Rusko-ukrajinski kibernetički konflikti

Nadoveza, Marija

Undergraduate thesis / Završni rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Humanities and Social Sciences / Sveučilište u Zagrebu, Filozofski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:131:033173

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-09-02**

Sveučilište u Zagrebu
Filozofski fakultet
University of Zagreb
Faculty of Humanities
and Social Sciences

Repository / Repozitorij:

ODRAZ - open repository of the University of Zagreb
Faculty of Humanities and Social Sciences

zir.nsk.hr

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2023./2024.

Marija Nadoveza

Rusko-ukrajinski kibernetički konflikti

Završni rad

Mentor: dr. sc. Vjera Lopina, v.asist

Zagreb, svibanj 2024.

Izjava o akademskoj čestitosti

Izjavljujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Zahvaljujem se svom dečku Mirzi na svoj podršci koju mi je pružio prilikom pisanja ovog završnog rada.

Sadržaj

1. Uvod

U posljednje vrijeme kibernetičko ratovanje je u sve većem porastu. Velik broj zemalja se koristi digitalnim sredstvima ne bi li dobile prevlast nad svojim protivnicima. Teme kibernetičkih sukoba veoma su aktualne danas, a ovakav se tip napada stalno razvija i shvaća sve ozbiljnije. S razvojem kibernetičke prijetnje, razvijaju se i načini obrane od ovakvih napada. Kao što su Lange-Ionatamishvili i Svetoka (2015) istaknule, sukob se može dobiti bez ispaljivanja ijednog metka, a ključne bitke mogu se odvijati u kibernetičkim i komunikacijskim domenama, a ne na kopnu, u zraku i moru. Jednom od takvih sukoba pripada i tekući kibernetički sukob između Rusije i Ukrajine, koji se sve više zahuktava od 2014. godine, kada je Rusija anektirala Krim. U sukob su uključeni hakeri koje sponzorira država, ali i neovisne skupine i pojedinci. Rusko-ukrajinski sukob veoma je aktualan i danas, kada se kibernetičke taktike koriste u kombinaciji s tradicionalnim vojnim operacijama. Ovakvi napadi predstavljaju veliku opasnost, budući da imaju široke implikacije na sigurnost, gospodarstvo i stabilnost obiju zemalja. Ovaj rad pružit će pregled rusko-ukrajinskih kibernetičkih konflikata, uključujući glavne uključene aktere, korištene taktike i utjecaj na obje zemlje. Nakon objašnjenja temeljnih pojmova potrebnih za razumijevanje značenja kibernetičkog konflikta, bit će analizirana povijest rusko-ukrajinskih kibernetičkih sukoba i nekih ključnih događaja koje oni uključuju. Prilikom pisanja ovog rada korištena je literatura na hrvatskom, engleskom i ruskom jeziku.

2. Kibernetički napad

Kibernetički napadi, sukobi i ratovi stalno se razvijaju i predstavljaju izazov nacionalnoj sigurnosti i međunarodnoj stabilnosti. Predstavljaju sjecište tehnologije, politike i ratovanja u digitalnom dobu. Kako bi razumjeli važnost ove prijetnje i značenje rada u cjelosti, potrebno je pobliže objasniti što je to kibernetički napad ili sukob, te kakve vrste kibernetičkih napada se koriste.

2.1. Definicija kibernetičkog napada

Postoji mnogo različitih definicija kibernetičkog napada (eng. *cyberattack*) , a varijacije u definicijama proizlaze uglavnom zbog razlika u perspektivi, stručnosti ili fokusu, budući da je polje kibernetičke sigurnosti ogromno i stalno se razvija. Prema Hathawayu i sur. (2012), bilo koja radnja poduzeta za potkopavanje funkcija računalne mreže u svrhu političke ili nacionalne sigurnosti se može nazvati kibernetičkim napadom. Hathaway i sur. objašnjavaju kako radnja mora biti aktivna, bilo napad ili aktivna obrana. Aktivna obrana uključuje elektroničke protumjere osmišljene za napad računalnih sustava koji napadaju i za zaustavljanje kibernetičkih napada koji su u tijeku. Aktivna i pasivna obrana su često osmišljene za rad u tandemu, ali pasivna obrana sama po sebi se ne može smatrati kibernetičkim napadom. Kibernetički napad se može izvesti bilo kojom radnjom, ali mora imati za cilj potkopavanje ili prekid rada računalne mreže. Budući da Hathaway i sur. definiraju kibernetički napad prema njegovom cilju, bilo koje sredstvo se može koristiti za njegovo izvršenje. Kibernetička špijunaža i kibernetičko iskorištavanje nisu kibernetički napadi jer ne uključuju mijenjanje računalnih mreža na način koji utječe na njihovu sadašnju ili buduću sposobnost funkcioniranja. Da bi se „potkopala funkcija“ računalnog sustava, mora biti učinjeno više od pasivnog promatranja računalne mreže ili kopiranja podataka, čak i ako je to promatranje tajno. Mora se utjecati na rad sustava bilo oštećenjem operativnog sustava ili dodavanjem lažnih, pogrešnih ili nepoželjnih informacija. Kibernetički napad mora biti usmjeren na računalnu mrežu, pri čemu se računalna mreža definira kao sustav računala i uređaja povezanih komunikacijskim kanalima, a koncept računala obuhvaća više od jednostavnog stolnog ili prijenosnog računala. Kibernetički kriminal koji nije izvršen u svrhu političke ili nacionalne sigurnosti nije kibernetički napad.

Uma i Padmavathi (2013) opisuju kibernetički napad kao iskorištavanje kibernetičkog prostora u svrhu pristupa neovlaštenim ili sigurnosnim informacijama, špijuniranja,

onemogućavanja mreža, krađe podataka i novca. Priroda, složenost i ozbiljnost ovih napada s vremenom se povećavaju. Trenutačno postoji relativan nedostatak razumijevanja različitih vrsta napada, njihovog načina širenja i njihove ozbiljnosti što je mnoge zemlje učinilo ranjivima na takve napade.

Roscini (2014) definira kibernetički napad kao operacije, bilo u napadu ili obrani, namijenjene izmjeni, brisanju, oštećenju ili uskraćivanju pristupa računalnim podatcima ili softveru, te je naveo tri moguće svrhe ovih napada. Prva svrha je propaganda ili prijevara, druga je djelomično ili potpuno ometanje funkcioniranja ciljanog računala, računalnog sustava ili mreže i povezane fizičke infrastrukture kojom upravlja računalo (ako postoji), a treća je stvaranje fizičke štete izvan računala, računalnog sustava ili mreže.

Prema članku Geersa (2010), kibernetički napadi se naziru kao prijetnja koju je najbolje shvatiti kao sredstvo za širok raspon političkih i vojnih ciljeva, od kojih mnogi mogu imati ozbiljne posljedice za nacionalnu sigurnost. Na primjer, računalno se hakiranje može koristiti za krađu tehnologije ofenzivnog oružja ili za onesposobljavanje protivničke obrane tijekom konvencionalnog vojnog napada. Prema tome, kibernetički napadi mogu biti bitan dio nacionalnih vojnih strategija.

Unatoč velikom broju definicija, sve se slažu u tome da temeljna ideja kibernetičkih napada uključuje zlonamjerne radnje za ugrožavanje računalnih sustava, mreža ili podataka. Kibernetički napadi mogu imati različite oblike, a napadači koriste niz tehnika kako bi postigli svoje ciljeve.

2.2. Kibernetički prostor

Kibernetički ratovi vode se, naravno, u kibernetičkom prostoru (eng. *cyberspace*), koji je svuda oko nas. Pojam kibernetičkog prostora prilično je apstraktan. „To nije određeno geografsko mjesto o kojem možemo govoriti i nije ga jednostavno definirati. To je prijenosno računalo koje vi ili vaše dijete nosite u školu, stolno računalo na poslu. To je jednolična zgrada bez prozora u centru grada i cijevi ispod ulice“ (Clarke i Knake, 2010). Laari (2019), kako je navedeno u radu Juutilaiena (2022) navodi da se u kontekstu finskih obrambenih snaga cyberspace obično shvaća kao domena koju tvore digitalni informacijski sustavi, što također uključuje fizičku komunikacijsku infrastrukturu i sve krajnje korisnike ili entitete. Tipična karakteristika je uporaba elektronike i elektromagnetskog spektra (EMS) za prijenos, modificiranje i pohranu podataka. Juutilaien (2022) navodi da vojne doktrine sjedinjenih

država definiraju kibernetički prostor kao „globalnu domenu unutar informacijskog okruženja koja se sastoji od međuovisne mreže infrastruktura informacijske tehnologije i rezidentnih podataka, uključujući internet, telekomunikacijske mreže, računalne sustave i ugrađene procesore i kontrolere“ (Joint Chiefs of Staff, 2014, navedeno u Juutilaien, 2022). Možemo zaključiti da kibernetički prostor predstavlja nekakvu vrstu virtualnog okruženja u kojem su međusobno povezani računalni sustavi. Ovaj virtualni prostor uvelike je olakšao svakidašnji život, no unutar njega kriju se brojne opasnosti zbog kojih može postati ratnom zonom.

