DCAF Geneva Centre for Security Sector Governance

# UVOD U UPRAVLJANJE SAJBER BEZBEDNOŠĆU – PRIRUČNIK ZA NARODNE POSLANIKE

# UVOD U UPRAVLJANJE SAJBER BEZBEDNOŠĆU – PRIRUČNIK ZA NARODNE POSLANIKE


## Autori

### Franziska Klopfer

Franziska je projektni koordinator Odeljenja za Evropu i Centralnu Aziju DCAF-a.

### Irina Rizmal

Irina je projektni službenikOdeljenja za Evropu i Centralnu Aziju DCAF-a.

### Milan Sekuloski

Milan je viši savetnik Odeljenja za Evropu i Centralnu Aziju DCAF-a.

### Teresa Hatzl

Teresa je bivši projektni službenik u Odeljenju za javno-privatno partnerstvo DCAF-a.

### Doktor Dragan Mladenović

Dragan je ekspert u polju sajber bezbednosti i sajber odbrane.

# Sadržina

## Uvod

Sajber bezbednost je jedno od najnovijih područja državnih bezbednosnih politika koje postaje sve važnije u sektorima bezbednosti država u Evropi. Kreatori politika još uvek kaskaju za tehnološkim novinama koje koristi mnoštvo prijateljskih i neprijateljskih aktera. Ovo zahteva brz i sveobuhvatan razvoj novih pravnih i političkih okvira. Pored osiguranja državne bezbednosti, bezbedne i sigurne mreže su važne u podsticanju privrede u državi i modernizaciji upravljanja u javnom sektoru u državama JIE (razmislite, na primer, koliko je ključna uloga bezbednih mreža za dobro funkcionisanje usluga e-uprave koje se uvode). Bezbedan sajber prostor je takođe neophodan za garantovanje mogućnosti građanima da uživaju svoja prava, kao što su pristup informacijama i sloboda izražavanja. Prema tome, od suštinske je važnosti imati razvijenu svest o mogućnostima, rizicima i pretnjama koje nosi sajber prostor.

Narodni poslanici imaju ključnu ulogu u razvijanju zakonodavnih i institucionalnih okvira sajber bezbednosti, kao i u garantovanju da se principi dorbrog upravljanja primenjuju u sajber bezbednosti. Pored odgovornosti za usvajanje novog zakonodavstva, oni takođe imaju moć da sazovu različite zainteresovane strane za diskusije o politikama, čime se obezbeđuju sveobuhvatni modeli upravljanja uključujući više zainteresovanih strana – nešto što je od posebnog značaja u sajber bezbednosti. Na kraju, narodni poslanici imaju nadzornu ulogu, nadzirući sprovođenje zakona i politika o (ili vezanih za) sajber bezbednost.

Imajući ove odgovornosti na umu, od ogromne je važnosti da narodni poslanici budu upućeni u najnovija dešavanja u oblasti sajber bezbednosti i da poseduju odgovarajuće znanje i razumevanje kako bi mogli da rade na pitanjima politika i pristupaju ovom pitanju na osnovu relevantnih informacija koje su na raspolaganju. Ova publikacija ima za cilj da obezbedi onim poslanicima koji su uključeni u izradu zakonodavstva i nadzor pitanja sajber bezbednosti osnovni pregled glavnih pitanja, trendova i izazova u upravljanju ovom oblašću.

Ovaj uvod, Priručnik za narodne poslanike, objašnjava glavne elemente sajber bezbednosti i njenog upravljanja: sajber kriminal, sajber ratovanje, sajber terorizam, sajber špijunažu i haktivizam, kao i izazove i mogućnosti u njihovom upravljanju. Ssvaki deo prati i spisak mogućih pitanja koja poslanici mogu da postave u vezi sa ovom temom. Pitanja imaju za cilj povećanje odgovornosti vlade i drugih ključnih aktera u oblasti sajber bezbednosti. Pitanja mogu biti upućena vladi, mogu biti razmatrana na javnim slušanjima i raspravama ili se mogu koristiti za parlamentarne istrage.

# DEO I – KLJUČNI KONCEPTI

## Potrebe, politike i strateški ciljevi sajber bezbednosti

Pojavom Interneta i sve većim prelaskom na život na njemu, postalo je neophodno ponovo proceniti bezbednosne rizike i odgovore na njih. Sadašnje informatičko doba stavilo je informacije i sajber bezbednost u prvi plan, kao važan aspekt individualne, organizacijske, državne

i međunarodne bezbednosti. Prema standardu ISO/IEC, sajber bezbednost znači "očuvanje poverljivosti, integriteta i dostupnosti informacija"[1] između ostalih njihovih karakteristika.[2]

U okviru koncepta dobrog upravljanja sektorom bezbednosti, bezbednosna politika ima za cilj ne samo da osigura bezbednost države, već i bezbednost pojedinca. Primena ovog principa na svet interneta znači da sajber bezbednost treba da teži ka stvaranju bezbednog Internet prostora za sve. Da bi se ovo ostvarilo, politika sajber bezbednosti mora dotaći veliki broj pitanja, od zaštite integriteta države i obezbeđivanja ljudskih prava, do sprovođenja zakona i sprečavanja kriminala koji se vrši u ili putem sajber prostora. Prema tome, pitanje upravljanja sajber bezbednošću se ne treba odnositi samo na održanje bezbednosti i otpornosti interneta, već i na građenje sigurnosti i podsticanje mogućnosti na internetu.

Prvi korak u pripremi uspešne politike i strategije o sajber bezbednosti je definisanje bezbednosnih ciljeva i utvrđivanje šta znači bezbednost i građenje bezbednosti na internetu za državu i njene građane. Moraju se definisati ključni resursi koji su od suštinskog značaja za zaštitu normalnog funkcionisanja države i zaštitu opšteg integriteta života na internetu. Mreže za napajanje električnom energijom i ključne internet usluge su očigledni primeri ključnih resursa koji zahtevaju veliku pažnju i zaštitu. Istovremeno, glavni faktori slabosti u sajber bezbednosti se javljaju zbog ljudskih grešaka i tehničkih defekata. Neupućeni internet korisnici koji kliknu na pogrešan link su najčešći razlog sajber incidenata. Prema tome, obrazovanje i podizanje svesti korisnika je od jednake važnosti za prevenciju u sajber bezbednosti kao i dobra tehnologija i adekvatni stručnjaci za korišćenje te tehnologije.

## Izazovi u upravljanju sajber bezbednošću

Kada se jednom definišu ciljevi sajber bezbednosti, mora se postaviti i okvir upravljanja koji određuje uloge i odgovornosti različitih strana u postizanju tih ciljeva. Suštinski izazov u upravljanju sajber bezbednošću je činjenica da uloge i odgovornosti različitih strana još uvek nisu jasno definisane međunarodnim zakonima ili standardima. Takođe, mnogi državni pravni i politički okviri još uvek ne odražavaju uticaj različitih strana. Na primer, ko kontroliše i ko je odgovoran za bezbednu infrastrukturu ili bezbedne sadržaje na internetu? Kakve dužnosti ili prava proizilaze iz ove odgovornosti?

