DOI: 10.5937/vojdelo1607164M

AKTIVNOSTI SAVREMENIH OBAVEŠTAJNIH SLUŽBI U KIBER PROSTORU

Milan Miljković
Ministarstvo odbrane Republike Srbije
Nenad Putnik*
Univerzitet u Beogradu, Fakultet bezbednosti

Špijunaža između država je stara stotinama godina. Od puštanja interneta u komercijalnu upotrebu razvijene zemlje počinju da koriste prednosti računara i interneta u toj aktivnosti. Obaveštajna delatnost teži da iskoristi sve prednosti i mane masovne upotrebe informaciono-komunikacione tehnologije (IKT) za obavljanje obaveštajnih aktivnosti. Nema ozbiljne obaveštajne službe u svetu koja nije zainteresovana za ovaj način obaveštajnog istraživanja, pogotovo zbog ekonomičnosti ovakve aktivnosti u odnosu na druge načine prikupljanja poverljivih podataka. U aktuelnoj navali međusobnog optuživanja velikih država za kiber špijunažu nema nevinih. Suštinska pitanja su *kada* je neko nekoga špijunirao, i *ko* je *koga* unajmio u te svrhe. Kiber prostor se, po svojoj prirodi, protivi pronalaženju odgovora na ova pitanja – u njemu je veoma teško otkriti identitet zlonamernog aktera, kao i dokazati sprovođenje i naručivanje takvih nelegalnih operacija. Zbog toga će i aktivnosti obaveštajnih službi u kiber prostoru biti sve izraženije, što će, po svoj prilici, voditi ka promenama u načinu prikupljanja obaveštajnih podataka.

Ključne reči: *obaveštajne službe, prikupljanje podataka, kiber špijunaža, kiber napad, kiber bezbednost*

Uvod

Nova tehnologija nije stvorila samo nove pretnje već je i otežala identifikaciju aktera bezbednosnih pretnji i njihovog razlikovanja. Akteri pretnji u novom ambijentu, kiber prostoru, mogu biti različiti – državni, poddržavni i transnacionalni subjekti. To su najčešće zlonamerni pojedinci, kriminalne grupe, terorističke organizacije, privredni subjekti, ali i države i njihove institucije (nacionalne armije i obaveštajne službe), sa različitim motivima za delovanje: ekonomskim, političkim, ideološkim, religijskim ili vojnim.[1] Države su, razume se, naročito zabrinute za nacionalnu bezbednost i mogućnost da državni ili nedržavni akteri ukradu, promene, unište ili na drugi način kompromituju ključne informacije i informacione

* Doc. dr Nenad Putnik, nputnik@fb.bg.ac.rs

[1] Nenad Putnik, *Sajber prostor i bezbednosni izazovi* (Beograd: Univerzitet u Beogradu, Fakultet bezbednosti, 2009), str. 11.

infrastrukture. Sa druge strane, države mogu biti i izvor kiber pretnji. U vezi s tim, strane obaveštajne službe koriste IKT sredstva za prikupljanje informacija i špijunažu. Ova aktivnost može biti usmerena ka drugim državama (prijateljskim i neprijateljskim) ili ka nedržavnim subjektima. Države, takođe, mogu napadati strane rivale sa ciljem dezinformisanja, destabilizacije, zastrašivanja ili čak potpunog kiber rata.[2]

U strategijama kiber bezbednosti pojedinih zemalja, u delu u kojem se navodi uloga oružanih snaga u ostvarivanju sposobnosti kiber odbrane, jasno se navodi da oružane snage moraju da razvijaju kapacitete za obaveštajni rad, kiber napad i kiber odbranu. U Strategiji kiber bezbednosti Finske, na primer, navodi se da će odbrambene snage zaštititi svoje sisteme na takav način da su u stanju da izvršavaju sve zakonom propisane zadatke, bez obzira na pretnje u kiber prostoru. Garantovane sposobnosti za obaveštajni rad i primenu proaktivnih mera u kiber prostoru, razvijaće se na istovetan način, kao i ostale vojne sposobnosti i druge elemente vojne sile.[3]

Iz navedenog se može zaključiti da su obaveštajne službe jedan od važnih subjekata pretnji u kiber prostoru. Obaveštajne službe, međutim, imaju dvojaku ulogu. One su i važan akter u reagovanju na kiber pretnje. Eksperti Međunarodne unije za telekomunikacije (ITU) smatraju da obaveštajne agencije mogu da imaju važnu ulogu u planiranju i sprovođenju nacionalnih strategija kiber bezbednosti, jer su najstručnije u pogledu razvijanja tehnika kriptografije i kriptoanalize. I pored toga što je angažovanje obaveštajnih agencija kontraverzno i izaziva negativne reakcije civilnog društva i pokretanje pitanja „civilnih sloboda", smatra se da su one najkompetentnije za ocenjivanje efikasnosti tehničkih mera zaštite nacionalnih informaciono-komunikacionih sistema.[4]

Vrste napadnih operacija u kiber prostoru

Kiber prostor predstavlja poligon na kojem se nadmeću velike sile i drugi brojni akteri, u političkoj, ideološkoj, ekonomskoj, vojnoj i mnogim drugim sferama. Posmatrano sa vojnog aspekta, kiber prostor je još krajem prošlog veka stekao status petog borbenog prostora uz kopno, more, vazduh i svemir. Virtuelni prostor, kao novi domen[5] vođenja borbenih dejstava, karakteriše upotreba elektronskog i elektromagnetnog spektra alata za čuvanje, modifikovanje i razmenu podataka preko umreženih sistema povezanih sa fizičkom infrastrukturom. U tom smislu, imajući u vidu da kiber prostor predstavlja jednu ogromnu bazu podataka, posebno tajnih, on je danas u fokusu interesovanja savremenih obaveštajnih službi.

Fenomen špijuniranja putem kiber prostora aktuelizuje se, kako u populističkoj, tako i u savremenoj stručnoj i naučnoj literaturi. Vlade mnogih razvijenih zemalja, među kojima su

[2] Prema: United States Government Accountability Office, *Information Security: Cyber Threats and Vulnerabilities* (Washington DC: US GAO, 2009); William A. Wulf and Anita K. Jones, "Reflections on Cybersecurity", *Science* Vol. 326, Issue 5955 (2009): p. 947; Martin Charles Golumbic, *Fighting Terror Online: The Convergence of Security, Technology, and the Law* (New York: Springer, 2007).

[3] Vidi: „Finland´s Cyber Security Strategy", http://*www.yhteiskunnanturvallisuus.fi/.../38-finlan* (preuzeto 04.05.2016).

[4] International Telecommunication Union, *The ITU National Cyber Security Strategy Guide*, Frederick Wamala (Geneva: ITU, 2011) http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf (preuzeto 04.05.2016).

[5] Kiber domen uključuje svu energiju koja teče kroz elektromagnetni spektar (radio-talasi, mikro-talasi, h-talasi, gama-zračenja i „usmerena energija").

SAD, Kina i Ruska Federacija, žale se na problem kiber špijunaže. Da bezbednost računarskih mreža nije više samo tehnički problem, nego i važno strateško pitanje, potvrđuje i poziv, koji je 2011. godine uputio veteran američke diplomatije Henri Kisindžer predstavnicima SAD i Kine da započnu „sajber detant". Kisindžer se zalaže za sklapanje neke vrste sporazuma između dve zemlje, kojima bi se pojedine oblasti sajber prostora proglasile nedodirljivim za računarske špijune, provalnike i hakere.[6] Teorijski gledano, mogućnost prikupljanja obaveštajnih podataka postoji, čak i kada su takve obaveštajne operacije usmerene prema vrlo važnim i osetljivim političkim i vojnim komunikacijama, i to sa velike udaljenosti i iz bilo kojeg kraja sveta. Težnja svih tajnih službi je postizanje tzv. „ziro-dey-difens", odnosno mogućnosti da se tajno infiltriraju u tuđe sisteme (ne praveći, pri tom, nikakvu štetu), tako da vlasnik sistema ne zna da je objekat „tihe" prismotre.

Postoji više tipova kiber napada. Jedna od najopštijih podela, koja se povezuje sa obaveštajnim radom, jeste ona koja je izvršena u zavisnosti od pozicije napadača. U tom smislu mogu se razlikovati:

1) unutrašnji i

2) spoljni napadi.