2.3. Vrste kibernetičkih napada

Kibernetički napadi novi su oblik ratovanja ili konflikta. Samim time, vrste ovakvih napada mijenjaju se i sve ih je više. Razvoj tehnologije doprinosi mogućnostima razvoja novih oblika kibernetičkih napada. U radu pod nazivom Kibernetički napadi i njihove različite vrste, Biju, Gopal i Prakash (2019) naveli su neke od vrsta kibernetičkih napada i opisali ih. Prvi su napadi uskraćivanjima usluge (eng. *Denial of service*, odnosno DoS) i distribuirani napadi uskraćivanjima usluge (eng. *Distributed denial of service*, odnosno DDoS). Denial of service napad prekoračuje resurse sustava tako da sustav ne može odgovoriti na zahtjev usluge. Prema Šinceku i Vrbancu (2010), ovi napadi su jedni od najkontroverznijih, najkompleksnijih te najozbiljnijih: DDoS napadi uključuju prvotno provaljivanje u stotine ili tisuće računala putem Interneta. Nakon toga, napadač instalira DDoS program na sve njih, čime zadobije kontrolu nad njima za pokretanje koordiniranog napada na krajnju žrtvu. Ti napadi obično iskorištavaju kapacitet usmjerivača ili mrežne resurse što prekida povezanost mreže i korisnika.

Druga vrsta su Man in the middle (MitM) napadi. MitM napad se događa kada treća strana uđe u komunikaciju između klijenta i poslužitelja. Treća strana oponaša i klijenta i poslužitelja i dobiva pristup informacijama između njih. Mallik (2019) piše o ciljevima ovakvog napada, a to je uzimanje pojedinačnih informacija, na primjer certifikata za prijavu, interesnih točaka računa i brojeva kartica, a mete su uglavnom klijenti financijskih aplikacija i drugih stranica na kojima je potrebna prijava. Informacije dobivene tijekom napada mogu se koristiti u mnoge svrhe, uključujući prijevaru, neodobrenu razmjenu podrške ili nezakonitu promjenu šifre.

Treća navedena vrsta su Phishing poruke. Phishing napad je slanje lažne e-pošte koja izgleda kao da dolazi iz pouzdanih izvora. Glavni cilj ove vrste napada je dobivanje osobnih

podataka i informacija. Alkhalill i sur. (2021) u svom radu opisuju phishing kao primjer vrlo učinkovitog oblika kibernetičkog kriminala koji kriminalcima omogućuje prevaru korisnika i krađu važnih podataka. Trenutno se phishing smatra jednim od najčešćih primjera prijevara na Internetu. Phishing napadi mogu dovesti do ozbiljnih gubitaka za žrtve, uključujući osjetljive informacije, krađu identiteta, tvrtke i državne tajne.

Slijede napadi umetanjem SQL koda, koji se koriste zlonamjernim kodom kako bi se pristupilo informacijama, manipulirajući bazom podataka u pozadini. Halfond, Viegs i Orso (2006) opisuju ovakve napade kao ozbiljnu sigurnosnu prijetnju web aplikacijama jer napadačima omogućuju neograničeni pristup bazama podataka koje se nalaze u pozadini aplikacija i potencijalno osjetljivim informacijama koje te baze podataka sadrže. U nekim slučajevima napadači mogu koristiti SQL kod kako bi preuzeli kontrolu i oštetili sustav koji hostira web aplikaciju.

Slijede napadi zlonamjernim softverom (engl. *malware*). To je vrsta kibernetičkog napada u kojem se zlonamjerni softver instalira na računalo korisnika bez ikakvog pristanka korisnika. „Zlonamjerni softver, koji je okarakteriziran kao štetan softver, infiltrira se u sustave domaćina, oštećuje operativne sustave ili mreže i uzrokuje mnoge komplikacije, uključujući krađu podataka“ (Ferdous i sur. 2023).

Ovo su samo neki od tipova kibernetičkih napada koji se mogu dogoditi. Ovakvi napadi mogu imati ozbiljne posljedice, uključujući povrede podataka, financijske gubitke, štetu reputaciji i poremećaje kritične infrastrukture. Napadači neprestano razvijaju nove vrste napada. Kako tehnologija napreduje i otkrivaju se nove ranjivosti, kibernetički kriminalci brzo pronalaze načine da ih iskoriste.

2.4. Kibernetički napad kao oružani napad

Kibernetički napadi mogu nanijeti štete ogromnih razmjera, no znači li to da se oni mogu smatrati oružanim napadima? Kako Graham naovodi, ni sam pojam oružanog napada nije jasno definiran, stoga nije lako ni odgovoriti na ovo pitanje. „Međunarodni sud pravde istaknuo je nužnost razlikovanja najtežih oblika uporabe sile (onih koji predstavljaju oružani napad) od manje teških oblika te je naveo da će se radnja kvalificirati kao oružani napad ako postigne određeni razmjer i posljedice. Međunarodni konsenzus smatra da kriteriji koje je iznio Jean Pictet kako bi se utvrdilo postojanje međunarodnog oružanog sukoba prema zajedničkom članku broj 2 Ženevskih konvencija iz 1949. također služe kao koristan vodič za

procjenu je li određena uporaba sile dosegla razinu oružanog napada. Prema ovom testu, uporaba sile smatra se oružanim napadom kada je sila dovoljnog opsega, trajanja i intenziteta“ (Graham, 2010). Graham navodi tri kriterija Jeana Picteta. Prvi od njih je pristup temeljen na instrumentima, kod kojeg se procjenjuje je li se šteta uzrokovana kibernetičkim napadom prethodno mogla postići samo kinetičkim napadom. Drugi analitički model je "pristup temeljen na učincima". Ovdje se razmatra ukupni učinak kibernetičkog napada na stanje žrtve. Treći model je model "striktne odgovornosti" koji bi automatski smatrao svaki cyber napad na kritičnu nacionalnu infrastrukturu (CNI) oružanim napadom, koji se temelji na teškim posljedicama koje bi mogle proizaći iz bilo kakvog napada na takve infrastrukturne sustave. Na temelju svega ovoga, zaključeno je da kibernetički napadi mogu predstavljati oružane napade u određenim slučajima. Ako kibernetički napad rezultira značajnom štetom ili gubitkom života, potencijalno bi mogao eskalirati u veći, konvencionalniji sukob.

Libicki (2020) se u svom članku bavio poveznicama između kinetičkog i kibernetičkog ratovanja te je došao do nekoliko zaključaka. Jedan od njih je da zemlje još uvijek ne reagiraju na kibernetičke napade kao što bi reagirale na kinetičke napade, jer tada bi eskalacije u kibernetičkom prostoru mogle rezultirati usporedivom eskalacijom u fizičkom prostoru. Kinetički vojni učinci obično uključuju smrt i uništenje. Nijedan kibernetički napad nije nikoga izravno ubio, a malo ih je zapravo slomilo fizičke stvari; brisanje tvrdog diska – kao što su učinili mnogi kibernetički napadi – još uvijek tvrdi disk ostavlja fizički netaknutim. Smatra se da je vjerojatnost da će kibernetički napad izazvati kinetički odgovor mala, budući da kibernetički napadi općenito nisu smrtnosni i od njih se lakše oporaviti. Sve u svemu, iako je kibernetičko ratovanje ozbiljna prijetnja samo po sebi, nije nužno oružani sukob osim ako ne dovede do fizičkog sukoba ili je dio veće vojne strategije.