Mnoge ključne usluge u sajber bezbednosti su u vlasništvu i njima upravljaju privatni akteri, dok država zavisi od njihove aktivne saradnje, na primer u obezbeđivanju svojih vlastitih mreža i usluga. Saradnja između različitih zainteresovanih strana i njihova uključenost je, prema tome, suštinska u efektivnoj i efikasnoj sajber bezbednosti i garantovanju da je izrada politika o sajber bezbednosti participativna i odgovorna. Na primer, sve češće javni i privatni akteri razmenjuju informacije u cilju bolje prevencije i otkrivanja sajber incidenata. Istovremeno, mnoge privatne firme često poseduju napredniju tehnologiju i znanje od javnog sektora koje mogu podeliti zarad povećanja sveukupne sajber bezbednosti u državi, čime će na kraju i njihovo poslovanje biti bezbednije. Konačno, sve

1 Međunarodna organizacija za standardizaciju. (2016). ISO/IEC 27000:2016(en) Informacione tehnologije — Tehnike bezbednosti — Sistemi menadžmenta bezbednošću informacija — Pregled i rečnik.

2 Neke od definicija sajber bezbednosti uključuju i druge karakteristike informacija, kao što su autentičnost, odgovornost, nepobijanje i pouzdanost, pored triju gore navedenih.

zainteresovane strane u sajber bezbednosti – vlada, zakonodavac, privatni sektor, građansko društvo, tehnička zajednica i akademski svet – imaju svoju ulogu u procesu izrade politika o sajber bezbednosti, bez razlike da li je to doprinos u planiranju politika, saradnji u sprovođenju politika ili nadziranju celog procesa politika.

Međutim, konkretan obim odgovornosti i uloga koje ove zainteresovane strane treba da odigraju se moraju definisati u kontekstu svake politike. Sve u svemu, kredibilitet i primena celog procesa zavisi od njegove sveobuhvatnosti i transparetnosti.

## Novo poimanje pružanja bezbednosti, kontrole i nadzora

Sajber bezbednost mora biti odgovorna. Mehanizmi za kontrolu i nadzor su često nejasni zbog složenog spoja uključenih državnih i nedržavnih aktera. Zbog toga se moraju razviti novi mehanizmi ne samo za saradnju, već i za kontrolu i nadzor.

Narodni poslanici treba da imaju važnu ulogu u nadzoru nad upravljanjem sajber bezbednošću. Kako se sajber bezbednost ne odnosi samo na bezbednosne politike već i na druge oblasti politika, nadzor nad sajber bezbednošću treba da spoji članove odbora za bezbednost i obdranu, između ostalih, sa odborima zaduženim za telekomunikacije, obrazovanje, informatičko društvo i ljudska prava.

## Primeri pitanja za sprovođenje nadzora:

- Da li država ima strategiju o sajber bezbednosti sa jasno definisanom vizijom? Koje je ministarstvo ili državni organ je odgovoran za njeno sprovođenje? Da li je strategija pripremljena u postupku koji uključuje sve relevantne zainteresovane strane (državne i nedržavne)?
- Da li postoji spisak utvrđene kritične informacione infrastrukture i, ukoliko postoji, da li je spisak sveobuhvatan? Koji je državni organ odgovoran za ažuriranje tog spiska? Ko je odgovoran za kontrolu zaštite kritične informacione infrastrukture?
- Koji su različiti iakterii sajber bezbednosti? Koje su njihove uloge? Šta bi trebalo da budu njihove odgovornosti?
- Da li postoje kontrolni i nadzorni mehanizmi za ključne državne i nedržavne aktere sajber bezbednosti? Da li funkcioniše kontrola ključnih državnih i nedržavnih aktera sajber bezbednosti? Da li oni podležu odgovornosti, kako bismo bili sigurni da njihove aktivnosti nisu samo efektivne, već i u granicama zakona?

# DEO II – SAJBER KRIMINAL (VISOKOTEHNOLOŠKI KRIMINAL)

## Definicija

Sajber kriminal (visokotehnološki kriminal) se generalno shvata kao krivično delo gde su kompjuteri i mreže glavna meta, koriste se kao sredstva za izvršenje krivičnog dela ili su mesto gde se vrši krivično delo.

Iako ne postoji univerzalno prihvaćena definicija, može se napraviti razlika između dve glavne vrste sajber kriminala:

- Kriminal omogućen sajber sredstvima, koji se odnosi na "tradicionalne" oblike kriminaliteta koji se sada prenose u sajber prostor, kao što su privredna krivična dela, dela protiv bezbednosti dece i mladih odraslih osoba i čak i dela terorizma; i
- Napredni sajber kriminal (poznat i kao visokotehnološki kriminal), koji se odnosi na sofisticirane napade usmerene protiv kompjuterskog hardvera i softvera.[3]

Pre svega, važno je ne mešati sajber kriminal i sajber bezbednost. Ove dve sajber pretnje podrazumevanju različite motive, namere, upotrebljena sredstva, mete, obim, posledice, a razlikuju se i strane koje su uključene u prevenciji i smanjenju pretnji. U praksi, sajber kriminal varira od spam i phishing email-ova, mahinacija i prevara na mreži i lažnog predstavljanja, do zabranjenog, uvredljivog i nezakonitog sadržaja, krađe identiteta, kao i materijala sa seksualnom zloupotrebom dece na internetu. Generalno, glavni motiv za dela sajber kriminala, kao što je i slučaj sa "tradicionalnim" kriminalom, je finansijska dobit. Sajber kriminalci su, u suštini, hakeri sa malicioznim namerama.

## Kompjuteri i mreže kao glavne mete

Najčešće upotrebljavana sredstva su maliciozni softveri kao što su virusi, trojanci, adware i spyware za omogućavanje pristupa sistemima, praćenje aktivnosti i prikupljanje podataka; botnet (bot mreže) ili oteti lični računari koji vrše zadatke na daljinu bez znanja njihovih korisnika; i napadi za uskraćivanje usluge (Denial of Service (DoS)) koji imaju za cilj iscrpljivanje resursa koji su dostupni mreži, aplikaciji ili servisu i na taj način sprečavanje pristupa njenim korisnicima.

Posledice tih napada su višestrane. Fizička lica mogu pretrpeti finansijske gubitke, ali mogu biti i žrtve krađe ličnih i osetljivih informacija, kao i krađe identiteta. Firme koje su žrtve napada sajber kriminalaca se suočavaju sa potencijalnim finansijskim gubicima, ali i gubicima osetljivih poslovnih informacija, podataka ili patenta ili ličnih podataka njihovih klijenata i korisnika, što sve posredno izaziva ozbiljne posledice po reputaciju. Javne institucije i neprofitne organizacije mogu postati žrtve iznude ili krađe ličnih podataka korisnika kojima pružaju usluge.

