojiti iz ovog istraživanja.

Prvo, kibernetičko ratovanje postalo je neizbježna stvarnost suvremenog svijeta. Tehnološki napredak omogućio je napadačima da iskoriste ranjivosti u digitalnom prostoru i nanose štetu državama, organizacijama i pojedincima. Sveprisutnost interneta i povezanost digitalnih sustava čini nas ranjivima na kibernetičke napade iz različitih izvora.

Drugo, kibernetičko ratovanje je izuzetno dinamično i neprestano evoluira. Napadači su iznimno vješti u prilagodbi novim tehnikama i taktikama, dok se obrambeni kapaciteti pokušavaju sustići s tom evolucijom.

Treće, međunarodna zajednica mora zajedno raditi na suzbijanju kibernetičkog ratovanja. Ograničavanje širenja kibernetičkih oružja, uspostavljanje jasnih normi ponašanja u kibernetičkom prostoru i jačanje međunarodne suradnje ključni su elementi za suočavanje s ovom prijetnjom. Diplomacija i međunarodni pregovori igraju važnu ulogu u izgradnji povjerenja između država.

Četvrto, obrazovanje i svijest o kibernetičkoj sigurnosti su ključni. Svaka organizacija i pojedinac trebao bi razumjeti osnovne koncepte kibernetičke sigurnosti i pridržavati se najboljih praksi kako bi se smanjio rizik od napada. Također je važno educirati ljude o mogućim posljedicama kibernetičkih napada kako bi se stvorila veća svijest o ovoj temi.

Peto, kibernetičko ratovanje ima ozbiljne posljedice. Osim gubitka podataka i financijskih šteta, kibernetički napadi mogu dovesti do ozbiljnih političkih, društvenih i ekonomskih poremećaja. Stoga je važno da države i organizacije razvijaju planove za reagiranje na kibernetičke incidente i minimiziranje njihovih posljedica.

Kod istraživanja i pisanja proveden je kratki razgovor s jednim ekspertom na polju virtualne zaštite, koji je dao smjernice za prava mjesta za početak istraživanja te objasnio neke pojmove. Bavio se time duži niz godina, između ostalog spriječio je i teroristički napad, ali taj posao ostavio je veće posljedice na njegov duševni mir.

Korporacije, vlade, privatni akteri su u konstantnom ratu u virtualnoj stvarnosti, u ratu o kojem šira populacija nema puno saznanja, ali je itekako dio toga, barem na onoj

(dez)informacijskoj razini. Propaganda je odavno prešla na virtualni svijet i mi kao korisnici interneta u dobu kad je sve spojeno na internet izloženi smo bombardiranju raznih informacija i dezinformacija od strane različitih aktera. Osim toga, pojavom kompjutera i širokopojasnog interneta povećao se i broj virusa, crva, ransomwarea, botova i ostalih zloćudnih programa kojima je cilj prouzročiti štetu krajnjoj žrtvi. S obzirom da tehnika i tehnologija konstatno napreduje, zapravo jedini način da se zaštitimo od napada na nas osobno je praćenje tog razvoja, ažuriranje programa, korištenje firewalla i najbitnije od svega, izbjegavanje sumnjivih linkova.

U zaključku, sukobi u virtualnom prostoru predstavljaju kompleksnu i ozbiljnu prijetnju koja zahtijeva pažnju međunarodne zajednice. Suvremeni svijet sve više ovisi o digitalnim tehnologijama, što čini kibernetički prostor izrazito važnim. Iako se suočavamo s izazovima, suradnjom, obrazovanjem i inovacijama možemo smanjiti rizik od kibernetičkih napada i zaštititi naše digitalne resurse. Kibernetičko ratovanje ostaje trajna prijetnja, ali uz adekvatne mjere možemo minimizirati njegove posljedice i zajedno

Bibliografija

Knjige i članci

Andress, Jason i Steve Winterfeld: Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, SAD, 2013.

Andress, J. i Steve Winterfeld. The Basics of Cyber Warfare in Theory and Practice, SAD, 2012.

Even, Shmuel i David Siman-Tov. Cyber Warfare: Concepts and Strategic Trends, Izrael, 2012.

Janczewski, Lech J. i Colarik, Andrew M. Cyber Warfare and Cyber Terrorism, SAD, 2008.

Tabansky, Lior. Basic Concepts in Cyber Warfare, SAD, 2011.

Yuchong Li, Qinghui Liu. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments; https://www.sciencedirect.com/science/article/pii/S2352484721007289?via%3Dihub (posjećeno 2023.)

Web članci

Americas Quarterly The Dramatic Cyberattack That Put Latin America on Alert (posjećeno 2023.)

IEEE Spectrum The Real Story of Stuxnet - IEEE Spectrum (posjećeno 2023.)

TechTarget.com 13 Common Types of Cyber Attacks and How to Prevent Them (posjećeno 2023.)

Time magazin, https://time.com/5565991/russia-influence-2016-election/ (posjećeno 2023.)

Wired.com https://www.wired.com/story/russian-hackers-attack-ukraine/ (posjećeno 2023.)

Wired.com https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (posjećeno 2023.)

Wired.com https://www.wired.com/story/crash-override-malware/ (posjećeno 2023.)

Wired.com https://www.wired.com/2014/12/sony-hack-what-we-know/ (posjećeno 2023.)

Wired.com https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (posjećeno 2023.)

Wired.com https://www.wired.com/story/costa-rica-ransomware-conti/ (posjećeno 2023.)

Audio i video materijali

Cinemagic: The Sony Picures hack explained The Sony Pictures Hack Explained (posjećeno 2023.)

CNBC The SolarWinds Hack And The Future Of Cyber Espionage The SolarWinds Hack And The Future Of Cyber Espionage (posjećeno 2023.)

Deutsche Welle Documentary: Drones, hackers and mercenaries - The future of warfare Drones, hackers and mercenaries - The future of war | DW Documentary (posjećeno 2023.)

DarkNet Diaries https://darknetdiaries.com/episode/54/ (posjećeno 2023.)

DarkNet Diaries https://darknetdiaries.com/episode/73/ (posjećeno 2023.)

Fallout 1, videoigra, Intro, 1997.

Popis ilustracija