3. Rusko-ukrajinski kibernetički konflikti

3.1. Hibridno ratovanje

Hibridno ratovanje odnosi se na strategiju koja kombinira konvencionalne vojne metode s netradicionalnim taktikama kao što su kibernetički napadi. Ovaj pristup briše granice između vojnih i nevojnih akcija, zbog čega je teško učinkovito odgovoriti na ovakve napade. Od ruske aneksije Krima 2014. godine, sukob je uključivao kombinaciju konvencionalnih vojnih operacija i širokog spektra nekonvencionalnih taktika. Limnell (2015) ističe važnost razumijevanja rata u Ukrajini kao hibridnog ratovanja. Rat u Ukrajini naširoko se smatra najvažnijom sigurnosnom krizom u Europi od kraja Hladnog rata, ali također se smatra primjerom onoga što se čini kao nova vrsta sukoba zvanog hibridno ratovanje, koje kombinira vojne, gospodarske, diplomatske, političke i druge uglavnom nefizičke aktivnosti za postizanje dugoročnih strateških ciljeva. Hibridni rat sam po sebi nije nov koncept, ali mnoge korištene tehnologije u ovom ratu otkrivaju nove izazove. Otkako je NATO počeo ove događaje službeno opisivati kao hibridni rat, ovaj koncept sve više dominira na zapadu. Prema Limnellu, hibridno ratovanje se može smatrati inteligentnijim i učinkovitijim načinom vođenja rata jer nastoji postići političke ciljeve bez široke upotrebe oružanih snaga i nasilja. Hibridni rat se ne objavljuje (kao što se to dogodilo u Ukrajini), njegovo započinjanje obično prolazi nezapaženo, a može i ne mora dovesti do oružanog ratovanja velikih razmjera.

Lanoszka (2016) konceptualizira hibridno ratovanje kao strategiju, a ne kao novi oblik rata. Prema njemu, to je strategija jer namjerno integrira korištenje različitih instrumenata nacionalne moći kako bi se postigli međunarodni ciljevi, te može pokriti niz pomoćnih sredstava sve dok sveobuhvatni cilj vodi njihovu svrhu. Kao takvo, hibridno ratovanje uključuje korištenje regularnih i neregularnih vojnih sredstava prema različitim, ali komplementarnim ciljevima.

Jarno Limnell (2015) u svom radu ističe kako su se kibernetičke operacije dobro uklopile u političko vojno hibridno okruženje u Ukrajini i navodi neke od razloga za to. Jedan od njih je da je protivnika obično teško locirati i odgovoriti mu. Gotovo je nemoguće pripisati kibernetički napad određenoj zemlji. Kibernetički prostor omogućuje veliku količinu anonimnosti, a napadi se mogu usmjeravati preko poslužitelja diljem svijeta kako bi se prikrilo njihovo podrijetlo. To je bio slučaj u rusko-ukrajinskom ratu, i obje su strane snažno zanijekale da su izvodile bilo kakve kibernetičke operacije.

3.2. Proukrajinske hakerske skupine

Ukrajina je zemlja koja se bori s geopolitičkim napetostima i sukobima, stoga nije ni čudo da postoje hakerske skupine povezane s proukrajinskim pokretom. Te grupe su uključene u kibernetičke aktivnosti s raznim ciljevima, kao što su obrana nacionalnih interesa ili pokazivanje svoje prisutnosti u digitalnom svijetu. Kako navodi stranica RSMD (2023), pojava u Ukrajini formaliziranih hakerskih skupina i volonterskih pokreta, koji su službeno objavili svoju uključenost u kibernetičke akcije u obrani državnog sustava, datira iz najdramatičnijeg razdoblja unutarnje političke krize u proljeće 2014. Baezner (2018) daje popis i opis nekih od proukrajinskih hakerskih skupina.

Jedna od njih je Cyber Hunta, volonterska haktivistička grupa čiji je cilj razotkriti umiješanost Moskve u sukob u Ukrajini. Ova grupa tvrdi da nije povezana s ukrajinskom vladom (Miller, 2016 navedeno u Baezner, 2018). Kako piše RSMD (2023), grupa Cyber Hunta stvorena je 2014. godine, a 2016. godine glavni dio članova grupe pridružio se hakerskoj zajednici Ukrainian Cyber Alliance. U veljači 2020. haker Sean Brian objavio je na svojoj Facebook stranici da je hakerska grupa Cyber Hunta prestala djelovati.

Sljedeća grupa koju Baezner (2018) navodi je Cyber Hundred8. Cilj ove grupe je ukloniti proruske trolove s ukrajinskih web stranica i zaštititi ukrajinske web stranice od proruskih hakera. Ova grupa podučava o načinima borbe protiv internetskih trolova i pomaže u odmazdi protiv kibernetičkih napada, no jako malo se zna o njenoj strukturi (Ukraine investigations, 2014 navedeno u Baezner 2018).

Prema stranici RSMD (2023) najveća prukrajinska hakerska grupa je Ukrainian Cyber Alliance. Ukrajinski kibernetički savez formiran je 2016. godine nakon ujedinjenja grupa Falcons Flame i Trinity, koje su svojim ciljem proglasile suprotstavljanje ruskoj agresiji na internetu. Kasnije su se savezu pridružili haktivistička grupa RUH8 i pojedini predstavnici grupe CyberHunta.

3.3. Proruske hakerske skupine

„Iako je izravne veze s ruskom vladom teško uvjerljivo dokazati (a ruska vlada poriče da sponzorira hakerske skupine), postoji niz skupina čije su aktivnosti usko povezane s Kremljom i ruskim vojnim ciljevima. Rusija nije jedinstvena u tom pogledu: poznato je da Kina, Iran, Sjeverna Koreja i drugi kibernetički protivnici SAD-a povjeravaju kibernetičke

operacije nedržavnim akterima. Ono u čemu se Rusija razlikuje od ovih drugih protivnika je njezin uspjeh u tom pogledu. Ruski i drugi istočnoeuropski hakeri također se naširoko smatraju najboljima na svijetu, do te mjere da ih ponekad unajmljuju druge države da u njihovo ime izvode kibernetičke napade. Na primjer, ruski hakeri bili su osumnjičeni da stoje iza sjevernokorejskog hakiranja Sony Picturesa“ (Connel, Vogler, 2016).

Kao prvu od proruskih hakerskih skupina Baezner (2018) navodi CyberBerkut. Ova hakerska skupina podržava separatističke skupine u istočnoj Ukrajini, no ostaje neizvjesno je li sastavljena od proruskih Ukrajinaca ili Rusa. Grupa CyberBerkut potvrdila je da stoji iza nekoliko kibernetičkih napada, u rasponu od DDoS-a na NATO web stranice do ugradnje zlonamjernog softvera u CEC.

Sljedeća proruska hakerska skupina je APT28. „Ova hakerska skupina prvi put je otkrivena 2008. godine tijekom sukoba između Rusije i Gruzije. Vjeruje se da je skupina povezana s ruskom Glavnom obavještajnom upravom (GRU). Vrlo su profesionalni i koriste zlonamjerni softver razvijen na računalima s postavkama na ruskom jeziku. Poznato je da dizajniraju svoj zlonamjerni softver kako bi odgovarao njihovim ciljevima i da koriste spear phishing kako bi zarazili svoje žrtve, kao i korištenje zero-day ranjivosti. Infiltrirali su se u mreže ruskih disidenata, europskih sigurnosnih organizacija, obrambenih izvođača, zapadnih vladinih institucija i medijskih kuća“ (Baezner, 2018).

Među proruskim hakerskim skupinama Baezner navodi i internetske trolove, kojima se ruska vlada koristi za širenje proruske propagande na društvenim medjima, blogovima i forumima u inozemstvu i Rusiji. Organizirane su u “farme ili tvornice trolova”, odnosno institucije iz kojih trolovi objavljuju svoje poruke, komentare ili objave.

3.4. Povijest ruskih kibernetičkih napada na Ukrajinu

Kibernetički sukob između Rusije i Ukrajine traje već jedno desetljeće i dio je šireg geopolitičkog suparništva između dviju zemalja. Ovaj sukob ima duboke povijesne korijene, uključujući teritorijalne sporove i etničke napetosti. „Važno je napomenuti da je Rusija pokrenula ofenzivne kibernetičke operacije protiv Ukrajine još 2009. godine u sklopu šire kampanje informacijskog rata protiv zemalja NATO-a i EU. Tek su se u ožujku 2014. godine operacije informacijskog rata intenzivirale protiv Ukrajine. Tog je mjeseca ruski parlament odobrio vojnu silu u Ukrajini, predsjednik Vladimir Putin potpisao je zakon o uključivanju Krima u Rusku Federaciju, a ruske vojne snage su se nagomilale duž ukrajinske državne

granice“ (Unwala i Ghori, 2016). Kako Conell i Vogler (2017) pišu, kibernetički napadi korišteni su za prekid komunikacija, dobivanje i curenje vladinih dokumenata i planova te za deformaciju ili rušenje javnih i privatnih web stranica i računalnih sustava. Ovi kibernetički napadi koincidirali su s ključnim događajima sukoba, kao što su prosvjedi na Majdanu, ukrajinski parlamentarni izbori i kretanje ruskih snaga na Krim.