3 Interpol definicija sajber kriminala.

## Kompjuteri i mreže kao alati za izvršenje krivičnog dela

Druga krivična dela koja se isto tako šire u sajber prostoru uključuju nezakonitu trgovinu drogom, oružjem i osetljivim podacima i informacijama, trgovinu ljudima, čak i plaćena ubistva, fizičke napade i druge oblike nasilja. Generalno, ovakvi dogovori se odvijaju na takozvanom **'darknetu'** gde korisnici mogu da deluju potpuno anonimno. Korišćenjem darkneta, pojedinci i kriminalne organizacije koriste šifrovane usluge za slanje poruka u komunikaciji i kripto valute za vršenje finansijskih transakcija, zbog čega su praćenje i identifikacija izuzetno teški. Black-hat hakeri (kriminalci sa tehničkim znanjem ili tehnički stručnjaci koje angažuju kriminalci, pogledajte poglavlje o haktivizmu) isto tako koriste potencijal darkneta zloupotrebljavajući slabe tačke softvera koje su otkrili, anonimno ih prodavajući svima koji traže načine da zloupotrebe konkretne sisteme.

## Kompjuteri i mreže kao mesto vršenja krivičnih dela

Kriminalne organizacije su do sada ekstremno efikasno prešle u digitalnu sferu. Rrazvile su čak i nove modele poslovanja koji nalikuju najnaprednijim legitimnim preduzećima. Kao što neke firme nude "bezbednost kao uslugu" i grade sajber bezbednosne kapacitete zainteresovanih kupaca, tako i kriminalne organizacije nude "kriminal kao uslugu" na tržištu sajber kriminala. Još jedan razlog za zabrinutost je moguća saradnja između različitih malicioznih strana. Na primer, sajber kriminalci mogu nuditi svoje usluge terorističkim grupama za vršenje krivičnih dela u sajber prostoru podržanih od strane država, isključivo za novčanu dobit. Drugim rečima, digitalna sfera nudi kriminalnim organizacijama nove kanale i mogućnosti za vršenje nezakonitih radnji koji inače možda ne bi bili dostupni.

## Trendovi i odgovori na sajber kriminal

Sveukupno, kriminal omogućen sajber sredstvima je u visokom porastu u razvijenim i zemljama u razvoju. Prema svojoj prirodi, sajber kriminal je međunarodan i prevazilazi državne granice. Počinitelji ne moraju biti u istoj državi kao žrtve ili policija koja ih goni. Ovo predstavlja jedan od ključnih izazova u borbi protiv sajber kriminala, jer razlike u pravnim sistemima i praksama različitih uključenih država mogu da utiču na efikasnost i mogućnost saradnje, kao i na razmenu operativnih saznanja i dokaza.

Dalje, vrlo malo policija u svetu ima kapacitete za nezavisnu borbu protiv sajber kriminala, iako mnoge imaju posebne jedinice za borbu protiv sajber ili "visokotehnološkog" kriminala. Kao i sa drugim vrstama malicioznih aktivnosti u sajber prostoru (pogledajte poglavlje o sajber špijunaži), postoji očigledna asimetrija povezanih troškova. Kao rezultat toga, tradicionalni pristup u policijskom radu na krivičnim delima je do određene mere izmenjen u sajber sferi. Umesto neposrednog hapšenja počinitelja, policijske jedinice za sajber kriminal se fokusiraju na suzbijanje tekućih krivičnih dela i prevazilaženje bezbednosnih slabosti koje su već bile zloupotrebljene. Zbog podjednako prisutnog izazova atribucije u celom sajber spektru i dugih i zahtevnih istražnih postupaka, uključujući forenziku podataka, postizanje pravosnažnih presuda isto tako traje duže nego u slučaju tradicionalnih krivičnih dela.

Borba protiv sajber kriminala na državnom nivou isto tako zahteva saradnju svih uključenih strana. Privatni sektor je najčešća meta sajber kriminalaca i treba da se uzmu u obzir njegova iskustva i interesi u planiranju strategija o sajber kriminalu. Eksperti za sajber kriminal iz privatnog sektora, kao i akademska zajednica i građansko društvo, mogu doprineti planiranju politika za borbu protiv sajber kriminala tehničkim kapacitetima i znanjem. Prema tome, za efikasnu borbu protiv sajber kriminala vlade moraju negovati javno-privatnu saradnju i podržavati uspostavljanje mreže poverenja. Podjednako su važni prevencija sajber kriminala i podrška pojedinim korisnicima. Opštim podizanjem svestu i građenjem kapaciteta korisnici treba da nauče kako da prepoznaju email poruke sa potencijalnim prevarama, malicioznom sadržinom i potencijalno lažnim kontaktima. Čak i relativno mali napori, kao što je obučavanje korisnika da održavaju osnovnu sajber higijenu i koriste jake lozinke ili da koriste ažurirani licencirani softver i enkripciju, mogu imati veliki uticaj u prevenciji sajber kriminala.

Na međunarodnom nivou je postignut napredak usvajanjem Konvencije o visokotehnološkom kriminalu Saveta Evrope[4], koja se naziva i Budimpeštanska konvencija. Budimpeštanska konvencija je jedini obavezujući međunarodni instrument o sajber kriminalu do danas i propisuje smernice državama za rad na razvijanju sveobuhvatnih nacionalnih zakonskih okvira za borbu protiv sajber kriminala i uspostavljanje okvira za međunarodnu saradnju između država potpisnica. Međutim, sa šezdeset i jednom potpisnicom i još deset za koje se očekuje da će se priključiti, Budimpeštanska konvencija još uvek nije univerzalni globalni dokument. Bez obzira na to, poslednjih se godinama mogu videti slučajevi međunarodne saradnje. Na primer, organizacije za međunarodnu policijsku saradnju, posebno Europol i Interpol, su se uključile u okvire za jačanje međunarodnih kapaciteta i olakšanje prekogranične saradnje između policijskih službi. Zbog prethodno navedene zahtevnosti održavanja nacionalnih jedinica za sajber kriminal, ovakvi okviri mogu nadoknaditi ograničene nacionalne kapacitete, uključujući i razvoj javno-privatnih partnerstava i mreža poverenja između stručnjaka iz različitih delova društva.

## Primeri pitanja za sprovođenje nadzora:

- Da li država ima zakonodavstvo o sajber kriminalu koje prepoznaje različite oblike sajber kriminala i utvrđuje jasno definisani sistem sankcija? U kojoj je meri ono usaglašeno sa međunarodnim konvencijama koje je država potpisala?
- Da li su pravosuđe i policija dobro opremljeni u pogledu tehničkog znanja, stručnosti i kapaciteta?
- Koji su delovi društva najizloženiji kompjuterskom kriminalu? Da li postoje neke inicijative prevencije koje ciljaju te sektore?
- Da li funkcioniše kontrola i nadzor ključnih državnih i nedržavnih strana? Da li bezbednosni organi podležu odgovornosti kako bi se garantovalo da njihove aktivnosti nisu samo efektivne, već i u granicama zakona/ne krše zagarantovano pravo na privatnost građana?

