Foreign, Commonwealth & Development Office

DCAF Geneva Centre for Security Sector Governance

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

DCSD
PARTENAIRE POUR UNE SÉCURITÉ DURABLE

Vodič za dobro upravljanje u oblasti sajber bezbednosti

Sadržaj

Uvod

Sve veći broj ljudi koji ima pristup sajber prostoru i njegovim resursima utiče na svakodnevni život i ostavlja značajne posledice po društvo u celini. Već je u velikoj meri transformisalo način na koji živimo, radimo i komuniciramo. Sajber prostor nudi bezbroj mogućnosti za ekonomski razvoj, društvenu interakciju i političku saradnju. Isto tako on pruža alatke za nezakoniti nadzor, prikupljanje ličnih podataka, uticanje na demokratske procese, izvršavanje krivičnih dela i razmenu načina i metoda ratovanja.

Vlade, privatni sektor i civilno društvo moraju da pronađu način da zajedno odgovore na sve ove izazove kako bi rešili probleme koji se javljaju kod upravljanja sajber prostorom. Dodatno, pravni okviri i politike moraju da se prilagode kako bi bolje poštovali i primenjivali međunarodne norme zaštite ljudskih prava, a da se pri tome delotvorno suprotstavljaju i bore protiv sajber kriminala, sajber zlonamernih postupaka, sajber napada kao i korišćenja interneta za terorističke aktivnosti i promovisanje nasilnog ekstremizma. Jedino odlučnim aktivnostima u ovom smeru možemo da omogućimo postojanje bezbednog, stabilnog i otvorenog sajber prostora.

Upravo iz ovog razloga su Uprava za saradnju iz oblasti bezbednosti i odbrane (engl. DCSD) francuskog Ministarstva za Evropu i spoljne poslove i Centar za upravljanje sektorom bezbednosti ženevskog DCAF-a pokrenuli 2018.godine pisanje ovog vodiča za dobre prakse u cilju promovisanja dobrog upravljanja u oblasti sajber prostorom. Ovaj vodič je 2020.godine preveden na srpski, albanski, makedonski i engleski jezik kao deo DCAF-ovog projekta pod nazivom Unapređenje upravljanja sajber bezbednošću u zemljama Zapadnog Balkana uz podršku Ministarstva spoljnih poslova i međunarodnog razvoja (engl. FCDO) Ujedinjenog Kraljevstva.

Ovaj Vodič je namenjen donosiocima politika, tehničkim stručnjacima, civilnom društvu i svim onima koji žele da nauče nešto o najboljim praksama upravljanja sajber bezbednošću. Nastao je na osnovu DCAF-ovog iskustva u promovisanju dobrog upravljanja sektorom bezbednosti.

Ovaj knjiga ima šest poglavlja koja objašnjavaju kako možemo da primenimo principe dobrog upravljanja na oblast sajber bezbednosti. Poglavlja se prevashodno bave sledećim temama:

- Dobrim upravljanjem sektorom bezbednosti i primenom na sajber prostor;
- Vezom između sajber prostora, sajber bezbednosti i upravljanja sektorom bezbednosti;
- Međunarodnim i regionalnim pravnim okvirima koji mogu da se primene na sajber prostor;
- Primenom međunarodnih i regionalnih standarda;
- Nacionalnim strategijama sajber bezbednosti;
- Promovisanjem uspešne saradnje između javnog i privatnog sektora u sajber prostoru.

POGLAVLJE 1

DOBRO UPRAVLJANJE SEKTOROM BEZBEDNOSTI: UVOD

CILJEVI

Ovo poglavlje ima za cilj da unapredi poznavanje i razumevanje ključnih termina, a koji se odnose na dobro upravljanje sektorom bezbednosti, postavljajući ih u kontekst sajber prostora. Kako bismo to postigli, ovo poglavlje se bavi i usredsređuje na tri osnovne odlike dobre uprave sektorom bezbednosti koje se mogu preneti i na sajber prostor, a to su:

- a. odgovornost,
- b. transparentnost,
- c. vladavina prava.

Prvo želimo da definišemo osnovne pojmove, a nakon toga i da prikažemo specifične izazove koji se tiču sprovođenja principa dobre uprave u sajber prostoru putem određenih primera dobre prakse.

Šta ćemo naučiti ovom poglavlju?

- Upoznaćemo ključne termine i definicije koje se odnose na upravljanje, upravljanje sektorom bezbednosti i dobrim upravljanjem sektorom bezbednosti.
- Bolje ćemo razumeti osnovni koncept principa koji leži u osnovi dobrog upravljanja, a čine ga odgovornost, transparentnost i vladavina prava.
- Saznaćemo više o principima koji leže u osnovi dobre uprave sektorom bezbednosti.
- Shvatićemo važnost promovisanja osnovnih principa dobrog upravljanja u sajber prostoru.

1. Uvod

Termini: uprava, uprava sektorom bezbednosti, dobra uprava sektorom bezbednosti

Upravljanje se definiše kao 'vršenje ovlašćenja'. Uopšteno govoreći, termin uprava ili upravljanje može da se upotrebi kako bismo opisali pravila vođenja jedne organizacije, uključujući privatna, komercijalna i neprofitna preduzeća. U okviru sektora bezbednosti uprava se odnosi na sve formalne i neformalne odluke, procese i učesnike koji imaju uticaj na obezbeđivanje javnih dobara, kao što su zdravstvo, obrazovanje ili bezbednost.

Upravljanje sektorom bezbednosti (na engleskom SSG) se definiše kao 'vršenje ovlašćenja u okviru određenog državnog sektora bezbednosti.'[1] Ovo je jedan analitički koncept koji se zasniva na određenim normama ili vrednostima koje su obavezujuće.

Termin dobra uprava sektorom bezbednosti (USB) definiše načine na koje sektor bezbednosti možemo učiniti delotvornijim i odgovornijim u okvirima.

> Dobro upravljanje sektorom bezbednosti je posebno usredsređeno na primenu principa dobrog upravljanja bezbednosnim odredbama, upravljanje i nadzor u državnim okvirima.

Termin dobra uprava sektorom bezbednosti (USB) definiše načine na koje sektor bezbednosti možemo učiniti delotvornijim i odgovornijim u okvirima demokratske civilne kontrole, poštovanja ljudskih prava i principa vladavine prava i zakona[2].

Štaviše, dobra USB se zasniva na pretpostavci da bi sektor bezbednosti trebalo da se drži istih visokih nivoa standarda pružanja javnih usluga, kao i drugi državni sektori koji obezbeđuju javne usluge. Stoga sektor bezbednosti koji to ne čini može da dovede u pitanje političku, ekonomsku i socijalnu stabilnost u državnim okvirima (opisujemo pojmom 'loš USB').

1 DCAF, Uvod u reformu sektora bezbednosti (engl. Security Sector Reform Backgrounder).
2 Ibid.

Šta predstavlja sektor bezbednosti?

Uopšteno govoreći, sektor bezbednosti se sastoji od svih struktura, institucija i zaposlenih koji su odgovorni za obezbeđivanje bezbednosti, kao i rukovođenje i nadzor na državnom nivou i lokalnim nivoima.[3]

Stoga sektor bezbednosti ne mora neophodno da bude ograničen samo na državu kao jedinog pružaoca bezbednosti i pravde. Građani sami često obezbeđuju bezbednost i pravdu u svojim domovima i zajednicama, bez obzira na to da li se država ponaša u skladu sa tim potrebama ili ne. Ljudi mogu sami da se organizuju i obezbede bezbednost na različite načine: preko grupa koje kontrolišu i sprečavaju kršenje zakona u svom kraju, preko ženskih grupa i udruženja ili preko komercijalnih načina obezbeđivanja bezbednosti.

Štaviše, uobičajene uloge važnih ličnosti zajednice u procesu donošenja odluka koje se tiču bezbednosti i pravde, alternativni mehanizmi rešavanja sukoba i nesporazuma, tradicije i neformalna pravila mogu da oblikuju obezbeđivanje bezbednosti i pravde u okviru jedne zajednice. Stoga su ove društvene grupe takođe deo sektora bezbednosti i pravde u širem smislu.

Sektor bezbednosti se sastoji od svih struktura, institucija i zaposlenih odgovornih za obezbeđivanje bezbednosti, rukovođenje i nadzor na državnom nivou i lokanim nivoima, uključujući:

- pružaoce bezbednosti, kao što su oružane snage, policija, granična policija, obaveštajne službe, kaznene i zatvorske institucije i komercijalne i nedržavne bezbednosne aktere;
- tela za rukovođenje i nadzor bezbednosti, kao što su ministarstva vlade, skupština, posebne ustavne institucije za kontrolu rada institucija, delovi pravosudnog sistema, civilna društva, akteri koji učestvuju u obezbeđivanju visokih standarda državne bezbednosti, uključujući i ženske organizacije i medije.

Važno je da napomenemo da se reforma sektora bezbednosti (engl. SSR) zasniva na jednom širem razumevanju sektora bezbednosti. SSR je proces sa krajnjim ciljem postizanja dobre uprave sektora bezbednosti kako bi se unapredila bezbednost ljudi i države.

Source : DCAF, Document d'information sur la RSS, Secteur de la sécurité (cf. Bibliographie)

3 Ibid.

Nedržavni pružaoci bezbednosti i pravde su uključeni u širu definiciju sektora bezbednosti zbog njihovog direktnog uticaja na upravljanje sektorom bezbednosti. Poslednje dve decenije privatni sektor se u sve većoj meri angažuje u cilju obezbeđivanja bezbednosti i pružanja usluga zaštite ljudi i imovine. To se posebno odnosi na privatne vojne kompanije i obezbeđenja koja funkcionišu po komercijalnim principima i koja su postala važni akteri bezbednosti.

Šta je reforma sektora bezbednosti?

Sektor bezbednosti, koji nije ni delotvoran ni odgovoran, ne može da obezbedi bezbednost za sve s obzirom na to da ne može da izvršava zadatke na verodostojan način, poput nacionalne odbrane, sprovođenja zakona ili pomoći javnosti. Velika je verovatnoća da će neefikasan sektor bezbednosti nepotrebno trošiti javne resurse i tako oduzimati finansije neophodne za druge državne službe.[4]

Reforma sektora bezbednosti (engl. SSR) je politički i tehnički proces unapređivanja ljudske i državne bezbednosti donošenjem niza bezbedonosnih odredbi, delotvornijim rukovođenjem i nadzorom, kao i odgovornim ponašanjem u okvirima demokratske civilne kontrole, vladavine prava i poštovanja ljudskih prava[5] .

Dobra praksa: Razumevanje činjenice da pojedinci i zajednice imaju različite bezbednosne potrebe, uključujući to i u sajber prostoru

Svaka osoba koja koristi sajber prostor ima drugačije individualne bezbednosne potrebe. Žene i devojčice su u sajber prostoru mnogo više izložene predrasudama, govoru mržnje i mizoginiji. Ukoliko ovo prepoznamo, i kao posledicu toga obezbedimo delotvorne mehanizme prijavljivanja incidenata i pokrenemo krivične istrage, mogli bismo da doprinesemo većoj bezbednosti ugroženih ranjivih grupa.

4 Ibid.

5 DCAF, Dokument o reformi sektora bezbednosti, strana 2, dostupan na https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_2_Security%20Sector%20Reform.pdf

PRIMERI DOBRE PRAKSE

Benin je upravo pokrenuo godišnju kampanju sajber bezbednosti kao deo nacionalnih aktivnosti usmerenih ka podizanju svesti o sajber bezbednosti širom zemlje. Ova kampanja je posebno usmerena ka mladima u ovoj zemlji i biće ozakonjena u dokumentu državne strategije sajber bezbednosti.

Kao deo pokreta protiv govora mržnje zemlje članice Saveta Evrope pokrenule su nacionalne kampanje, kao i nacionalna tela za prijavljivanje, kako bi uvele državne procedure i mehanizme prijavljivanja govora mržnje, zločina počinjenih iz mržnje i sajber zlostavljanja.

Ministarstvo unutrašnjih poslova Austrije ima mehanizam prijavljivanja slučajeva nasilnog ekstremizma i radikalnih video snimaka kako bi zaštitili platforme od govora mržnje.

(Izvor: Federalno Ministarstvo unutrašnjih poslova Austrije, http://bvt.bmi.gv.at/601/)

Ukrajinska policija je postavila osobu za kontakt radi prijavljivanja slučajeva sajber zlostavljanja i govora mržnje kako bi omogućili ugroženim pojedincima da podnesu žalbu.

(Izvor: Savet Evrope, https://www.coe.int/en/web/no-hate-campaign/reporting-to-national-bodies#{%2237117314%22:[8]})

U Senegalu je osnovana Nacionalna škola za sajber bezbednost (fr. Ecole Nationale en Cybersécurité à Vocation Régionale - ENVR) uz francusku pomoć, novembra 2018. godine, kako bi se ojačala odbrana Zapadne Afrike od kompjuterskih hakera i korišćenja interneta za finansiranje terora i propagande. Ova škola obučava službe bezbednosti, sudstvo i privatne kompanije za borbu protiv sajber kriminala i tako dobija „regionalnu ulogu" pružanja pomoći drugim zemljama Zapadne Afrike.

(Izvor: https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/le-cadre-institutionnel-de-l-action-de-la-france/la-cooperation-de-securite-et-de-defense/les-ecoles-nationales-a-vocation-regionale/article/senegal-inauguration-de-l-ecole-nationale-de-cybersecurite-a-vocation-regionale) -Ministarstvo za Evropu i spoljne poslove Francuske)

2. Dobro upravljanje sektorom bezbednosti u sajber prostoru

Šta je dobra uprava sektorom bezbednosti?

Dobra USB se odnosi na primenu principa dobrog upravljanja, na pružanje usluga sektora bezbednosti, njegovo rukovođenje i nadzor na državnom nivou. Postoji sedam principa dobrog upravljanja:

- **Odgovornost**: Prilikom obezbeđivanja bezbednosti postoje jasna očekivanja i nezavisna tela koja kontrolišu da li su ta očekivanja ispunjena ili ne (ukoliko nisu, uvode sankcije).
- **Transparentnost:** Informacije su dostupne i pristupačne svima onima na koje utiču odluke ili njihova primena.
- **Vladavina prava:** Sve osobe i institucije, uključujući i državu, podležu zakonima sa kojima je javnost upoznata. Oni se primenjuju nepristrasno i dosledno, u skladu sa međunarodnim i nacionalnim normama poštovanja ljudskih prava i standarda.
- **Učešće:** Sve žene i svi muškarci, bez obzira na poreklo, imaju mogućnost da učestvuju u procesima donošenja odluka i pružanju usluga na slobodan, jednak i inkluzivan način, bilo da je to direktno ili preko legitimnih institucija.
- **Reagovanje:** Institucije imaju osećaja za različite bezbednosne potrebe svih grupa stanovnika i izvršavaju svoju misiju u duhu poštovanja kulture službe.
- **Delotvornost:** Institucije ispunjavaju svoje odgovarajuće uloge, zaduženja i misije na visoko profesionalnom nivou.
- **Efikasnost:** Institucije na najbolji mogući način koriste državne resurse pri ispunjavanju svojih odgovarajućih uloga, zaduženja i misija.

Primena principa dobrog upravljanja u sajber prostoru

Kada bi sajber prostor bio zemlja, to bi bila najveća i najnaseljenija zemlja na svetu. Ipak, ona ne bi imala zakonodavna tela ili neko drugo reprezentativno telo za donošenje odluka, niti bi postojali određeni mehanizmi za primenu zakona ili mehanizmi zaštite ljudskih prava građana s obzirom na to da ne postoji jedan entitet, jedno lice koje je ovlašćeno da upravlja i kontroliše celim digitalnim prostorom.[6]

Naprotiv, upravljanje sajber prostorom odlikuje prisustvo velikog broja različitih aktera koji imaju razne uloge i zaduženja i utiču na donošenje odluka iz oblasti politika i regulativnih rasprava.

Nedržavni akteri u sajber prostoru uključuju civilna društva, nevladine organizacije, grupe akademskih istraživača i medije, privatni sektor, i posebno privatne kompanije i privredna tela, kao i međunarodne i regionalne organizacije.

Zbog ovog velikog broja aktera koji su uključeni u razvoj i primenu politika i regulatornih okvira u sajber prostoru, ovi procesi su često naporni, složeni i/ili neefikasni.

Ovo zajedno, sa nedostatkom poznavanja na koji način bi trebalo da se delotvorno primene principi dobre uprave u sajber prostoru, može da dovede do lošeg upravljanja, pri čemu je sektor bezbednosti, uopšteno govoreći, neefikasan kod pružanja podrške ljudskoj bezbednosti i bezbednosti država. U sledećim poglavljima detaljnije ćemo razmotriti tri principa dobre uprave: odgovornost, transparentnost i vladavinu prava.

6 Anja Mihr, Dobra sajber uprava, pristup iz ugla ljudskih prava i višestrukih učesnika u procesu, 2014, (engl. Good Cyber Governance, Human Rights and Multi-stakeholder Approach, Georgetown Journal of International Affairs, dostupno na https://www.jstor.org/stable/43773646

STUDIJA SLUČAJA: PROGRAM NADZORA AMERIČKE DRŽAVNE BEZBEDNOSNE AGENCIJE

Godine 2013. Edvard Snouden, koji je radio za CIA-u, obelodanio je dokumenta koja su imala oznaku državne tajne. Tako je otkriveno da su američke i britanske obaveštajne agencije sprovodile masovne programe nadzora širom sveta, uključujući, ali ne isključivo samo to, presretanje protoka na Internetu i presretanje telefonskih veza koje su išle ispod mora putem vlakana optičkih kablova, prikupljanje podataka s naloga korisnika Gugla i Jahua; koristile su snimke razgovora mobilnim telefonom, špijunirale strane vlade, hakovale i zarazile kompjutere malverom.

Zapravo su kompanije dobijale sudske naloge od američkog Suda za inostrani obaveštajni nadzor (engl. FISA) da predaju podatke o svojim klijentima. Štaviše, razotkrivene su obimne prakse razmene obaveštajnih podataka između članova 'Petokoke alijanse' i drugih zemalja. Iako je bivši predsednik Obama reagovao tako što je sproveo reformu programa nadzora Državne bezbednosne agencije (engl. NSA), kao i FISA suda, kako bi povećao transparentnost njihovog rada, američki Kongres i dalje tapka u mestu i ne može da uspostavi sistem koji bi obezbedio suštinsku zaštitu privatnosti, a da pritom zadrži istražne sposobnosti.

(Izvor: ACLU, dostupno na https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance?redirect=nsa-surveillance i https://www.aclu.org/blog/national-security/nsa-legislation-leaks-began?redirect=NSAreform)

2.1. Razvoj normi i institucija koje doprinose i jačaju odgovornost sektora bezbednosti u sajber prostoru.

Kako bismo imali delotvorno odgovorne službe, neophodno je da postoji demokratska i civilna kontrola. Nju mogu da sprovode državne skupštine, kao i, uopšteno gledano, civilna društva. Ovaj oblik nadzora je neophodan kako bismo bili sigurni da je sektor bezbednosti odgovoran prema društvu. Ipak, u sajber prostoru, demokratska i civilna kontrola sektora bezbednosti često biva podrivena iz velikog broja razloga.

Ovo su neke od prepreka na koje često nailazi demokratski nadzor[7]:

- **Složenost onlajn mreže**

Kao prvo, složenost mreže usložnjava probleme nadzora. Veliki i različiti broj država, privatnih, međunarodnih i drugih nedržavnih aktera uključen je u sajber bezbednost. Slično tome, razne grupe učestvuju u onome što je obuhvaćeno jednim širim terminom 'sajber napadi'.Tehnička složenost mreže otežava rad nadzornih tela, kao što su skupštinski odbori koji su često ograničenih kapaciteta da bi vodili evidenciju odgovarajućih aktera, stekli znanja o njihovom postojanju i aktivnostima, ili čak dobili zakonski mandat da to čine.