Unutrašnji napad je onaj koji inicira entitet unutar bezbednosnog perimetra (insajder). Od insajderskih napada teško je braniti se zato što napadač zloupotrebljava privilegije pristupa koje ima na osnovu legitimnih poslovnih funkcija koje obavlja u organizaciji. Sa druge strane, ne autorizovani ili nelegitimni korisnici iniciraju spoljne napade van bezbednosnih perimetara. Spoljne napade sprovode različito motivisani subjekti pretnji, poput hakera, organizovanih kriminalnih grupa ili država. Pomenute dve vrste napada međusobno se ne isključuju, jer se, u praksi, akteri spoljnih napada često oslanjaju na insajdere.

Eksperti Međunarodne telekomunikacione unije (ITU) klasifikuju kiber napade u dve klase: 1) aktivni napadi i 2) pasivni napadi.

Aktivni napad ima za cilj da menja sistemske resurse ili utiče na rad sistema. Sa druge strane, pasivni napad ima za cilj da dođe u posed informacije iz sistema, ali ne i da utiče na resurse napadnutog sistema.

Navedena podela na aktivni i pasivni napad može se dalje granati u zavisnosti od toga šta je cilj konkretnog kiber napada. Opšte uzevši, može se reći da je svaki kiber napad usmeren na bar jedno od tri osnovna svojstva informacije: *tajnost* ili *poverljivost* (engl. *privacy*, *confidentiality*), *integritet* (engl. *integrity*) i *raspoloživost* (engl. *availability*). Pojedini autori pod osnovna svojstva informacije podvode i *autentičnost* (engl. *authentication*) i *neopozivost* (engl. *non-repudiation*).[7]

Tajnost se definiše kao način postupanja sa podatkom koji obezbeđuje da on, tokom obrade i čuvanja, nije postao dostupan neovlašćenim licima, odnosno nije neovlašćeno obrađivan.[8] Prema tome, cilj tajnosti jeste da dozvoli pristup informaciji isključivo autorizovanim licima, procesima ili programima. Na primer, ukoliko dođe do ne autorizovanog pribavljanja informacija iz štićenog sistema, uključujući i „skrivenu analizu saobraćaja" u kojoj napadač donosi zaključke o sadržaju komunikacije samo na osnovu posmatranja

[6] „Vreme je za sajber detant", *Politika*, rubrika Svet, 15.06.2011.

[7] Nenad Putnik, *Sajber prostor i bezbednosni izazovi* (Beograd: Univerzitet u Beogradu, Fakultet bezbednosti, 2009), str. 57.

[8] *Zakon o informacionoj bezbednosti Republike Srbije* (Beograd: „Službeni glasnik RS" broj 6/16 od 28.01.2016), str. 2.

komunikacionih obrazaca, možemo smatrati da je narušeno svojstvo tajnosti. Nemačka strategija kiber bezbednosti navodi da kiber špijunaža, odnosno prikupljanje obaveštajnih podataka u kiber prostoru, predstavlja kiber napad koji je usmeren prema tajnosti IKT sistema i koji je izvela strana obaveštajna služba.[9] Prikupljanje obaveštajnih podataka u kiber prostoru, pre svega osetljivih podataka, upravo predstavlja vrstu kiber napada koja je usmerena na tajnost informacija i podataka u protivničkoj mreži.

Integritet znači očuvanost izvornog sadržaja i kompletnosti podatka, odnosno sredstva.[10] Napad na integritet predstavlja ne autorizovanu modifikaciju podatka ili baza podataka. Napadači mogu da koriste hakerske tehnike da modifikuju, unište ili na drugi način kompromituju integritet podataka. Napad na integritet može da uključuje sabotažu baze podataka radi ostvarenja kriminalnih, političkih ili vojnih ciljeva. Napad na integritet podatka u kiber prostoru i računarskom sistemu protivnika ne spada u kiber špijunažu (prikupljanje obaveštajnih podataka u kiber prostoru), ali se može posmatrati i svrstati u vrste tajnih operacija obaveštajnih službi u tom prostoru, kao pandan obmanjivanju i dezinformisanju. U takvu vrstu napada spada kiber dezinformisanje i obmanjivanje, čiji je cilj modifikacija ili manipulacija podacima ili ubacivanje kontradiktornih podataka radi uticaja na političke ili poslovne rezultate ili destabilizaciju stranih vlada.

Raspoloživost je karakteristika načina upravljanja podatkom koja obezbeđuje da je podatak dostupan i upotrebljiv na zahtev ovlašćenih lica u trenutku kada im je potreban. Napad koji ugrožava raspoloživost informacije ima za cilj da autorizovanog korisnika spreči da ostvari pristup svom sistemu ili bazi podataka. Najzastupljenija napadačka tehnika kojom se narušava raspoloživost informacije je distribuirana opstrukcija usluga (eng. *Distributed-Denial-of-Service – DDoS*). Krivično delo kiber sabotaže predstavlja, na primer, kiber napad usmeren prema integritetu i dostupnosti IKT sistema, ne samo u domaćoj već i u legislativi drugih država. Kiber sabotaža se, takođe, može svrstati u spektar tajnih operacija uticaja obaveštajnih službi u kiber prostoru.[11]

Autentičnost je mera bezbednosti koja teži da odredi vrednost i validnost prenosa, poruke ili pošiljaoca. Ovom merom se, takođe, kontroliše i autorizacija korisnika da primi specifične kategorije informacija.

Neopozivost je mera bezbednosti čiji je cilj da osigura tok komunikacije. Njome se postiže da pošiljalac informacije ima dokaz o njenoj isporuci, ali i da primalac informacije ima podatak o identitetu pošiljaoca, tako da nijedan od učesnika u prenosu kasnije ne može negirati izvršenu razmenu.

Stepen važnosti navedenih svojstava informacija, sa bezbednosnog stanovišta, varira u zavisnosti od konteksta u kojem se razmena informacija vrši. U vojnim sistemima, na primer, najveća pažnja posvećuje se tajnosti informacija, dok je u finansijskim transakcijama između banaka težište na integritetu i autentičnosti.

---

[9] Federal Ministry of Interior, *Cyber Security Strategy for Germany*, (Berlin: Federal Ministry of the Interior, 2011). https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_-Strategy_for_Germany.pdf?__blob=publicationFile (preuzeto 10.04.2012), str 14.

[10] *Zakon o informacionoj bezbednosti Republike Srbije* (Beograd: „Službeni glasnik RS" broj 6/16 od 28.01.2016), str. 2.

[11] Federal Ministry of Interior, *Cyber Security Strategy for Germany*, (Berlin: Federal Ministry of the Interior, 2011) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile (preuzeto 10.04.2012), str 14.

Definisanje obaveštajnog rada u kiber prostoru

U stranoj i domaćoj literaturi postoje brojni izrazi i definicije koje se dovode u vezu sa obaveštajnim radom u kiber prostoru. Za ovu aktivnost koriste se različiti termini: računarsko-mrežna eksploatacija (*Computer network exploitation – CNE*), kiber špijunaža (*Cyber* espionage – *CyberESP*), kiber istraživanje, kiber obaveštajni rad (*Cyberintelligence – CyberINT).* Nepostojanje jedinstvenog naziva i definicije obaveštajnog rada u kiber prostoru predstavlja dodatnu poteškoću za dalji rad na objašnjenju i analizi ovih aktivnosti, kao i određivanju njenog mesta u savremenim disciplinama obaveštajnog rada.

U anglosaksonskom govornom području u upotrebi su posebni tehnički termini za vojne operacije. Tako se računarsko-mrežne operacije dele na: napadne (*Computer Network Attack – CNA*), odbrambene (*Computer Network Defense – CND*) i povezane računarske operacije za eksploataciju (*Computer Network Exploitation – CNE*). Računarske operacije za eksploataciju ili istraživanje omogućavaju obaveštajno prikupljanje podataka preko računarskih mreža iz protivničkih baza podataka.