4 Konvencija o visokotehnološkom kriminalu. Savet Evrope. Ugovor br. 185.

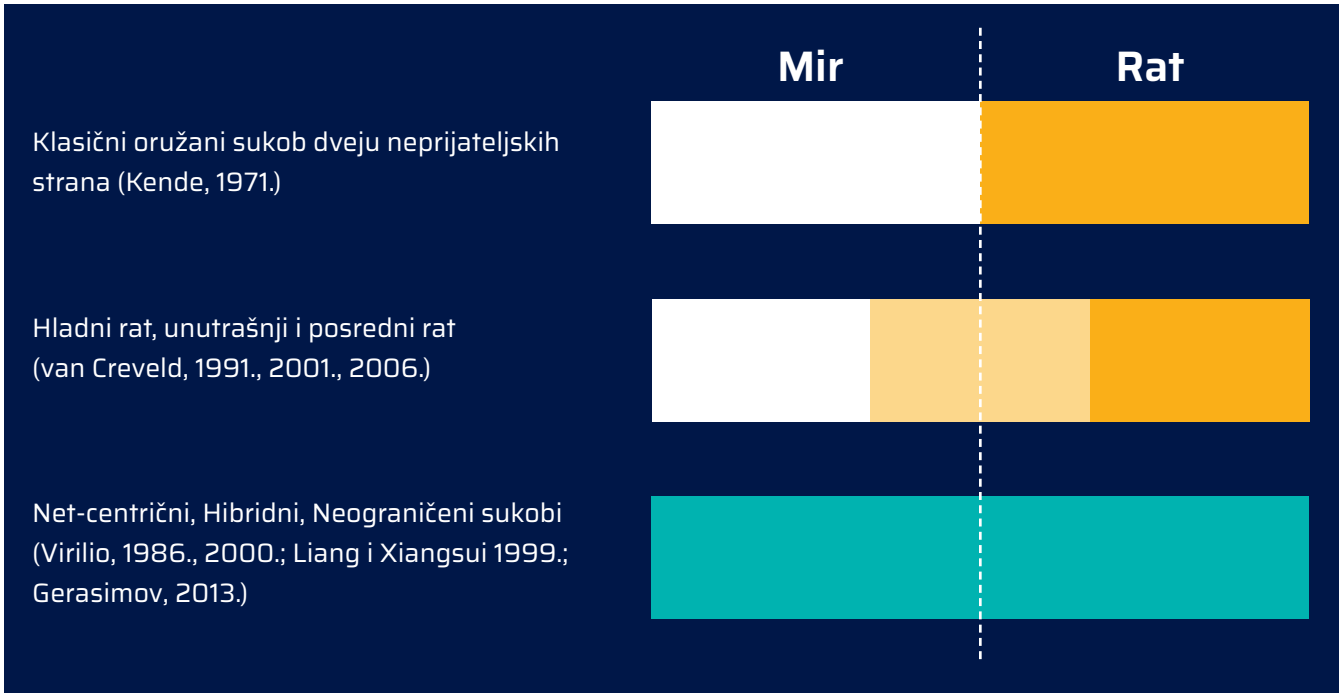
- Da li policija i pravosuđe koriste sve dostupne pravne mogućnosti za efektivnu međunarodnu saradnju? Da li se treba izmeniti zakonski okvir za postizanje bolje efikanosti? Istovremeno, kakvi zaštitni mehanizmi postoje za zaštitu ličnih podataka građana koji se razmenjuju sa trećim zemljama? Da li je komunikacija sa privatnim sektorom efikasna i transparentna (u svom obliku, ako ne i u sadržini koja treba biti poverljiva)?

# DEO III – SAJBER RATOVANJE

## Definicija

Sajber ratovanje se može definisati kao čin "ratovanja u sajber prostoru ili kroz sajber prostor". To je nova, specifična vrsta ratovanja[5] koja koristi informaciono-komunikacione tehnologije (IKT) za postizanje vojnih ciljeva i efekata u fizičkom, informacionom i sajber prostoru. Vojni efekti mogu biti jednaki efektima kinetičkog, nuklearnog, biološkog ili hemijskog naoružanja.

Međutim, ne postoji međunarodni ugovor o načinu definisanja sadržine, metoda, tehnika, sredstava i ciljeva sajber ratovanja. Isto tako, međunarodna zajednica se još uvek nije dogovorila o načinu razvijanja nacionalnih mera za građenje kapaciteta i međunarodnih mera za građenje poverenja, ili o tome kako primeniti postojeće međunarodno pravo na sajber ratovanje.




5 Ratovanje je proces vođenja međunarodnog oružanog sukoba. Rat je oružani sukob između najmanje dve neprijateljske oružane snage koje imaju najmanje minimalnu centralnu organizaciju i komandu, dok je najmanje jedna od strana predstavljena nekom vrstom vlasti (kao redovna vojska ili policija ili paravojna snaga), i on se vodi u kontinuitetu saglasno ujedinjenom planu i strategiji neprijateljskih snaga. Tradicionalno ratovanje se odvija na kopnu, moru, u vazduhu i svemiru.

## Problemi u regulisanju sajber sukoba

Nove tehnologije sa ofanzivnim kapacitetima se javljaju brže od kapaciteta pojedinih zemalja da razviju neophodnu odbranu od njih. Za njima kaska i sposobnost međunarodne zajednice da pronađe rešenja za regulisanje sajber sukoba.

Počinitelji sajber napada često rade prikriveno, a efekti njihovih sajber napada su često sa odloženim dejstvom. Može proći nekoliko godina od sajber eksploatacije i instalacije malicioznog oružja do otkrivanja njegovih efekata. Napadači mogu biti vladini organi i agencije, kao i privatna preduzeća, kriminalne organizacije, teroristi ili neformalne grupe i pojedinci.

Nasuprot konvencionalnom ratovanju, efekti sajber sukoba često ne dostižu prag "čina agresije"[6], "upotrebe sile"[7], "oružane snage"[8] ili "oružanog napada"[9] prema definiciji Povelje UN, zbog čega je teško primeniti ius ad bellum i ius in bello pravila Međunarodnog zakona o oružanim sukobima.

Takođe, većina država nema dovoljno kapaciteta za:

- precizno otkrivanje sajber napada;
- identifikaciju i atribuciju napadača; i
- blagovremenu, preciznu i pravnu reakciju na sajber napade.

## Međunarodne aktivnosti za regulisanje sajber ratovanja

Nedostatak pravne regulative stvara prostor za potencijalnu zloupotrebu sajber napada, što potencijalno čak vodi do pojave međunarodnih i regionalnih kriza, posebno u regionima opterećenim hroničnim političkim tenzijama.