3.4.1. Aneksija Krima

Događaji na Krimu igrali su ključnu ulogu u razvoju kibernetičkog sukoba među Rusijom i Ukrajinom. „Tijek događaja – od preuzimanja parlamenta u Simferopolju i demontiranja ukrajinske vojne prisutnosti na poluotoku, do spornog referenduma i de facto pripojenja tog područja Ruskoj Federaciji – bio je popraćen intenzivnom aktivnošću usmjerenom na kontrolu protoka informacija. Ova se aktivnost proširila na cijeli spektar komunikacije i uključivala je kinetičke, kibernetičke i informacijske operacije usmjerene na fizičke, logičke i društvene slojeve komunikacije“ (Jaitner i Mattsson, 2015).

Kako Unwala i Ghori pišu (2016), ruske snage su zatvorile telekomunikacijsku infrastrukturu Krima, onesposobile ukrajinske web stranice i ometale mobilne telefone ključnih ukrajinskih službenika, već kada su došle na krimski poluotok 2. ožujka 2014. godine. Prema tome, nedvojbeno je da je rusko korištenje kibernetičke moći bilo ključno u ofenzivi protiv ukrajine i aneksiji Krima.

Stinissen i Geers (2015) u svom su radu opisali kibernetičke aktivnosti za vrijeme vojne operacije na Krimu. Provedene su operacije protiv ukrajinske mobilne infrastrukture, mobilnih telefona članova ukrajinskog parlamenta i sigurnosnih komunikacija. Korištene su neke tradicionalne metode, uključujući zauzimanje ureda Ukrtelecoma i fizičko rezanje telefonskih i internetskih kabela. Digitalni napadi uključivali su DDoS usmjeren na ukrajinske, krimske, NATO i ruske web stranice. Proruska hakerska skupina CyberBerkut bila je posebno aktivna protiv NATO-a, dok su skupine poput OpRussia i Russian CyberCommand svoje akcije usmjerile protiv ruskih web stranica.

3.4.2. Napad na ukrajinsku izbornu infrastrukturu 2014.

Kako Nikolaj Koval piše (2015), najsenzacionalniji haktivistički napad dogodio se tijekom predsjedničkih izbora u Ukrajini 2014. godine. Dana 21. svibnja 2014. CyberBerkut je

kompromitirao Središnje izborno povjerenstvo (CEC), onesposobivši središnje mrežne čvorove CEC-a i brojne komponente izbornog sustava. Softver, koji je dizajniran za prikaz ažuriranja brojanja glasova u stvarnom vremenu, nije ispravno radio gotovo 20 sati. Dana 25. svibnja, na dan izbora, 12 minuta prije zatvaranja birališta, napadači su na web stranicu CEC-a postavili sliku čelnika ukrajinskog Desnog sektora Dmitrija Jaroša, netočno tvrdeći da je on pobijedio na izborima. Ova slika je odmah prikazana na ruskim televizijskim kanalima. Važno je napomenuti da ovaj napad nije ni na koji način mogao odrediti ishod izbora, budući da u Ukrajini svaki građanin potpisuje svoj glas na glasačkom listiću, a svi se glasovi kasnije ručno provjeravaju. Unatoč tome, ne treba podcjenjivati sposobnosti hakera. Napad na ukrajinsku izbornu infrastrukturu smatra se upozorenjem drugim zemljama o potencijalu kibernetičkih napada da poremete demokratske procese. Napad je također istaknuo rastuću prijetnju kibernetičkih napada koje sponzorira država, posebice onih koje izvodi Rusija.

3.4.3. Kibernetički napad na električnu mrežu

Connell i Vogler (2016) u svom radu objašnjavaju kibernetički napad na električnu mrežu Ukrajine. Naime, krajem prosinca 2015. godine, ruski kibernetički aktori počinili su ono za što se vjeruje da je bio prvi kibernetički napad na električnu mrežu druge zemlje. U napadu koji se naširoko pripisuje Rusiji, 40 koordiniranih i sinkroniziranih kibernetičkih napada ciljala su tri odvojena distribucijska centra ukrajinske elektroenergetske tvrtke u zapadnoj Ukrajini. Koristeći daljinski pristup za kontrolu i upravljanje prekidačima, napadači su isključili distribucijske centre uzrokujući nestanak struje koji je pogodio više od 220.000 stanovnika Ukrajine. Kibernetički akteri su potom izbrisali neke sustave pokretanjem zlonamjernog softvera KillDisk na kraju kibernetičkog napada. Napad je opisan kao posebno sofisticiran: napadači su mjesecima provodili izviđanja u mrežama elektroprivrede, dobili su vjerodajnice administratora sustava, a zatim su koordinirali i sinkronizirali operaciju za rušenje distribucijskih centara istovremeno. Stručnjaci za kibernetičke napade nagađaju da su hakeri mogli prouzročiti veću štetu, poput nanošenja fizičke štete prekidačima, što bi uzrokovalo trajno isključenje elektrane. Međutim, činjenica da to nisu napravili, još je jedan dokaz sofisticiranosti napada. Umjesto toga, struja je nestala na samo 1-6 sati u pogođenim regijama (ali distribucijski centri nisu bili u potpunosti operativni mnogo mjeseci nakon napada). Ovo je možda trebao biti signal da je Rusija sposobna napasti fizičku infrastrukturu Ukrajine, ali bez nanošenja nepopravljive štete.

Zetter (2016) se u svom članku bavi pitanjem krivca tog napada. Ukrajinska obavještajna zajednica izjavila je s potpunom sigurnošću da iza napada stoji Rusija, iako nije ponudila nikakav dokaz koji bi potkrijepio tu tvrdnju. Ali, s obzirom na političke napetosti među tim dvjema nacijama, to nije nemoguć scenarij. Neposredno prije nestanka struje u Ukrajini, proukrajinski aktivisti fizički su napali trafostanice koje su napajale Krim, ostavivši bez struje dva milijuna stanovnika Krima u regiji koju je Rusija anektirala, kao i rusku pomorsku bazu. Počele su se širiti špekulacije da su isključenja struje u Ukrajini bila odmazda za napad na krimske trafostanice. Ali napadači koji su ciljali ukrajinske elektroprivrede započeli su s operacijom najmanje šest mjeseci prije nego što su napadnute trafostanice na Krimu, tako da bi poticaj napada mogao biti nešto sasvim drugo. Nedugo prije isključenja struje, ukrajinski parlament razmatrao je prijedlog zakona o nacionalizaciji privatnih energetskih kompanija u Ukrajini. Neke od tih tvrtki su u vlasništvu moćnog ruskog oligarha koji ima bliske veze s Putinom. Moguće je da je napad na ukrajinske elektroprivrede bio poruka ukrajinskim vlastima da ne provode nacionalizaciju. Kakva god bila namjera nestanka struje, bio je to prvi napad te vrste koji je postavio zlokobni presedan za sigurnost električnih mreža posvuda. Napad na elektroenergetsku mrežu iz 2015. bio je značajan jer je bio jedan od prvih poznatih primjera kibernetičkog napada koji je izazvao rasprostranjeni nestanak struje. Ovaj napad je također pokazao potencijal hakera koje sponzorira država da ciljaju na kritičnu infrastrukturu, naglašavajući potrebu za pojačanim mjerama kibernetičke sigurnosti u energetskom sektoru i drugim kritičnim industrijama.