Računarsko-mrežna eksploatacija obuhvata prikupljanje obaveštajnih podataka i druge operacije koje omogućavaju da se dođe do podataka protivnika kroz njegov informacioni sistem.[12] Računarsko-mrežna eksploatacija, kao oblik računarsko-mrežnih operacija, obuhvata prikupljanje informacija i manipulaciju sa njima. Ovako pribavljene informacije koriste se da povećaju savezničku obaveštajnu sliku o protivniku i bojištu, kao i da neprijatelju „zamagle" pravu sliku stanja na bojištu. Zbog toga se ova aktivnost svrstava u vodeću i najmoderniju poddisciplinu signalnog obaveštajnog rada (*SIGINT*) u informacionom dobu.[13]

Računarsko-mrežna eksploatacija je nameran i promišljen akt infiltriranja u protivnički informacioni sistem, sa ciljem da se utiče na proces donošenja odluka kod protivnika, kao i da se pojačaju obaveštajna saznanja savezničkih snaga. Tim operacijama postiže se izvlačenje informacija iz protivničkih mreža (pasivni oblik), kao i ubacivanje podataka i informacija u protivničke mreže, čime se degradira suparnikova sposobnost da pravilno proceni borbeni prostor (aktivni oblik, odnosno tzv. *tajna operacija uticaja*). Operacije izvlačenja i ubacivanja podataka se definišu na sledeći način:

– *izvlačenje podataka* (eng. *extraction*) predstavlja pasivnu tehniku koja podrazumeva hvatanje podataka koji saobraćaju protivničkom mrežom ili vađenje informacija iz protivničke baze podataka. Pristup protivničkim vezama i čvorovima je, prema tome, neophodan da bi se došlo do informacije. Obaveštajni podaci koji su dobijeni tehnikom ekstrahovanja mogu kasnije da budu iskorišćeni, modifikovani i vraćeni u protivničku mrežu;

– *ubacivanje* (eng. *injection*) predstavlja aktivnu tehniku koja podrazumeva ubacivanje podataka u protivničku bazu, čime se ostvaruje manipulacija protivničkim informacijama. Ovom tehnikom postiže se da protivnička strana stiče pogrešnu obaveštajnu sliku, što daje prednost savezničkoj strani.

---

[12] Cooperative Cyber Defence Centre of Excellence, *International Cyber incidents: Legal considerations, Abbrevations and glossary*, Eneken Tikk, Kadri Kaska, Liis Vihul (Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010) http://www.ccdcoe.or (preuzeto 12.07.2014).

[13] Vidi: Ron Deibert and Rafal Rohozinski, "Tracking GhostNet: Investigating a Cyber Espionage Network", *Information Warfare Monitor*, 29.03.2009, The SecDev Group &The Citizen Lab,http:// www.nsi.org/pdf/reports/Cyber%20Espionage%20Network.pdf (preuzeto 05.05.2016).

Za razliku od računarsko-mrežne eksploatacije, *kiber špijunaža* predstavlja relativno nov tip obaveštajnog prikupljanja podataka zasnovanog na različitim strategijama, taktikama i alatima. Kiber špijunaža se definiše kao korišćenje računara ili digitalne komunikacije na međunarodnom planu sa ciljem da se ostvari pristup osetljivim informacijama o protivniku radi zadobijanja prednosti u političkom, vojnom, ekonomskom i drugom smislu, ili prodaje pribavljene informacije i ostvarivanja novčane dobiti.[14]

Prema definiciji Sejmura Herša (Seymour M. Hersh), kiber špijunaža je „aktivnost tajnog presretanja i hvatanja imejl saobraćaja, tekstualnih poruka, druge elektronske komunikacije, korporativnih podataka, iz razloga prikupljanja obaveštajnih podataka za potrebe nacionalne bezbednosti i ekonomske špijunaže".[15] Ova aktivnost zasniva se na prikupljanju tajnih podataka bez znanja i odobrenja vlasnika i držalaca informacije (individue, rivali, grupe ili vladine institucije), radi sticanja lične ekonomske, političke ili vojne prednosti. Špijuniranje u kiber svetu podrazumeva korišćenje ilegalnih metoda za prikupljanje podataka putem interneta, umreženih ili individualnih računara, korišćenjem hakerskih tehnika i malicioznih kodova. Celokupna operacija kiber špijuniranja može biti realizovana u realnom vremenu, sa prostorno udaljenih računara. Ova aktivnost, isto tako, može da se sprovodi uz pomoć infiltriranih insajdera koje su obučili profesionalni špijuni ili obaveštajni operativci.

Kiber špijunaža, dakle, podrazumeva zadobijanje ilegalnog pristupa nad IKT sistemom protivnika i njegovim poverljivim i tajnim informacijama, radi ostvarenja strategijske prednosti, kao i izvođenja psiholoških operacija ili drugih subverzivnih aktivnosti. U poslednje vreme, kiber špijunaža uključuje analizu javnih aktivnosti na društvenim mrežama kao što su Fejsbuk (eng. Facebook) i Tviter (eng. Twitter). Analiza aktivnosti protivnika na socijalnim mrežama izrodila je novu disciplinu prikupljanja obaveštajnih podataka pod nazivom *Social Network Intelligence – SOCINT*).

Prema Heršu postoji razlika između kiber ratovanja i kiber špijuniranja. On zastupa tezu da je kiber špijuniranje aktivnost prikrivenog presretanja i hvatanja imejl saobraćaja, tekstualnih SMS poruka i drugih vidova elektronske komunikacije, kao i korporativnih podataka radi prikupljanja obaveštajnih podataka koji su značajni za nacionalnu bezbednost, ekonomiju i privredu. Sa druge strane, prema ovom autoru, kiber ratovanje obuhvata prodor u računarsku mrežu protivnika, sa ciljem izazivanja njene neoperativnosti, odnosno privremene ili trajne disfunkcije.[16]

Kiber špijunaža se ne smatra aktom ratovanja, ali je diskutabilno kako bi takav akt, u slučaju otkrivanja, okarakterisale ugrožene države.[17] Za sprovođenje aktivnosti kiber špijunaže i kiber ratovanja koriste se gotovo identične tehnike, metode i sredstva. Međutim, kiber špijunaža se, za razliku od kiber ratovanja, prema međunarodnom pravu nikako ne bi mogla

[14] Kevin Coleman, „The Growing Risk of Cyber Attack and Other Security Threats", *The risk report* Volume XXXI, No. 3, November 2008, p. 5.
http://www.hwphillips.com/wp-content/uploads/2012/09/The-Growing-Risk-of-Cyber-Attack-and-Other-Security-Threats.pdf(preuzeto 07.02.2016).

[15] Seymour M. Hersh, "The Online Threat: Should We Be Worried About a Cyber War?", *The New Yorker*, 01.11. 2010, http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh? (preuzeto 18.12.2015).

[16] *Ibid.*

[17] Dosadašnji slučajevi, poput afere sa velikom mrežom GhostNet preko koje je špijunirana kancelarija Dalaj Lame i koja je bila raširena u mnogim državama sveta, uglavnom na računarima ambasada i konzularnih predstavništva mnogih država (uključujući i ambasadu Indije u Beogradu), nisu bili označeni kao akti agresije.

okarakterisati kao akt agresije.[18] Ni u realnom svetu špijunaža se ne poistovećuje sa agresijom. U prilog ovoj tvrdnji svedoči odluka Saveta bezbednosti UN u vezi sa poznatim incidentom iz vremena hladnog rata, kada je SSSR iznad svoje teritorije oborio američki avion koji se nalazio u neovlašćenoj špijunskoj misiji.[19] Tada je Savet bezbednosti odbacio tvrdnju SSSR-a da je ta akcija čin agresije SAD. Odluka Saveta bezbednosti je odražavala stav da pomenuti akt nije značio nezakonitu upotrebu sile, bez obzira na očiglednu povredu vazdušnog prostora Sovjetskog Saveza.[20] Po analogiji sa ovim događajem, priznati stručnjaci iz oblasti kiber bezbednosti izvode zaključak da ni špijunski kiber upad u informacione mreže neke zemlje nije akt nezakonite primene sile.[21] Međutim, u takvom slučaju dopuštene su akcije samoodbrane zemlje čiji je prostor povređen (kopneni, vazdušni, kiber ili bilo koji drugi prostor), jer ni u jednoj državi, prema nacionalnom pravu, špijunaža nije dozvoljena. Situacija je mnogo složenija u slučaju kiber upada u informacione sisteme neke države kojim se onesposobljavaju njeni informacioni kapaciteti, čime se, direktno ili posredno, nanosi šteta njenoj sposobnosti da se brani, materijalnim i finansijskim resursima ili celokupnom stanovništvu.[22]