Međunarodna zajednica još uvek pokušava da postigne ugovor o načinima regulisanja sajber ratovanja. Postoje različiti predlozi, od kojih je jedan Talinski priručnik (Tallinn Manual)[10], pripremljen od strane grupe akademika u NATO Centru izvrsnosti za zajedničku sajber odbranu (Cooperative Cyber Defence Centre of Excellence) u Talinu, Estoniji.

## Međunaordni pravni odgovori na sajber rat

Mogući praktični odgovor na sajber pretnje može biti usvajanje i primena mera za građenje kapaciteta i poverenja na državnom, regionalnom i međunarodnom nivou.

S tim ciljem Ujedinjene nacije su okupile Grupu vladinih eksperata za razvoj u oblasti informacija i telekomunikacija u kontekstu međunarodne bezbednosti (UN GGE). Grupa se sastala pet puta u razdoblju između 2004. i 2017. godine da razmatra postojeće i potencijalne

6 Povelja Ujedinjenih nacija. 24. oktobar 1945. Ujedinjene nacije. 1 UNTS XVI, Čl. 39.
7 Isto., 1 UNTS XVI, Čl. 2, stav 4.
8 Isto., 1 UNTS XVI, Preambula.
9 Isto., 1 UNTS XVI, Čl. 51.
10 Schmitt, Michael N. (ed.) 2017. Tallinn priručnik 2.0 o međunarodnom pravu primenjivom na sajber operacije. Cambridge University Press.

pretnje; norme, pravila i principe odgovornog ponašanja država; i mere za građenje poverenja i kapaciteta. U Izveštaju 2013. godine, GGE je zaključila da je "Međunarodno pravo, a naročito Povelja Ujedinjenih nacija, primenjiva i suštinski važna u očuvanju mira i stabilnosti i promovisanju otvorenog, bezbednog, mirnog i dostupnog IKT okruženja".11

Organizacija za evropsku bezbednost i saradnju (OEBS) je uložila dodatne napore usvajanjem Mera za izgradnju poverenja za smanjenje rizika od sukoba izazvanih upotrebom IKT (CBM).12 CBM su usredsređene na razmenu informacija i dijalog; zaštitu kritične infrastrukture i nacionalnu bezbednost; i promovisanje i poboljšanje javno-privatne saradnje.

Međutim, obe su inicijative dobrovoljne (nisu obavezne za zemlje članice OEBS i UN) i njihovo postojanje nije direkna, čvrsta garancija postizanja mira i bezbednosti u sajber prostoru na međunarodnom nivou.

Bilateralni i multilateralni ugovori između različitih država mogu biti drugo moguće rešenje. Ovi ugovori mogu definisati norme, standarde i principe mirnog ponašanja; utvrditi pravila i procedure u slučaju ozbljinih sajber incidenata; olakšati saradnju i kreiranje zajedničkih kapaciteta za otkrivanje sajber napada, identifikaciju napadača i atribuciju.

## Primeri pitanja za sprovođenje nadzora:

- Da li su definisani strateški ciljevi sajber odbrane?
- Da li postoji procena svesnosti o situaciji? Da li se uzimaju u obzir svi elementi u državi koje treba zaštiti?
- Koje su glavne slabosti i rizici? Da li se redovno identifikuju, revidiraju i rešavaju?
- Koliko su razvijeni postojeći nacionalni kapaciteti za sajber odbranu?
- Ko su različiti akteri, na nacionalnom i međunarodnom nivou, koji doprinose sajber odbrani?
- Kakvi okviri postoje za saradnju odgovornih strana? Kako su oni organizovani i koliko su odgovorni, transparentni i efektivni?
- Da li se dovoljno često i u dovoljnom obimu organizuju obuke za odgovorno osoblje?
- Da li država učestvuje u regionalnim i međunarodnim obukama i vežbama? Koliko se često one održavaju?

11 Izveštaj grupe vladinih eksperata o novinama u polju informacija i telekomunikacija u kontekstu međunarodne bezbednosti. 24. jun 2013. Generalna skupština UN. Rezolucija A/68/98.

12 Odluka br. 1106. Inicijalni set OEBS mera za građenje poverenja za smanjenje rizika od sukoba koji proizilaze iz uporebe informacionih i komunikacijskih tehnologija 3.12.2013. Organizacija za evropsku bezbenost i saradnju. PC. DEC/1106. Odluka br. 1202. OEBS mere za građenje poverenja za smanjenje rizika od sukoba koji proizilaze iz upotrebe informacionih i komunikacijskih tehnologija. 10.3.2016. Organizacija za evropsku bezbenost i saradnju. PC.DEC/1202.

# DEO IV – SAJBER ŠPIJUNAŽA

## Definicija

Sajber špijunaža se definiše kao radnja preduzeta u tajnosti ili pod lažnom pretpostavkom koristeći sajber kapacitete za prikupljanje (ili pokušaj prikupljanja) informacija sa namerom njihovog prenošenja suprotnoj strani.[13] Pristup se dobija time što se osoba predstavlja legitimnim korisnikom ili korišćenjem sofisticiranih, ciljanih napada (kao što je društveni inženjering) kojim se manipulišu legitimni korisnici na način koji otvara vrata osobama koje žele da dobiju nezakoniti pristup.

## Specifični izazovi u sajber špijunaži

Jedna od osnovnih karakteristika sajber špijunaže je izuzetna asimetrija troškova koji proizilaze iz nje. Trošak za zaštitu i odbranu od svih slabosti je nesrazmerno visok u poređenju sa troškom napadača, koji treba da otkrije i iskoristi jednu jedinu slabu tačku. Dalje, uzimajući u obzir potrebno vreme za otkrivanje upada, sajber špijunaža je efektivno ofanzivno oruđe za dobijanje informacija o sistemima, procesima i pojedincima. Procene potrebnog vremena za otkrivanje upada variraju od jednog do tri meseca[14], tokom kojih napadač može da dobije pristup širokom dijapazonu osetljivih informacija. Zbog obima prisutnosti interneta i mrežnih usluga u društvima u celom svetu, sajber špijunaža otvara mnogo veće mogućnosti da se dođe do osetljivih informacija o protivniku.

## Prihvatljivo ponašanje, sajber kriminal ili čin agresije?

Sve je šire mišljenje da sajber špijunaža generalno postaje neodrživa. Međutim, odluka o tome šta predstavlja prihvatljivo ponašanje, a šta treba sankcionisati još uvek predstavlja veliki izazov. Činjenica da se tradicionalna špijunaža od strane država smatrala prihvatljivim ponašanjem u prošlosti današnju sajber špijunažu ostavlja neregulisanom. Stoga se u praksi običan upad u sistem i narušavanje njegove poverljivosti još uvek smatra prihvatljivim. Međutim, narušavanje integriteta ili dostupnosti sistema, koje može nastati kao rezultat tog upada, se smatra oblikom sajber napada i smatra se neprihvatljivim. Prema tome, sajber špijunaža se normativno smatra i prihvatljivom i neprihvatljivom, u zavisnosti od posledica.