3.4.4. NotPetya napad

NotPetya je vrsta zlonamjernog softvera koji je izazvao globalni kibernetički napad u lipnju 2017. Andy Greenberg (2019) dao je detaljan opis napada, njegov utjecaj na Ukrajinu i globalno širenje. Napad zlonamjernim softverom NotPetya započeo je 27. lipnja 2017., kada su ukrajinske tvrtke i vladine agencije počele prijavljivati probleme sa svojim računalnim mrežama. Napad je prvo otkriven u Ukrajini, gdje je zahvatio niz organizacija, uključujući banke, energetske tvrtke i vladine agencije. Sigurnosne tvrtke diljem svijeta odmah su počele ispitivati novog crva. Istraživači tvrtke Kaspersky primijetili su da kod novog zlonamjernog softvera donekle nalikuje dijelu kriminalnog ucjenjivačkog softvera (engl. *ransomware*) pod nazivom Petya koji je kružio od početka 2016. godine. Poput tog starijeg ransomwarea, novi primjerak je odmah, čim je zarazio novi stroj, krenuo sa šifriranjem računalne takozvane glavne tablice datoteka – dijela operacijskog sustava računala koji prati lokaciju podataka u

pohrani. Također je šifrirao svaku datoteku na stroju pojedinačno. Ali novi ransomware razlikovao se od tog ranijeg koda po ključnim izmjenama - otuda i njegovo ime. U roku od dvadeset i četiri sata, francuski istraživač sigurnosti po imenu Matthieu Suiche otkrio je da kod zapravo nije dopuštao dešifriranje nakon što je otkupnina plaćena. Umjesto toga, njegove poruke iznuđivanja činile su se kao nekakva smicalica, prikrivajući njegovu pravu namjeru jednostavnog, trajnog uništenja podataka. NotPetya je zapravo bio destruktivniji, nego što su vjerojatno čak i njegovi tvorci namjeravali. Za nekoliko sati proširio se izvan Ukrajine na bezbrojne strojeve diljem svijeta. Proširio se čak i na Rusiju - neposrednog glavnog osumnjičenika zajednice za kibernetičku sigurnost za podrijetlo NotPetya. Ali na nacionalnoj razini nijedna zemlja nije osjetila NotPetyin učinak kao Ukrajina. Ukratko, do kraja 27. lipnja, NotPetya je pogodio najmanje četiri bolnice samo u Kijevu, zajedno sa šest elektroenergetskih kompanija, dvije zračne luke, više od dvadeset i dvije ukrajinske banke, bankomate i sustave kartičnog plaćanja, te praktički cijelu saveznu vladu.

Bendiek i Schulze (2021) govore o pitanju krivca za ovaj napad. Prema izvješću Washington Posta u siječnju 2018., CIA je s "visokim stupnjem sigurnosti" pretpostavila da ruska vojska stoji iza NotPetya napada. Međutim, nisu predstavljeni nikakvi dokazi. Javno pripisivanje dogodilo se sredinom veljače 2018., kad je savez Five Eyes pripisao napade ruskoj vladi. Danska, Latvija, Švedska i Finska izjavile su da se slažu s Five Eyes. Općenito se vjeruje da su zlonamjerni softver NotPetya stvorili hakeri koje sponzorira ruska država, iako je Rusija zanijekala bilo kakvu umiješanost. Napad je viđen kao dio tekućeg sukoba između Rusije i Ukrajine, te je istaknuo rastuću prijetnju kibernetičkih napada na kritičnu infrastrukturu i poduzeća diljem svijeta.

3.4.5. BadRabbit

Greenberg (2019) opisuje BadRabbit kao naknadni potres NotPetyae. Zlonamjerni softver se širio ukrajinskim mrežama, te je ubrzo pogodio zračnu luku u Odesi i kijevski metro, ponovno paralizirajući plaćanje kreditnom karticom u sustavu prijevoza. Kao i prije, zlonamjerni softver koristio je Mimikatz i NSA tehnike kako bi razgranao svoje infekcije. Ali iznenađujuće, nije uključivao EternalBlue koji se koristio u NotPetya napadu. Kako opisuje Baezner (2018), BadRabbit je zarazio svoje žrtve lažnim ažuriranjem Adobe Flasha, no za razliku od NotPetya, BadRabbit je dekriptirao podatke nakon što je otkupnina plaćena. Greenberg (2019) također navodi da je ovaj crv šifrirao samo nekliko stotina strojeva, što nije

ni blizu destruktivnim rezultatima koje je počinio softver NotPetya. I što je najčudnije od svega, velika većina zaraženih računala nije bila u Ukrajini, već u Rusiji. Ali nije bilo sumnje da su Bad Rabbita pustili isti hakeri kao NotPetya. Prema sigurnosnoj tvrtki CrowdStrike, sadržavao je čak 67 posto istog koda. Nekoliko sati nakon napada, Kaspersky je otkrio da je NotPetya također distribuiran watering hole napadom u najmanje jednom slučaju. Kaspersky je otkrio da je ukrajinska stranica s vijestima Bahmut.com.ua bila hakirana i korištena za isporuku NotPetyae 27. lipnja. Analitičari tvrtke zatim su provalu te web stranice povezali s nizom napada na trideset drugih stranica, od kojih su mnoge sada širile Bad Rabbit. Raymond (2022) bilježi da su neki istraživači i komentatori smatrali da je Bad Rabbit državno financirana skupina usmjerena na disonantne medijske organizacije. Međutim, nema uvjerljivih dokaza koji podupiru tu tvrdnju.

3.4.6. Kibernetički napad na Ukrajinu 2022. godine

Kako prenosi BBC (2022), 14. siječnja 2022. godine u napadu na Ukrajinu 70 vladinih web stranica je privremeno bilo u kvaru. Prije nego što su se stranice ugasile, pojavila se poruka koja upozorava Ukrajince da se "pripreme na najgore". Na hakiranim web stranicama objavljena je poruka na tri jezika: ukrajinskom, ruskom i poljskom, a glasila je ovako: Ukrajinci! Svi vaši osobni podatci postavljeni su na javni internet. Ovo je za vašu prošlost, sadašnjost i budućnost. Poruka na poljskom jeziku sadržavala je ozbiljne pogreške i nije se činilo da ju je napisao izvorni govornik, navodi se u izjavi koju je objavila poljska vlada, koja je okrivila Rusiju za napad. No, nikakvi osobni podatci nisu procurili i nikakav sadržaj nije promijenjen, a pristup većini stranica vraćen je u roku od nekoliko sati. Polityuk i Holland (2022) pišu kako je Ukrajinska državna sigurnosna služba izjavila da su uočeni neki znakovi koji upućuju na upletenost hakerskih skupina povezanih s ruskim obavještajnim službama. Naime, poruka na hakiranim web stranicama je bila prožeta referencama koje su odražavale dugotrajne optužbe Rusije da je Ukrajina u ropstvu krajnje desnih nacionalističkih skupina. NATO je odgovorio najavom da će za nekoliko dana potpisati novi sporazum s Kijevom o bližoj suradnji u kibernetičkoj obrani, uključujući davanje Ukrajini pristupa sustavu zapadnog vojnog saveza za razmjenu informacija o zlonamjernom softveru.

3.5. Povijest ukrajinskih kibernetičkih napada na Rusiju

„Za razliku od Rusije, ukrajinski napadi bili su općenito rudimentarni i ograničenog učinka. Ukrajina pati od nedostatka stručnosti u kibernetičkoj sigurnosti, loše regulative, ograničenog kapaciteta odgovora i nedostatka koordinacije između različitih agencija, a sve su to nedostaci koje Kijev pokušava popraviti“ (Mohee, 2022). Dok su informacije o ruskim napadima na Ukrajinu dostupnije, informacija o ukrajinskim napadima na Rusiju je znatno manje i do njih je teže doći

3.5.1. Operacija Prikormka

Kako piše Kovacs (2016) , u svibnju 2016. godine razotkrivena je operacija Prikormka, usmjerena na, između ostalog, protuvladine separatiste u regijama Luhansk i Donjeck. Zlonamjerni softver, dizajniran za rad na 32- i 64-bitnim Windows sustavima, koristi više od desetak modula pohranjenih na disku kao DLL i EXE datoteke za obavljanje različitih zadataka. Trojanac je bio sposoban krasti dokumente, bilježiti pritiske tipki, hvatati snimke zaslona, snimati zvuk s mikrofona i Skype poziva te prikupljati spremljene lozinke iz aplikacija. U mnogim su slučajevima napadači isporučili zlonamjerni softver putem e-poruka za krađu identiteta koje su nosile dokumente mamaca koji se odnose na geopolitičku situaciju u Ukrajini i oružani sukob u regiji Donbas. Zlonamjerni softver nazvan je Prikormka (rus. mamac) jer je u jednom od napada koje je promatrala zaštitarska tvrtka prijetnja prikazivala cjenik za ribičku primamu.