7 Videti Buckland, B., F. Schreier, and Th. H. Winkler, op. cit., strane 18,19, dostupno na t https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf

- **Neophodno je posedovati stručno znanje iz oblasti tehnike za pisanje i primenu uspešne regulative**

Kao drugo, probleme nadzora otežava tehnička priroda sajber prostora na visokom nivou. Kao rezultat toga, nadzorna tela, kao što su skupštine, nemaju dovoljno neophodnih stručnih znanja kako bi ispravno razumela i uradila predlog zakona koji bi trebalo da reguliše aktivnosti u sajber prostoru na delotvoran način. Javno-privatna saradnja može da dovede do dodatnih komplikacija zbog podela koje postoje između dobro plaćenih i uglađenih tehničkih stručnjaka koji su uključeni u razvoj i primenu uspešne regulative, s jedne strane i loše plaćenih i manje informisanih predstavnika Vlade koji su zaduženi za nadzor, s druge strane.

- **Pravne začkoljice specifične za sajber prostor kao što su jurisdikcija i atribucija**

Kao treće, pravne začkoljice usložnjavaju problem nadzora. Međupovezana priroda sajber prostora „bez granica" predstavlja stvaran problem za tradicionalne okvire teritorijalne primene zakona. Podaci i sajber aktivnosti mogu da se kreću od servera koji se nalazi pod jednom upravom do drugog u drugoj upravi i to brzinom svetlosti. Štaviše, iako se često kaže da bi isti zakoni za tzv. oflajn aktivnosti trebalo da važe i za onlajn, nije baš jasno šta to zapravo znači u praksi. Sajber bezbednost postavlja složena pravna pitanja koja se pre svega odnose na pravo na privatnost i slobodu izražavanja. Ovu složenost dodatno usložnjava javno-privatna saradnja i s tim u vezi pravna pitanja koja se odnose na odgovornost i kontrolu.

- **Raznolika priroda uključenih aktera koji preuzimaju na sebe tradicionalne uloge odgovornosti i nadzora**

Kao četvrto, problem nadzora je otežan zbog raznolike prirode uključenih aktera. U najvećem broju slučajeva, institucije nacionalnog nadzora prate rad većeg broja agencija ili funkcionalnih linija uprave. Na primer, skupštinski odbor može da nadgleda rad obaveštajnih službi, oružanih snaga ili pravosudnih organa. Ipak, javno-privatna saradnja u oblasti sajber bezbednosti prevazilazi granice pojedinačnih agencija i stoga se prepliću stručne oblasti i mandati nadzora. Kao posledicu toga imamo veliki broj oblasti u kojima je nadzor, ili neodgovarajući, ili ne postoji.

Po pitanju preklapanja linija odgovornosti i kontrole, postupci svake vladine agencije su povezani u jedan lanac odgovornosti od prvog do poslednjeg. Na primer, pariski policajac je preko svojih nadređenih povezan sa šefom policije (političko postavljenje sa vrha) i na kraju, s Ministarstvom unutrašnjih poslova i ministrom. Dakle, tu postoji jedna veza odgovornosti i nadzora između institucija demokratske uprave (kao što je skupština) i pojedinaca ili agencija koje sprovode vladine direktive. Ove veze mogu da se prekinu uvođenjem privatnih aktera i stvaranjem javno-privatnih mehanizama saradnje. Može da deluje da jedna IT kompanija koju je angažovala državna agencija radi samo za državu, ali taj odnos je najčešće mnogo složeniji i zamagljen brojnim informacionim asimetrijama koje smanjuju transparentnost i sprečavaju da mehanizmi nadzora i kontrole funkcionišu neometano i uspešno.

- **Razumevanje mandata samog nadzornog tela**

Uopšteno govoreći, vladina nadzorna tela kontrolišu vladine agencije za koje su direktno odgovorna. Ovo može da dovede do izostavljanja privatnih partnera ovih agencija iz vidokruga nadzora, čak i u slučajevima kada su direktno finansirana ili kada rade i blisko sarađuju s ovim agencijama.

STUDIJA SLUČAJA: NEMAČKI BUNDESTAG; UVID U PRODAJU TEHNOLOGIJE NADZORA STRANIM VLADAMA

Godine 2014. poslanici nemačkog parlamenta su zatražili uvid u prodaju tehnologija nadzora stranima vladama. Vlada Nemačke je u odgovoru izjavila da je u poslednjih deset godina izdavala dozvole za izvoz tehnologije za nadzor nemačkim kompanijama koje su izvozile u najmanje 25 zemalja od kojih su mnoge poznate po zloupotrebama ljudskih prava.

Nemačka Vlada je zbog ovoga izjavila da će nastaviti da lobira kako bi se regulisao izvoz tehnologija za nadzor koje nanose štetu ljudskim pravima.

(Izvor: EDRi Protecting Digital Freedom, dostupno na: https://edri.org/germany-exports-surveillance-technologies-to-human-rights-violators/)

Tehnička složenost sajber prostora dodatno otežava već tradicionalne probleme sa kojima se suočavaju poslanici koji imaju zadatak da vrše kontrolu sektora bezbednosti. Ovo može da umanji delotvorno pozivanje na odgovornost. Zajedno sa teškoćom pouzdanog određivanja prekršioca zakona u sajber prostoru može da dovede do otežanog ili čak nemogućeg pozivanja na odgovornost sektora bezbednosti za civilne vlasti, što doprinosi nastajanju prakse nekažnjavanja.

Na primer, pravosudni sektor može da da specijalna ovlašćenja agencijama za sprovođenje zakona, kao i obaveštajnim službama, putem izdavanja naloga za pretres. Ovo je posebno važno u kontekstu presretanja komunikacije. Ipak, sudska kontrola često bude zaobiđena ili ograničena u svom delovanju iz razloga očuvanja nacionalne bezbednosti u uslovima vanrednog stanja.

STUDIJA SLUČAJA: PARLAMENTARNA KONTROLA SAJBER BEZBEDNOSTI U ŠVEDSKOJ; GLAVNI PROBLEMI I DOBRE PRAKSE

Švedski parlament ima petnaest odbora. Uloge ovih parlamentarnih odbora su raznovrsne. Oni, na primer, mogu da vode javna saslušanja kako bi stekli uvid i saznanja o određenim pitanjima o kojima bi trebalo da donose zakone. Nejasno je koji tačno parlamentarni odbor ima samo za zadatak da kontroliše upravljanje sajber bezbednošću. Velika je verovatnoća da će to činiti više odbora u zavisnosti od konteksta. Na primer, Odbor za odbranu može da dobije za zadatak da se bavi pitanjima sajber bezbednosti.

Nacionalna strategija sajber bezbednosti Švedske iz 2016. godine pokriva čitav niz tema, od pravne regulative IKT-a i onih koji ih obezbeđuju do zaštite kritične infrastrukture. Ipak, čini se da ne postoji samo jedan odbor ili pododbor koji se bavi samo sajber bezbednošću. Ovo pitanje često zahteva odgovor više tela vlade, i to je izgleda slučaj upravo u Švedskoj. Ovo se dodatno usložnjava činjenicom da važan deo sajber zaštite obezbeđuju privatna lica, a parlamentarni odbori nemaju odgovarajući mandat da kontrolišu takvu vrstu aktivnosti. Ipak, za razliku od nekoliko nacionalnih strategija sajber bezbednosti, švedska strategija sadrži strateške principe i akcioni plan što pomaže parlamentu da poziva aktere u procesu na odgovornost.

Kao dodatak funkcijama parlamentarne i sudske kontrole civilno društvo igra ključnu ulogu u kontroli sektora bezbednosti. Civilno društvo može da da svoj doprinos putem pružanja saveta po pitanju politika, kao i tehničke ekspertize, može da vodi dijalog i pregovore vršeći svoju ulogu javnog kontrolora.

Civilno društvo dodatno doprinosi povećanju nivoa svesti o različitim pitanjima i može da usmerava donošenje odgovarajućih politika. Ovde posebno mislimo na medije koji mogu da istražuju i pruže pomoć prilikom pristupa informacijama tako što će se detaljnije pozabaviti datim problemom

STUDIJA SLUČAJA: ULOGA PRIVATNIH KOMPANIJA PRILIKOM PRODAJE TEHNOLOGIJE NADZORA VLADAMA

Privatna kompanija, kao što je italijanska kompanija Heking tim ("Hacking Team"), prodala je daljinske sisteme za zaštitu od upada raznim zemljama, uključujući Egipat, Nigeriju, Uzbekistan, Tursku, Maroko i Kolumbiju. Ovaj trend, koji je u porastu, doveo je do rasprave na temu potencijalne upotrebe ovih tehnologija kao sredstva represije i kršenja ljudskih prava.

Ovakav masovni nadzor stvara novi problem, a privatne kompanije nastavljaju da prodaju uređaje i tehnologije za nadzor raznim zemljama. Ovo pitanje i dalje ostaje u velikoj meri neregulisano iako organizacije civilnog društva skreću pažnju na ove poslovne prakse i javno objavljuju baze podataka o više od 520 kompanija za nadzor koje prodaju svoje proizvode vladama širom sveta.

2.2. Razvoj normi i institucija koje promovišu i jačaju transparentnost i čine informacije slobodno dostupnim i pristupačnim

Dostizanje dobre uprave sektorom bezbednosti je proces i cilj reforme sektora bezbednosti.

Transparentnost, uopšteno govoreći, ima dvostruku svrhu: da omogući deljenje informacija, čime se ojačava efikasnost institucija sektora bezbednosti, a i da bude preduslov njihove odgovornosti. Kao dodatak tome, informacione i komunikacione tehnologije (IKT) su alatka sama po sebi koja promoviše i ojačava transparentnost, čineći informacije dostupne svim građanima.

Ipak, apsolutna transparentnost je neizvodljiva i nije uvek preporučljiva u zavisnosti od konteksta sektora bezbednosti.

Važno je da razumemo ovu 'dilemu transparentnosti' u svetlu promovisanja kulture poverenja i otvorenosti između javnog i privatnog sektora bezbednosti. Transparentnost bi ipak trebalo da bude pravilo, a njeno ograničavanje izuzetak koji potvrđuje pravilo i trebalo bi da bude jasno definisana u nacionalnom zakonodavstvu.[8]

Transparentnost isto tako može da pomogne kod boljeg razumevanja rizika po sajber bezbednost i može da ohrabri vlade, privatne kompanije i civilna društva da uspešnije sarađuju i koordiniraju svoje postupke u cilju sprečavanja i pružanja odgovora na ove rizike po sajber bezbednost.

Razumevanje ovih sajber rizika može da pomogne pojedinačnim korisnicima da donose odluke na informisan način. Ovo je veoma važno, jer pojedinačni korisnici tehnologija često se smatraju najslabijom karikom u lancu (sajber) bezbednosti. Bolji kanali informisanja mogu da podrže bolje onlajn ponašanje (što se takođe naziva dobra 'sajber higijena'), što će zauzvrat smanjiti stopu uspeha velike većine zlonamernih aktivnosti.

8 Iulian F. Popa, Extensive Transparency as a Principle of Cyberspace Governance and Cyber Security Dilemma Prevention, dostupno na https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2603326

Zato ovi pristupi koji uzimaju u obzir sve učesnike u procesu mogu takođe da doprinesu jačanju transparentnosti i povećanju svesnosti o sajber bezbednosnim rizicima..

PRIMERI DOBRE PRAKSE

Organizacija za bezbednost i saradnju u Evropi - OEBS (engl. OSCE) godine 2014. usvojila je Sporazum o merama izgradnje poverenja. Proizvoljne mere obuhvataju donošenje nacionalnog viđenja sajber doktrine, strategije i pretnji. Zemlje članice OEBS-a su se još dogovorile i da će deliti informacije o nacionalnim organizacijama, programima ili strategijama, a koje se tiču sajber bezbednosti, da će odrediti osobu za kontakt kako bi olakšale komunikaciju i dijalog o pitanjima bezbednosti IKT-a.

El Salvador je doneo Zakon o zaštiti podataka i pristupu informacijama od javnog značaja, kojim su uspostavljene norme transparentnosti i slobode informisanja

(Izvor: https://publications.iadb.org/handle/11319/7449, strana 74)

Organizacija američkih država je objavila Izveštaj o timovima za reagovanje na bezbednosne kompjuterske incidente (engl. CSIRT), kojim su određeni različiti načini unapređenja komunikacije između ovih timova u cilju razmene informacija.

(Izvor: https://www.sites.oas.org/cyber/Documents/2016%20-%20Best%20Practices%20CSIRT.pdf)

Ohrabrivanje uspostavljanja državno-javnog partnerstva može da doprinese stvaranju okruženja za deljenje i pristup informacijama.

2.3. Jačanje principa vladavine prava u sajber prostoru.

Sajber prostor takođe otvara nove mogućnosti i prostore za nezakonita ponašanja, na primer, širenje govora mržnje i dečje pornografije, podsticanje nasilja, kršenje autorskih prava, prevare, krađu identiteta, pranje novca ili takozvane napade “internet veza ne radi”.[9] Ova krivična dela imaju sve više transnacionalni karakter.

„Priroda digitalnog okruženja je takva da može da ugrozi privatnost i druga osnovna prava, kao i da naruši odgovorno donošenje odluka”.[10] Stoga kao posledicu imamo sve veći potencijal narušavanja principa vladavine prava putem ugrožavanja prava na privatnost i drugih osnovnih prava i sloboda, kao što je sloboda izražavanja.

9 Savet Evrope, Vladavina prava na Internetu i širem digitalnom svetu, dokument koji je objavio Komesar za ljudska prava Sveta Evrope, Izvršni sižei preporuke Komesara, 2014, dostupno na http://www.statewatch.org/news/2014/dec/coe-hr-comm-rule-of-law-on-the%20internet-summary.pdf

10 Ibid. str. 6.

Princip vladavine prava tumače međunarodni sudovi, a medju njima je i Evropski sud za ljudska prava (engl. ECHR). Ovaj sud je razvio jedan test vladavine prava po kome „sva ograničenja osnovnih prava moraju da se zasnivaju na jasnim, preciznim, dostupnim i predvidljivim pravnim odredbama i moraju da imaju svrhu dostizanja jasno legitimnih ciljeva; moraju da budu 'neophodni' i 'proporcionalni' odgovarajućem legitimnom cilju [...], a mora i da postoji 'delotvoran [po mogućnosti sudski] pravni lek'".[11]

Vlade traže od privatnih kompanija koje su vlasnici platformi društvenih medija da obezbede da njihove usluge ne preuzmu nasilni ekstremisti i teroristi.

Generalni sekretar Ujedinjenih nacija objašnjava pojam vladavine prava na sledeći način:

Za Ujedinjene nacije vladavina prava odnosi se na princip upravljanja, po kome su sve osobe, institucije i lica, javna i privatna, uključujući i samu državu, odgovorne pred zakonima koji se javno oglašavaju, jednako primenjuju i nezavisno presuđuju, a koji su u skladu sa normama i standardima međunarodnog ljudskog prava. Takođe je neophodno da postoje mere kojima se osigurava poštovanje principa vrhovne vlasti zakona, jednakost pred zakonom, lična odgovornost, pravičnost kod primene zakona, podela vlasti, učešće u procesu odlučivanja, pravna sigurnost, izbegavanje pravila i arbitrarnost, kao i proceduralna i zakonska transparentnost.

(Izvor: Izveštaj Generalnog sekretara UN-a, Vladavina prava i transnacionalna pravda u konfliktnim i post-konfliktnim društvima, S/2004/616 (23. avgust 2004.), pasus 6, dostupno na https://www.un.org/ruleoflaw/files/2004%20report.pdf.

Kako bi izašli u susret tim zahtevima vlada, privatne kompanije, a posebno one kompanije koje drže društvene medije, kao što su Fejsbuk, Gugl i Tviter, razvile su posebne uslove i pravila ponašanja kako bi mogle da kontrolišu sadržaj koji se postavlja na ovim platformama društvenih medija, i na taj način de facto stvorile pravila i norme na Internetu. Međutim, ti uslovi i pravila ponašanja nisu isti na svim platformama, što stvara dvosmislenost i pravne nedoumice po pitanju toga koja vrsta sadržaja je zabranjena na kojoj platformi.

11 Ibid, str. 8

STUDIJA SLUČAJA: ULOGA KOMPANIJA VLASNIKA DRUŠTVENIH MEDIJA U KONTROLI NJIHOVIH PLATFORMI

Ne dovodi se u pitanje da li kompanije koje su vlasnici društvenih medija imaju pravo da kontrolišu svoje platforme i odrede standarde date zajednice. Kada govorimo o terorizmu kompanije, vlasnici društvenih medija bi de facto trebalo da se ponašaju kao sudije koje mogu da ograniče slobodu govora na svojim platformama bez obaveza prema međunarodnom zakonu o ljudskim pravima. Štaviše, ove kompanije se nalaze pod sve većim pritiskom od strane država da oslobode svoje platforme govora mržnje koji podstiče, glorifikuje i opravdava terorizam.

Upravo, iz ovog razloga, ove kompanije koje su vlasnici društvenih medija morale su da ažuriraju svoje standarde kako bi ispunile sve učestalije zahteve država, što često ima za posledicu postojanje protivrečnih odredbi.

Fejsbuk, na primer, ne dozvoljava prisustvo organizacijama i pojedincima koji su uključeni u neku terorističku aktivnost.Teroristička organizacija se definiše kao „bilo koja nevladina organizacija koja je uključena u smišljeno nasilje sa predumišljajem protiv osoba ili imovine u cilju zastrašivanja građana, vlade, ili međunarodne organizacije kako bi postigle političke, religiozne ili ideološke ciljeve“. Teroristička aktivnost se definiše kao „smišljeno nasilje sa predumišljajem protiv osoba ili imovine, a sprovedeno od strane nevladinih aktera u cilju zastrašivanja građana, vlade, ili međunarodne organizacije kako bi se postigli politički, religiozni ili ideološki ciljevi“.

(Izvor: https://www.facebook.com/communitystandards/dangerous_individuals_organizations)

Tviter se, za razliku od Fejsbuka, ne poziva na terorizam u svojim Tviter pravilima. Tviter zabranjuje sadržaj koji širi mržnju i promoviše nasilje, predstavlja pretnju ljudima na osnovu rase, etniciteta, nacionalnosti, porekla, seksualne orjentacije, roda, vere, uzrasta, hendikepa, ili ozbiljne bolesti. Kao dodatak tome, Tviter zabranjuje uzdizanje nasilja na svojim platformama, kao i nasilne pretnje. Primeri uzdizanja nasilja mogu da se odnose na masovna ubistva, terorističke napade, silovanja i seksualne napade.

(Izvor: https://help.twitter.com/en/rules-and-policies/violent-threats-glorification)

Snoudenova otkrića su pokazala da se obaveštajne agencije rutinski uključuju, prisluškuju privatne razgovore i presreću ih na 'zadnjem ulazu'. Drugim rečima, kada govorimo o državnoj bezbednosti ne postoji stvarno utemeljena potreba primene vladavine prava, iako imamo u najmanju ruku osnovne principe koji bi mogli da budu osnova jednog toliko važnog dela univerzalne tvrđave ljudskih prava. S obzirom na sve češće partnerstvo između agencija za sprovođenje zakona i obaveštajnih i službi bezbednosti, ovo slabljenje vladavine prava preti da se proširi i prenese na policiju i tužioce. Odsustvo jasnih pravnih okvira u ovoj oblasti, kako na domaćem, tako na međunarodnom terenu, predstavlja dodatnu pretnju za vladavinu prava na Internetu i u globalnom digitalnom okruženju.

Principi vladavine prava se takođe dovode u pitanje u kontekstu međunarodnog prava, s obzirom na to da postoji tendencija ka usvajanju proizvoljnih, pravno neobavezujućih, i u velikoj meri ad-hoc pravila i pravnih okvira, koji upravljaju ponašanjem aktera sektora bezbednosti u sajber prostoru. (Pogledajte pregled postojećih međunarodnih i regionalnih zakonskih okvira u Poglavlju 3).

STUDIJA SLUČAJA: PRIVATNE KOMPANIJE ZA SPROVOĐENJE ZAKONA U SAJBER PROSTORU

Činjenica da Internet i globalno digitalno okruženje u velikoj meri kontrolišu privatna lica (posebno, ali ne samo američke korporacije) takođe predstavlja određenu pretnju vladavini prava. Ove privatne kompanije mogu da nametnu (čak da budu „ohrabrene" da to učine) ograničen pristup informacijama bez razmatranja ustavnog i međunarodnog prava koji se primenjuje u slučaju kada država ograničava pravo na slobodu izražavanja. Ovim privatnim licima mogu takođe domaći sudovi, koji deluju po zahtevu drugih privatnih lica, da narede da sprovedu veoma intruzivne analize podataka kako bi otkrile verovatno (ili samo moguće) kršenje prava privatne svojine, a često prava intelektualne svojine.