Dodatni problem predstavlja izazov pravljenja razlike između aktivnosti usmerenih na prikupljanje informacija i onih sa malicioznom namerom koje mogu predstavljati čin agresije. To takođe zavisi i od toga za šta će se upotrebiti dobijene informacije. Prema tome, postoji tanka linija između radnji čiji je glavni cilj sajber špijunaža i radnji koje se smatraju neposrednim sajber napadima. Zbog toga je izuzetno teško utvrditi međunarodne principe i režime koji upravljaju idejom o sajber špijunaži koja, za sada, ostaje relativno neregulisana.

---

13 Prema gore navedenom Priručniku iz Talina.

14 Izveštaj Mandiant (2013) procenjuje da je prosečno vreme potrebno da se pristupi mreži žrtve 356 dana. Global Space (2013) procenjuje da prosečni upad ostaje neotkriven u proseku 90 dana. Foreign Policy (2015) procenjuje da u proseku treba 205 dana žrtvi da otkrije da je bila izložena napadu. Ponemon Institut (2015) je otkrio da upadi u proseku ostaju neotkriveni 46 dana. Kreps, Fletcher i Griffiths (2016) procenjuju da upad ostaje neotkriven u proseku 3 meseca.

Sa bezbednosnog aspekta, smatra se da se sajber špijunaža potencijalno preklapa sa idejama o sajber kriminalu. U tom smislu, sajber kriminalci mogu biti unajmljeni od trećih strana sa zadatkom da prodru u vladine i/ili korporativne sisteme i izvuku osetljive informacije.

## Posrednici, privatne armije i hibridni sukobi

Dalji izazov je problem kampanja sajber špijunaže pod pokroviteljstvom države, gde države posredno sponzorišu strane koje imaju kapacitete da prodru u sisteme njihovih protivnika. U tom smislu, hakeri su postali potencijalne privatne armije špijuna digitalnog doba i stoje na raspolaganju najbogatijem kupcu. Porast sajber špijunaže je isto tako dodao još jedan element hibridnim konfliktima i asimetričnom ratovanju, u kojem sukobi više nisu crno-beli, već se javljaju u različitim oblicima i sa različitim intenzitetom. Uključivanjem u sajber špijunažu, države su sada sposobne da razviju hibridne odnose sa svojim protivnicima. Efektivno to znači da se odnosi u fizičkom svetu nastavljaju normalnim putem, dok se neprijateljske aktivnosti i sukobi odvijaju u digitalnoj sferi, korišćenjem sajber špijunaže zajedno sa hakovanjem i haktivizmom, sajber kriminalnom i ofanzivnim sajber aktivnostima.

Kao i kod drugih oblika odbrane i zaštite od malicioznih aktivnosti u sajber prostoru, kod sajber špijunaže se javljaju poteškoće u otkrivanju i atribuciji. Pored toga, sajber špijunažu ne vrše uvek države ili strane pod pokroviteljstvom država. Ona se može upotrebiti kao alat od strana sajber kriminalaca, haktivista i privatnih osoba za jednostavno sticanje ekonomske dobiti.

## Odgovor na, regulisanje i mere protiv sajber špijunaže

Prema tome, najbolja odbrambena strategija protiv sajber špijunaže – barem za sada – je odvraćanje. To podrazumeva povećanje realnih ili procenjenih troškova potencijalnog napada protivnika. Pored uspostavljanja snažnijih odbrana, ovo takođe podrazumeva i promovisanje bilateralne i multilateralne saradnje za postizanje ugovora i/ili kodeksa ponašanja kojima se reguliše pitanje sajber špijunaže, između ostalih vrsta ponašanja u sajber prostoru. Naizgled uspešan primer ovoga je ugovor između SAD-a i Kine iz 2015. godine o ekonomskoj špijunaži, koji utvrđuje da nijedna država neće vršiti ili svesno podržavati sajber omogućene krađe intelektualne svojine sa namerom obezbeđivanja konkurentskih prednosti firmama ili privrednim sektorima.

Međutim, sajber špijunaža za dobijanje obaveštajnih informacije za ciljeve nacionalne bezbednosti ostaje neregulisana, isto kao i tradicionalni oblici špijunaže. Zbog toga se u inicijativama koje predvode države sve više razgovara o pravu na "osvetu" ili povratno hakovanje u slučaju otkrivenog upada u sistem, kao o ubedljivijem obliku odvraćanja. Jedna od poslednjih država koja se priključila ovoj debati je Nemačka, gde državna obaveštajna zajednica traži pravo da koristi aktivnu odbranu. Ovo bi podrazumevalo ovlašćenja za uništavanje podataka koji su ukradeni ili preneseni sa nemačkih servera, kao i za kompromitaciju stranih servera kako bi se ojačali nacionalni kapaciteti za nadzor. Ideja iza ovih inicijativa je odvraćanje potencijalnih napadača pretnjom osvete.

## Primeri pitanja za sprovođenje nadzora:

- Šta se radi kako bi se građani i njihovi podaci zaštitili od sajber špijunaže? Koja su ministarstva ili državni organi odgovorni za borbu protiv sajber špijunaže?
- Da li postoji procena slabosti i potreba države u pogledu sajber špijunaže i koje su protivmere preduzete?
- Kako se može bolje definisati i regulisati sajber špijunaža u nacionalnom zakonodavstvu i na međunarodnom nivou?

# DEO IV – SAJBER TERORIZAM

## Definicija

Sajber terorizam spaja dva najistaknutija razvoja u svetu: sve veću internet zavisnost društva i pretnju međunarodnog terorizma.[15] Anonimna, lako dostupna i često neregulisana priroda interneta ga čini izuzetno sklonim iskorišćavanju i zloupotrebama od strane terorističkih organizacija i drugih nedržavnih aktera. Međutim, dok korišćenje interneta za terorističke ciljeve predstavlja izazov za međunarodnu zajednicu, istovremeno predstavlja i novo sredstvo za borbu protiv terorizma.

## Sajber terorizam nasuprot upotrebi interneta za terorističke ciljeve

Iako ne postoji univerzalno prihvaćena definicija sajber terorizma, većina definicija država govori o napadu koji koristi elektronska sredstva za upad u i/ili ozbiljno ometanje nacionalne kritične infrastrukture.[16] Na primer, Organizacija za evropsku bezbednost i saradnju (OEBS) definiše sajber terorizam kao "sajber povezani terorizam i konkretnije, [...], kao terorističke napade na sajber infrastrukturu, a posebno na kontrolne sisteme nenuklearne kritične energetske infrastrukture".[17]

Scenariji sa pretnjama sajber terorizmom uključuju paralizovanje velikih urbanih područja, zdravstvenog sistema ili ometanje finansijskog sektora "promenom nekoliko jedinica i nula".[18] Porast Interneta stvari[19] predstavlja još jednu važnu opasnost koju lako mogu iskoristiti terorističke organizacije za izvršenje dela sajber terorizma. Dela sajber terorizma koja mogu imati realni fizički

---

15 Lentz, Christopher E. Lentz. 2010. Dužnost države da spreči i reaguje na činove sajber terorizma. Čikago žurnal međunarodnog prava (Chicago Journal of International Law) 10. br. 2.