3.5.2. Operacija 9. svibnja

Anna Shamanska (2016) dala je uvid u proukrajinsku operaciju koja se dogodila na dan obilježavanja pobjede Sovjetskog Saveza nad nacističkom Njemačkom. Proukrajinske hakerske skupine preuzele su devet ruskih internet stranica. Jedna od njih bila je stranica separatističke skupine Donjecka, na kojoj su objavljeni videozapisi o ukrajinskom sudjelovanju u porazu nacizma u Drugom svjetskom ratu. To je bilo simbolično, budući da su se 9. svibnja 1945. Godine nacisti predali Sovjetskom Savezu. Neke od hakiranih web stranica prikazale su lažnu poruku pripisanu Aleksandru Zaharčenku, samoproglašenom vođi donjeckih separatista, izražavajući nadu da će ovogodišnji Dan pobjede "biti nad rusko-fašističkim režimom".

3.5.3. Hakiranje korporativnog servera ruskog „Prvog programa“

U lipnju 2016. godine, hakeri iz grupa FalconsFlame, Trinity i RUH8 hakirali su korporativni portal ruskog državnog „Prvog programa“, kako prenosi SecurityLab (2016). Kako je objavljeno na web stranici hakerske grupe RUH8, napad je izveden uz pomoć informacija koje je objavio ukrajinski portal „Mirotvorec“. Hakeri su od Ruske Federacije tražili provođenje Minskog sporazuma. Kao rezultat hakiranja, hakeri su dobili pristup bazi podataka s podatcima za kontakt zaposlenika televizijskog kanala. Članovi RUH8 objavili su arhivu s osobnim podatcima zaposlenih.

3.5.4. Objavljivanje pisma Surkova

Kako piše Cibuljski (2016), Ukrajinski hakeri objavili su niz pisama koje nazivaju korespondencijom pomoćnika ruskog predsjednika Vladislava Surkova. Smatra se da su barem neke od poruka prave. U rujnu 2013. godine Surkov je postao pomoćnik predsjednika i preuzeo vanjsku politiku, formalno je odgovoran i za uspostavljanje odnosa s Abhazijom i Južnom Osetijom, a neformalno i s Ukrajinom. Iza hakiranja e-pošte Surkova stoji neformalna udruga hakera Cyberhunta. Nakon hakiranja, na svojoj su web stranici objavili dva posta: prvi je bio dokument s planom „destabilizacije društveno-političke situacije“ u Ukrajini i dokument koji opisuje „plan osiguranja federalnog statusa Zakarpatja“, a drugi post je sadržavao pisma iz poštanskog sandučića. Neke ukrajinske političke ličnosti spomenute u prepisci odmah su zanijekle autentičnost tih dokumenata.

3.5.5. Ukrajinska IT vojska

Ukrajinska IT vojska krenula se formirati još u samom početku Specijalne vojne operacije Rusije, kako piše Leonid Cukanov za RSMD (2023). Unatoč tome, određene naznake o namjeri Kijeva da stvori sličnu strukturu poznate su i ranije. Značajan dio vojske nisu državljani Ukrajine, već strani stručnjaci koje je regrutiralo ukrajinsko ministarstvo obrane na specijaliziranim forumima. U svojim aktivnostima proukrajinski hakeri koriste klasičan skup radnji: defacement (objavljivanje materijala provokativne i demoralizirajuće prirode), phishing, distribucija zlonamjernog softvera i DDoS napadi. Osim toga, u prvim se fazama aktivno koristio doxxing - pretraživanje i objavljivanje osobnih ili povjerljivih podataka.

Ukupno, prema ruskom FSB-u, broj kibernetičkih napada na ruski CII od početka 2023. premašio je 5 tisuća; ukupan broj cyber incidenata je 8,5 tisuća.

3.5.6. Napad proukrajinskih hakera iz Bjelorusije

U članku za Fortune, Ryan Gallagher i Bloomberg (2022) pišu o provali proukrajinskih bjeloruskih hakera u računala koja kontroliraju vlakove u Bjelorusiji i o zaustavljanju nekih od tih vlakova. Cyber Partisants, kako sebe nazivaju ovi hakerski aktivisti, izjavili su da je svrha napada bila usporiti transfer ruskih trupa koje putuju iz baza u Bjelorusiji u sjevernu Ukrajinu i kupiti više vremena za Ukrajince kako bi odbili napad Rusije na zemlju. Sergej Voitehovič, bivši zaposlenik bjeloruske državne tvrtke Bjeloruske željeznice koji pomaže u vođenju online foruma za radnike bjeloruske željeznice, rekao je da su hakeri oštetili sustav kontrole prometa vlakova. To je uzrokovalo poremećaje u kretanju vlakova, posebno na raskrižju između Minska i Orshe.

4. Uloga Amerike i Europe

Kako piše Ahmad Mohee (2022), „Ukrajina također dobro koristi izdašnu pomoć koju dobiva od saveznika, predvođenih Europskom unijom i Sjedinjenim Američkim Državama. Sjedinjene Države poslale su stručnjake i sredstva za jačanje kibernetičke obrane Ukrajine i sasvim je jasno je da će to zahtijevati dugoročne napore. SAD je stoga spreman voditi ukrajinsku kibernetičku frontu kako bi izvršio obrambene dužnosti kada je to potrebno. Čvrsti dokaz za to bila je izjava američkog predsjednika Joea Bidena, tijekom siječnja 2022., upozoravajući Rusiju na posljedice u vezi s kibernetičkim napadima, rekavši: „ako nastave koristiti kibernetičke napore, pa, možemo odgovoriti na isti način.““ Fan Wenjin (2013) rusko-američke odnose naziva međunarodnim žarištem koje je oduvijek privlačilo široku pozornost. Prema njemu, rusko-ukrajinski sukob je sveobuhvatna igra supersila koja uključuje natjecanje vojne i ekonomske snage, ali i natjecanje snage predstavljene „informacijskim ratom“. „Trenutačno su odnosi Rusije s Amerikom i zapadnim zemljama na povijesno najnižoj točki. Na području informiranja, većina zemalja svijeta sudjelovala je u ovom sukobu, tvoreći načelo “ne pružanje podrške znači protivljenje”. Stoga se rusko-ukrajinski sukob može smatrati “svjetskim ratom” na polju informacija. Kakav god bio ishod rusko-ukrajinskog sukoba, beskrajni informacijski rat između Rusije i Sjedinjenih Država će se nastaviti“ (Wenjin, 2023).

Prema Willetu (2023), kibernetička sigurnost Ukrajine poboljšana je pomoću obavještajnih, kibernetičkih i drugih vladinih agencija SAD-a i Ujedinjenog Kraljevstva. U godinama koje su prethodile ruskoj invaziji, Sjedinjene Američke Države znatno su uložile u izgradnju kapaciteta i otpornosti ukrajinske kibernetičke sigurnosti. SAD je od 2020. godine angažirao tehničke stručnjake unutar ukrajinske vlade zbog implementacije softvera i hardvera za poboljšanje sigurnosti i otpornosti kritične infrastrukture. Američko kibernetičko zapovjedništvo je 2021. godine rasporedilo stručnjake koji su provodili obrambene kibernetičke operacije zajedno s Ukrajinskim kibernetičkim zapovjedništvom. Nakon početka rata, američki FBI i agencija za kibernetičku sigurnost i infrastukturu pružili su dodatnu istražnu podršku i tehničke savjete, a američka Agencija za međunarodni razvoj osigurala je više američkih tehničkih stručnjaka i komunikacijskih uređaja za Ukrajinu.

„U kontekstu rata između Rusije i Ukrajine, kibernetički napad u Ukrajini je od velike pomoći Rusiji, koja je trenutno pod velikim pritiskom SAD-a i NATO-a oko pitanja ukrajinske granice, bez obzira na to je li pritisak prouzročen državnom naredbom Rusije ili

ne. Nedržavni akteri ili bilo tko tko djeluje u ime određenih država ili skupina može iskorištavati kibernetički prostor, što je izuzetno štetno za globalnu sigurnost jer ga treće strane mogu koristiti za povećanje napetosti među državama“ (Priyono, 2022).

5. Kibernetički odnosi u budućnosti

Kibernetički sukob između Rusije i Ukrajine traje već nekoliko godina, a postoje različiti mogući scenariji kako bi se mogao razvijati. Kako Willet (2022) piše, „rusko-ukrajinski rat nedvojbeno je definirao mnoge kriterije za moderni kibernetički rat, ali ne sve. Na primjer, obje strane još uvijek ne koriste vrhunske ofenzivne kibernetičke sposobnosti jedna protiv druge. Nadalje, kibernetički sukob između Rusije i države sa slabijom kibernetičkom sigurnošću od Rusije ili sukob između NATO-a i Rusije (ili Kine) možda bi doveo do drugačije ravnoteže između napada i obrane“. Willet kao najveći rizik navodi mogućnost eskalacije rusko-ukrajinskog rata izvan kibernetičkog prostora do šireg sukoba između Rusije i NATO-a. „To bi se sigurno moglo dogoditi kad bi Rusija uspjela izvršiti destruktivan kibernetički napad na zapadnu kritičnu infrastrukturu ili kad bi država članica NATO-a upotrijebila kibernetičku operaciju koja bi bila jednaka uporabi sile ili oružanom napadu na Ruse u Ukrajini“ (Willet, 2022).