Može da im bude naloženo da „izvuku" podatke, uključujući vladine, komercijalne i lične podatke iz servera drugih zemalja u cilju primene zakona ili državne bezbednosti, a da nemaju pristanak te druge zemlje, ili pristanak kompanija, ili pojedinaca iz druge zemlje. Ovo predstavlja kršenje suvereniteta druge zemlje, komercijalne tajnosti na koju kompanije imaju prava i ljudskih prava datih pojedinaca.

Odgovornost kompanija društvenih medija („odgovornost posrednika") tumači se veoma usko gledano. Drugim rečima, ukoliko su platforme, kao što su Gugl, Fejsbuk, Jutjub, odgovorne za sadržaj koji njihovi korisnici stavljaju na date platforme, neophodna je veoma pažljiva procena, s obzirom na to da može direktno da se odrazi na slobodu izražavanja i druga ljudska prava. Ipak, vlade širom sveta vrše sve veći pritisak na ove kompanije da uvedu strožu kontrolu sadržaja, podstičući na taj način kulturu 'samocenzure'.

PRIMERI DOBRE PRAKSE

Manilski principi odgovornosti posrednika određuju da se „od posrednika ne sme zahtevati da izbaci sadržaj, osim ukoliko nije izdat nalog za to od strane nezavisnog i nepristrasnog sudskog organa koji je doneo odluku da je problematični materijal nezakonit". Manilski principi dalje tvrde da je neophodno obezbediti „dokaz koji je dovoljan da dokumentuje pravnu osnovu naloga" pre nego što posrednik zabrani bilo koji sadržaj. Oni takođe ističu važnost ugrađivanja transparentnosti i odgovornosti u zakone, napominjući da vlade ne smeju da primenjuju mere uklanjanja sadržaja bez odgovarajuće odluke suda, uključujući posredni pritisak kako bi se nametnula izmena po pitanju izvršenja odluke, ne smeju da promovišu ili nameću takozvane „proizvoljne" prakse, kao i da sklapaju sporazume kojima će moći da kontrolišu razmenu ili javno širenje sadržaja.

(Izvor: https://www.manilaprinciples.org/)

Argentinski nacrt Zakona o odgovornosti posrednika nalaže da „pružaoci internet usluga nisu odgovorni za sadržaj koji kreira treća strana, osim u slučaju kada su na odgovarajući način obavešteni putem sudske odluke da sklone ili blokiraju sadržaj".

(Izvor: Comisión de Sistemas de Communicación y Libertad de Expresión, https://www.infobae.com/tecno/2017/11/21/como-es-el-proyecto-de-ley-que-regula-la-responsabilidad-de-los-intermediarios-de-internet/)

ZAKLJUČAK

- Već samo razmišljanje o bezbednosti i upravljanju njome je korisno s obzirom da stavlja akcenat na to kako različiti državni i nedržavni akteri izvršavaju svoja ovlašćenja u sektoru bezbednosti, kako formalno, tako i neformalno, na međunarodnim, nacionalnim i lokalnim nivoima.
- Uprava ili upravljanje je ključni termin koji može da se primeni na bezbednost uopšteno, a objašnjava kakvu ulogu imaju međunarodni, nacionalni i lokalni akteri zajedno, prilikom donošenja i sprovođenja odluka koje se odnose na sektor bezbednosti.
- Osnovni principi dobre USB su: odgovornost, transparentnost, vladavina prava, učešće, reagovanje, delotvornost i efikasnost.
- Dobra USB se zasniva na ideji da sektor bezbednosti treba da bude na istom nivou, da ispunjava visoke standarde državne uprave, kao i ostali pružaoci usluga u državnom sektoru.
- Dobra USB se definiše kao skup principa i stoga se isti ključni principi dobre uprave primenjuju u svakom sektoru bezbednosti na drugačiji način.
- Uspostavljanje dobre USB podrazumeva stalan proces prilagođavanja s obzirom na to da se bezbednosne pretnje konstantno usložnjavaju i razvijaju.
- USB unapređuje sposobnost sektora bezbednosti da obezbedi bezbednost same države i njenih građana.
- USB čini upotrebu javnih resursa u sektoru bezbednosti efikasnijom.
- USB smanjuje mogućnost korupcije tako što unapređuje kontrolu i profesionalizam.
- USB štiti profesionalnu nezavisnost zaposlenih u sektoru bezbednosti tako da oni mogu na efikasan način da ispune svoje legitimne zadatke i podiže nivo profesionalnih standarda, ojačava odgovornost pri radu, čime smanjuje zloupotrebu stanovništva.
- USB promoviše bezbednost za sve, kao i jednake mogućnosti u okviru sektora bezbednosti.
- USB sprečava nastanak sukoba tako što promoviše jedinstvo, političku neutralnost, jednakost i profesionalizam u sektoru bezbednosti.

IZVORI

DCAF SSR Backgrounder, Security Sector Governance. Applying the principles of good governance to the security sector, available at https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_1_Security_Sector_Governance_EN.pdf

DCAF SSR Backgrounder, Security Sector Reform. Applying the principles of good governance to the security sector, available at https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_2_Security%20Sector%20Reform.pdf

DCAF, The International Security Sector Advisory Team, SSR in a Nutshell. Manual For Introductory Training on Security Sector Reform, available at https://issat.dcaf.ch/download/2970/25352/ISSAT%20LEVEL%201%20TRAINING%20MANUAL%20-%20SSR%20IN%20A%20NUTSHELL%20-%205.3.pdf

DCAF-ISSAT, Introduction to Security Sector Reform A free e-learning course available on the DCAF-ISSAT Community of Practice website: http://issat.dcaf.ch

Heiner Hänggi Security Sector Reform – Concepts and Contexts in Transformation: A Security Sector Reform Reader (Pasig: INCITEGov, 2011, pp. 11–40)

Hans Born and Albrecht Schnabel (eds) Security Sector Reform in Challenging Environments (Münster: LIT Verlag, 2009)

Global Forum on Cyber Expertise, Raising cybersecurity awareness by building trust through transparency, available at https://thegfce.org/raising-cybersecurity-awareness-by-building-trust-through-transparency/

Evert A. Lindquist and Irene Huse, Accountability and monitoring government in the digital era: Promise, realism and research for digital?era governance (Canadian Public Administration, 2017), available at https://onlinelibrary.wiley.com/doi/full/10.1111/capa.12243

POGLAVLJE 2

U KAKVOJ SU VEZI SAJBER PROSTOR I SAJBER BEZBEDNOST SA DOBROM UPRAVOM SEKTOROM BEZBEDNOSTI?

CILJEVI

Ovo poglavlje pruža učesnicima detaljniji uvid u sajber prostor i sajber bezbednost. Cilj ovog poglavlja je da unapredi znanja korisnika o sajber prostoru i sajber bezbednosti, kao i da istakne složenost u primeni praksi dobre uprave sektorom bezbednosti u ovim oblastima.

Šta ćemo naučiti ovom poglavlju?

- Unapredićemo znanja iz oblasti medija sajber prostora po pitanju obima, učesnika i rizika.
- Unapredićemo znanja iz oblasti sajber bezbednosti i njenog uticaja na ljudsku bezbednost, državnu bezbednost i pružanje usluga.
- Razumećemo ograničenja i način na koji prakse USB mogu da se primene u kontekstu sajber prostora.

1. Uvod

Kao što smo već napomenuli u prethodnom poglavlju, dobre prakse USB su važne kako bi podržale efikasno i odgovorno okruženje u kome se poštuju ljudska prava i principi vladavine prava. S obzirom na činjenicu da se sektor bezbednosti odnosi na državne i nedržavne aktere, principi dobre USB bi trebalo da se prošire i izvan državnih praksi.

Dobra USB u sajber prostoru je relativno nov koncept koji ima značajan uticaj kako na vlade tako i na pojedinačne građane. S obzirom na to da sajber prostor, kao i aktivnosti i usluge u njemu, postaju sastavni deo svakodnevnog života, zaštita ličnih podataka i informacija u sajber prostoru je izuzetno važna.

Uprkos ovome, a moguće i zbog svoje raznovrsne upotrebe, koncept sajber prostora i njegovih različitih delova nije dobro definisan. Kako bismo mogli na najbolji način da pristupimo dobroj USB u sajber prostoru, neophodno je preciznije razumevanje značenja termina „sajber prostor" i „sajber bezbednost".

Šta je sajber prostor?

Priroda sajber prostora je jedan apstraktan pojam i čini se da nema korene u fizičkom svetu, što je dovelo do nejasnoća po pitanju značenja samog termina.

Organizacije i narodi često definišu sajber prostor na način koji njima ili njegovoj upotrebi najviše odgovara. Ove definicije se stoga neretko usredsređuju na bezbednost, militarizaciju ili ranjivosti koje su prisutne u sajber prostoru, i kod svake organizacije, naroda ili grupe se naglašavaju njegovi različiti aspekti. Ipak postoji jedna zajednička tema koja provejava kroz većinu definicija: sajber prostor je okruženje koje stvaraju kako fizičke tako i virtuelne komponente u kome se skladište, modifikuju ili razmenjuju podaci, informacije ili komunikacija.

I dok je Internet, po svemu sudeći, najučestaliji i lako dostupni oblik sajber prostora prosečnom građaninu, on je mnogo više od toga.[1] Sajber prostor obuhvata sve kompjuterske mrežne sisteme koji služe, kao što smo prethodno naveli, za skladištenje, modifikovanje ili razmenu[2], koju imamo u sve većem broju satova, uređaja i nekih drugih stvari koje su povezane u sajber prostoru (poznato pod nazivom Internet stvari – na engleskom Internet of Things – IoT). Svi zajedno, ovi različiti protoci podataka i informacija čine jednu „virtuelnu" građu koja se naziva sajber prostor.

1 Fred Schreier, Barbara Weekes, Theodor H. Winkler, Cyber security: The Road Forward, DCAF Horizon 2015 Working Paper No. 4 Geneva: Democratic Control of Armed Force, p. 8. https://www.dcaf.ch/sites/default/files/publications/documents/Cyber2.pdf

2 Benjamin Buckland, Fred Schreier, and Theodor H. Winkler, Democratic Governance Challenges of Cybersecurity DCAF Horizon 2015 Working Paper no. 1. Geneva: Democratic Control of Armed Forces, p. 9. available at: https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf

Sajber prostor je globalni domen prepun izvora, informacija i mogućnosti. Postao je sastavni deo našeg svakodnevnog života u toj meri da je Savet za ljudska prava UN-a 2016. godine potvrdio da „ista prava koja ljudi imaju oflajn moraju da budu zaštićena i onlajn, a posebno sloboda izražavanja koja se primenjuje bez obzira na granice i preko odabranog medijuma, što je u skladu sa članom 19. Univerzalne deklaracije o ljudskim pravima i Međunarodne konvencije o građanskim i političkim pravima[3]".

Sajber prostor ima takođe i svoje fizičke aspekte, uključujući i kompjutere, laptopove, tablete i pametne telefone, kao i servere i fizičke kablove koji čine infrastrukturu interneta. Sajber prostor je medijum u kome aktivnosti veoma često liče na aktivnosti iz fizičkog sveta; ljudi se oslanjaju na sajber prostor kako bi razgovarali jedni sa drugima, bavili se trgovinom, vršili pretrage, uključivali se u rekreativne aktivnosti i bili u toku sa vestima. Svaka vrsta aktivnosti u sajber prostoru nije ipak bezazlena; ovaj isti medij može da bude prostor na kome se odvijaju kriminalne aktivnosti, vojni napadi i druge zlonamerne aktivnosti.

3 Promovisanje, zaštita i uživanje ljudskih prava na Internetu. 32. Skupština Saveta za ljudska prava, (27.juni 2016.), A/HRC/32/L.20

Definsanje sajber prostora
Pred nama su neki primeri definicija sajber prostora koji su trenutno u upotrebi.

Međunarodna telekomunikaciona unija
Sajber prostor je okruženje u kome se odigrava komunikacija preko kompjuterskih mreža i skoro svako je na ovaj ili onaj način povezan.

Međunarodna organizacija za standardizaciju
Sajber prostor je složeno okruženje koje nastaje kao rezultat interakcije ljudi, softvera i usluga na Internetu preko tehnoloških uređaja i mreža na koje su povezani, a koje ne postoji u fizičkom obliku.

Evropska unija
Sajber prostor je skup opipljivljivih i neopipljivih vrednosti koje su uslovljene vremenom, a koje čuvaju i/ili prenose elektronske informacije.

Južna Afrika
„Sajber prostor" označava fizički i nefizički teren koji je sastavljen od nekih ili svih elemenata: kompjutera, kompjuterskih sistema, mreža i njihovih kompjuterskih programa, kompjuterskih podataka, podataka sadržaja, protoka i korisnika.

(Izvori: CCDCOE, dostupno na: https://ccdcoe.org/; ENISA, ENISA pregled sajber bezbednosti i povezane terminologije, verzija 1. Evropska unija, septembar, 2017. dostupno na: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology; Državna bezbednosna agencija, "Nacionalni okvir politike sajber bezbednosti Južne Afrike", Službeni list Vlade, broj 609 (decembar, 2015.), 8.)

PRIMERI DOBRE PRAKSE

Francuska je na početku 21.veka imala jednu od najnižih stopa upada na Internet i kompjutere u Evropskoj uniji. Ipak, danas velika većina stanovništva učestvuje u sajber prostoru. Kako bi poboljšala pristup i jednostavnost korišćenja sajber prostora, Francuska je pokrenula Visok protok ("Très Haut Débit"), jednu novu inicijativu, u cilju promocije brzog pristupa Internetu, posebno u ruralnim i ne tako dobro povezanim zajednicama. Kroz sklapanje partnerstava sa javnim i privatnim grupama Francuska je postavila sebi cilj od 100% pokrivenosti brzom internet vezom i digitalnim pristupom za sve građane do 2022.godine.

Izvor: http://www.francethd.fr/le-plan-france-tres-haut-debit/qu-est-ce-que-le-plan-france-tres-haut-debit.html

Iako ima dosta toga zajedničkog među različitim institucionalnim definicijama sajber prostora, ova ne tako precizna priroda definicija pruža mogućnost akterima u sajber prostoru da oblikuju njene različite aspekte onako kako najbolje odgovara njihovim potrebama i opravdava njihove postupke. Ovo je posebno očigledno kada se opisuje najbolji način korišćenja i zaštite ovog medija. Definicije takođe pokazuju kako države vide sajber prostor, bilo kao sredstvo za vojsku, platformu sa koje mogu da se pružaju usluge, bilo kao prostor za trgovinu i komunikaciju

Mi ćemo ovde da definišemo sajber prostor kao globalno, umreženo okruženje u kome se razmenjuju, skladište, modifikuju podaci i informacije, i koje je dostupno kako državnim tako i nedržavnim akterima.

Upotreba i ovlašćenja u sajber prostoru

S obzirom na to da sajber prostor ima široku upotrebu, logično je da su njegovi korisnici i upotreba podjednako raznovrsni kao i sam medijum. Akteri su, i državni, i nedržavni. Države koriste sajber prostor za održavanje izbora i pružanje usluga široj populaciji, kao sredstvo zaštite državne bezbednosti i državnih vitalnih interesa.[4] Nedržavni akteri obuhvataju sve od kompanija do građana, i svi koriste sajber prostor za različite namene. Svi ovi akteri doprinose i utiču na oblikovanje sajber prostora.

Ova globalna priroda sajber prostora takođe postavlja i ograničenja vladama po pitanju regulativa i upravljanja. Iako je jačanje sajber prostora kao sastavnog dela politika nacionalne bezbednosti važno, podrška dobroj USB u sajber prostoru ima takođe značajan uticaj na privrednu i ljudsku bezbednost.[5] Kako se svet sve više oslanja na usluge i slobode koje obezbeđuje sajber prostor, zaštita ljudskih prava i bezbednosti ljudi, podjednako kao i nacionalna bezbednost, postaje sve veća obaveza[6] .

4 Liaropoulos, Andrew N. 2017, Cyberspace Governance and State Sovereignty,In Democracy and an Open-Economic World Order, (Upravljanje sajber prostorom i suverenitet države, U demokratskom i otvoreno ekonomskom svetskom poretku), uredio George C. Bitros i Nicholas C. Kyriazis, 25-35. Springer International Publishing AG.

5 Cole, Kristina, et all, Cybersecurity in Africa: An Assessment. Atlanta: Georgia Institute of Technology. https://www.researchgate.net/publication/267971678

6 Benjamin Buckland, Fred Schreier, and Theodor H. Winkler, Democratic Governance Challenges of Cybersecurity, DCAF Horizon 2015 Working Paper no. 1. Geneva: Democratic Control of Armed Forces, p. 9. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf

STUDIJA SLUČAJA: OBEZBEĐIVANJE FIZIČKE KOMPONENTE

U poslednje vreme sve više se ističe neophodnost bolje zaštite i bezbednosti kompjuterski rukovođenih uređaja, kao što su laptopovi, tableti i pametni telefoni. Evropska unija i njene države članice, kao i Sjedinjene Američke Države, počele su da vrše pritisak na proizvođače tehnologija da obezbede odgovarajuću zaštitu svojih proizvoda.

Američko Ministarstvo za unutrašnju bezbednost (engl. the Department of Homeland Security of the United States of America) je 2016. godine objavilo veliki broj strateških predloga u cilju obezbeđivanja Interneta stvari. Prvi korak ovog pristupa je obezbedjivanje uređaja tokom proizvodnje, a zatim održavanje tog nivoa bezbednosti tokom ažuriranja i rukovodjenje ranjivostima sistema.

Ujedinjeno Kraljevstvo je napravilo „bezbednosni kodeks prakse" za proizvođače kako bi ih ohrabrili da poboljšaju bezbednost uređaja u fazi razvoja. Kako bi se unapredila bezbednost samih uređaja, šifre za uređaje Interneta stvari moraju da imaju jedinstvenije zahteve za postavljanje lozinki, a trebalo bi da postoji i veća transparentnost kod bezbednosnih prekršaja tako što će se podstaći javno obelodanjivanje ranjivih delova uređaja. Trenutno se ove šifre primenjuju samo na dobrovoljnoj bazi, ali UK nije isključilo mogućnost da ih učini obaveznim za sve uređaje koje se prave u ovoj zemlji.

Iako je pristup Evropske Unije u cilju povećanja bezbednosti uređaja još uvek u fazi nacrta, doći će do procesa izrade sertifikata za uređaje Interneta stvari širom Unije. Svi ovi pristupi imaju za cilj da ohrabre druge države da razviju svoje pristupe i politike koje će zaštititi uređaje povezane u sajber prostoru.

Izvor: https://www.ft.com/content/d21079b0-8a79-11e8-affd-da9960227309

Sajber bezbednost

Sa sve većom upotrebom sajber prostora od strane vlada, pojedinaca i kompanija, količina osetljivih podataka i informacija u okviru sajber prostora postaje u sve većoj meri izložena i podvrgnuta novim ranjivostima koje se stalno menjaju.[7] Uspešna zaštita ovih informacija je neophodna kako bi se stvorilo bezbedno okruženje unutar i izvan sajber prostora. Sajber bezbednost, kako i samo ime kaže, sastoji se od niza praksi i metoda za zaštitu podataka, informacija i integriteta različitih delova sajber prostora, uključujući, ali ne samo njih, fizičke aspekte ovog medijuma.[8]

7 Fred Schreier, Barbara Weekes, Theodor H. Winkler, Cyber security: The Road Forward, DCAF Horizon 2015 Working Paper No. 4 Geneva: Democratic Control of Armed Force, p. 11. https://www.dcaf.ch/sites/default/files/publications/documents/Cyber2.pdf

8 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

Iako se sajber bezbednost često dovodi u vezu sa strategijama nacionalne bezbednosti, važno je da sagledamo šire posledice ovog termina. ITU opisuje sajber bezbednost kao sredstvo, smernice, i druge pristupe u cilju zaštite integriteta i poverljive prirode sajber prostora za privatne organizacije, vlade i civilno društvo[9] .