Centralna obaveštajna agencija (CIA) zastupa stav da kiber špijunaža ne potpada pod aktivnosti kiber ratovanja, verovatno zato što vlada SAD, kao i mnoge vlade razvijenih zemalja, rutinski primenjuje špijunažu komunikacionih mreža. Sličan stav ima i Nacionalni savet SAD za istraživanje (*U.S. National Research Council*). Savet pravi razliku između kiber špijunaže i kiber istraživanja (eng. *cyber exploitation*) koje uključuje akcije za prikupljanje informacija iz kiber domena. Međunarodno ratno pravo naglašava da postoji jasna razlika između upotrebe sile i špijunaže, te da špijunaža ne obuhvata upotrebu sile. Sličan je stav i Ministarstva odbrane SAD prema kojem se mora praviti razlika između kiber pretnji i kiber napada. Distinktivno obeležje kiber napada je upravo to što on obavezno ugrožava funkcionalnost računarske mreže.[23]

Iz navedenih stavova evidentno je da postoji razlika u definicijama računarsko-mrežne eksploatacije i kiber špijunaže. Kiber špijunaža, kako je navedeno u definicijama, podrazumeva samo pasivnu obaveštajnu praksu, dok računarsko-mrežna eksploatacija podrazumeva i primenu operacija ubacivanja pogrešnih informacija, tj. manipulaciju informacijama da bi se uticalo na protivnički računarski sistem. U tom smislu, smatramo da je definicija računarsko-mrežne eksploatacije kompletnija, jer obuhvata i prikupljanje informacija i operacije uticaja, odnosno obe aktivnosti koje ulaze u spektar savremenog obaveštajnog rada. Zbog toga predlažemo sledeću operacionalnu definiciju obaveštajnog rada u kiber prostoru: *Obaveštajni rad u kiber prostoru obuhvata računarsko-mrežne operacije koje se sprovode radi tajnog prikupljanja i analize podataka, kao i uticaja na informacije i onesposobljavanja informacionih, računarskih mreža i povezanih sistema protivnika.*

---

[18] Младен Милошевић и Ненад Путник, „Проблем правне (не) регулисаности конфликата у кибер простору", *Трећи програм*, свеска бр. 162 (2/2014).

[19] Vidi: Arie J. Schaap, „Cyber warfare operations: Development and use under international Law", *The Air Force Law Review - Cyberlaw Edition*, Vol. 64, 2009: p. 143.

[20] Заседања Савета безбедности УН 857, 858, 859 и 860, према: Драган Младеновић, Мирјана Дракулић и Данко Јовановић, „Међународно право и сајбер ратовање", *Војно дело*, пролеће 2012, стр. 24.

[21] Драган Младеновић, Мирјана Дракулић и Данко Јовановић, „Међународно право и сајбер ратовање", *Војно дело*, пролеће 2012, стр. 24.

[22] *Ibid*.

[23] Vidi: Oona A. Hathaway, Rebecca Crootof *et. al*., „The law of cyber-attack", *California Law Review*, 2012, p. 14.

Klasifikacija obaveštajnog rada u kiber prostoru

Sumirajući prethodno iznete stavove u kojima smo upoređivali kategorije napada u kiber prostoru i oblike savremenog obaveštajnog rada, proizilazi da se mogu razlikovati dve vrste obaveštajne aktivnosti u kiber prostoru: pasivna i aktivna.

Pasivnim aktivnostima (prikupljanjem podataka) ne vrši se uticaj na protivnika i nema direktnih posledica po suprotstavljenu stranu, dok je cilj aktivnog obaveštajnog rada uticaj na protivnika u željenom pravcu. S tim u vezi, obaveštajni rad u kiber prostoru delimo na: 1) pasivni obaveštajni rad čiji je cilj prikupljanje i analiza podataka o protivniku i 2) aktivni, čiji je cilj uticanje na informacije, računarske mreže i druge povezane sisteme protivnika. Aktivni obaveštajni rad u kiber prostoru naziva se i tajnim operacijama uticaja u ovom prostoru, jer je cilj i jednih i drugih operacija istovetan. Kao što je ranije navedeno, pasivnim oblicima obaveštajnog rada napada se i ugrožava tajnost protivničke informacije u kiber prostoru, dok se aktivnim oblicima napada integritet, autentičnost i raspoloživost protivničke informacije. Takođe, cilj aktivnih oblika obaveštajnog rada u kiber prostoru jeste i onesposobljavanje funkcije protivničke mreže, pa se može zaključiti da tajne operacije uticaja obaveštajnih službi u kiber prostoru, čiji je cilj onesposobljavanje funkcije računarske mreže protivnika, imaju sve karakteristike kiber napada i zadovoljavaju zahteve definicije koju smo naveli.

Na sličan zaključak u vezi sa naglašavanjem razlike između pasivnog i aktivnog obaveštajnog rada u kiber prostoru dolazi se i analizom odredbi Evropske konvencije o visokotehnološkom kriminalu (u daljem tekstu Konvencija), Krivičnog zakonika Republike Srbije i drugih evropskih zemalja. Tu se, pre svega, radi o delima *nelegalnog pristupa elektronskim podacima* i *nelegalnog presretanja podataka*, kao pasivnim oblicima i delu *izmena podataka na računaru*, kao aktivnom obliku. Iz ovih dela proističu još dva krivična dela – *izmena tajnih podataka* i *upad u računarsku mrežu*. Ova dela najčešće se označavaju kao dela špijunaže i odavanje tajne.[24]

Nelegalni pristup informacijama sadržanim na računaru ili računarskom sistemu podrazumeva upad u računar ili računarski sistem u nameri da se određene informacije prisvoje, izmene ili unište.[25] *Nelegalno presretanje privatnih podataka* koji se prenose na bilo koji način između dva računara (ili mreže) predstavlja posebno osetljivo pitanje u elektronskim komunikacijama. Presretanje podataka u elektronskoj komunikaciji predstavlja zapravo, u terminologiji klasičnog krivičnog prava, prisluškivanje komunikacija.[26]

Izmena podataka na računaru u smislu namernog, potpunog ili delimičnog oštećenja, brisanja, promene sadržine, kompresije i bilo kojeg drugog načina izmene originalnih podataka određena je Konvencijom kao posebno krivično delo koje države potpisnice moraju uvrstiti u svoje zakonodavstvo. Ovo delo se u mnogim nacionalnim zakonodavstvima susreće kao *uskraćivanje usluga*. Konvencija sadrži dva oblika ovog dela – *ometanje poda-*

[24] Марио Рељановић, „Кривично правна заштита електронских тајних података", у *Приступ информацијама од јавног значаја и заштита тајних података* (Београд: ОЕБС, 2013), стр. 41.

[25] Закон о потврђивању Конвенције о високотехнолошком криминалу (Београд: „Сл. гласник РС", бр. 19 од 19. марта 2009), члан 2.

[26] Закон о потврђивању Конвенције о високотехнолошком криминалу (Београд: „Сл. гласник РС", бр. 19 од 19. марта 2009), члан 3.

taka i *ometanje sistema*[27] i ostavlja mogućnost da države izmenu podataka mogu smatrati krivičnim delom samo ako je počinjena veća šteta. Ovo delo naglašava da se i u krivičnom zakonodavstvu EU pravi razlika između aktivnog obaveštajnog rada – *izmena podataka na računaru*, i pasivnog obaveštajnog rada koje se u krivičnom zakonodavstvu definiše *delima nelegalnog pristupa informacijama* i *nelegalnog presretanja privatnih podataka*.

Krivični zakonik Srbije poznaje čitav niz dela koja korespondiraju inkriminacijama iz Konvencije. U njemu je jasno dat opis i kvalifikacija onih dela koja klasifikujemo u aktivne oblike obaveštajnog rada u kiber prostoru.[28] U tom smislu navedena su sledeća dela: oštećenje računarskih podataka i programa (član 298), računarska sabotaža (član 299), pravljenje i unošenje računarskih virusa (član 300), neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (član 302), sprečavanje i ograničavanje pristupa računarskoj mreži (član 303).[29]

Tehnike pasivnog oblika obaveštajnog rada u kiber prostoru

Kiber špijuniranje podrazumeva korišćenje hakerskih tehnika od strane obaveštajnih organizacija sa ciljem da se pribave informacije ili pristupi stranim računarskim sistemima, radi realizacije špijuniranja ili vršenja sabotaže u pogodnom momentu.[30]

Informacije se mogu pribaviti na više načina. Praktično posmatrano, može se praviti razlika između spoljašnjih i unutrašnjih kanala oticanja informacija, odnosno spoljašnjih i unutrašnjih napada.