„Iako će ruska vojska nedvojbeno nastaviti cijeniti konvencionalna sredstva i ulagati u modernu ratnu tehnologiju, sve veća važnost nekonvencionalnih sredstava, posebice digitalnih, u njenom stalnom natjecanju sa zapadom sugerira da će te sposobnosti privući dodatnu pozornost u vojnoj doktrini, radovima ruskih vojnih znanstvenika i državnoj politici“ (Lilly i Cheravitch, 2020).

6. Zaključak

Kibernetički napadi su napadi koji se služe raznim zlonamjernim radnjama, ne bi li ugrozili računalne sustave, mreže ili podatke. Rusija i Ukrajina već su dugi niz godina u kibernetičkom sukobu u koji su uključeni akteri koje sponzorira država, ali i neovisne skupine i pojedinci. Ovaj sukob, koji se zahuktava od 2014. godine, kad je Rusija anektirala Krim, u današnje vrijeme dostiže svoj vrhunac, budući da je trenutno u pitanju hibridno ratovanje. Konflikt naglašava šire geopolitičke napetosti između Rusije i Ukrajine, pri čemu kibernetički prostor predstavlja dodatno bojno polje. Rusko-ukrajinski kibernetički sukob nije utjecao samo na dvije izravno uključene nacije, već ima i implikacije na regionalnu stabilnost i globalnu sigurnost. Obje strane služe se raznim metodama i već su izvršile mnoge napade ne bi li dobile prednost jedna nad drugom. Ishod rusko-ukrajinskog konflikta još nije moguće jasno pretpostaviti, ali vjeruje se da će obje države nastaviti razvijati svoje napade i kibernetičku sigurnost. Ovaj oblik ratovanja još uvijek je nov i neprestano se razvija, te će se u budućnosti shvaćati sve ozbiljnije i ozbiljnije.

7. Literatura

Alkhalil, Z., Hewage, C., Nawaf, L., Khan, I. (2021) Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science* [*online*], 3, 563060. Dostupno na: file:///C:/Users/PC/Downloads/fcomp-03-563060.pdf [7. ožujka 2024.]

Baezner, M. (2018) *Cyber and Information warfare in the Ukrainian conflict* [*online*], verzija 2. Zurich: Center for Security Studies (CSS). Dostupno na: https://www.researchcollection.ethz.ch/bitstream/handle/20.500.11850/321570/20181003_MB_HS_RUS- UKRV2_rev.pdf?sequence=1 [9. ožujka 2024.]

BBC, Ukraine cyber-attack: Government and embassy websites targeted (2022) Dostupno na: https://www.bbc.com/news/world-europe-59992531 [22. ožujka 2024.]

Bendiek, A., Schulze, M. (2021) *Attribution: A major challenge for EU cyber sanctions. An analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the attack on the OPCW* [*online*], 11. Dostupno na: https://www.econstor.eu/handle/10419/253242 [25. svibnja 2023.]

Biju, J. M., Gopal, N., Prakash, A. J. (2019) Cyber attacks and its different types. *International Research Journal of Engineering and Technology* [*online*], *6*(3), 4849-4852. Dostupno na: https://www.academia.edu/download/60557348/IRJET-V6I31244201909 11-33891-1hcvf72.pdf [6. ožujka 2024.]

Bilyana, L., Cheravitch, J. (2020) The past, present, and future of Russia's cyber strategy and forces. *2020 12th International Conference on Cyber Conflict (CyCon)* [*online*], vol. 1300. Dostupno na:https://www.ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf [15. travnja 2024.]

Clarke, R. A., Knake, R. K. (2010) *The next treat to national security and what to do about it* [*online*]. Dostupno na: https://indianstrategicknowledgeonline.com/web/Cyber%20War%20-%20The%20Next%20Threat%20to%20National%20Security%20and%20What%20to%20Do

%20About%20It%20%28Richard%20A%20Clarke%29%20%282010%29.pdf [13. ožujka 2024.]

Cibuljski, V. (2016) *Хакеры опубликовали переписку Владислава Суркова. Фальшивую и настоящую* [*online*]. Meduza. Dostupno na: https://meduza.io/feature/2016/10/26/hakery-opublikovali-perepisku-vladislava-surkova-falshivuyu-i-nastoyaschuyu?ysclid=ltlsi8s610977316134 [15. travnja 2024.]

Connell, M., Vogler, S. (2017) *Russia's approach to cyber warfare* [*online*]. Dostupno na: https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf [2. ožujka 2024.]

Cukanov, L. (2023) *Украинская «IT-армия»: между ударом и пиаром* [*online*]. РСМД. Dostupno na: https://russiancouncil.ru/analytics-and-comments/analytics/ukrainskaya-it-armiya-mezhdu-udarom-i-piarom/?ysclid=lv16enfq53597294472 [15. travnja 2024.]

Ferdous, J., Islam, R., Mahboubi, A., Islam, M. Z. (2023) A review of state-of-the-art malware attack trends and defense mechanisms. *IEEE Access* [*online*], 11, 121118-121141. Dostupno na: https://researchoutput.csu.edu.au/files/413658138/413657913_published_article.pdf [24. veljače 2024.]

Gallagher, R., Bloomberg (2022) *Hackers in Belarus claim to have disrupted trains to 'slow down the tranfer' of Russian troops into Ukraine* [*online*]. Forrune. Dostupno na: https://fortune.com/2022/02/27/belarus-hackers-disrupt-trains-russia-invasion-ukraine-cyber-partisans/ [9. ožujka 2024.]

Geers, K. (2010) The challenge of cyber attack deterrence. *Computer Law & Security Review* [*online*], 26, 298-303. Dostupno na: https://www.sciencedirect.com/science/article/pii/S0267364910000506 [15. svibnja 2023.]

Graham, D. E. (2010) Cyber threats and the law of war. *J. Nat'l Sec. L. & Pol'y* [*online*], 4, 87. Dostupno na: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/jnatselp4&section=10&casa_token=WyAYFpzwjgAA

AAAA:iJXmYTErThSos2hJGPFwwWZlpX1uW71Lf-les01HeemEZRczTY_hRTRfgt3mt-xlH_v-T4yIa3A [22. veljače 2024.]

Greenberg, A. (2019) *Sandwarm.* New York: Doubleday.

Halfond, W. G. J., Viegas, J., Orso. A. (2006) A classification of SQL-injection attacks and countermeasures. *Proceedings of the IEEE international symposium on secure software engineering* [*online*], vol. 1. Dostupno na: http://www.cc.gatech.edu/fac/Alex.Orso/papers/halfond.viegas.orso.ISSSE06.pdf [7. ožujka 2024.]

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J. (2012) The law of cyber attack. *California Law Review* [*online*], 100, 817. Dostupno na: https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/calr100&id=823&men_tab=srchresults [25. travnja 2023.]

Jaitner, M. i Mattsson, A. P. (2015) Russian information warfare of 2014. *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace* [*online*]. Dostupno na: https://www.academia.edu/download/88580055/03_jaitner_mattsson.pdf [18. ožujka 2024.]

Jensen, B., Mueller, G. B., Valeriano, B., Maness, R. C., Macias, J. M. (2023) *Cyber Operations during the Russo-Ukrainian War* [*online*], CSIS. Dostupno na: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war [15. ožujka 2024.]

Juutilainen, J. (2022) *Cyber Warfare: A Part of the RussoUkrainian War in 2022* [*online*]. Dostupno na: *https://www.theseus.fi/bitstream/handle/10024/780757/Juutilainen_Jari.pdf?sequence=2* [13. ožujka 2024.]

Kovacs, E. (2016) Ukraine Separatists, Politicians Targeted in Surveillance Operation. *Security Week* [*online*], 19. Dostupno na: https://www.securityweek.com/ukraine-separatists-politicians-targeted-surveillance-operation/ [22. veljače 2024.]