16 Nacionalna vitalna infrastruktura je resurs ili sistem od vitalnog značaja za održanje društvenih funkcija koji, ako nije povezan na mrežu duže vreme, dovodi do ozbiljnog rizika po javno zdravlje, privredu, životnu sredinu i nacionalnu bezbednost.

17 Priručnik o dobrim praksama za zaštitu nenuklearne kritične energetske infrastrukture (NNCEIP) od terorističkih napada fokusirajući se na pretnje koje proizilaze iz sajber prostora. 2013. Organizacija za evropsku bezbednost i saradnju. Br.16.

18 Gen. Votel, Joseph L. Jul 2015.Shvatanje terorizma danas i sutra. CTC Sentinel 8. Izdanje 7, str. 2–6.

19 Cambridge rečnik definiše "Internet stvari" (Internet of Things) kao predmete koji sadrže računarske uređaje koji imaju sposobnost da se međusobno povežu i razmene podatke korišćenjem interneta. Internet stvari je snažno utkan u nacionalnu vitalnu infrastrukturu.

efekat uništenja se smatraju manje verovatnim i, zbog toga, manjim izazovom za države zbog ogromne količine resursa potrebnih za izvršenje takvog dela.[20]

Dalje, mnoge terorističke organizacije koriste internet za izvršenje tradicionalnih krivičnih dela kao što su prevare, nezakoniti pristup i neovlašćeni upad u kompjuterske sisteme. Ovo dovodi do preklapanja između sajber kriminala (pogledajte poglavlje o sajber kriminalu), sajber napada (pogledajte poglavlje o sajber ratovanju) i sajber terorizma, zbog čega je na kraju teško napraviti razliku između njih. Rezolucija Saveta bezbednosti Ujedinjenih nacija 1566 nudi određena uputstva o ovom pitanju, jer potencira politički motivisani elemenat, identifikujući "terorističke činove" kao:

> "[...] krivična dela, uključujući dela protiv civila, počinjena sa namerom izazivanja smrti ili teških telesnih povreda, ili uzimanje talaca, sa ciljem izazivanja stanja terora [...], zastrašivanja stanovništva ili prinuđivanja vlade ili međunarodne organizacije da izvrši ili da se suzdrži od izvršenja neke radnje, što predstavlja krivično delo u okviru i prema definicijama međunarodnih konvencija i protokola o terorizmu [...]."21

Pored toga, terorističke organizacije koriste internet na svakodnevnoj osnovi za različite aktivnosti, kao što su propaganda (uključujući radikalizaciju, navođenje na terorizam, vrbovanje), finansiranje, obuka i planiranje (uključujući putem tajnih komunikacija i informacija iz otvorenih izvora), kao i za vršenje sajber napada.[22] Dok je korišćenje interneta za propagandne ciljeve postalo vrlo važna tema u međunarodnoj zajednici, praćena pozivima na stvaranje snažnih partnerstava, uključujući i ona sa IT industrijom,[23] problem korišćenja interneta za ciljeve finansiranja je dosta često zanemarivan. U međuvremenu, opšti prelaz na korišćenje tehnologije u međunarodnom trgovanju je pretvorio internet u sredstvo terorističkih organizacija za pranje novca, prikupljanje i transfer sredstava.[24]

Shodno tome, organi za sprovođenje zakona i obaveštajni rad sve više prate sumnjive finansijske transakcije na mreži i razvijaju alate i veštine za proaktivno sprečavanje, otkrivanje i reagovanje na terorističke aktivnosti koje uključuju internet. Vlade su počele da odgovaraju i na upotrebu interneta za propagandne ciljeve strateškim komunikacijama kao što su alternativne priče, kontraporuke i regulisanje sadržaja.[25] Međutim, svaka antiteroristička aktivnost na internetu pretpostavlja zajedničke aktivnosti država, privatnog sektora i građanskog društva kako bi se efektivno odgovorilo na ove nove izazove.

---

20 Weimann, Gabriel. Mart 2004. https://www.usip.org/publications/2004/03/wwwterrornet-how-modern-terrorism-uses-internetwww.terror.net:%20How%20Modern%20Terrorism%20Uses%20the%20Internet. Specijalni izveštaj br.116. Institut za mir Sjedinjenih Država.

21 Rezolucija Saveta bezbednosti 1566 (2004) o Pretnjama po međunarodni mir i bezbednost izazvanim terorističkim činovima. 8. oktobar 2004. Savet bezbednosti Ujedinjenih nacija. Rezolucija S/RES/1566.Op. stav 3.

22 Pogledajte:Upotreba interneta za terorističke ciljeve. 2012. Kancelarija UN za pitanja droge i kriminala.

23 Pogledajte:SC Counter-Terrorism Committee; Tech Against Terrorism; Global Internet Forum to Counter Terrorism.

24 Jacobson, Michael. Jun 2009. Finansiranje terorizma na internetu. CTC Sentinel 2. Izdanje 6, str. 17–20.

25 Pogledajte:Cirih-London preporuke o sprečavanju i borbi protiv nasilnog ekstremizma i terorizma na internetu. 2017. Globalni forum za borbu protiv terorizma.

## Pitanja vladavine prava

Generalno, antiterorističke aktivnosti na internetu mogu uticati na različita ljudska prava (uključujući privatnost i slobodu izražavanja, udruživanje, mirno okupljanje i religiju ili veru). U pogledu korišćenja interneta za propagandne ciljeve, vlade su usvojile nove mere, počevši odbijanjem pokušaja za opravdavanje ili veličanje (apologiju) terorističkih činova do zakonske zabrane navođenja na njihovo vršenje.[26] Međutim, treba istaći da govor koji je moralno odvratan, šokantan, uznemirujući ili uvredljiv ne mora sam po sebi dostići nivo kriminala; ali "takvi su zahtevi pluralizma, tolerancije i slobodoumlja bez kojih ne postoji 'demokratsko društvo".[27] Međutim, izazov je utvrditi tačku prelamanja gde polemika ili kritika postaje govor mržnje ili veličanje (apologija), kao i navođenje na vršenje terorističkih činova. Nije uvek jednostavno utvrditi ove tačke prelamanja.

U suštini, važno je da vlade jasno definišu relevantna krivična dela u krivičnim zakonicima svojih država, kako bi omogućili građanima da predvide posledice vezane uz određene radnje i izbegnu preoštre zakone koji dovode do "efekta smrzavanja" ljudskih prava. Garancije odgovarajućeg procesa, kao što su pretpostavka nevinosti i pravo na pravedno suđenje, su suštinski važne u osiguranju učinkovitosti protivterorističkih mera i poštovanja vladavine prava. Dalje, efektivni nadzor nad akterima u javnoj bezbednosti uključenim u borbu protiv terorizma (na mreži i van nje) je od suštinskog značaja u promovisanju reformskih procesa u borbi protiv terorizma koji su usklađeni sa ljudskim pravima.