U skladu sa porastom značaja sajber prostora za profesionalne, rekreativne i političke aktivnosti, sajber bezbednost postaje oblast u razvoju u carstvu sektora bezbednosti i dobre uprave sektorom bezbednosti. Norme koje se primenjuju na bezbednost u sajber prostoru se razvijaju kako bi mogle da odgovore na brzo širenje praksi i tehnika sajber bezbednosti, kao i na aktere koji se stalno menjaju.[10] Pojavljuju se određene norme po pitanju granice kontrole sajber prostorom pošto države propisuju svoje nacionalne pristupe u cilju obezbeđivanja bezbednijeg okruženja sajber prostora u okviru svojih zemalja, kao i načini na koji države mogu da nametnu kontrolu nad sajber prostorom[11] .

Merenje sajber bezbednosti

S obzirom na široke i konkurentne definicije sajber prostora i sajber bezbednosti, analiza sajber bezbednosti nije lak poduhvat. ITU je napravio Globalni indeks sajber bezbednosti kako bi odredio koliko su zemlje članice posvećene jačanju sajber bezbednosti. Ovaj indeks ocenjuje pet različitih aspekata sajber bezbednosti (pravni, tehnološki, organizacioni, izgradnju kapaciteta i saradnju) i pokazuje koliko su države posvećene ovoj temi. I dok je ovo dobar način da se ustanovi odgovor vlada i aktivnosti kod upravljanja sajber prostorom, uloga nevladinih aktera u sajber prostoru i sajber bezbednosti ostaje zapostavljena. Njime se ocenjuju politike, ali ne i prakse, i na taj način ne uzima u obzir praktične uticaje ili efikasnost ovog rada.

9 ITU vodič za razvoj NCSS, 13.

10 Međunarodne norme sajber bezbednosti, International Cybersecurity Norms, Microsoft Policy Papers Microsoft. Dostupno na: https://www.microsoft.com/en-us/cybersecurity/content-hub/international-cybersecurity-norms-overview

11 Ibid.

2. USB u sajber prostoru

Sajber prostor predstavlja niz sloboda, ograničenja i složenih pitanja koja su specifična i jedinstvena za prirodu ovog medijuma. S obzirom na veliku lepezu učesnika u sajber prostoru i način na koji ova činjenica može da bude iskorišćena ili zloupotrebljena, stvaranje okvira dobrih praksi USB se suočava sa različitim nizovima prepreka kao što su one tradicionalno 'teritorijalne'. Sa nekim od ovih prepreka ćemo se detaljnije baviti u poslednjem poglavlju, a prvenstveno onima koje slabe vladavinu prava, transparentnost i odgovornost.

Kada gledamo USB kroz prizmu sajber prostora, važno je da uzmemo u obzir različite učesnike u ovoj sferi, da procenimo ko kontroliše koji aspekat sajber prostora i odredimo na koji način najbolje možemo da utičemo na ponašanja i prakse ili ih stimulišemo, a koje će na kraju ojačati dobru USB u areni sajber prostora. Različiti učesnici u sajber prostoru i sajber bezbednosti čine jedan zanimljiv uzorak koji bi trebalo da istraže donosioci politika, s obzirom na to da država nije u stanju da jednostrano obezbedi efikasnu bezbednost i regulativu ovog medijuma.

Dobra praksa: Primena sajber bezbednosnog pristupa koji uključuje učesnike iz javnog i privatnog sektora u sajber prostoru

S obzirom da je sajber prostor jedna platforma na kojoj su zajedno privatni i javni akteri, pisanje i primena različitih politika koje imaju uticaj na USB mora da obuvati sva lica koja postoje izvan javne sfere. Prepoznavanje uloge IKT kompanija i privatnih sajber bezbednosnih korporacija igra važnu ulogu u formiranju i zaštiti prava korisnika, a zaštita je jedan važan korak ka stvaranju bezbednijeg sajber okruženja.

PRIMERI DOBRE PRAKSE

Vlada Kameruna sarađuje sa velikim brojem partnera iz privatnog sektora po pitanjima koja se odnose na sajber bezbednost i uspostavila je radne odnose poslovnu saradnju sa drugim zemljama po pitanju rukovodjenja i odgovaranja na sajber pretnje. Na primer, nakon onlajn prevare u koju je bila uključena farmaceutska kompanija, Kamerun se udružio sa Republikom Češkom, INTERPOL-om i Nigerijom kako bi sproveli digitalnu istragu. Kamerunske vlasti promovišu nekoliko mera izgradnje poverenja i sporazume o međunarodnoj saradnji u sajber prostoru putem razmene informacija o sajber incidentima i najboljim praksama za sajber bezbednost.

Trenutni problemi sa USB u sajber prostoru

Dobre prakse USB u sajber prostoru mogu da pomognu da se osigura ljudska bezbednost, vladavina prava i drugi aspekti dobre uprave koji se kontrolišu i štite u sajber prostoru.

Kao što je već kratko pomenuto u poslednjem poglavlju, jedan od problema sa kojim se suočava upravljanje sektorom bezbednosti u sajber prostoru je nedostatak razumevanja osnova primene uspešne uprave u sajber prostoru, što za posledicu ima donošenje neodgovarajućih politika i regulativa, kao i stvaranje okruženja koje omogućava vršenje

kriminalnih aktivnosti.[12] Ovaj nedostatak znanja može takođe da utiče na delotvorne regulative država nad akterima iz privatnog sektora i može da podriva sposobnost države da primeni dobre prakse USB u sajber prostoru.

Trenutno mnoga privatna komercijalna lica se angažuju kao bezbednosne službe sajber bezbednosti što stvara probleme za delotvornu primenu praksi USB u sajber prostoru. Jedan aspekt dobre uprave je da za države postaje sve teže da primenjuju svoju transparentnost. Prvi problem je da definicija transparentnosti u sajber prostoru iz ugla dobre USB nije usaglašena. Došlo je ipak do sve većeg pozivanja na transparentnost u ovom kontekstu koje se vezuje za otkrivanje kada i do kog nivoa je došlo do upada u informacione sisteme.

Pružanje podrške ili obavezivanje aktera da otkriju prestupe u sajber prostoru jedan je od načina na koji država može da unapredi prakse dobre USB, s obzirom na to da se na taj način, ne samo povećava transparentnost u sajber prostoru, već i osigurava da se reše nedostaci u sadašnjim praksama sajber bezbednosti, pomažući da se spreče sajber napadi i unaprede bezbednosne prakse u sajber prostoru. Nedostatak transparentnosti sajber napada u velikoj meri podriva ljudsku bezbednost u sajber prostoru zato što može da dovede do zlonamernih sajber napada i time naudi većem broju žrtava[13]

STUDIJA SLUČAJA: OBAVEZIVANJE NA TRANSPARENTNOST

Australija

Australijski parlament je 2017.godine usvojio dopunu i izmenu Zakona o privatnosti iz 1998. godine koji nalaže organizacijama vlada Komonvelta, organizacijama privatnog sektora i drugim određenim telima da obelodane informacije o sajber bezbednosnim prestupima onima na koje ti prestupi utiču. Kršenje ovog novog zakona povlači sa sobom novčanu kaznu, javno priznanje i izvinjenje što nisu postupili kako je bilo naloženo, velike novčane kompenzacije za žrtve, za one koji su više puta osetili kršenje ovog zakona.

Izvore: Ben Allen, Australia: Cybercrime – New Mandatory Data Breach Reporting Requirements (Australija: Sajber kriminal – novi obavezni zahtevi za prijavu zloupotrebe podataka) www.mondaq.com. Dostupno na : http://www.mondaq.com/australia/x/573188/Security/Cybercrime+New+Mandatory+Data+Breach+Reporting+Requirements

Amerika

Američka komisija za hartije od vrednosti naplatila je Jahuu (Yahoo) veliku kaznu od 35 miliona američkih dolara zato što nisu uspeli da otkriju sajber napad koji je uticao na preko 500 miliona naloga. Ovo je bio prvi primer da je neka kompanija novčano kažnjena jer nije postupila po pravilima za otkrivanje koja su obavezna za državne kompanije.

Izvor: Kadhim Shubber, "Yahoo's $35m Fine Sends a Message" (Jahuova kazna od 35 miliona dolara šalje poruku), Financial Times, www.ft.com. Dostupno na: https://www.ft.com/content/4c0932f0-6d8a-11e8-8863-a9bb262c5f53

Pružanje podrške ili obavezivanje aktera da otkriju prestupe u sajber prostoru jedan je od načina na koji država može da unapredi prakse dobre USB, s obzirom na to da se na taj način, ne samo povećava transparentnost u sajber prostoru, već i osigurava da se reše nedostaci u sadašnjim praksama sajber bezbednosti, pomažući da se

12 Buzatu, SSG/SSR u sajber prostoru, strane 7-8.

13 Vidi, na primer, ICANN Organization's Cybersecurity Transparency Guidelines (Smernice za transparentnost sajber bezbednosti organizacija) (2018.), dostupne onlajn na: https://www.icann.org/en/system/files/files/cybersecurity-transparency-guidelines-03aug18-en.pdf

spreče sajber napadi i unaprede bezbednosne prakse u sajber prostoru.[14] Nedostatak transparentnosti sajber napada u velikoj meri podriva ljudsku bezbednost u sajber prostoru zato što može da dovede do zlonamernih sajber napada i time naudi većem broju žrtava.

Transnacionalna priroda sajber prostora takođe postavlja određenu dilemu pred države koje žele da primene dobre prakse USB. S obzirom na to da građani redovno učestvuju u transakcijama koje prevazilaze međunarodne teritorijalne granice, sposobnost države da izvršava svoja ovlašćenja nad onim što utiče na njeno stanovništvo u velikoj meri se smanjuje. U većini slučajeva države moraju da se oslanjaju na komercijalne posrednike, kao što su platforme društvenih mreža, kako bi mogle da kontrolišu i regulišu onlajn ponašanja.[15] Ovo podriva dobre prakse USB zato što države nemaju često uvid u to kako se informacije filtriraju ili skidaju. Još jedan problem je transnacionalne prirode, a to su informacije na Internetu koje mogu da se čuvaju na jednom ili više servera koji su locirani u više uprava. Oslanjanje na druge države da sprovode istrage, krivično gone i osuđuju sajber kriminalce, dovodi do stvaranja drugačije dinamike. Na ovaj način sajber prostor podriva prakse dobre uprave jer se oslanja ne samo na aktere u okviru jedne uprave, već utiče na međunarodnu grupu aktera.

STUDIJA SLUČAJA: MEĐUNARODNE ISTRAGE

Međunarodne istrage i krivična gonjenja iz oblasti sajber bezbednosti su poznat fenomen. Aprila 2018.godine jedan sajt koji je prodavao usluge napada na mreže (na engleskom Distributed Denial of Service (DDoS)), Webstresser.org, ugašen je, a njegovi administratori su optuženi za sajber kriminal zahvaljujući međunarodnoj istrazi holandske Državne jedinice za visoko-tehnološki kriminal, kao i britanske Agencije za državni kriminal (NCA) uz podršku mnogih drugih organizacija. Operacija Power Off (Isključenje) je samo jedan primer kako međunarodni akteri mogu da rade zajedno kako bi stvorili bezbednije sajber okruženje za korisnike.

Izvori: Cal Jeffrey, Operation Power OFF pulls the plug on 'DDoS-for-hire' website, (Operacija Power OFF izvlači utikač sajta za iznajmljivanja zlonamernog proizvoda za napade na mreže) TechSpot www.techspot.com. 25.april 2018.godine Dostupno na: https://www.techspot.com/news/74327-operation-power-off-pulls-plug-ddos-hire-website.html i "World's Biggest Marketplace Selling Internet Paralysing DDoS Attacks Taken Down" (Oboreno najveće svetsko prodajno mesto koje prodaje DDoS napade koji parališu internet) Europol.europa.org, objava za štampu. 25.april 2018. Dostupno na: https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down

Iako možda deluje kao primena praksi, dobra USB u sajber prostoru nailazi na puno prepreka, ali nije nemoguća. Neki međunarodni okviri i norme koji daju smernice kako da se USB integriše u sajber prostor, počeli su da se ostvaruju. I dok prakse i politike moraju da budu takve da odgovaraju nacionalnom kontekstu, otkrivanje koji međunarodni i regionalni okviri postoje za sajber prostor, ključni je korak napred ka dobroj USB u sajber prostoru.

14 Paul Smith, New mandatory data breach notifications laws to drag Australia into cyber age Financial Review, afr.com, Feb. 23, 2018. https://www.afr.com/technology/new-mandatory-data-breach-notifications-laws-to-drag-australia-into-cyber-age-20180222-h0whxa

15 Niva Elkin-Koren; Eldar Haber, Governance by Proxy: Cyber Challenges to Civil Liberties, Brooklyn Law Review 82 no. 1. 105

ZAKLJUČAK

- Sajber prostor postoji, i na fizičkom, i na nefizičkom nivou, i čini ga bilo koja platforma preko koje mogu da se prebace, transformišu ili izmene informacije, podaci i komunikacija s jednog kompjutera na drugi. Takođe obuhvata fizičku infrastrukturu interneta koji se nalazi svuda.
- Vlade, građani i kompanije se sve više oslanjaju na izvore koje sajber prostor pruža u svakodnevnom životu.
- Postoji veliki broj različitih učesnika u okviru sajber prostora i sajber bezbednosti.
- Postoje razne prepreke kod USB u sajber prostoru, počevši od višestrukih aktera koji utiču na različite aspekte sajber prostora do opšteg nedostatka znanja po pitanju bezbednog korišćenja sajber prostora.
- Iako neke države imaju politike i okvire za upravljanje sajber bezbednošću i sajber prostorom, opšti nedostatak znanja o ovoj temi otežava pravilnu i ispravnu primenu praksi USB u sajber prostoru.

Izvori

Buckland, Benjamin, Fred Schreier, and Theodor H. Winkler, Democratic Governance Challenges of Cybersecurity (Izazovi demokratske uprave u sajber prostoru) DCAF Horizon 2015 Working Paper no. 1. Geneva: Democratic Control of Armed Forces, https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf

Elkin-Koren, Niva, and Eldar Haber, Governance by Proxy:Cyber Challenges to Civil Liberties, (Upravljanje preko posrednika: Sajber izazovi i građanske slobode), 82 Brook. L. Rev.105 (2016)

Fred Schreier, Barbara Weekes, Theodor H. Winkler, Cyber security: The Road Forward (Sajber bezbednost: Kako dalje), DCAF Horizon 2015 Working Paper No. 4 Geneva: Democratic Control of Armed Force, https://www.dcaf.ch/sites/default/files/publications/documents/Cyber2.pdf

Liaropoulos, Andrew N. 2017, Cyberspace Governance and State Sovereignty (Upravljanje sajber prostorom i suverenitet država) In Democracy and an Open-Economic World Order, edited by George C. Bitros and Nicholas C. Kyriazis, 25-35. Springer International Publishing AG.

Paul Smith, New mandatory data breach notifications laws to drag Australia into cyber age (Novi obavezujući zakoni projave kršenja zaštite podataka će odvući Australiju u sajber doba), Financial Review, afr.com, Feb. 23, 2018. https://www.afr.com/technology/new-mandatory-data-breach-notifications-laws-to-drag-australia-into-cyber-age-20180222-h0whxa

Cole, Kristina, Marshini Chetty, Christopher LaRosa, Frank Rietta, Danika K. Schmitt and Seymour E. Goodman, Cybersecurity in Africa: An Assessment. (Sajber bezbednost u Africi: Procena), Atlanta: Georgia Institute of Technology. https://www.researchgate.net/publication/267971678

POGLAVLJE 3

MEĐUNARODNI I REGIONALNI PRAVNI OKVIRI U SAJBER PROSTORU

CILJEVI

Ovo poglavlje daje korisnicima pregled međunarodnih i regionalnih pravnih okvira koji se odnose na sajber prostor i ističe zanimljive i inovativne pristupe i inicijative.

Šta ćemo naučiti u ovom poglavlju?

- Unapredićemo znanja o raznim međunarodnim i regionalnim organizacijama koje se bave sajber prostorom i sajber bezbednošću.
- Postaćemo svesniji dostupnih resursa koji su na raspolaganju kako bismo pomogli proces sprovođenja međunarodnih i regionalnih pravnih okvira na nacionalnom nivou.
- Unapredićemo znanja o sajber kriminalu, sajber terorizmu i korišćenju Interneta u terorističke svrhe.

Uvod

Efektivni pravni okviri na međunarodnim, regionalnim i nacionalnim nivoima jedan su od stubova dobre uprave i preduslov poštovanja principa vladavine prava. Pravni okviri su uopšteno govoreći neophodni za kontrolnu zakonskog ponašanja i za kontrolu zabrane ili kazne nezakonite aktivnosti. Pravni okviri u sajber prostoru su važni i za poštovanje ljudskih prava.

Dosta se govori, ali se ne razume na koji način pravni okviri mogu da se primene u sajber prostoru. Njegova prekogranična priroda fokusirana na informacije predstavlja problem za centralizovan pristup upravljanju jedne države. Sa jedne strane fizička infrastruktura koja čini sajber prostor je pod nacionalnim pravosuđem i upravom, a sa druge strane protok podataka i informacija preko te strukture stalno prelazi iz jedne u drugu teritorijalnu upravu što otežava zakonsku efektivnu kontrolu nad ovim protokom informacija. Upravo iz ovog razloga javila se potreba za stvaranjem novih normativnih režima kako bi se uspostavila regulativa sajber prostora.

Danas je neosporna primena principa međunarodnog prava u sajber prostoru. Ono što je manje jasno je kako da se ovi principi prevedu u praksu. Otuda ovaj jaz između politika i prakse koji dovodi do pravnih nedoumica, čak i do pravne praznine koja može da podrije zaštitu ljudskih prava korisnika na internetu. Stoga su međunarodne i regionalne organizacije preuzele na sebe da pokrenu inicijative sa ciljem da pronađu i protumače na koji način postojeći pravni principi međunarodnog prava mogu da se primene u sajber prostoru.

1.Međunarodni i regionalni pravni okviri

Postoje brojne inicijative na međunarodnom i regionalnom nivou koje imaju za cilj da promovišu odgovornije ponašanje u sajber prostoru i razviju regulatorne okvire i mere izgradnje poverenja u njemu. Sledi pregled većeg broja ovih inicijativa.

Ujedinjene nacije

Trenutno ne postoji pravno obavezujući instrument na međunarodnom nivou koji reguliše ponašanje u sajber prostoru. Ipak, postoji veliki broj takozvanih 'mekih zakonskih' (engl. 'soft-law') inicijativa (koje nisu pravno obavezujuće), a koje određuju norme u sajber prostoru i daju smernice državama kako da ih primene.

Danas je neosporno da međunarodno pravo, a posebno Povelja Ujedinjenih nacija, Međunarodni zakon o zaštiti ljudskih prava i Međunarodno humanitarno pravo imaju svoju primenu u sajber prostoru.

STUDIJA SLUČAJA: IZVEŠTAJ UN GRUPE VLADINIH STRUČNJAKA

Ovaj izveštaj UN GGE-a iz 2015. godine sadrži spisak sledećih preporuka za odgovorno ponašanje država kako bi dale svoj doprinos otvorenom, bezbednom, stabilnom, dostupnom i mirnom sajber prostoru.

Pozitivne norme

- Države bi trebalo da sarađuju kako bi se unapredila stabilnost i bezbednost upotrebe IKT-a i sprečile štetne IKT prakse korišćenja.
- Države bi trebalo da daju sve dostupne informacije po pitanju atribucije u IKT okruženju.
- Države bi trebalo da preduzmu odgovarajuće mere zaštite nacionalne kritične infrastrukture od IKT pretnji i odgovore na zahteve za pomoć drugih država.
- Države bi trebalo da preduzmu razumne korake kako bi obezbedile integritet lanca snabdevanja i sprečile širenje zlonamernih IKT alatki i tehnika.
- Države bi trebalo da ohrabre odgovorno prijavljivanje ranjivosti IKT-a i podele date informacije.