Spoljašnji kanali oticanja informacija odnose se na tehnička sredstva i njihova inherentna svojstva koja ih čine izvorom informacija. Oni su definisani načinom dobijanja informacija, fizičkom prirodom informativnih signala i sredinom njihovog prostiranja. U spoljašnje kanale oticanja informacija spadaju: tehnički kanali (električni, indukcioni), akustički kanali (vazdušni, vibracioni, elektroakustički, optoelektronski), kanali prijema pri predaji informacija sistemima veze (na prenosnom putu) i računarski kanali oticanja informacija.

Unutrašnji kanali oticanja informacija vezani su za personal (saradnike), njihove motive, želje, sklonosti i radne navike. Unutrašnji kanali su predmet istraživanja bezbednosnih nauka i odražavaju socijalno-psihološki aspekt informacione bezbednosti.

Za realizaciju spoljašnjih napada izviđanje računara se realizuje:

1) prikupljanjem podataka pomoću interneta (izviđanje upotrebom hakerskih programa i hakerske tehnike) i

2) prikupljanjem podataka registrovanjem elektromagnetne energije (EME) ili kompromitujućeg elektromagnetnog zračenja (KEMZ) koju emituju računarske komponente (pasivno izviđanje uz pomoć opreme za primenu elektronske podrške, odnosno izviđanje radio-veza).

---

[27] Закон о потврђивању Конвенције о високотехнолошком криминалу (Београд: „Сл. гласник РС", бр. 19 од 19. марта 2009), чланови 4 и 5.

[28] Марио Рељановић, „Кривично правна заштита електронских тајних података", у: *Приступ информацијама од јавног значаја и заштита тајних података* (Београд: ОЕБС, 2013), стр. 44.

[29] Види шире: Кривични Законик („Сл. гласник РС", бр. 85/2005, 88/2005 – испр., 107/2005 – испр., 72/2009, 111/2009, 121/2012, 104/2013 и 108/2014).

[30] Bonnie Adkins, *The spectrum of cyber conflict from hacking to information warfare: what is law enforcement's role* (Alabama: Air Command and Staff College Air University, USAF, 2001), r. 26.

Prikupljanje podataka pomoću interneta podrazumeva upotrebu posebnih hakerskih tehnika i alata, kao i malicioznih kodova (eng. *malware*)[31] za izvođenje spoljašnjih napada. Dakle, može se tvrditi da spoljašnji napadi koriste bilo koji oblik slabosti ili ranjivosti (tehničke ili ljudske) sistema žrtve.

Prema dostupnim izvorima, za ove namene koriste se tehnike i alati koji su slične onima koje koriste pripadnici kriminalnih grupa.[32] One podrazumevaju tajno ubacivanje malicioznih kodova u računarske sisteme protivnika preko imejl poruka, spoljnih medija (CD-ROM, fleš memorija, memorijske kartice i sl.) ili primenu fišing (eng. *phishing*) tehnike (privlačenje protivnika da pristupi unapred pripremljenom internet sajtu).

Maliciozni kodovi označavaju posebnu kategoriju informatičkih programa čiji je cilj da oštete računarski sistem korisnika ili da naruše neko od svojstava informacija. Maliciozni kod inficira računarski sistem putem ne autorizovanih i za korisnika neočekivanih procesa. Postoje različite vrste malicioznih kodova, ali njihova kompozicija[33] i konstantna evolucija otežavaju koherentnu klasifikaciju. U ovu grupu mogu se svrstati sledeći informatički programi: *virusi* (*eng*. virus), *crvi* (*eng. w*orm), *trojanski konji* (*eng.* trojanhorse), *sporedna vrata* (*eng.* backdoor)*, programi za ne autorizovano praćenje aktivnosti korisnika* (*eng.* spyware), *programi za praćenje i snimanje operativnog rada korisnika računara na nivou mikrooperacija* (*eng.* keylogger) i *otmičari* (*eng.* hijacker).

Maliciozni kodovi često su u funkciji prikupljanja podataka u korist kiber napadača. Prikupljanje podataka se ostvaruje njihovim diskretnim ubacivanjem na računar korisnika dok je povezan na internet.[34] Ovi zlоćudni kodovi reklamiraju se kao besplatni alati za različite namene na internet sajtovima, a najčešće kao programi „mamci" koji, navodno, treba da pospeše rad računara ili poboljšaju neku uslugu korisniku. Nakon inficiranja računara, prisustvo malicioznog koda manifestuje se na različite načine – od narušavanja ispravnog rada računara do njegovog potpunog blokiranja. Međutim, ovi kodovi sve češće se koriste za diskretno prikupljanje podataka sa inficiranog računara.

Teško je nabrojati sve moguće vrste spoljašnjih napada, s obzirom na to da je njihov kvalitet i kvantitet ograničen jedino kreativnošću napadača. Osim toga, realni napadi često se izvode kombinacijom različitih tehnika, što otežava njihovu klasifikaciju. Jedna od mogućih kategorizacija sadržala bi sledeće tehnike: *interception, man in the middle attack, replay, spoofing, buffer overflow, saturation and delay, embedded attack*. Poslednjih godina najzastupljenije su tehnike *embedded attack* i *saturation and delayattack*.[35] U prvu kategoriju spadaju napadi koji se izvode pomoću tzv. malicioznih kodova, a u drugu napadi usmereni na opstrukciju usluga ciljanog računarskog sistema (eng. *denial of service attack – DoS*) ili, u novijem obliku, distribuirani napadi usmereni na opstrukciju usluga (eng. *distributed denial of service attack – DDoS*).

---

[31] Termin potiče od spoja engleskih reči *malicious* i *software,* tako da njegov bukvalni prevod glasi: *maliciozni program* ili *maliciozni kod*.

[32] „Nemačka se sprema za sajber rat", *PressOnline*, rubrika Globus, 25.02.2009. http://www.pressonline.rs-/svet/globus/59380/nemacka-se-sprema-za-sajber-rat.html

[33] Najčešće su sačinjeni od više modularnih i međusobno zavisnih delova.

[34] Горан Калаузовић, „Офанзивне кибер активности", *Нови гласник*, број 1-4, јануар-децембар 2011, стр. 110.

[35] Cliff Berg, *High-Assurance Design: Architecting Secure and Reliable Enterprise Applications* (Amsterdam: Addison-Wesley Longman, 2005).

Znajući da se sistemi za zaštitu računara neprekidno usavršavaju, pojedine institucije otišle su „korak" dalje u smislu stvaranja načina da se dođe do informacija sa obaveštajno-bezbednosno interesantnih računara i računarskih mreža. Otuda su razvijene i tehnike za prikupljanje podataka putem neovlašćenog pristupa deljenim (tzv. šerovanim) datotekama računara koji koriste bežični (eng. *wireless*) internet i registrovanjem elektromagnetne energije, koju zrače pojedini delovi računara koji se nalaze pod električnim naponom.

Interesovanje za elektromagnetno zračenje i elektromagnetno prisluškivanje datira unazad više od četrdeset godina.[36] Skoro sve armije sveta i obaveštajne agencije oduvek su znale da elektromagnetni uređaji, bez odgovarajuće zaštite, generišu visoki nivo signala radio-frekvencije (RF) koji se mogu snimiti i posebnim, često jednostavnim metodama, pretvoriti u jasne i otvorene informacije. Još šezdesetih godina prošlog veka,[37] vršeni su pokušaji da se prikupe podaci na osnovu registrovanja EME koju zrače računari i pojedine računarske komponente (periferije računara).[38] Zbog toga što nedostaju stručna saznanja o opasnostima od kompromitujućeg elektromagnetnog zračenja (KEMZ), ovoj problematici je nedovoljno posvećena pažnja, posebno u oblasti računarske tehnologije.

Problem neovlašćenog pristupa informacijama putem KEMZ postoji u vojnim, diplomatskim i obaveštajnim krugovima više od četrdeset godina. U zapadnoj literaturi ova problematika najčešće se podvodi pod akronim američke vlade TEMPEST (*Transient Electro Magnetic Pulse Emanation Standard – TEMPEST*) mada se javljaju i tvrdnje da je to samo kodni naziv bez nekog posebnog značenja.[39] U svakom slučaju, radi se o strogo poverljivim standardima koji definišu dozvoljene granice i metode merenja TEMPEST-a, odnosno KEMZ-a.