## Primeri pitanja za sprovođenje nadzora:

- Da li postoji jasan pravni okvir koji utvrđuje zabranjene radnje na internetu?
- Da li je Ustavom zagarantovano pravo slobode izražavanja i neizloženosti proizvoljnom ili nezakonitom mešanju u sopstvenu privatnost?
- Da li postoji skupštinski odbor koji ima zakonsko ovlašćenje da nadzire rad državnih organa zaduženih za borbu protiv terorizma?
- Da li je zakonodavstvo koje uređuje antiterorističke aktivnosti na internetu u skladu sa standardima o ljudskim pravima? Da li je zakonodavstvo usvojeno nakon javnog i inkluzivnog procesa konsultacija?
- Koje su mogućnosti Skupštine da vrši nadzor nad radom privatnih preduzeća u prikupljanju ličnih informacija svojih korisnika?

---

26 Pogledajte Suzbijanje terorističkih priča, 2017. Savet bezbednosti Ujedinjenih nacija.S /RES/2354 (2017). Preambula stav 12 i Zabrana za navođenje na izvršenje terorističkih dela, 2005. Savet bezbednosti Ujedinjenih nacija.S/RES/1624 (2005). Preambula stav 4 i Operativni stav 1(a).

27 Handyside protiv Ujedinjenog Kraljevstva. 4. novembar 1976. Savet Evrope: Evropski sud za ljudska prava. 5493/72, op. cit., stav 49

# DEO V – HAKTIVIZAM

## Definicija

Prema definiciji, haktivizam je spoj hakovanja i tradicionalnog aktivizma. Samu reč nisu prisvojili sami "haktivisti", već je bila pripisana od strane istraživača, novinara i stručnjaka za sajber bezbednost u pokušaju da se napravi razlika između različitih aktera u sajber prostoru. Haktivizam daje nove oblike mobilizacije aktivistima na mreži u njihovoj borbi za određenu vrednost, odnosno cilj (npr. ljudska prava, sloboda govora, itd.). Na taj način haktivizam omogućava aktivnost na daljinu i mobilizaciju velikog obima jednim klikom miša. U pogledu posledica, obični haktivizam generalno izaziva manje štete, zbog čega se vrlo malo slučajeva završi gonjenjem, osobito zbog dodatnog izazova atribucije koji je podjednako prisutan ovde kao i u svim drugim vrstama aktivnosti u sajber prostoru.

## Motivi haktivista i razlika od sajber kriminala i sajber terorizma

U suštini, haktivizam se smatra disruptivnim, a ne destruktivnim. To ga razlikuje od drugih oblika zlonamernih aktivnosti u sajber prostoru, kao što su sajber kriminal i sajber terorizam. Haktivisti uglavnom koriste taktike širenja crva i virusa, distribuirane napade za uskraćivanje usluga (Distributed Denial of Service (DDoS)), manipulaciju internet stranicama i slično. Do koje mere se haktivisti generalno smatraju sitnom pretnjom se može prikazati karakterizacijom da su njihovi DDoS napadi jednaki mirnim protestima iz 1960-ih godina.

Međutim haktivisti se isto tako uključuju u aktivnosti preuzimanja korisničkih naloga na Tviteru i Fejsbuku, a kradu i/ili otkrivaju osetljive i lične informacije iz i na sistemima u koje prodru.

## White, Grey i Black Hat hakeri

Zbog toga što su haktivisti, u suštini hakeri sa ciljem, na osnovu konkretnih aktivnosti koje oni preduzimaju kada uđu u sistem pravi se razlika između različitih vrsta hakera. Oni mogu biti:

- White hat hakeri (hakeri sa belim šeširom) koji slabe tačke sistema koje otkriju prijave sistemskim projektantima, kako bi se razvile konkretne zakrpe i poboljšala sveukupna bezbednost sistema. White hat hakeri se opisuju i kao "etički hakeri".
- Grey hat hakeri (hakeri sa sivim šeširom) isto tako prijavljuju otkrivene slabe tačke sistemskim projektantima, ali mogu tražiti novčanu naknadu ili neku drugu vrstu nagrade za informacije koje su dali.
- Black hat hakeri (hakeri sa crnim šeširom) ne prijavljuju otkrivene slabe tačke sistemskim projektantima i umesto toga žele da profitiraju ili neposrednim iskorišćavanjem ili prodajom tih informacija na crnom tržištu drugim stranama, kao što su sajber kriminalci.

Veoma je tanka granica između haktivizma i napada u sajber prostoru. U nekim slučajevima haktivisti mogu sarađivati sa sajber kriminalcima. Pored toga, direktne javne pretnje izrečene od strane nekih grupa haktivista protiv različitih vlada, preduzeća i pojedinaca mogu potencijalno da izazovu paniku i strah kod civilnog stanovništva, što je jedan od osnovnih elemenata definicije terorizma. Na kraju, nedavne diskusije su naglasile sve veće navode o državnom sponzorisanju haktivizma, koji je praktično nemoguće dokazati i pored toga što se mogu napraviti razumne pretpostavke o njegovom postojanju.

## Primeri pitanja za sprovođenje nadzora:

- Koje kapacitete poseduju organi za sprovođenje zakona za identifikaciju haktivizma i njegovog razlikovanja od drugih oblika sajber pretnji? Da li su oni dovoljni?
- Da li važeće zakonodavstvo jasno definiše koje su aktivnosti uključene u termin “haktivizam” nezakonite (t.j. kada prelaze granicu slobode govora)?
- Šta mogu vlasti uraditi da podrže ‘white hat hakere’ ili da ih izbegnu mešati sa ‘grey’ ili ‘black hat hakerima’? Da li su neki od mehanizama za zaštitu uzbunjivača primenjivi na ‘white hat hakere’?
- Šta se preduzima za identifikaciju potencijalnih haktivista i sprečavanje kriminalnog ponašanja? Da li postoje pravne i operativne zaštitne mere za sprečavanje bezbednosnih službi u zloupotrebi ovlašćenja i podrivanja/onemogućavanja legitimnog aktivizma?
- Šta se preduzima za povećanje međunarodne saradnje u borbi protiv malicioznog haktivizma?

DCAF Geneva Centre for Security Sector Governance


**DCAF Geneva**
P.O. Box 1360
CH-1211 Geneva 1
Switzerland
Tel: +41 (22) 730 94 00
Email: info@dcaf.ch

**DCAF Brussels**
/ EU SSG Facility
24 Avenue des Arts (boîte 8)
1000 Brussels
Belgium

**DCAF Ljubljana**
Gospodinjska ulica 8
1000 Ljubljana
Slovenia

**DCAF Ramallah**
Al-Maaref Street 34
Ramallah / Al-Bireh
West Bank, Palestine

**DCAF Beirut**
Gefinor Bloc C
Office 604, Ras Beirut
Lebanon

**DCAF Tunis**
Rue Ibn Zohr 14
1082 Tunis
Tunisia