Ograničavajuće norme

- Države ne bi trebalo da svesno dozvole da se njihova teritorija koristi za vršenje međunarodnih prestupa upotrebom IKT-a.
- Države bi trebalo da se pridržavaju rezolucija Generalne Skupštine UN-a o ljudskim pravima.
- Države ne bi trebalo da rukovode ili svesno podržavaju IKT aktivnosti koje su suprotne njihovim obavezama prema međunarodnom pravu.
- Države ne bi trebalo da rukovode ili svesno podržavaju aktivnosti koje nanose štetu informacionim sistemima ovlašćenih timova za reagovanje u vanrednim situacijama.

Ujedinjene nacije su, na primer, osnovale šest uzastopnih Grupa vladinih stručnjaka (engl. UN GGE), po principu 'ravnomerne geografske zastupljenosti', uključujući ključne 'sajber sile' kao što su SAD, Kina, Rusija , Francuska, UK i Nemačka, sa ciljem predlaganja normi odgovornog ponašanja u sajber prostoru, od 2004.godine.

STUDIJA SLUČAJA: MEŠANJE U IZBORE PUTEM ONLAJN INFORMACIONIH KAMPANJA I DA LI JE TO MEŠANJE SLUČAJ ZA MEĐUNARODNO PRAVO

I dok mešanje u političke procese primenom otvorenih i prikrivenih sredstava nije ništa novo u međunarodnim odnosima, vladini zvaničnici iz pretežno zapadnih država su od 2016. godine izrazili svoju zabrinutost oko mešanja u izbore putem ciljanih sajber operacija i kampanja širenja lažnih informacija.

Godine 2014. operacija pod nazivom CyberBerkut je imala za metu Centralnu izbornu komisiju Ukrajine tako što su oborili delove mreža Komisije u trajanju od skoro dvadeset sati i objavili lažnog pobednika u izbornom danu. Godine 2016. hakerska jedinica 'Fancy Bear' je napala nemački Bundestag, nemačko Ministarstvo spoljnih poslova i Ministarstvo finansija i sisteme Hrišćansko-demokratske unije. Godine 2017. sajber operacije, koje su imale za cilj da ugrade malver na sajt kampanje, ciljale su na kampanju Emanuela Makrona za predsednika Francuske.

Na osnovu međunarodnog prava ova dela verovatno krše suverenitet država. Suverenitet je opštepoznat i smatra se osnovnim i primarnim pravilom međunarodnog prava, kao što je i istaknuto u Izveštaju UN GGE-a iz 2015. godine:

'Suverenitet država i međunarodne norme i principi koji iz njega proističu se primenjuju i na ponašanje država u odnosu na IKT aktivnosti i njihovo zakonsko upravljanje IKT infrastrukturom na datoj teritoriji'.

Opšti principi cilja i svrhe suvereniteta su 'da omoguće državama punu kontrolu nad pristupom i aktivnostima na njihovoj teritoriji'.

Šta ovo znači kada govorimo o mešanju u izbore putem sajber operacija?

Stručnjaci kažu da nije presudno prilikom procene aktivnosti kršenja principa suvereniteta da li postoji veza između ciljanog sistema i izbora, već da li je data operacija nanela nužnu štetu ili dovela do gubitka funkcionalnosti. Na osnovu Talinskog uputstva 2.0 aktivnosti koje mogu da se kvalifikuju pod kršenje suvereniteta su: sajber operacije koje dovode do toga da sajber infrastruktura ili programi rade na izmenjen način; menjanje ili brisanje podataka koji se čuvaju u sajber infrastrukturi bez prouzrokovanja fizičkih ili funkcionalnih posledica, kao što je opisano gore; ubacivanje malvera u sistem; instaliranje 'zadnjih vrata'; dovođenje do privremenog, ali značajnog gubitka funkcionalnosti, kao u slučaju operacije širenja prekida rada mreže u vidu sajber napada (engl. denial of service).

Značajan pomak je učinjen 2013. godine kada je UN GGE, koja je u to vreme imala samo petnaest članova, usvojila konsenzusom svoj izveštaj kojim se potvrđuje primena međunarodnog prava u sajber prostoru. Izveštaj UN GGE-a iz 2015.godine je potvrdio ovu odluku i dalje odredio normativne okvire za države i njihovu upotrebu sajber kapaciteta. Ovde je od posebnog značaja deo koji se odnosi na 'norme, pravila i principe odgovornog ponašanja država'.

Nažalost, od 2016. godine do 2017. godine UN GGE nije uspela da usvoji konsenzusom izveštaj čime je dovela međunarodnu zajednicu u nedoumicu po pitanju najboljeg pristupa međunarodnom pravu u sajber prostoru. Ipak, oktobra 2018. godine Generalna skupština UN-a (engl. UNGA) usvojila je rezoluciju A/C.1/73/L.37 u cilju formiranja još jedne GGE 2019.godine koja će imati za zadatak da podnese izveštaj 2021.godine na 76. zasedanju UNGA-e. Istovremeno je ovom rezolucijom UNGA oformljena i jedna Otvorena radna grupa (engl. Open-Ended Working Group) koja se sastala u junu 2019. godine kako bi donela pravila, norme i principe odgovornog ponašanja država u sajber prostoru, kao i razmotrila njihovu praktičnu primenu.

ANONIMNOST NA INTERNETU

Anoninmnost je od suštinske važnosti za zaštitu ljudskih prava. Sa pojavom Interneta postalo je jasno da značaj anonimnosti ne može da bude ograničen samo na slobodu pojedinaca koji komuniciraju međusobno, razmenjuju informacije i ideje, već i na zaštitu pojedinaca od nepotrebne i neprikladne kontrole.
Ipak ovo pravo na onlajn anonimnost, međunarodno pravo ne prepoznaje u potpunosti. Tradicionalno je zaštita anonimnosti onlajn više puta dovedena u vezu sa zaštitom prava na privatnost i ličnih podataka (vidi Član 12 UDHR, 17 ICCPR).
Dodatno moramo da napomenemo da je anonimnost jedna od ključnih koncepata zaštite slobode izražavanja, kao i prava na privatnost. Najjednostavije rečeno, anonimnost znači da niste identifikovani, i u ovom smislu predstavlja nešto kroz šta prolazimo u svakodnevnom životu, na primer, dok šetamo ili stojimo u redu sa nepoznatim ljudima.
Na ovaj način neka aktivnost može da bude anonimna iako je u isto vreme i javna.

Izvor: https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf

Opšte je prihvaćeno da okvir međunarodnog prava o zaštiti ljudskih prava, uključujući Univerzalnu deklaraciju o ljudskim pravima i Međunarodni pakt o građanskim i političkim pravima, ima svoju primenu u digitalnom prostoru. Ovu činjenicu je potvrdio Savet za ljudska prava (engl. HRC) rezolucijom A/HRC/20/L.13 koja kaže da 'ista prava koja ljudi imaju oflajn moraju da se poštuju onlajn'.[1] Ova rezolucija je izuzetno važna jer je njome prvi put jedan međunarodni organ izričito naglasio da se poštovanje ljudskih prava primenjuje u sajber prostoru.

Nakon Snoudenovih otkrovenja[2] UNGA je odlučila da postavi novog Specijalnog izvestioca za pravo na privatnost kako bi se detaljnije bavili pitanjem privatnosti u digitalnom dobu i stvorili bezbednije digitalno okruženje 2015. godine. Ovaj Specijalni izvestilac za pravo na privatnost ima mandat da organizuje državne posete, daje preporuke i prima pojedinačne žalbe.

Još jedna važna rezolucija UNGA-e je A/RES/57/239 koja govori o stvaranju jedne globalne kulture sajber bezbednosti koja prepoznaje sajber kriminal kao najveći problem za sajber bezbednost.[3]

Rukovodeća načela UN-a o biznisu i ljudskim pravima Human Rights[4] iz 2011. godine (poznata pod imenom Ragijevi principi, na engleskom 'Ruggie Principles') predstavljaju još jedan instrument UN-a koji određuje norme u sajber prostoru i nudi državama i biznisima smernice po pitanju zaštite ljudskih prava. Ragijevi principi se zasnivaju na

1 United Nations General Assembly, Human Rights Council on the promotion, protection and enjoyment of human rights on the Internet, (Generalna skupština Ujedinjenih nacija, Savet za ljudska prava o promociji, zaštiti i uživanju ljudskih prava na Internetu), IA/HRC/20/L.13, 29.06. 2012

2 The Guardian, The NSA files, (Gardijan, NSA dosijei), dostupno na https://www.theguardian.com/us-news/the-nsa-files

3 https://digitallibrary.un.org/record/482184?ln=en

4 OHCHR, Guiding Principle on Business and Human Rights, (OHCHR, Vodeći principi poslovanja i ljudskih prava), dostupno na https://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf

paroli UN-a 'Poštuj, zaštiti i izleči'. U uvodnom delu ovih rukovodećih načela navodi se da 'uloga poslovnih preduzeća kao specijalizovanih organa društva, koji obavljaju specijalizovane funkcije, zahteva od njih da se pridržavaju svih odgovarajućih zakona i poštuju ljudska prava'. [5]

Kada govorimo o regulisanju određenih vrsta nezakonitih govora na Internetu, posebno govora mržnje, izveštaj Visokog komesara UN-a za ljudska prava, koji je usvojio Savet za ljudska prava 2013.godine (poznat pod nazivom 'Rabatski akcioni plan'), navodi kriterijume koji služe za određivanje da li je nešto govor mržnje, a može takođe da da i smernice za onlajn carstvo [6].

STUDIJA SLUČAJA: RABATSKI AKCIONI PLAN

Rabatski akcioni plan sadrži test određivanja praga (iz šest delova) koji nam govori kako da procenimo težinu određenih izraza koji se smatraju kriivčnim prestupima. Ovih šest kriterijuma su: kontekst, govornik, namera, sadržaj i forma, opseg govora, verovatnoća, uključujući i pretnje.

Po pitanju elemenata 'konteksta' Rabatski akcioni plan konkretno kaže da je kontekst 'veoma važan kada procenjujemo da li neka određena izjava ili rečenica može da podstakne diskriminaciju, netrpeljivost ili nasilje protiv neke ciljne grupe, i može direktno da utiče na nameru ili uzrok. Analiza konteksta bi trebalo da postavi izrečeno u društveno politički kontekst koji preovladava u vreme kada je nešto rečeno i podeljeno, tj. prošireno'.

Izvor: https://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf

Različite UN agencije i kancelarije, kao što su Institut UN-a za istraživanje razoružanja (engl. UNIDIR), Institut UN-a za istraživanje međuregionalnog kriminala i pravosuđa i Kancelarija UN-a za drogu i kriminal (engl. UNODC), bave se problemima sajber bezbednosti, kao i Radna grupa za borbu protiv upotrebe interneta u terorističke svrhe koja je pod Operativnom grupom UN--a za primenu borbe protiv terorizma.[7]

Međunarodna telekomunikacijska unija (engl. ITU), agencija UN-a specijalizovana za telekomunikacije, bavi se sajber bezbednošću kao sastavnim delom svog mandata. U tu svrhu je ITU razvila modele zakona i profile sajber bezbednosti zemalja koji su javno dostupni i pružaju podršku zemljama članicama UN-a pri razvijanju delotvornih normativnih okrvira za sajber prostor.

5 https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf p 1

6 OHCHR, Rabat Plan of action, (OHCHR, Rabatski akcioni plan), dostupno na https://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf

7 United Nations Office on Drugs and Crime (2012): The use of the Internet for terrorist purposes, (UN Kancelarija za drogu i krminal (2012): Upotreba interneta u terorističke svrhe), dostupno na https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

STUDIJA SLUČAJA: PROJEKAT MEĐUNARODNE TELEKOMUNIKACIONE UNIJE KAO PODRŠKA PROCESU USLAĐIVANJA POLITIKA IKT-A U SUBSAHARSKOJ AFRICI (ENGL. HIPSSA)

HIPSSA je nastala kao rezultat zahteva od strane organizacija za ekonomsku integraciju Afrike, kao i drugih regionalnih regulatornih udruženja, upućenog ITU-u i Evropskoj komisiji kao molba za pomoć pri usklađivanju politika IKT-a i zakonodavstva u Subsaharskoj Africi.

HIPSSA je postala važna karika u lancu uspostavljanja globalnih panafričkih usklađenih politika i okvira IKT-a.

Izvor: https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx

Savet Evrope

Savet Evrope (engl. CoE) okuplja 47 zemalja članica. Njegova Konvencija o sajber kriminalu (poznata kao 'Budimpeštanska konvencija')[8] smatra se, za sada, najrelevantnijim međunarodnim pravnim instrumentom koji daje pravni okvir za borbu protiv sajber kriminala. Budimpeštanska konvencija je otvorena i sve zemlje članice Saveta Evrope mogu da joj pristupe kao i one koje to nisu. Do danas je Budimpeštansku konvenciju ratifikovala 61 država.[9] Ona je dopunjena Protokolom o ksenofobiji i rasizmu i prekršajima iz tih oblasti koji se počine preko kompjuterskih sistema.[10]

Važno je da istaknemo da Budimpeštanska konvencija pruža državama i spisak napada koji se smatraju prekršajima, a počinjeni su preko kompjutera, i proceduralne pravne alate za sprovođenje istraga o sajber kriminalu, kao i efektivno čuvanje elektronskih dokaza o počinjenim prekršajima, a omogućava i međunarodnu policijsku i sudsku saradnju po pitanju sajber krminala i razmene e-dokaza.

Dodatno je CoE sastavio Konvenciju o zaštiti pojedinaca i automatske obrade ličnih podataka (konvencija pod brojem CETS 108),[11] koja ima za cilj da 'zaštiti svakog pojedinca, bez obzira na njegovu nacionalnost ili mesto prebivališta, kao i obradu njihovih ličnih podataka i na taj način doprinese poštovanju njihovih ljudskih prava i fundamentalnih sloboda, a posebno prava na privatnost'.[12]

Ova Konvencija je prvi zakonski obavezujući međunarodni instrument u oblasti zaštite ličnih podataka. Ona nalaže svim stranama da obavezno preduzmu neophodne korake u okviru svog nacionalnog zakonodavstva i primene principe kako bi osigurali poštovanje osnovnih ljudskih prava svih svojih građana po pitanju obrade njihovih ličnih podataka.

8 Council of Europe, Convention on Cybercrime, (Savet Evrope, Konvencija o sajber kriminalu) CETS No. 185, dostupno na https://www.coe.int/en/web/cybercrime/the-budapest-convention

9 Napomena, Senegal je potpisnik Budimpeštanske konvencije; Tunis i Maroko su u procesu potpisivanja i ratifikacije Budimpeštanske konvencije.

10 Council of Europe, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, (Savet Evrope, Dopunski protokol Konvencije o sajber krminalu koji se odnosi na gonjenje dela rasizma i ksenofibije počinjenih preko kompjuterskih sistema), ETS No. 189, dostupno na https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

11 Council of Europe, Convention for the protection of individuals with regard to the processing of personal data, (Savet Evrope, Konvencija za zaštitu pojedinaca po pitanju obrade ličnih podataka), CETS No. 180, dostupno na https://www.coe.int/en/web/data-protection/home

12 Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, (Savet Evrope, Modernizovana konvencija za zaštitu pojedinaca po pitanju obrade ličnih podataka), dostupno na https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8

Konvencija broj 108 je ažurirana maja 2018.godine kako bi obuhvatila novine modernih tehnologija i u oblasti zaštite podataka. Do danas ju je ratifikovalo 53 zemalja članica Saveta Evrope, kao i one koje to nisu.[13]

Savet Evrope takođe nudi smernice i pomoć pri tumačenju ovih konvencija, kao i raznovrsne programe izgradnje kapaciteta poput GLACY+ programa koji pomaže državama da razviju efektivno zakonodavstvo za sajber prostor.[14] .

Budimpeštanska konvencija predstavlja samo jedan međunarodni pravni okvir kojim se regulišu pitanja sajber kriminala, ali je za zaštitu ljudskih prava posebno važna činjenica da se ona zasniva na pretpostavci da države imaju na snazi sva moguća pravna sredstva koji štite ljudska prava.

Ipak, zemlje koje nisu članice Saveta Evrope nemaju uvek iste strandarde i pravila poštovanja i čuvanja ljudskih prava

Afrička unija

Afrička unija je 2014.godine usvojila Konvenciju o sajber bezbednosti i zaštiti ličnih podataka (poznatu pod nazivom 'Malabo konvencija').[15] Ova konvencija ipak još nije stupila na snagu s obzirom na to da ju je usvojilo samo pet država članica Afričke unije (Senegal, Mauricijus, Gvineja, Namibija i Gana), a potpisalo devet država članica. Njen Član 25 (1) kaže da će 'svaka država potpisnica da usvoji odgovarajuće zakonodavne i/ili regulatorne mere koje se smatraju efektivnim i sadrže odredbe o značanjim krivičnim prestupima, koji utiču na poverljivost, integritet, dostupnost i opstanak informaciono-komunikacionih tehnoloških sistema, podataka koje oni obrađuju i mrežne infrastrukure koja leži u njihovoj osnovi, kao i delotovorne proceduralne mere za gonjenje i suđenje počiniocima prekršaja. Države potpisnice moraju takođe da imaju u vidu odabir jezika koji se koristi u međunarodnim najboljim praksama'.

STUDIJA SLUČAJA: KONVENCIJA AFRIČKE UNIJE O SAJBER BEZBEDNOSTI I BUDIMPEŠTANSKA KONVENCIJA

Budimpeštanska konvencija je trenutno jedini pravno obavezujući međunarodni pravni okvir za sajber bezbednost i ulogu država u toj areni. Iako ju je samo mali broj akričkih država direktno potpisao ili bio pozvan da joj se priključi, ona je predstavljala smernicu i uzor pri pisanju Konvencije o sajber bezbednosti Afričke unije. Ovo je jedan primer načina na koji šire međunarodne norme mogu da budu usvojene i prilagođene određenom regionalnom kontekstu.

Izvor: 'Comparative Analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime' (Komparativna analiza Malabo konvencije Afričke unije i Budimpeštanske konvencije i sajber kriminalu) Global Action on Cybercrime Extended. 20 (novembar, 2016), 3-5.

Ekonomska zajednica zapadno afričkih zemalja

Ekonomska zajednica zapadno afričkih zemalja (engl. ECOWAS) je usvojila Zakon o zaštiti ličnih podataka u okviru ECOWAS-a 2010.godine,[16] nastao pod uticajem Direktiva o zaštiti podataka Evropske unije, koji uređuje neophodni sadržaj zakona o privatnosti podataka i obavezuje države članice da uspostave ovlašćeno telo za zaštitu podataka.

13 Konvenciju broj 108 ratifikovali su Kabo Verde, Mauricijus, Senegal i Tunis.

14 Council of Europe, Global Action on Cybercrime (GLACY), (Savet Evrope, Globalne aktivnosti protiv sajber kriminala), dostupno na https://www.coe.int/en/web/cybercrime/glacyplus

15 African Union Convention on Cyber Security and Personal Data Protection, (Konvencija o sajber bezbednosti i zaštiti ličnih podataka Afričke unije), 27.06. 2014, dostupno na https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

16 ECOWAS, Supplementary Act on Personal Data Protection, (Zakon o zaštiti ličnih podataka), vidi http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

ECOWAS je takođe usvojila Direktivu o borbi protiv sajber kriminala (2011), kao i Zakon o elektronskim transakcijama u okviru ECOWAS-a[17] .

Organizacija za evropsku bezbednost i saradnju

Organizacija za evropsku bezbednost i saradnju (engl. OSCE) bavi se sajber/IKT bezbednosnim problemima, a posebno u svetlu borbe protiv terorizma i sajber kriminala. OEBS je 2013.godine usvojio mere izgradnje poverenja (engl. CBMs) za sajber prostor putem Odluke Stalnog saveta broj 1106, 3.decembra 2013. godine.[18] Ove mere imaju za cilj da smanje sukobe koji se javljaju kao posledica korišćenja informaciono-komunikacionih tehnologija.

OEBS je između ostalog odredio sledeće mere: razmenu informacija o sajber pretnjama, bezbednosti i upotrebi IKT-a, nacionalnim organizacijama strategijama i terminologiji; održavanje konsultacija kako bi se smanjio rizik od postojanja pogrešnih percepcija i javljanja mogućih tenzija; deljenje informacija o preduzetim merama koje omogućavaju otvoreno i bezbedno korišćenje interneta; razmenu osoba za kontakt, kao i korišćenje OEBS-a kao platforme za dijalog.