Po svojoj prirodi KEMZ je pojava ista kao i ostale elektromagnetne smetnje. Razlika je jedino u tome što se radi o signalima koji nose informaciju koja ne sme biti dostupna neovlašćenim licima, odnosno ne sme biti prisluškivana. Nivo signala koji može da se prisluškuje znatno je niži od nivoa signala koji potencijalno mogu ometati rad drugih uređaja, pa je problem sprečavanja kompromitujućeg elektromagnetnog zračenja teže rešiti od problema elektromagnetne kompatibilnosti. Međutim, mehanizmi nastajanja obe vrste signala su potpuno jednaki, a ustaljena je praksa da se ove pojave zovu smetnjama.[40]

Elektronsko prisluškivanje putem ovakvih kompromitujućih elektromagnetnih zračenja, kao pasivna infiltracija koju je teško otkriti, predstavlja jedan od značajnih načina ugrožavanja bezbednosti, posebno za kompaktne i fizički izolovane računarske i informacione sisteme.

---

[36] Види шире: Милорад Маркагић, „КЕМЗ и информациона безбедност", у *Злоупотреба информационих технологија и заштита*, уредник Слободан Петровић (Београд: Удружење судских вештака за информационе технологије, 2010).

[37] Pripadnik obaveštajno-bezbednosne službe V. Britanije *MI5*, Piter Rajt (*Peter Wright*) godine 1960., je za potrebe svoje vlade, koja je pregovarala za članstvo u Evropsku ekonomsku zajednicu – EEZ, sa ciljem da sazna stav francuskog premijera De Gola po tom pitanju, registrovao sekundarne talase EME koje je emitovao zaštićeni šifarski komunikacioni sistem, a koji je koristila francuska diplomatska mreža, prema: MarkusG. KuhnandRossJ. Anderson, „Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations ?", in *Information Hiding*, David Aucsmith (Ed.) (Berlin, Heidelberg: Springer, 1998).

[38] Za razliku od aktivnosti SIGINT, koje podrazumevaju prikupljanje podataka na osnovu registrovane elektromagnetne energije komunikacijskih i radarskih sredstava, tehnika TEMPEST počiva na detekciji zračene elektromagnetne energije računara i računarskih sredstava.

[39] Američki akronim*TEMPEST – Transient Electromagnetic Pulse Surveillance Technology* ili *Transient Electromagnetic Pulse Emanation Standard.*

[40] Види шире: Милорад Маркагић, „КЕМЗ и информациона безбедност", у *Злоупотреба информационих технологија и заштита*, уредник Слободан Петровић (Београд: Удружење судских вештака за информационе технологије, 2010).

Tehnika prikupljanja informacija zasniva se na prikupljanju podataka putem registrovanja zračene elektromagnetne energije (EME), kojom se napajaju računarske jedinice, monitor, tastatura, kablovi i portovi (ulaz/izlaz) računara, kao i skeneri i printeri koji su manje izloženi jer se manje koriste. Činjenica je da navedene komponente za napajanje koriste mrežnu električnu energiju, koja se oslobađa i zrači u lokalnoj sredini (gde se komponenta nalazi), u većoj ili manjoj meri, zavisno od snage uređaja. Za ispisivanje teksta na displeju laptopa ili monitora potrebna je EME. Tu funkciju obavlja grafička jedinica – kartica, koja preneti signal od tastature, prosleđuje od memorije do displeja. Treća deonica na kojoj se prenosi EME i koja nosi informaciju o sadržaju (tekstu) prenosi se od računara do printera ili od skenera do računara. Dokazano je u praksi da čak i *RS-232* kabl (za povezivanje portova) emituje VF frekvencije koje nose koristan signal.[41]

Takođe, svako pritiskanje tipke na tastaturi praćeno je emitovanjem EME čije je trajanje proporcionalno vremenu potrebnom za kucanje različitih tipki. Osim kablom povezanih, za prijem signala još su pogodnije bežične tastature, koje rade na principu emitovanja radio-veze u VVF opsegu, čime pospešuju emitovanje EME i signal. One su naročito pogodne kada je cilj zainteresovanog lica (hakera) da sazna korisničko ime, lozinku ili imejl adresu korisnika. U periodu od 2001. do 2008. godine usavršena su četiri različita načina da se jasno rekonstruiše tekst na osnovu praćenja EME emitovane tipkama tastature, sa udaljenosti od 20 m, uključujući nekoliko pregrada od zidova čvrste gradnje.[42]

Eksperimenti su uspešno realizovani bez obzira na to da li se radi sa žičanim i bežičnim tastaturama (*PS/2, USB* konektorima, kao i sa tastature laptopa).[43] Nakon dugogodišnjeg ispitivanja u praksi, početkom devedesetih godina prošlog veka, Holanđanin Vim Van Ek, uspeo je u pokušaju da registruje emisije EME sa udaljenog računara pomoću jednostavne opreme zasnovane na modifikovanom TV prijemniku sa ručno kontrolisanim oscilatorom (ili laptopom opremljenim TV karticom), usmerenom antenom i pojačivačem signala. Registrovanjem ovih signala prikupljani su podaci koji su uz pomoć tehnike podešavanja vertikalne i horizontalne reflektovane frekvencije monitora pretvarani u tekst, odnosno u korisne informacije.[44]

Takozvana nenamerna zračenja (*unintentional emissions*), iako male snage, mogu da budu detektovana i pretvorena u određenu informaciju, upotrebom adekvatnih antena i osetljivih prijemnika za registrovanje radio-signala u različitim frekventnim opsezima (FO), sa manje ili veće udaljenosti.[45] Oslobođena EME je najveća sa monitora računara, a kreće se u FO od 55 do 245 MHz i može da bude registrovana sa udaljenosti od jednog metra do preko jednog kilometra, u skladu sa opremom i uslovima (okruženju) u kojima se računar nalazi.[46]

Registrovanje EME može da se realizuje i u vanradno vreme, jer vrlo često računari ostaju uključeni (s obzirom na tehničke karakteristike) u radnim prostorijama. Čak i ako su samo monitori uključeni, na osnovu zračenja kabla monitora povezanog na računar, mogu se registrovati

[41] *Ibid*.

[42] Горан Калаузовић, „Офанзивне кибер активности", *Нови гласник*, број 1-4, јануар-децембар 2011, стр. 110.

[43] *Ibid*.

[44] Vidi: Wim Van Eck, „Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?", *Computers & Security*, 4 (1985).

[45] *Ibid*.

[46] *Ibid*.

emisije koje mogu da daju informaciju o fizičkom prisustvu lica u prostoriji u kojoj se nalazi računar. I obratno, kada je monitor isključen, a računar uključen, kabl monitora može da predstavlja antenu sa koje se može detektovati koristan signal grafičke jedinice računara.[47]

Tehnike aktivnog oblika obaveštajnog rada u kiber prostoru

Među tehnike aktivnog oblika obaveštajnog rada u kiber prostoru mogu se svrstati: napadi distribuiranog uskraćivanja usluga, ubacivanje netačne informacije i infiltracija u obezbeđenu računarsku mrežu.

1) Napadi distribuiranog uskraćivanja usluga (Distributed Denialof Service Attacks – DDOS) imaju za cilj da onemoguće klijente ili organizaciju da koriste usluge računarske mreže ili informacionih resursa. Opstrukcija elektronskih usluga postiže se napadom na sisteme koji omogućavaju te usluge (na primer, napadom na server na kojem su uskladišteni web sajtovi ili na server elektronske pošte). Distribuirano uskraćivanje usluge je vrsta napada koja je usmerena na *raspoloživost* informacija, a ne na njihovu *poverljivost*. Nakon ovih napada najčešće nema krađe informacija ili ostalih gubitaka informacija poverljive prirode.

Najčešće korišćen metod za izvođenje ove vrste napada je izlaganje računara ili računarskih mreža, ogromnom broju zahteva[48] koncentrisanih u kratkom periodu. Napad distribuiranog uskraćivanja usluge započinje tako što napadač prisvaja kontrolu nad prvim računarom koji postaje „master" napada. Preko mastera hiljade drugih računara inficira se crvom ili bot-om,[49] pa postaju takozvani „zombiji". Zombi-računar sada može da izvrši bilo koju akciju predviđenu programom crva, koju, pozivanjem jedne jedine komande sa distance, inicira napadač, a da pri tom legitiman korisnik računara toga ne bude svestan. Korišćenjem ove izuzetno jednostavne operacije, hiljade inficiranih računara (koji čine kompromitovanu računarsku mrežu *botnet*) mogu istovremeno da pokrenu napad DDoS protiv cilja koji je napadač izabrao. Zombi-računar može se isprogramirati i tako da omogući otvaranje *sporednih vrata* (eng. *back door*) unutar lokalne mreže organizacije kojoj računar pripada i, na taj način, deplasira sve primenjene bezbednosne mere organizacije.