Koval, N. (2015) Revolution hacking. *Cyber war in perspective: Russian aggression against Ukraine* [*online*], 55-65. Dostupno na: https://www.ccdcoe.org/uploads/2018/10/Ch06_CyberWarinPerspective_Koval.pdf [18. ožujka 2024.]

Lange-Ionatamishvili, E., Svetoka, S. (2015) Strategic communications and social media in the Russia Ukraine conflict. U K. Geers (Ur.) *NATO Strategic Communications Centre of Excellence* [*online*]. Dostupno na: https://ccdcoe.org/uploads/2018/10/Ch12_CyberWarinPerspective_Lange_Svetoka.pdf [28. veljače 2024.]

Lanoszka, A. (2016) Russian hybrid warfare and extended deterrence in eastern Europe. *International affairs* [*online*] 92.1, 175-195. Dostupno na: https://academic.oup.com/ia/article-abstract/92/1/175/2199942 [8. ožujka 2024.]

Libicki, M. C. (2020) Correlations between cyberspace attacks and kinetic attacks. *2020 12th International Conference on Cyber Conflict (CyCon)* [*online*], vol. 1300. Dostupno na: https://www.academia.edu/download/81933340/CyCon_2020_11_Libicki.pdf [8. ožujka 2023.]

Limnell, J. (2015) The exploitation of cyber domain as part of warfare: Russo-Ukrainian war. *International Journal of Cyber-Security and Digital Forensics* [*online*], 4.4, 521-532. Dostupno na: https://www.researchgate.net/profile/Natalie-Walker-15/publication/306263976_IJCSDF_Vol_4_No_4/links/57b59f4108ae19a365fc3dcd/IJCSDF-Vol-4-No-4.pdf#page=55 [8. ožujka 2024.]

Mallik, A. (2019) Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi* [*online*], 2.2, 109-134. Dostupno na:

https://jurnal.ar-raniry.ac.id/index.php/cyberspace/article/viewFile/3453/2707 [7. ožujka 2024.]

Mohee, A. (2022) *Cyber war: The hidden side of the Russian-Ukrainian crisis* [*online*]. Socarxiv Papers. Dostupno na: https://osf.io/preprints/socarxiv/2agd3/download [22. ožujka 2024.]

Polityuk, P., Balmforth, T. (2022) *Be afraid': Ukraine hit by cyberattack as Russia moves more troops* [*online*]. Reuters. Dostupno na: https://www.reuters.com/world/europe/expect-worst-ukraine-hit-by-cyberattack-russia-moves-more-troops-2022-01-14/ [22. ožujka 2024.]

Priyono, U. (2022) Cyber Warfare as Part of Russia and Ukraine Conflict. *Jurnal Diplomasi Pertahanan* [*online*], 8.2: 44-59. Dostupno na: https://jurnalprodi.idu.ac.id/index.php/DP/article/view/1005/845 [11. ožujka 2024.]

Raymond, M. (2023) *Bad Rabbit Ransomware* [*online*]. Varonis. Dostupno na: https://www.varonis.com/blog/bad-rabbit-ransomware [22. ožujka 2024.]

Roscini, M. (2014) *Cyber Operations and the Use of Force in International Law* [*online*]. USA: Oxford University Press. Dostupno na: https://books.google.com/books?hl=hr&lr=&id=yeokAwAAQBAJ&oi=fnd&pg=PP1&dq=Cyber+Operations+and+the+Use+of+Force+in+International+Law&ots=XphaUMVsS8&sig=QYrJp659sqA7FH1pDH6JaxeDQxo [5. svibnja 2023.]

RSMD (2023) Dostupno na: https://russiancouncil.ru/cyberukraine-groups?ysclid=lteg64w9h5516819047 [9. ožujka 2024.]

SecurityLab.ru (2016) Dostupno na: https://www.securitylab.ru/news/482805.php?ysclid=lv15hrr4yj284968607 [15. travnja 2024.]

Shamanska, A. (2016) *Hackers In Ukraine Deface Separatist Websites To Mark Victory Day.* Radio Free Europe/Radio Liberty. Dostupno na: https://www.rferl.org/a/hackers-ukraine-deface-separatist-websites-victory-day-opmay9/27724532.html [5. ožujka 2024.]

Stinissen, J. i Geers, K. (2015) A legal framework for cyber operations in Ukraine. *Cyber War in Perspective: Russian Aggression against Ukraine. NATO CCD COE Publications, Tallinn* [*online*], 123-134. Dsotupno na : https://ccdcoe.org/uploads/2018/10/Ch14_CyberWarinPerspective_Stinissen.pdf [4. ožujka 2024.]

Šincek, D., & Vrbanec, T. (2010) Distribuirani napad uskraćivanjem usluga. *International Convention With MIPRO To Knowledge Society. Section Students Papers* [*online*], 33; 2010. Dostupno na: https://www.bib.irb.hr:8443/481948/download/481948.Sincek-Vrbanec_-_DDoS.pdf [6. ožujka 2024.]

Uma, M., Padmavathi, G. (2013) A Survey on Various Cyber Attacks and their Classification. *International Journal of Network Security* [*online*], 15. Dostupno na: http://ijns.jalaxy.com.tw/contents/ijns-v15-n5/ijns-2013-v15-n5-p390-396.pdf [27. travnja 2023.]

Unwala, A., and Shaheen G. (2016) Brandishing the cybered bear: Information war and the Russia-Ukraine conflict. *Military Cyber Affairs* [*online*], 1.1 : 7. Dostupno na: https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1001&context=mca [25. svibnja 2023.]

Wenjin, Fan. (2023) Research on Russia-America Game: Taking Information Warfare as an Example. *Вестник КазНУ. Серия международные отношения и международное право* 103.3 [*online*], 75-86. Dostupno na: https://bulletin-ir-law.kaznu.kz/index.php/1-mo/article/download/1414/1177 11.3.2024. [11. ožujka 2024.]

Willett, M. (2023) The cyber dimension of the Russia–Ukraine War. *Survival: October-November 2022* [*online*], Routledge, 7-26. Dostupno na: https://www.tandfonline.com/doi/pdf/10.1080/00396338.2022.2126193 [15. travnja 2024.]

Zetter, K. (2016) *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid* [*online*]. Wired. Dostupno na: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. [25. svibnja 2023.]

Rusko-ukrajinski kibernetički konflikti

Sažetak

Kibernetički konflikti danas su veoma aktualni i sve više država se služi raznim metodama, ne bi li dobile kibernetičku prevlast nad protivnicima. Rusko-ukrajinski kibernetički sukob zahuktava se od 2014. godine, nakon ruske aneksije Krima. U ovom konfliktu sudjeluju mnoge hakerske skupine iz Rusije i Ukrajine. Osim njih, u konflikt su uključeni i hakeri iz drugih država. Napad na ukrajinsku izbornu infrastrukturu i kibernetički napad na električnu mrežu Ukrajine samo su neki od ruskih napada usmjerenih na Ukrajinu. Kibernetički napadi na Rusiju uključuju hakiranje ruskih web stranica i objavljivanje sadržaja na njima, kao i provalu u računala koja kontroliraju vlakove ruskih trupa. U sukob su također uključeni Europa i Sjedinjene Američke Države, uz čiju je pomoć ukrajinska kibernetička sigurnost znatno učvršćena. Postoje različiti scenariji kako bi se ovaj sukob mogao dalje razvijati i teško je točno predvidjeti budućnost konflikta, ali vjeruje se da će obe države nastaviti razvijati svoje kibernetičke sposobnosti.

Ključne riječi: kibernetički konflikt, hakeri, Rusija, Ukrajina, kibernetička sigurnost

Russian-Ukrainian cyber conflicts

Summary

Cyber conflicts are very relevant today and more and more countries are using various methods in order to gain cyber supremacy over their opponents. The Russian-Ukrainian cyber conflict has been heating up since 2014, after the Russian annexation of Crimea. Many hacker groups from Russia and Ukraine participate in this conflict. In addition to them, hackers from other countries are also involved in the conflict. An attack on Ukraine's election infrastructure and a cyberattack on Ukraine's power grid are just some of the Russian attacks targeting Ukraine. Cyber attacks on Russia include hacking Russian websites and publishing content on them, as well as breaking into computers that control Russian troop trains. Europe and the United States of America are also involved in the conflict, with whose help Ukrainian cyber security has been significantly strengthened. There are different scenarios for how this conflict could develop further and it is difficult to accurately predict the future of the conflict, but it is believed that both countries will continue to develop their cyber capabilities.

Key words: cyber conflict, hackers, Russia, Ukraine, cyber security