Ove mere ipak nisu pravno obavezujući instrument i njihova primena je na dobrovoljnoj bazi.

Organizacija američkih država

Organizacija američkih država (engl. OAS) je osnovala Radnu grupu za sajber kriminal već 1999. godine kao osnovni forum za 'jačanje međunarodne saradnje na temu prevencije, istraga i gonjenja sajber krminala, kao i omogućavanje razmene informacija i iskustava između njenih članova i davanja neophodnih preporuka za unapređivanje i obezbeđivanje aktivnosti u cilju borbe protiv ove vrste prestupa'.[19] Ova Radna grupa se sastaje dva puta godišnje i daje preporuke državama članicama.

OAS se bavi i sajber bezbednošću u širem smislu. Generalna skupština OAS-a je 2004. godine dala mandat Sekretarijatu OAS-ovog Među-američkog odbora za borbu protiv terorizma za sprovođenje Rezolucije AG/RES.2004 (XXXIV-O/04), pod nazivom 'Međuamerička integralna strategija borbe protiv pretnji sajber bezbednosti'. Glavni zadatak ovog Sekretarijata je da pruža pomoć prilikom osnivanja nacionalnih Timova za pružanje odgovora na kompjuterske bezbednosne incidente (engl. CSIRT), da pruža pomoć prilikom stvaranja mreže sastavljene od ovih CSIRT-ova i razvoja nacionalnih strategija sajber bezbednosti. Sekretarijat je od 2007.godine počeo da formira sveobuhvatne programe izgradnje kapaciteta u vidu radionica, tehničkih kurseva, razgovora o politikama, vežbi upravljanja krizama i razmene najboljih praksi.

17 ECOWAS, Economic Community of West African States (ECOWAS), Direktiva C/DIR.1/08/11 o borbi protiv sajber kriminala u okviru ECOWAS-a, 2011, dostupno na http://www.osiris.sn/Directive-C-DIR-1-08-11-du-19-aout.html i Član A/SA.2/01/10 o elektronskim transakcijama u okviru ECOWAS-a, 2010, dostupno na http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Electronic-Transaction-Act.pdf

18 OSCE Decision No. 1202, OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, (Odluka OEBS-a broj 1202, OEBS-ove mere izgradnje poverenja u cilju smanjivanja rizika od pojave konflikta kao posledica upotrebe IKT-a) PC.DEC/1202, 10.03.2016, dostupno na https://www.osce.org/pc/227281?download=true

19 http://www.oas.org/juridico/english/cyber_faq_en.htm#1

Šangajska organizacija za saradnju

Šangajska organizacija za saradnju (engl. SCO), međunarodna organizacija koja okuplja šest država članica (Kinu, Kazahstan, Kirgistan, Rusiju, Tadžikistan i Uzbekistan), usvojila je 2009.godine Sporazum između vlada zemalja članica SCO-a o saradnji na polju obezbeđivanja međunarodne informacione bezbednosti.[20] Četiri zemlje članice SCO-a su 2011. godine podnele Generalnoj skupštini UN-a nacrt Međunarodnog kodeksa ponašanja informacione bezbednosti, a 2015.godine je podnet novi nacrt[21].

STUDIJA SLUČAJA: NACRT MEĐUNARODNOG KODEKSA PONAŠANJA SCO-A 2015. GODINE

Sponzori ovog nacrta kodeksa, članice države SCO-a, kažu da im je namera bila 'da podstaknu međunarodnu debatu o međunarodnim normama informacione bezbednosti i tako pomognu da se postigne rani konsenzus o ovom pitanju'.

Neki analitičari kažu da ovaj nacrt kodeksa ističe suverenitet i teritorijalni integritet država u sajber prostoru i stavlja akcenat na obaveštajni rad, nacionalnu bezbednost i imperative stabilnosti režima, ali mu nedostaje posvećenost suštinskoj zaštiti ljudskih prava i uglavnom se bavi ograničavanjem slobode izražavanja koje države mogu da primene u skladu sa svojim zakonima. Takođe je potrebno da napomenemo da se ovaj nacrt kodeksa uopšte ne poziva na pravo na privatnost.

Izvor: https://citizenlab.ca/2015/09/international-code-of-conduct/

Azijsko- pacifička ekonomska saradnja

Azijsko-pacifička ekonomska saradnja (engl. APEC) je 2002.godine objavila Strategiju sajber bezbednosti APEC-a koja sadrži preporuke iz oblasti zakonodavstva, koje se odnose na sajber kriminal, bezbednosne i tehničke smernice, svesnosti javnosti, obuke i obrazovanja.[22] Limska deklaracija (2005) ima za cilj da unapredi informacione infrastrukture koje bi pomogle napretku informacionog društva.[23] Ova deklaracija govori i o bezbednosti mreže i o važnosti uspostavljanja pouzdanog, bezbednog i održivog onlajn okruženja i ima za cilj da osigura bezbednost informacija i mreže, da uskladi okvire za obezbeđivanje transakcija i komunikacija, kao i da se bori protiv sajber kriminala. Ovo sve više podrazumeva blisku saradnju sa privatnim sektorom i drugim međunarodnim organizacijama. APEC-ov TEL strateški akcioni plan od 2010. do 2015. godine ima za cilj da 'promoviše bezbedno, otporno i pouzdano IKT okruženje'

20 Agreement among Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security, (Sporazum između vlada zemalja članica SCO-a o obezbeđivanju međunarodne informacione bezbednosti), 2009, dostupno na https://unidir.org/cpp/en/organization-pdf-export/eyJvcmdhbml6YXRpb25fZ3JvdXBfaWQiOiIxMiJ9

21 Shanghai Cooperation Organisation, Draft International Code of Conduct, Letter dated 9. January 2015. to the United Nations General Assembly, (SCO, Nacrt međunarodnog kodeksa ponašanja od 9.januara.2015.godine poslatog Generalnog skupštini UN-a), A/69/723, dostupno na https://digitallibrary.un.org/record/786846?ln=en

22 APEC Cyber Security Strategy, (APEC-ova Strategija sajber bezbednosti), dostupno na https://www.ccdcoe.org/uploads/2018/10/APEC-020823-CyberSecurityStrategy.pdf

23 APEC, Lima Declaration, (APEC-ova Limska deklaracija), 2005, dostupno na https://www.apec.org/Meeting-Papers/Sectoral-Ministerial-Meetings/Telecommunications-and-Information/2005_tel

u sledećim ključnim oblastima: poboljšanju otpornosti kritične domaće infrastrukture, rukovođenju bezbednoćću i rizikom, izgradnji kapaciteta sajber bezbednosti, podizanju svesti o sajber bezbednosti, preduzimanju inicijativa sa industrijom po pitanju sajber bezbednosti, aktivnostima promovisanja bezbednog i sigurnog onlajn okruženja za ranjive grupe i internet privredu[24].

Asocijacija nacija jugoistočne Azije

Asocijacija nacija jugoistočne Azije (engl. ASEAN) koja okuplja deset država članica (Bruneje, Kambodžu, Indoneziju, Laos, Malaziju, Mijanmar (Burmu), Filipine, Singapur, Tajland i Vijetnam)) objavila je Odluku ministara spoljnih poslova o saradnji u cilju obezbeđivanja sajber bezbednosti i razgovarala o sajber bezbednosti u kontekstu borbe protiv terorizma i transnacionalnog kriminala[25].

Komonvelt nacija

SCO se odnosi na koncept 'internacionalne informacione bezbednosti', ističući značaj sadržaja kao jednog od izvora moguće bezbednosne pretnje

Komonvelt nacija se sastoji od 53 zemlje članice i usredsređena je na izgradnju kapaciteta, razmenu informacija i pružanje pomoći državama članicama Komonvelta prilikom sprovođenja pravnih okvira koji se tiču sajber kriminala. Postoje dve platforme u okviru Komonvelta nacija, a to su: Forum sajber bezbednosti i Inicijativa sajber bezbednosti koje rade pod upravom Telekomunikacijske organizacije Komonvelta nacija. Ova druga platforma je usvojila Komonvelt model sajber uprave,[26] koji je odobren Abujskom deklaracijom, u oktobru 2013. godine i pušten u rad na Forumu o sajber bezbednosti Komonvelta u Londonu, 2014. godine.[27]

Ovaj Komonvelt model sajber uprave[28] nudi nacrt niza principa koji bi trebalo da se uzmu u razmatranje kako bi dali doprinos bezbednom i uspešnom globalnom sajber prostoru; pružili podršku širem ekonomskom i društvenom napretku; primenjivali se pojedinačno ili kolektivno u borbi protiv sajber kriminala, sprovodili prava i ispunjavali obaveze u sajber prostoru

Evropska unija

Dokumenta koja je usvojila Evropska unija (engl. EU), a koja se tiču sajber bezbednosti su, ili pravno neobavezujuća (kao što su komunikacije), ili su različite vrste pravno obavezujućih dokumenata koji nameću obaveze državama članicama ili određenim pravnim licima.

24 https://ccdcoe.org/organisations/apec/

25 http://aseanregionalforum.asean.org/wp-content/uploads/2019/01/ARF-Statement-on-Cooperation-in-Ensuring-Cyber-Security.pdf

26 Commonwealth Cybergovernance Model, (Komonveltov model sajber upravljanja), dostupno na https://ccdcoe.org/uploads/2018/11/CommW-140304-CommonwealthCybergovernanceModel.pdf

27 Commonwealth Cybersecurity Forum in London in 2014, (Komonveltov Forum o sajber bezbednosti u Londonu 2014) dostupno na https://ccdcoe.org/uploads/2018/11/CommW-140304-CommonwealthCybergovernanceModel.pdf

28 https://ccdcoe.org/uploads/2018/11/CommW-140304-CommonwealthCybergovernanceModel.pdf

EU je 2013. godine objavila svoj prvi sveobuhvatni dokument, svoju Strategiju sajber bezbednosti, koja se odnosi na široki spektar sajber pretnji. EU je 2016. godine usvojila Direktivu o bezbednosti mreža i informacionih sistema (engl. NIS Directive).[29] Ova strategija izlaže viziju, uloge, odgovornosti i neophodne aktivnosti Evropske unije u domenu sajber bezbednosti. Važno je da napomenemo da ovaj dokument naglašava da centralizovani nadzor Evropske unije nije rešenje u kontekstu sajber bezbednosti i da bi stoga nacionalne vlade trebalo da ostanu glavna pravna lica zadužena za prevenciju i pružanje odgovora na sajber incidente na nacionalnom nivou.

Strategija sajber bezbednosti Evropske unije određuje rad prilikom razvijanja politika sajber odbrane i kapaciteta kao jedan od svojih ciljeva, a u skladu sa okvirom Zajedničke bezbednosne i odbrambene politike (engl. Common Security and Defence Policy) i daje spisak aktivnosti koje su neophodne za saradnju Evropske odbrambene agencije (engl. EDA) i država članica.

Digitalna agenda EU-e sadrži aktivnosti iz oblasti sajber bezbednosti i smatra da je poverenje u bezbednost Interneta od suštinskog značaja za živo digitalno društvo. Treba napomenuti da Evropska agenda o bezbednosti smatra sajber kriminal jednom od najvažnijih pretnji u porastu.

Strategija sajber bezbednosti EU-e naglašava da bi 'određeni ozbiljni sajber incidenti ili napadi mogli da budu osnova za zemlje članice da se pozovu na klauzulu solidarnosti EU-e (Član 222. Ugovora o funkcionisanju Evropske unije).

GDPR Evropske unije je stupio na snagu 25.05.2015. godine. (engl. General Data Protection Regulation).[30] Ova regulativa suštinski menja način na koji se rukuje podacima u svim sektorima, od zdravstva do bankarskog sektora, i ostalih. Važno je da istaknemo da se GDPR ne odnosi samo na organizacije u EU, već i izvan nje, ukoliko one nude robu i usluge ili kontrolišu ponašanje lica u zemljama EU-a.

Severno-atlantski savez

Prva politika sajber odbrane Severno-alantskog saveza (engl. NATO) je izašla 2008. godine. Na Lisabonskom samitu 2010. godine sajber odbrana je ušla u Strateški koncept NATO-a i deklaracija koja je usvojena na samitu predvidela je neophodnost ažuriranja Politike sajber bezbednosti iz 2011. godine i izradu pratećeg Akcionog plana iz 2012. godine.

Nova poboljšana Politika sajber bezbednosti odobrena je na Samitu u Velsu i kaže da član 5. (NATO) može da se primeni na ozbiljne digitalne napade na države članice.[31]

29 European Union, Directive on security of network and information systems, (EU, Direktiva o bezbednosti mreža i informacionih sistema), L 194/1, 2016, dostupno na https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

30 European Union General Data Protection Regulation, (EU GDPR), dostupno na https://eugdpr.org/the-regulation/gdpr-faqs/

31 North Atlantic Treaty, (NATO), 1949, dostupno na https://www.nato.int/cps/ie/natohq/official_texts_17120.htm

Ova politika dalje govori o boljoj razmeni informacija i pružanju međusobne pomoći između saveznika, poboljšanju obuke i vežbi, kao i nastavku saradnje sa sektorom industrije. Na Varšavskom samitu 2016. godine NATO je priznao sajber prostor domenom vršenja operacija i zatražio da se dodatno razvije NATO-EU saradnja iz sajber odbrane, kao i da se odvoji više resursa za izgradnju kapaciteta sajber odbrane. Ministri odbrane NATO zemalja članica su 2018. godine postigli dogovor o formiranju novog Sajber operativnog centra pri SHAPE-u kako bi pomogli proces integracije sajbera u planiranje i operacije NATO-a na svim nivoima.

U okiru NATO-a postoji Odbor za sajber odbranu (enlg. CDC), poznat pod starijim nazivom, Odbor za politiku odbrane i planiranje (sajber odbranu). Ovaj odbor je više savetodavno telo koje obavlja konsultacije sa državama članicama NATO-a i upravlja celokupnom internom sajber odbranom NATO--a. Kao dodatak tome postoji Odbor za rukovođenje sajber odbranom (engl. CDMB) koji radi pod pokroviteljstvom Uprave za nove bezbednosne probleme Vrhovnog štaba NATO-a (engl. Emerging Security Challenges Division) i okuplja predstavnike svih najvećih interesnih grupa iz oblasti sajber bezbednosti u okviru NATO-a. Važno je da napomenemo da je CDMB zadužen za strateško planiranje i izdavanje izvršnih direktiva koje se tiču NATO mreža, kao i za potpisivanje Memoranduma o razumevanju sa državama članicama u cilju omogućavanja razmene informacija i koordinisane pomoći.

GDPR se odnosi na sve kompanije koje obrađuju i drže lične podatke lica koja žive u EU, bez obzira na lokaciju same kompanije.

Dodatno, Odbor NATO-a za konsultacije, kontrolu i komandu (engl. NC3) glavni je odbor za tehničke konsultacije, kao i aspekte sprovođenja sajber odbrane.

Grupa Sedam (G7)

G7 je neformalna grupa koja okuplja sedam država (Kanadu, Francusku, Nemačku, Italiju, Japan, Ujedinjeno Kraljevstvo i SAD, plus EU koja ima status posmatrača) sastaje se redovno kako bi se razgovaralo o važnim političkim i ekonomskim pitanjima. G7 je od 2016.godine uradila veliki broj dokumenata koji se tiču sajber bezbezbednosti, koja zauzima važno mesto u raznim deklaracijama usvojenim na njihovim samitima[32].

2. Inicijative nedržavnih aktera

S obzirom na to da države nisu voljne da iskažu svoje opinio iuris i državne prakse u sajber prostoru, ne postoji zajedničko viđenje kako bi se međunarodno pravo primenjivalo u sajber prostoru, što sa druge strane ostavlja prostor nedržavnim akterima da krenu sa ispunjavanjem ove praznine. Privatne IKT kompanije i organizacije civilnog društva posebno su proaktivne prilikom predlaganja normi u sajber prostoru koje se tiču ljudskih prava, a imaju za cilj da doprinesu sigurnijem, bezbednijem, i pouzdanijem Internetu.

Grupa akademika i stručnjaka za međunarodno pravo napravila je Talinski priručnik o međunarodnom humanitarnom pravu primenjivom na sajber operacije.[33] Ovaj dokument, koji je prilično akademskog karaktera, ipak potvrđuje osnovne principe međunarodnog humanitarnog prava, kao što su princip razlikovanja, proporcionalnosti i neophodnosti u sajber prostoru. Dodatno je ova grupa stručnjaka objavila Talinski priručnik 2.0 koji se bavi primenom zakona u sajber prostoru u miru[34].

INFOBOX: SMERNICE ZA ZAŠTITU LIČNIH PODATAKA U AFRICI

Društvo za Internet i Komisija Afričke unije doneli su Smernice za zaštitu ličnih podataka u Africi u maju 2018. godine na Afričkom samitu o Internetu u Dakaru, glavnom gardu Senegala.

Ove smernice daju 18 preporuka koje su skoncentrisane oko sledeća tri pitanja:

1. preporuke za izgradnju poverenja, privatnosti i odgovornog korišćenja ličnih podataka;
2. preporuke za aktivnosti koje mogu da preduzmu vlade i donosioci politika, vlasti zadužene za zaštitu podataka, kontrolori podataka, kao i oni koji ih obrađuju;
3. preporuke rešenja za veći broj interesnih grupa, dobrobit digitalnih građana i mere koje to omogućavaju i čine održivim.

Izvor: https://www.internetsociety.org/blog/2018/05/the-internet-society-and-african-union-commission-launch-personal-data-protections-guidelines-for-africa/

32 Grupa 7, Charlevoix G7 summit communique, dostupno na https://www.consilium.europa.eu/en/press/press-releases/2018/06/09/the-charlevoix-g7-summit-communique/

33 Tallinn Manual, dostupno na https://ccdcoe.org/research/tallinn-manual/

34 Tallinn Manual 2.0 Factsheet, dostupno na https://www.almendron.com/tribuna/wp-content/uploads/2018/03/ccdcoe-tallinn-manual-onepager-web.pdf

STUDIJA SLUČAJA: ZNAČENJE 'ORUŽANOG NAPADA', 'UPOTREBE SILE' U SAJBER PROSTORU I PREMOŠĆAVANJE JEZIČKE DILEME IZMEĐU PRAVA, POLITIKA I TEHNIČKE ZAJEDNICE

Važno je da razlikujemo režime međunarodnog prava: (i) ius ad bellum (koji upravlja onda kada države mogu da odluče da primene silu kao instrument svoje nacionalne politike) i (ii) ius in bello (međunarodno humanitarno pravo koje donosi pravila o načinu na koji se mogu voditi operacije tokom oružanog napada).

U kontekstu ius ad bellum, a na osnovu Člana 51. Povelje UN-a, oružani napad povlači za sobom samoodbranu. Stoga je goruće pitanje odrediti kada jedna sajber operacija predstavlja oružani napad na koji država ima zakonski prava da odgovori sajber ili kinetičkom akcijom na nivou upotrebe sile. Akcenat je ovde na terminu 'oružani' s obzirom na to da Međunarodni sud pravde u slučaju Nikaragve kaže da 'postoje mere koje nisu oružani napad, ali ipak mogu da sadrže elemente upotrebe sile'. Kao posledica toga, države mogu da se suoče sa sajber operacijom koja sadrži elemente upotrebe sile, ali da ne budu u stanju da se odbrane s obzirom na to da sajber operacija ne spada u oružani napad. Kako bi rešili ovu dilemu, veliki broj stručnjaka za međunarodno pravo zalaže se za tumačenje 'oružanog napada' u sajber prostoru kao napada koji dovodi do istih posledica kao kinetički (fizičke posledice).

U kontekstu ius in bello, neophodno je da postoji napad pre primene međunarodnog humanitarnog prava (engl. IHL), koji se definiše tako što se 'napad' tumači preko posledica koje je izazvao.

Majkrosoft, privatna transnacionalna korporacija, predložila je u februaru, 2017. godine državama da usvoje 'Digitalnu ženevsku konvenciju' koja određuje norme za sajber prostor u miru. Majkrosoft redovno objavljuje svoje politike i blogove koji imaju za cilj da doprinesu izgradnji poverenja između različitih interesnih strana u sajber prostoru. Ipak, iako države, uopšteno govoreći, pozdravljaju proaktivne inicijative nedržavnih aktera, postoji i dalje određena doza skepticizma u odnosu na njihovu uspešnost.[35]

Istovremeno IKT kompanije sve više vrše pritisak na države da uspostave regulativu nad određenim malicioznim ponašanjima u sajber prostoru. Na primer, Majkrosoft je tražio od američkog Kongresa da usvoji regulativu o ograničavanju primene tehnologije za prepoznavanje lica[36].