2) Ubacivanje netačne informacije. Ova operacija podrazumeva tajno unošenje netačne informacije u računarski sistem i predstavlja još jedan oblik kiber napada, poznat kao semantički napad. Ova vrsta napada može se, takođe, svrstati u aktivne oblike obaveštajnog rada u kiber prostoru. On je složeniji od DDOS napada. Posledica ovog semantičkog napada jeste da stvara uverenje da računarski sistem funkcioniše normalno. Godine 1999, na primer, prema nekim izvorima, SAD su razvile plan za ubacivanje lažnih podataka o ciljevima NATO-a u komandni sistem PVO Vojske Jugoslavije, čime je trebalo da bude umanjena njena sposobnost da gađa NATO avijaciju.[50] Prema dostupnim informacijama, NATO je napustio ovaj plan

[47] Vidi: Markus G. Kuhn and Ross J. Anderson, „Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations", in *Information Hiding, Second International Workshop*, David Aucsmith (Ed.), (Portland: Springer-Verlag, 1998), p. 132.

[48] Obično se koriste poruke elektronske pošte, zahtevi za pristup web stranicama i slično.

[49] *Bot* (*eng.*bot, skraćenica od robot) su programi koji se krišom instaliraju na računar žrtve sa ciljem da ne autorizovanom korisniku omoguće kontrolu sa udaljenih lokacija (eng. *Remote control*). Bot programi su projektovani za stvaranje kompromitovanih računarskih mreža, takozvanih *botnet work* ili *botnet*, koje napadač može koristiti za izvođenje koordiniranih kiber napada.

[50] Vidi: William M. Arkin, „The Cyber Bomb in Yugoslavia", *The Washington Post*, 25.10.1999, http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm

zbog pravnih problema oko nastanka moguće kolateralne štete.[51] Vazduhoplovne snage Izraela primenile su sličnu strategiju 6. septembra 2007. godine tokom avio-napada na nuklearna postrojenja Sirije. Izraelski avioni stigli su neprimećeno do ciljeva napada zahvaljujući ranije izvršenim kiber napadima kojima je kompromitovan sirijski sistem PVO. Tačan metod napada je nepoznat, ali je očigledno Izrael ubacio lažne podatke u radare OS Sirije.[52] Ove vrste kiber napada često prate i olakšavaju konvencionalne napade i njihova atribucija nije problematična. Poteškoća koja je povezana sa ovom vrstom napada sastoji se u problemu određivanja vremena kada je napad izvršen, jer postoji vremenska distanca između tog momenta i vremena otkrivanja posledica napada.

3) Infiltracija u obezbeđenu računarsku mrežu. Ukoliko se napadač infiltrira u obezbeđenu računarsku mrežu protivnika, može da izvršava mnogo raznovrsnije operacije od pasivnog prikupljanja obaveštajnih podataka. Na primer, 2010. godine otkriven je semantički napad koji je bio zasnovan na upotrebi malicioznog crva Staksknet (eng. Stuxnet). Na meti napadača bile su računarske mreže u iranskoj nuklearci Bušer, radi ometanja funkcije nuklearnih postrojenja. Cilj infiltracije u obezbeđenu računarsku mrežu nije uvek uništavanje računarske mreže ili infrastrukture, nego i preuzimanje kontrole nad njom. Godine 2003, neposredno pre invazije na Irak, SAD su se infiltrirale u lokalni imejl sistem Ministarstva odbrane Iraka i kontaktirale sa iračkim oficirima, pozivajući ih na mirnu predaju.[53] Ovaj kiber napad takođe se može svrstati u aktivne oblike obaveštajnog rada u kiber prostoru, imajući u vidu da je ostvaren aktivan kontakt i uticaj prema oficirima iračke armije. Ovi incidenti pokazuju da ne moraju svi napadi da budu izvršeni preko interneta već da se mogu sprovesti i infiltracijom u lokalnu, od interneta odvojenu i zaštićenu mrežu protivnika.

Posebni aspekti kiber prostora koji pogoduju izvođenju obaveštajnog rada u tom domenu

Najmanje tri karakteristike kiber prostora mogu opredeliti obaveštajne službe za vršenje špijunaže i tajnih operacija u ovom domenu: 1) mogućnost pristupa sa distance, 2) teškoće identifikovanja napadača i pripisivanja odgovornosti za napad i 3) teškoće razlikovanja operacija kiber špijuniranja od kiber napada.

Mogućnost pristupa sa distance je važna karakteristika koja razlikuje kiber prostor od realnog sveta. Sa nastankom kiber prostora geografska razdaljina između žrtve i počinioca postaje manje važna – ona više ne predstavlja uslov za sprovođenje napada na osetljive državne infrastrukture. Špijunski programi (*Spyware i keystroke loggers*) mogu biti ubačeni u ciljane protivničke mreže putem insajdera ili *trojanskog* softvera, čime se omogućava daljinski pristup informacijama i osetljivim podacima.[54] Špijuni ne moraju da budu fizički locirani blizu osetljivih informacija, pa čak ni na teritoriji zemlje kojoj ta in-

[51] Vidi: Jeffrey T. G. Kelsey, „Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", *Michigan Law Review*, Vol. 106, (2008): p. 1434.

[52] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010), p. 9-10.

[53] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010), p. 12.

[54] Vidi: Susan W. Brenner & Anthony C. Crescenzi, „State-Sponsored Crime: The Futility of the Economic Espionage Act", *Houston journal of international law* Vol. 28:2 (2006): p. 418.

formacija pripada, kako bi izvršili upad u ciljani sistem i ukrali štićeni podatak.[55] Osim toga, neusklađenost nacionalnih legislativa i problemi vezani za nadležnost nad deliktom ograničavaju mogućnosti bezbednosnih službi u sprovođenju zakona, te suzbijanju i presecanju špijunskih aktivnosti koje se izvode sa udaljenih lokacija.

Teškoće identifikovanja napadača i pripisivanja odgovornosti za napad (atribucije) karakteristike su kiber prostora koje pogoduju obaveštajnim aktivnostima. Suština problema je u tome što kiber napad, odnosno upad u računarsku mrežu, najčešće biva pokrenut u tajnosti, a identitet aktera nije uvek moguće utvrditi. Na primer, kiber napad koji je naizgled poreklom iz Kine, mogu pokrenuti teroristi sa Bliskog istoka, koji prikrivaju svoj identitet.[56] Samim tim, nije jednostavno pripisati odgovornost za kiber napad nekoj državi – ni direktnu ni indirektnu.

Teškoće razlikovanja operacija kiber špijunaže od kiber napada. Sličnosti između kiber napada i kiber špijunaže su velike. Uspešno kiber špijuniranje, kao i kiber napad, zahtevaju postojanje ranjivosti sistema i pristup toj ranjivosti, upotrebu različitih softverskih alata (za prenos, uklanjanje sigurnosnih programa kod protivnika i sam maliciozni kod). U slučaju kiber špijunaže, maliciozni kod može da bude program koji nadgleda i krade informacije, dok u slučaju kiber napada maliciozni program može da bude program koji dovodi do prekida rada sistema. Na osnovnom nivou, u rešavanju dileme da li se radi o kiber napadu ili o kiber istraživanju, ne postoji jasan konsenzus o tome da li način kvalifikacije dela kao kiber napada ili kiber istraživanja (špijunaže) treba da bude izveden: 1) iz analize instrumenata koji su korišćeni u njegovom pokretanju, 2) od procene karakteristika infrastrukture žrtve napada/špijunaže ili 3) od analize posledica akta. U nedavnim analizama problema kiber napada i kiber istraživanja, učesnici Nacionalnog saveta za istraživanje SAD (*National Research Council*) objasnili su problem na ovaj način: kiber istraživanje razlikuje se od kiber napada u svojim ciljevima i pravnim konstrukcijama koje ih okružuju. Ipak, veći deo tehnologije koja je potrebna za kiber istraživanje potrebna je i za izvođenje kiber napada. Ova tehnička sličnost često znači da napadnuta strana ne može biti u stanju da lako razlikuje kiber napad od kiber istraživanja.[57]

Zaključak

Opravdano se može pretpostaviti da će obaveštajni rad u kiber prostoru u budućnosti dodatno dobiti na značaju. Računarsko-mrežna eksploatacija će u bliskoj budućnosti verovatno postati jedna od najvažnijih disciplina za prikupljanje obaveštajnih podataka.