Postoje i drugi pravno neobavezujući instrumenti, kao što su Manilski principi posredničke odgovornosti,[37] koji daju smernice državama po pitanju politika upravljanja

35 Microsoft Policy Paper, A Digital Geneva Convention to protect cyberspace, (Politika Majkrosofta, Digitalna ženevska konvencija o zaštiti sajber prostora), dostupno na https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH ; videti Smernice Majkrosofta o sajber bezbednosti), dostupno na https://www.microsoft.com/en-us/cybersecurity/default.aspx

36 Nataša Singer, Nju Jork Tajms (13.06.2018): Majkrosoft traži od Kongresa da uredi korišćenje prepoznavanja lica, dostupno na https://www.nytimes.com/2018/07/13/technology/microsoft-facial-recognition.html

37 Manila Principles on Intermediary Liability, (Manilski principi o odgovornosti posrednika), dostupno na https://www.manilaprinciples.org/

pravnom odgovornošću posrednika za sadržaj koji se postavlja na njihovim platformama. Nedržavni akteri, posebno IKT kompanije i organizacije civilnog društva, postaju proaktivnije prilikom predlaganja normi koje imaju primenu u sajber prostoru. Majkrosoft poslednjih nekoliko godina vodi u ovome[38].

Organizacije civilnog društva su takođe postale aktivnije i angažovanije oko popunjavanja vakuma koji države ostavljaju u sajber prostoru, predlažući norme koje imaju za cilj promovisanje ljudskih prava u sajber prostoru. Primer za to je Član 19. jedne nevladine organizacije iz Londona, koja podržava (zajedno sa velikim brojem drugih NVO-a) Kamdenske principe slobode izražavanja i jednakosti na Internetu.[39] Dodatno su usvojeni i drugi pravno neobavezujući instrumenti kao što su Manilski principi o posredničkoj odgovornosti.

Inicijativa globalne mreže je inicijativa koja uključuje veći broj interesnih grupa koje rade na razvijanju globalnih standarda za Internet. Njeni Principi slobode izražavanja i privatnosti predstavljaju smernice i određuju pravac za IKT industriju i njene strane po pitanju zaštite i unapređivanja ljudskih prava širom sveta[40].

Kada govorimo o zaštiti od nasilnog ekstremizma na Internetu, jedna koalicija sastavljena od kompanija društvenih medija, tačnije Fejsbuka, Tvitera, Jutjuba i Majkrosofta, priključila se Globalnom internet forumu za borbu protiv terorizma,[41] u okviru koga ovi divovi interneta razvijaju normativne standarde kako bi regulisali probleme nasilnog ekstremizma na svojim platformama.

ODGOVORNOST POSREDNIKA

Sva komunikacija koja se odvija na internetu dešava se iz pomoć posrednika. Postoji veliki broj različitih tipova posrednika s obzirom na samu složenost Interneta, a to su:

- oni koji su zaduženi za pružanje usluga Interneta (engl. Internet service providers (ISPs)) i koji omogućavaju pristup internetu;
- oni koji su zaduženi za veb-sajtove (engl. Web hosting providers ('hosts')), a to može da bude bilo koja osoba ili kompanija koja kontroliše veb-sajt ili veb-stranicu i omogućava bilo kojoj trećoj strani da postavi ili skine sadržaj;
- platforme društvenih medija, kao što su Fejsbuk, Tviter, Jutjub, i dr. koji ohrabruju pojedince da se povežu i uspostave interakciju sa drugim korisnicima i dele sadržaj;
- pretraživači, kao što je Gugl, koji su softverski programi i koriste algoritme kako bi uzeli podatke, fajlove ili dokumenta koja dobiju svojom pretragom.

Ovo su posrednici koji omogućavaju pristup internetu, društvene mreže i pretraživači. Odgovornost posrednika se odnosi na politike koje upravljaju pravnom odgovornošću posrednika za saržaj ovih vrsta komunikacija. Izvor: https://www.manilaprinciples.org/#:~:text=Intermediaries%20should%20be%20shielded%20from,precise%2C%20clear%2C%20and%20accessible.&text=Intermediaries%20must%20not%20be%20held%20liable%20for%20failing%20to%20restrict%20lawful%20content

Uopšteno govoreći, privatne IKT kompanije bi trebalo da preduzimaju delotvornu, proaktivnu i inkluzivnu procenu poštovanja ljudskih prava, uključujući i smislenu saradnju i razgovor sa pojedincima čija ljudska prava mogu da budu ugrožena od strane privatnih IKT kompanija.

Vodeći principi poslovanja i ljudskih prava (engl. GPBHR) nalažu postojanje korporativne odgovornosti u poštovanju ljudskih prava. Ovo znači da IKT kompanije treba da uzmu u obzir pitanja koja su specifična za različite grane industrije, kao što su sloboda izražavanja, privatnost i bezbednost. Važno je napomenuti da neka od najvažnijih pitanja procene i dubinske analize proizilaze iz načina korišćenja proizvoda kompanije, usluga, tehnologija i aplikacija od strane korisnika, kao i rada vlada na ograničavanju tih korisničkih prava.

38 Microsoft policy paper, A Digital Geneva Convention to protect cyberspace, (Politika Majkrosofta, Digitalna ženevska konvencija o zaštiti sajber prostora dostupno na https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace

39 Član 19, The Camden Principles on Freedom of Expression and Equality, (Kamden principi slobode izražavanja i jednakosti), dostupno na https://www.article19.org/data/files/pdfs/standards/the-camden-principles-on-freedom-of-expression-and-equality.pdf

40 Više informacija o Inicijativi globalne mreže je dostupno na https://globalnetworkinitiative.org/

41 Google public policy, Update on the Global Internet Forum to Counter Terrorism, (Javna politika kompanije Gugl, Ažurirani podaci na Globalnom Internet forumu o borbi protiv terorizma), 4.12.2017, dostupno na https://www.blog.google/around-the-globe/google-europe/update-global-internet-forum-counter-terrorism/

Zaključak

- Neosuđivanje i praznine u zakonu u bilo kojoj zemlji predstavljaju utočište za prestupnike što može da utiče na druge zemlje, globalno gledano.
- Razlike u osuđivanju i gonjenju predstavljaju izazov za međunarodnu saradnju po pitanju krivičnih prestupa iz oblasti sajber kriminala, a posebno kada govorimo o principima dvostrukog kriminaliteta.
- Komparativna analiza prekšaja iz domena sajber kriminala može da istraži dobre prakse koje države primenjuju prilikom pisanja svojih nacionalnih zakona, u skladu sa sve većim brojem međunarodnih standarda iz ove oblasti.

Izvori

https://manypossibilities.net/african-undersea-cables/

https://socialsciences.exeter.ac.uk/media/universityofexeter/collegeofsocialsciencesandinternationalstudies/lawimages/research/Schmitt_-_Virtual_Disenfranchisement_ECIL_WP_2018-3.pdf

POGLAVLJE 4

PRIMENA MEĐUNARODNIH I REGIONALNIH NORMI I STANDARDA U NACIONALNOM KONTEKSTU

CILJEVI

Ovo poglavlje istražuje kako međunarodni i regionalni pravni okviri iz prethodnog poglavlja, kao i druge norme u sajber prostoru mogu da se primene na nacionalnom nivou posebno preko odgovarajućeg zakonodavstva, politika i strategija.

U ovom poglavlju ćemo naučiti da:

- bolje razumemo okvire i druge norme u sajber prostoru i njihovu primenu u nacionalnom kontekstu;
- bolje shvatamo neophodnost nacionalnog zakonodavstva, politika i strategija u sajber prostoru;
- bolje napišemo ili dopunimo nacionalno zakonodavstvo, politike i strategije koje se tiču sajber prostora, na osnovu dobrih praksi USB.

Uvod

Pojedinci, vlade i kompanije sve više koriste sajber prostor za preuzimanje informacija, obezbeđivanje i prijem javnih i privatnih usluga i za održavanje operativnih procesa. Ova činjenica o sve većoj upotrebi sajber prostora govori nam i o podložnosti svih ovih aktera većem broju sajber prekšaja i napada što može da ugrozi ljudska prava, državnu i ljudsku bezbednost.

Određene norme za bezbedno sprovođenje praksi i opšti okvir zakonskih (očekivanja) prava u sajber prostoru uspostavljeni su na međunarodnim i regionalnim nivoima. Sada se sve veća pažnja usmerava na potrebu usaglašenih i holističkih nacionalnih pristupa prilikom rešavanja problema u sajber prostoru. Jačanje otpornosti u sajber prostoru ukazuje na postojanje delotvornog državnog zakonodavstva, politika i strategija koje se sve više pokazuju neophodnim kako bi se zaštitili podaci i informacije koje se prebacuju i koriste u sajber prostoru i povećala bezbednost građana u njemu.

Međunarodni i regionalni okviri o kojima smo govorili u prošlom poglavlju, a koji se sastoje od rezolucija, izveštaja, konvencija i sporazuma o ljudskim pravima i koji regulišu sajber prostor, postavili su set normi koje bi zemlje trebalo da ispoštuju prilikom uređivanja svog zakonodavstva, politika i strategija po pitanju sajber prostora i sajber bezbednosti. Kao dodatak tome, privatne kompanije i nevladine organizacije su tražile način da prošire ove gore pomenute okvire kako bi detaljni pristupi sajber bezbednosti bili uvršteni. Države mogu da uzmu u obzir sve ove različite elemente kako bi uspostavile jednu holističku upravu sajber prostorom i sajber bezbednošću koja se zasniva na principima dobrog upravljanja sektorom bezbednosti.

Sledeće dobre prakse naglašavaju ključne regulatorne aspekte kojima bi države trebalo da se pozabave i ojačaju kada kreiraju ili menjaju državne strategije sajber bezbednosti.[1]

Štaviše, nacionalne politike i strategije bi trebalo da obuhvate međunarodno stanovište ili da ih dopune politikama i strategijama koje su usredsređene posebno na međunarodnu saradnju, tako da sajber regulativa i sajber bezbednost ne budu ograničeni državnim granicama.

1 Cybersecurity Policy Framework. A Practical guide to the development of national cybersecurity policy. (Okvir politike sajber bezbednosti. Praktični vodič za razvoj nacionalne politike sajber bezbednosti), Microsoft, 2018

Dobra praksa 1: Vlade bi trebalo da razviju i usvoje nacionalne zakone, politike i strategije u cilju regulisanja sajber prostora.

Iako je sajber prostor u praksi jedan globalni medij, pravno govoreći, na državama je da sprovode obaveze njegovog regulisanja i obezbede dobro upravljanje s obzirom na to da ne postoji međunarodna upravna struktura.[2] Takođe, važno je napomenuti da „ista prava koja ljudi imaju oflajn moraju da budu zaštićena onlajn."[3] Stoga, ukoliko dozvolimo IKT kompanijama da rade bez dovoljno regulatornih okvira, dovešćemo do postojanja praksi koje su odvojene od javnog interesa i potencijalno krše ljudska prava.[4] Države zato kao primarni nosioci obaveza zaštite ljudskih prava i čuvari javnog interesa treba da imaju u vidu najnovija tehnološka dostignuća kao i da ih uvrste u svoje zakone kako bi ograničili prostor za moguće negativne posledice delovanja privatnog sektora. Nacionalno zakonodavstvo, politike i strategije, kao i uloga sektora bezbednosti u regulisanju sajber prostora i osiguravanju sajber bezbednosti su neophodne za sprovođenje praksi dobre uprave.

Međunarodni i regionalni okviri i norme su opštiji po prirodi dok nacionalno zakonodavstvo, politike i strategije omogućavaju bavljenje nacionalnim potrebama i specifičnim osobinama sajber prostora i sajber bezbednosti.

Međutim, oslanjanje samo na okvire i norme koje su uspostavljene na međunarodnom i regionalnom nivou, ne garantuje da druge države neće kršiti ove pravno neobavezujuće principe, niti se time osigurava da će ih poštovati privatni i javni akteri u okviru jedne države.[5] Uspostavljanje ili izmena zakonodavstva, politika i strategija koje se odnose na upravljanje sajber prostorom i sajber bezbednošću može da bude sveobuhvatniji i kohezivniji način koji će obezbediti poštovanje zakona i ljudskih prava u sajber prostoru u datoj državi.

Tokom pisanja zakonodavstva koje se odnosi na sajber kriminal trebalo bi voditi računa da:

- bude dovoljno (tehnološki) neutralno kako bi pratilo neprestani razvoj tehnologije i kriminala, jer u suprotnom rizikuje da postane zastarelo već u trenutku stupanja na snagu;
- zakon bude sproveden, a lica koja imaju ovlašćenje da ga sprovode budu zaštićena kako bi se osiguralo poštovanje vladavina prava i ljudskih prava;
- bude dovoljno usaglašen ili u najmanju ruku kompatibilan sa zakonima drugih zemalja kako bi bila moguća međunarodna saradnja, na primer, pri ispunjavanju uslova isporučivanja počinilaca.

2 ITU National Cybersecurity Strategy Guide 26. (ITU Nacionalna strategija sajber bezbednosti Vodič 26)

3 United Nations Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, A/HRC/20/L.13, 29 June 2012, para. 1. (Savet Ujedinjenih nacija za ljudska prava, Rezolucija o promociji, zaštiti i uživanju ljudskih prava na Internetu, 29.06.2012. stav 1.)

4 Mihr, Anja, Good Cyber Governance: The Human Rights and Multi-Stakeholder Approach. Georgetown Journal of International Affairs, (2014): 34, (http://www.jstor.org/stable/43773646). (Dobra uprava sajberom: Ljudska prava i pristup iz ugla većeg broja učesnika)

5 Wolfgang Ischinger, Foreword in International Cybersecurity Norms: Reducing Conflict in an Internet-dependent World, Microsoft (2014), 1. (Uvod u međunarodne norme sajber bezbednosti: Smanjivanje konflikta u svetu zavisnom od interneta)

PRIMERI DOBRE PRAKSE

Sajber kriminal je ključna oblast za koju su nacionalno zakonodavstvo i politike od suštinske važnosti. Afričke države prilikom spremanja zakonodavstva o sajber kriminalu mogu da koriste smernice, naročito Konvencije Afričke unije o sajber bezbednosti i zaštiti ličnih podataka koja je usvojena u Malabou, juna, 2014.godine.[6]

Od 1997. godine Alžir je izuzetno napredovao u obezbeđivanju sredstava za borbu protiv sajber krminala. Rezultat toga je zakonodavstvo koje je u velikoj meri prilagođeno borbi protiv kriminala i u skladu sa mnogim osnovnim principima iako nije bez svojih slabosti. Alžirski zakon je preuzeo većinu odredbi iz Budimpeštanske konvencije uz određene jezičke izmene u pojedinim slučajevima. Odnosi se na sledeće prekršaje: neovlašćeni pristup i zadržavanje u sistemu; presretanje komunikacije i reči koje su razmenjene u privatnom razgovoru ili u poverenju; brisanje ili izmenu podataka iz sistema nakon neovlašćenog pristupa ili zadržavanja; promenu funkcionisanja sistema nakon neovlašćenog pristupa ili zadržavanja; zloupotrebu elektronskih uređaja; dečju pornografiju; kao i druge prestupe koji se odnose na prava intelektualne svojine.

Izvor : (https://www.coe.int/en/web/octopus/)

Dobra praksa 2: Vlade bi trebalo da ažuriraju nacionalna zakonodavstva u skladu sa trenutnim izazovima i problemima u sajber prostoru

Pri pisanju i usvajanju nacionalnog zakonodavstva koje se odnosi na sajber prostor i sajber bezbednost (bez obzira da li ažuriramo postojeće ili stvaramo novo), kreatori zakona i politika moraju da imaju na umu određen broj trenutnih izazova i problema.

Kao prvo, inovacije u sajber prostoru napreduju mnogo brže nego što to mogu da prate nacionalni zakonodavni procesi. Zbog toga čak i najmodernije sajber zakonodavstvo može – kao što najčešće i biva – da zaostaje za novim tehnologijama. Kao drugo, donošenje zakona koji upravljaju sajber prostorom zahteva obimna znanja i stručnost iz oblasti informacionih tehnologija lica koja se time bave, kojih nema mnogo u javnom sektoru s obzirom na to da su mnogo bolje plaćeni u privatnom. Kao treće, čak i kada državni zakonodavac uspe da usvoji odgovarajuće zakone koji upravljaju sajber prostorom, transnacionalni karakter sajber problema usložnjava i komplikuje primenu domaćih zakona i čini je ponekad nemogućom.

Brzi napredak tehnoloških inovacija je direktno suprotan sporim i često razvučenim procesima usvajanja nacionalnog zakondavstva.[7] Upravo iz ovog razloga se veliki broj tehnologija i sajber alatki koristi bez neophodne pravne regulative. Jedan tipičan primer ovog regulatornog vakuma je upotreba veštačke inteligencije (engl. AI). I dok velika

6 African Union Commission and Symantec, Cyber crime and cyber security trends in Africa Report (Komisija Afričke unije i Simantek, sajber kriminal i trendovi sajber bezbednosti u Afričkom izveštaju (2017) https://thegfce.org/wp-content/uploads/2020/06/CybersecuritytrendsreportAfrica-en-2-1.pdf

7 European Court of Auditors, Challenges to effective EU cybersecurity policy – Briefing Paper, (Evropski revizorski sud, Izazovi uspešne politike sajber bezbednosti EU-e, izveštaj) (2019.): 18, (https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf).

većina država nije uspela da usvoji odgovarajuće zakonodavstvo koje bi regulisalo sadržaj koji postavljaju kompanije društvenih medija uz angažovanje živih moderatora sadržaja, alati koji rade uz pomoć veštačke inteligencije su već u upotrebi i menjaju ljude na ovim poslovima[8].

Bez obzira na sve gore navedeno države ne žele da donose zakone po ubrzanim i nekoordinisanim procedurama. Javnost je zabrinuta zbog brzog tehnološkog napretka što može da motiviše političare da usvoje zakone kako bi pokazali svoje sposobnosti i opravdali rad državnih institucija. Veliki broj vanredno usvojenih normi može da ima više štete nego koristi. Bolje je pustiti privatne kompanije da rade bez upotpunjene pravne regulative dok se istovremeno nove tehnologije testiraju. Upravo iz ovog razloga bi države trebalo da posmatraju nove tehnologije i otkriju nove trendove, ali da donose zakone tek nakon pažljivog i zajedničkog učešća u procesu svih zainteresovanih strana, uključujući privatni sektor i civilno društvo.

Štaviše, kada usvajaju zakone koji uređuju ova pitanja, države bi trebalo da izbegavaju da budu previše preskriptivne s obzirom na to da bi to moglo da uspori proces inovacija i istraživanja, kao i da demotiviše manje IKT kompanije na tržištu, koje neće biti u stanju da ispune visoke standarde takvog previše preskriptivnog zakonodavstva. Imajući ovo na umu, države bi trebalo da razmotre i druge stvari izvan samog zakonodavstva kada donose odluku o tome da li da usvoje zakon o nekom pitanju u vezi sa sajberom. Na primer, ponekad usvajanje neobavezujućih pravila i praksi ponašanja ili niza principa u vidu smernica može da bude dovoljno kako bi se ispunio željeni cilj pravne regulative. Isto tako lakše je izmeniti i dopuniti neobavezujuće pravne instrumente koje bi imale mogućnost da bolje odražavaju najnovije trendove tehnološkog razvoja.

8 United Nations General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/73/348, 29 August 2018, para. 18. (Generalna skupština Ujedinjenih nacija, Izveštaj specijalnog izvestioca o promovisanju i zaštiti prava na slobodu mišljenja i izražavanja, 29.08.2019. pasus 18.)