Kapaciteti tehničko-tehnološki razvijenih zemalja, poput SAD, Izraela i Velike Britanije, za sprovođenje računarsko-mrežne eksploatacije su nesumnjivo veliki, budući da njihove strategije bezbednosti tretiraju virtuelni svet kao prostor od strategijskog značaja uz kopno, vazduh, more i svemir.

I druge velike sile, uključujući Kinu i Rusku Federaciju, svrstale su kiber prostor i operacije u tom prostoru među kamene temeljce svojih nacionalnih bezbednosnih strategija.

[55] Vidi: Mindi McDowell, „Cyber Security Tip ST04-015: Understanding Denial-of-Service Attacks", U.S. computer emergency readiness team, http://www.us-cert.gov/cas/tips/ST04-015.html (preuzeto 4.11.2010).

[56] Vidi: Richard L. Kugler, „Deterrence of Cyber Attacks", in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Eds.), *Cyberpower and National Security* (Washington, D.C.: National Defense University Press, 2009), p. 309, 317.

[57] Robert D. William, „(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action", *The George Washington Law Review*, Vol. 79, (2011): p. 1198.

Kina aktivno razvija operativne kapacitete za izvođenje operacija u kiber prostoru, percipirajući ovaj prostor kao domen u kojem može da postigne strategijsku prednost, a možda i superiornost u odnosu na vojne kiber kapacitete SAD i njenih saveznika. Zbog toga ne iznenađuje činjenica da Kina ulaže značajna sredstva u kiber defanzivne i ofanzivne kapacitete Narodnooslobodilačke armije Kine i svoje bezbednosne službe.

Nacionalne obaveštajne agencije će, ukoliko žele da prevaziđu nesigurnost i steknu stratešku prednost, morati da preispitaju svoje stavove oko budućih obaveštajnih meta i obaveštajnih disciplina, te da se brzo adaptiraju na izazove i prednosti informacionih tehnologija i informacionog doba.

Promenljiva priroda obaveštajnih meta, kao i neusklađenost između velikog broja zahteva korisnika za informacijama i kapaciteta obaveštajnih službi i njihovih sredstava za prikupljanje, vodiće, verovatno, izgradnji višenamenskih, integrisanih sistema za prikupljanje podataka. Različite discipline za prikupljanje obaveštajnih podataka, tehnički metod (Tehnical Intelligence – TECHINT), prikupljanje pomoću ljudskih izvora (Human Intelligence – HUMINT), prikupljanje iz otvorenih, tj. javnih izvora (Open Sources Intelligence – OSINT) i kiber obaveštajni rad (Cyber Intelligence – CYBERINT) nastaviće da igraju važnu ulogu, mada će se njihova relativna važnost menjati sa vremenom i u odnosu na konkretnu situaciju.

Uspeh u obaveštajnom radu zahtevaće integraciju prikupljačkih kapaciteta na svim nivoima, a van je svake sumnje da će u stvaranju integrisanog obaveštajnog proizvoda važnu ulogu imati podaci prikupljeni putem kiber obaveštajnog rada.

Literatura

[1] Adkins, Bonnie. *The spectrum of cyber conflict from hacking to information warfare: what is law enforcement's role*. Alabama: Air Command and Staff College Air University, USAF, 2001.

[2] Berg, Cliff. *High-Assurance Design: Architecting Secure and Reliable Enterprise Applications*. Amsterdam: Addison-Wesley Longman, 2005.

[3] Brenner, Susan W. & Crescenzi, Anthony C. „State-Sponsored Crime: The Futility of the Economic Espionage Act". *Houston journal of international law*, Vol. 28:2 (2006): pp. 389-465.

[4] Clarke, Richard A. and Knake, Robert K. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins, 2010.

[5] Coleman, Kevin. „The Growing Risk of Cyber Attack and Other Security Threats". *The risk report* Vol. XXXI, No. 3, November 2008. http://www.hwphillips.com/wp-content/uploads/2012/09/The-Growing-Risk-of-Cyber-Attack-and-Other-Security-Threats.pdf(preuzeto 07.02.2016).

[6] Cooperative Cyber Defence Centre of Excellence. *International Cyber incidents: Legal considerations, Abbrevations and glossary*, Eneken Tikk, Kadri Kaska, Liis Vihul. Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010. http://www.ccdcoe.or (preuzeto 12.07.2014).

[7] Deibert,Ron and Rohozinski, Rafal. „Tracking GhostNet: Investigating a Cyber Espionage Network", *Information Warfare Monitor*, 29.03.2009, The SecDev Group &The Citizen Lab,http://www.nsi.org/pdf/reports/Cyber%20Espionage%20Network.pdf (preuzeto 05.05.2016).

[8] Federal Ministry of Interior. *Cyber Security Strategy for Germany*. Berlin: Federal Ministry of the Interior, 2011.
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile (preuzeto 10.04.2012).
„Finland´s Cyber Security Strategy", http://*www.yhteiskunnanturvallisuus.fi/.../38-finlan* (preuzeto 04.05.2016).

[9] Golumbic, Martin Charles. *Fighting Terror Online: The Convergence of Security, Technology, and the Law*. New York: Springer, 2007.

[10] Hathaway, OonaA., Crootof ,Rebecca*et. al*.. „The law of cyber-attack". *California Law Review* (2012): pp. 817-885.

International Telecommunication Union. *The ITU National Cyber security Strategy Guide*, Frederick Wamala. Geneva: ITU, 2011. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf (preuzeto 04.05.2016).

[11] Калаузовић, Горан. „Офанзивне кибер активности", *Нови гласник*, број 1-4, јануар–децембар 2011.

[12] Kelsey, Jeffrey T. G. „Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare". *Michigan Law Review* Vol. 106, (2008), pp. 1427-1452.

[13] Кривични законик. Београд: „Сл. гласник РС", бр. 85/2005, 88/2005 - испр., 107/2005 испр., 72/2009, 111/2009, 121/2012, 104/2013 и 108/2014.

[14] Kugler, Richard L. „Deterrence of Cyber Attacks". In *Cyberpower and National Security*, Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Eds.). Washington, D.C.: National Defense University Press, 2009.

[15] Kuhn, Markus G. and Anderson, Ross J. „Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations?". In David Aucsmith (Ed.), *Information Hiding*, pp. 124–142. Berlin, Heidelberg: Springer, 1998.

[16] Маркагић, Милорад. „КЕМЗ и информациона безбедност". У *Злоупотреба информационих технологија и заштита*, уредник Слободан Петровић, стр. 185-192. Београд: Удружење судских вештака за информационе технологије, 2010.

[17] Младеновић, Драган, Дракулић, Мирјана и Јовановић, Данко. „Међународно право и сајбер ратовање". *Војно дело*, пролеће 2012, (2012): стр. 9-39.

[18] McDowell, Mindi. „Cyber Security Tip ST04-015: Understanding Denial-of-Service Attacks". U.S. computer emergency readiness team. http://www.us-cert.gov/cas/tips/ST04-015.html (preuzeto 4.11.2010).

[19] Милошевић, Младен и Путник, Ненад. „Проблем правне (не)регулисаности конфликата у кибер простору". *Трећи програм*, свеска бр. 162 (2/2014).

[20] Путник, Ненад. *Сајбер простор и безбедносни изазови.* Београд: Универзитет у Београду, Факултет безбедности, 2009.

[21] Рељановић, Марио. „Кривично правна заштита електронских тајних података". У *Приступ информацијама од јавног значаја и заштита тајних података*. Београд: ОЕБС, 2013.

[22] Schaap, Arie J. „Cyber warfare operations: Development and use under international Law", *The Air Force Law Review – Cyberlaw Edition*, Vol. 64, (2009): pp. 121-174.

[23] United States Government Accountability Office. *Information Security: Cyber Threats and Vulnerabilities*. Washington DC: US GAO, 2009.

[24] Van Eck, Wim. „Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? ". *Computers & Security*, 4 (1985): pp. 269-286.

[25] William, Robert D. „(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action". *The George Washington Law Review*, Vol. 79 (2011): pp. 1163-1200.

[26] Wulf, William A. and Jones, Anita K. „Reflections on Cybersecurity", *Science*Vol. 326, Issue 5955 (2009): pp. 943-944.

[27] *Закон о информационој безбедности Републике Србије*.Београд: „Службени гласник РС" број 6/16 од 28.01.2016.

[28] Закон о потврђивању Конвенције о високотехнолошком криминалу. Београд: „Сл. гласник РС", бр. 19 од 19. марта 2009.