PRIMERI DOBRE PRAKSE

U Gani je posebna regulativa za bankarske i finansijske institucije, sektora koji je prvi na udaru sajber kriminala, usvojena 2018.godine putem sajber bezbednosne Direktive za finansijske institucije banke Gane. Direktiva nalaže aktivno učešće viših izvršilaca i odbora u cilju ojačanja sajber bezbednosti. Sve banke u zemlji moraju da postave službenika zaduženog za sajber i informativnu bezbednost (engl. CISO) koji bi trebalo da savetuje više rukovodioce i odbor po pitanju problema sajber bezbednosti, kao i da formuliše adekvatne mere kako bi mogli da rukovode bezbednosnim rizicima po sajber i informativnu bezbednost.

(Izvor: https://www.bog.gov.gh/wp-content/uploads/2019/09/CYBER-AND-INFORMATION-SECURITY-DIRECTIVE.pdf)

Mnoge afričke privrede su ojačale mere primene zakona. U Južnoj Africi Zakon o zaštiti ličnih informacija (engl. POPI) iz 2013.godine omogućio je stvaranje Regulatora informacija kako bi se osigurala privatnost podataka. Regulator informacija je 2017. godine započeo istragu o najvećem kršenju zaštite podataka u zemlji, jer je ukradeno više od 30 miliona ličnih podataka građana. Ova agencija je takođe uputila formalne zahteve uključenim kompanijama tražeći objašnjenje.

(Izvor: https://www.justice.gov.za/inforeg/)

Dobra praksa 3: Vlade bi trebalo da unaprede stručna znanja iz oblasti sajbera.

Manjak IT ekspertize i znanja u državnom sektoru je još jedna ozbiljna prepreka za države kod usvajanja zakonodavstva koje uređuje pitanja iz oblasti sajbera.[9] Jedino rešenje ovog problema je da države pronađu načine da prikupe više stručnih znanja iz ove oblasti. Postoji mnogo mogućnosti za ostvarenje ovog cilja, a najdirektiniji bi bio da država zaposli neophodan broj službenika sa IT znanjem. Ipak države često imaju finansijska ograničenja i ograničenja drugih resursa u odnosu na privatne IKT kompanije i imaju problem da privuku i zadrže stručnjake koji se bave visokoprofilnim problemima kao što su sajber bezbednost, veštačka inteligencija ili analitika podataka.

Delimično rešenje se može naći preko alternativnih regulatornih dogovora, koji bi omogućili pristup stručnjacima iz privatnog sektora tako što bi im dozvolili da u određenoj meri učestvuju u regulatornom procesu pri čemu bi država zadržala ključnu odgovornost. S obzirom na to da privatne kompanije imaju ekspertizu na visokom nivou i neophodne tehničke informacije o pitanjima koja se tiču sajber prostora, pravila usvojena u saradnji sa privatnim sektorom mogu da pomognu da se premosti tradicionalni jaz između napretka tehnologije i nivoa nacionalnog zakonodavstva. Ovakve koregulatorne šeme bi takođe bile mnogo manje politički obojene od samih nacionalnih zakonodavnih procesa.

9 Raymond, Mark, Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot, Strategic Studies Quarterly10, no. 4 (2016): 137, (http://www.jstor.org/stable/26271532). (Rukovođenje decentralizovanom sajber upravom. Odgovornost za reagovanje i rešavanje problema)

PRIMERI DOBRE PRAKSE

Nacionalna sajber stručna znanja su unapređena u saradnji sa privatnim sektorom i stranim multinacionalnim kompanijama[10].

U Keniji su sajber bezbednosne inicijative koje potiču od privatnog sektora dovele do uspostavljanja Centra sajber potapanja (engl. Cyber Immersion Centre) u Najrobiju, marta 2018. godine, od strane Serianua, panafričke konsultantske firme, koja se bavi sajber bezbednošću i biznisom. Ovaj Centar obezbeđuje takvo okruženje firmama u kome mogu da vrše eksperimente i testiraju svoje kapacitete za sajber bezbednost. Takođe, pruža obrazovne programe u cilju razvijanja profesionalaca iz sajber bezbednosti. Sličan centar je otvoren i na Mauricijusu sredinom 2017.godine.

(Izvor: https://www.serianu.com/acic.html)

U Nigeriji se Majkrosoft udružio sa kompanijom Paradigm Initiative Nigeria (engl. PIN) kako bi učio Nigerijce o sajber krivičnim prestupima i tako stvorio ekonomske prilike. Nigerijska Komisija za ekonomski i finansijski kriminal (engl. EFCC) je objavila oktobra 2009.godine da je ugasila oko 800 veb-sajtova koji su dovedeni u vezu sa sajber kriminalom i uhapsila 18 sajber kriminalnih bandi. EFCC je napomenula da mu je „pametna tehnologija" koju je obezbedio Majkrosoft pomogla u tome.

(Izvor: https://paradigmhq.org/about/)

Dobra praksa 4: Vlade bi trebalo da razviju i ažuriraju zakone koji štite privatnost i lične podatke.

Zaštita privatnosti i ličnih podataka je od izuzetne važnosti za sajber bezbednost i jedna je od oblasti u kojoj je učinjen konkretan napredak po pitanju primene prava na privatnost i zaštite ličnih podataka, posebno u EU. Opšta uredba o zaštiti ličnih podataka Evropske unije (engl. GDPR – vidi Poglavlje 3) koja je stupila na snagu maja, 2018.godine dovela je do stvaranja jednog regionalnog regulatornog režima sa ciljem davanja kontrole pojedincima nad njihovim ličnim podacima. Ova uredba je povukla za sobom i veliki broj zakona o zaštiti privatnosti i ličnih podataka na nacionalnom nivou.

Afrička unija je 2014.godine usvojila Malabo konvenciju o sajber bezbednosti i zaštiti ličnih podataka (vidi Poglavlje 3). Ova konvencija još uvek nije stupila na snagu. Iz ovog razloga je Budimpeštanska konvencija trenutno jedini pravno obavezujući međunarodni zakonski okvir koji pokriva teme sajber bezbednosti, sajber prostora i uloge države u ovim oblastima. Iako je samo mali broj afričkih država direktno potpisao ili bio pozvan da pristupi, koristi se kao smernica za stvaranje Konvencije o sajber bezbednosti Afričke unije.

10 Nir Kshetri, Cybercrime and Cybersecurity in Africa, Journal of Global Information Technology Management, (2019), 77-81, DOI: 10.1080/1097198X.2019.1603527 (Sajber kriminal i sajber bezbednost u Africi, Žurnal za rukovođenje globalnom informativnom tehnologijom)

PRIMERI DOBRE PRAKSE

U Keniji je novi predlog zakona o zaštiti podataka predat na razmatranje parlamentu novembra, 2018.godine. Ovaj predlog zakona sadrži mnoge elemente evropske Opšte uredbe o zaštiti ličnih podataka (engl. GDPR). Na primer, predlog zakona zahteva od organizacija da obaveste korisnike zašto prikupljaju njihove podatke, u koju svrhu će se ti podaci koristitii koliko dugo će data organizacija čuvati te podatke. Ovaj predlog zakona takođe sadrži jednu odredbu koja daje korisnicima pravo da zahtevaju od organizacija da obrišu njihove podatke. Kao dodatak tome neophodno je da organizacije poštuju određeni nivo bezbednosnih standarda pri čuvanju podataka.

(Izvor: http://www.ict.go.ke/wp-content/uploads/2016/04/Kenya-Data-Protection-Bill-2018-14-08-2018.pdf)

Francuska je usvojila Zakon za zaštiti ličnih podataka (fr. Loi relative à la protection des données personnelles) juna, 2018.godine kako bi usaglasila francusko nacionalno zakonodavstvo sa Opštom uredbom o zaštiti ličnih podataka Evropske unije (engl. GDPR). Ovaj zakon je nadogradnja francuskog Zakona o zaštiti ličnih podataka iz januara, 1978. godine i proširuje ovlašćenja zaštite podataka Nacionalne komisije za informacije i slobode (fr. Commission national de l'informatique et des libertés (CNIL)) na sledeće načine:

• Daju se veća regulatorna ovlašćenja kod primene pravne regulative koja se odnosi na bezbednost, pravila ponašanja i razvijanje odgovarajućih dokumenata i preporuka. CNIL bi dodatno imala ovlašćenje da odobrava tela za izdavanje sertifikata kao i da ih sama izdaje u skladu sa odredbama GDPR-a i francuskih nacionalnih pravnih tvorevina, lica i procedura.

• Ojačana su ovlašćenja nadzora kojima se dozvoljava agentima CNIL-a da traže bilo koja dokumenta koja nisu pravno zaštićena. Agenti CNIL-a dodatno mogu da primenjuju nove vrste sankcija i administrativnih novčanih kazni koje su značajno podignute. U slučaju da neka kompanija ne zaštiti lične podatke novčana kazna se kreće od 10 miliona evra ili 2% njenih ukupnih prihoda do 20 miliona evra ili 4% njenih ukupnih prihoda (u zavisnosti koji je veći iznos) za najozbiljnije prekršaje.

(Izvor: https://www.francecompetences.fr/Protection-des-donnees-personnelles.html)

Dobre prakse 5: Vlade bi trebalo da razviju i ažuriraju zakone koji štite kritičnu infrastrukturu.

Instalacije kritične infrastukture, na engleskom jeziku poznate kao CIIs, neophodno su za život i dobrobit stanovništva. CIIs su sredstva, sistemi, mreže (fizičke i virtuelne) koji su neophodni za funkcionisanje društva, uključujući zdravlje, bezbednost, ekonomsko i socijalno blagostanje, a čije uništenje ili prestanak rada bi imao izuzetno negativan efekat na stanovništvo.

Primeri instalacija kritične infrastrukture su:

- elektrane,
- snabdevanje vodom i hranom,
- javna bezbednost (snage bezbednosti, organizacije za vanredne situacije, civilna odbrana),
- javno zdravlje (bolnice i medicinska nega, laboratorije),
- državna administracija,
- prevoz (na primer: put, pruga ili vazdušni saobraćaj),
- odlaganje otpada (otpad i otpadne vode),
- finansijske usluge (npr. rad banaka, osiguravajuća društva),
- mreže informacionih i komunikacionih tehnologija

Jedan veliki deo instalacija kritične infrastukture (CII) koristi nove tehnologije kako bi mogao da sprovede svoje operacije. Ova modernizacija koja je pomogla da infrastruktura bude efikasnija i bolje isporučuje javna dobra stanovništvu, izložila ih je i slabostima koje bi mogle da izazovu razarajuće posledice po lokalno stanovništvo.

Države imaju obavezu da zaštite svoje CIIs-ove od sajber napada u okviru svojih granica. Zaštita CIIs-a od sajber napada bi trebalo da bude na prvom mestu u državnoj strategiji sajber bezbednosti. Države bi zato trebalo da razviju i primene mere sajber odbrane koje štite ranjive delove informacionih sistema CIIs-ova. Ove mere bi trebalo da budu u stanju da sajber napade otkriju, odbrane se od njih i neutrališu ih.

PRIMERI DOBRE PRAKSE

Parlament Južne Afrike je u martu, 2019.godine usvojio zakonodavstvo koje se odnosi na CII u cilju, između ostalog, određivanja i proglašavanja infrastukture kritičnom infrastrukturom, obezbeđivanja smernica i faktora koji moraju da se uzmu u obzir kako bi se obezbedilo transparentno određivanje i proglašavanje kritične infrastrukture, obezbeđivanja mera zaštite, čuvanja i oporavljanja kritične infrastrukture. Zakonodavstvom je takođe uspostavljen Savet za kritične infrastrukture koji daje ministru unutrašnjih poslova diskreciono pravo da proglasi određene instalacije kritičinom infrastrukturom i propiše kako će se one zaštititi u interesu nacionalne bezbednosti.

(Izvor: http://www.policesecretariat.gov.za/downloads/bills/CIP_Bill_for_Publication.pdf)

ZAKLJUČAK

- Međunarodni i regionalni okviri obezbeđuju niz normi za razvoj, usvajanje, izmene i dopune zakonodavstva, politika i strategija iz oblasti sajber bezbednosti.
- Vlade igraju glavnu ulogu u osiguravanju dobre uprave sajber bezbednošću.
- Vlade bi trebalo da razvijaju, usvoje i ažuriraju nacionalne zakone, politike i strategije kako bi uspostavile regulativu u sajber prostoru i kako bi se suočile sa sadašnjim izazovima i problemima u sajber prostoru, uključujući zaštitu privatnosti i ličnih podataka, kao i zaštitu kritične infrastrukture.
- Za dobru upravu sajber bezbednošću je neophodno da se unaprede stručna znanja iz ove oblasti putem obuka, a posebno preko privatno-javnog partnerstva (PJP).

Izvori

The Rule of Law Checklist, Venice Commission of the Council of Europe (Spisak za vladavinu prava, Venecijanske komisije Saveta Evrope), 2016.

Cybersecurity Policy Framework. A Practical guide to the development of national cybersecurity policy. (Okvir politike sajber bezbednosti. Praktični vodič za razvoj nacionalne politike sajber bezbednosti), Microsoft, 2018.

International Cybersecurity Norms: Reducing Conflict in an Internet-dependent World, (Međunarodne norme sajber bezbednosti: Smanjivanje konflikata u svetu zavisnom od Interneta), Microsoft, 2014.

African Union Commission and Symantec, Cyber crime and cyber security trends in Africa Report (Komisija Afričke unije i Simantek, sajber kriminal i trendovi sajber bezbednosti u Afričkom izveštaju), 2017. https://thegfce.org/wp-content/uploads/2020/06/CybersecuritytrendsreportAfrica-en-2-1.pdf

POGLAVLJE 5
NACIONALNE STRATEGIJE SAJBER BEZBEDNOSTI

CILJEVI

U ovom poglavlju će se korisnici vodiča upoznati sa nacionalnim strategijama sajber bezbednosti (engl. NCSS). Ono ima za cilj da im pomogne da bolje upoznaju glavne elemente nacionalnih strategija, kao i najbolje prakse.

Šta ćemo naučiti ovom poglavlju?

- Bolje ćemo upoznati nacionalne strategije sajber bezbednosti uopšteno.
- Saznaćemo koji su to glavni elementi nacionalnih strategija sajber bezbednosti.
- Postaćemo svesniji koji su to dostupni resursi koji pomažu nacionalnim donosiocima zakona i politika da napišu nacionalnu strategiju sajber bezbednosti.

Uvod

Od samog početka sajber prostor je pružao veliki broj mogućnosti za privredni, tehnološki i društveni razvoj. Ipak istovremeno su se razvijale i transnacionalne pretnje, kao što je sajber špijunaža, koju su finansirale države, vojne sajber aktivnosti, sajber kriminal, sajber terorizam i upotreba Interneta u terorističke svrhe. Kada ovi bezbednosni rizici, koji se dovode u vezu ili se odigravaju u sajber prostoru, nisu na odgovarajući način u ravnoteži sa sveobuhvatnim strategijama i akcionim planovima, države nisu u mogućnosti da zaštite nacionalnu i ljudsku bezbednost ili održe privredni rast.

Države širom sveta razvijaju i usvajaju strategije kako bi mogle da reaguju na ove sve veće bezbednosne pretnje, što uključuje usvajanje novih ili izmenu i dopunu postojećih nacionalnih politika bezbednosti. Nacionalne politike bezbednosti koje se bave pretnjama u sajber prostoru nazivaju se nacionalne strategije sajber bezbednosti (engl. NCSS).

Postoje različite NCSS-e, i u zavisnosti od spremnosti države da se bavi sajber pretnjama, nisu sve podjednako detaljne. S obzirom na to da NCSS zavise od konteksta, ne postoji jedan određeni model uspešne NCSS-a. Ipak je moguće odrediti niz strateških prioriteta koji se nalaze u većini NCSS-a. To su regulatorni okviri, zaštita kritične infrastrukture, međunarodna i javno--privatna saradnja, kao i istraživanje i razvoj.

Iako ne postoji jedna opšte prihvaćena definicija NCSS-a, Međunarodna telekomunikaciona unija (engl. ITU) definiše nacionalnu strategiju sajber bezbednosti kao:

- izraz vizije najvažnijih ciljeva, principa i prioriteta kojima se jedna zemlja rukovodi u borbi protiv sajber pretnji;
- pregled interesnih strana koje imaju zadatak da poboljšaju sajber bezbednost države i njihove odgovarajuće uloge i odgovornosti;
- opis koraka, programa i inicijativa koje će zemlja da preduzme kako bi zaštitila svoju nacionalnu sajber infrastrukturu, i na taj način povećala bezbednost i prilagodljivost[1].

S obzirom na to da sajber pretnje brzo napreduju, delokrug NCSS-a se proširuju na isti način, od uloge zaštite samo pojedinaca i organizacija do zaštite celog društva.

1 ITU, Guide to developing a national cybersecurity strategy, 2018, str. 13 (Vodič za razvoj nacionalne strategije sajber bezbednosti)

NCSS u osnovi ima za cilj da dostigne dva međusobno povezana cilja:

- 1. da ojača sajber bezbednost Internet privrede kako bi mogla da vodi privredni i društveni razvoj;
- 2. da štiti društva koja zavise od sajber pretnji.

Sajber bezbednost je jedan složen problem koji se odnosi na višestruke različite aspekte uprave, politika, kao i operativne, tehničke i pravne aspekte. Nacionalne politike najčešće definišu metodologiju i predstavljaju načine za dostizanje nacionalnih prioriteta.

Dobra praksa 1: Nacionalna strategija sajber bezbednosti kao sastavni deo šire nacionalne politike bezbednosti vlade.

NCSS bi trebalo da bude dodatno sredstvo za postizanje nacionalnih strateških prioriteta, stoga je važno da zemlje vide NCSS kao deo svoje opšte strategije bezbednosti. Na ovaj način se postiže sveobuhvatni pristup nacionalnoj bezbednosti.

Uključivanje sajber bezbednosti je važan elemenat nacionalne strategije bezbednosti (i obrnuto), a i dokaz je da vlade razumeju da je sajber prostor ključni deo praktično svakog aspekta nacionalne bezbednosti.

PRIMERI DOBRE PRAKSE

Švedska nacionalna strategija sajber bezbednosti ističe da se njihova strategija „zasniva na ciljevima bezbednosti Švedske, zaštiti života i zdravlja stanovništva, funkcionisanju društva i očuvanju fundamentalnih vrednosti, kao što su demokratija, vladavina prava, ljudska prava i slobode".

(Izvor: https://www.government.se/4ac8ff/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213)

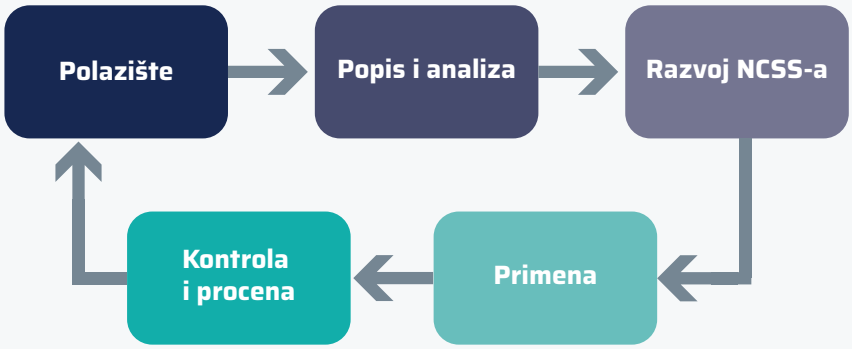
Finska se vodi principima i procedurama Strategije bezbednosti društva prilikom primene nacionalne strategije bezbednosti.

(Izvor: https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf)

Važno je da se vizija i ciljevi zemlje prevedu u konkretne aktivnosti kada se radi na razvoju jedne sveobuhvatne NCSS-a koje će na kraju da pomognu da se dostignu prvobitno postavljeni ciljevi i namere.

ITU je razvio sledeći prikaz životnog ciklusa jedne NCSS-a kako bi pomogao i usmerio strateško razmišljanje korisnika na nacionalnom nivou.

Neophodno je da vlade odrede ciljeve i svrhu ove strategije i jasno artikulišu njenu viziju u kontekstu sajber bezbednosti pre nego što počnu da je razvijaju.



Slika 1. Životni ciklus NCSS-a na osnovu ITU-ovog Vodiča za razvoj nacionalne strategije sajber bezbednosti

STUDIJA SLUČAJA: OAS-OVA MISIJA TEHNIČKE POMOĆI MEKSIKU

Organizacija američkih država (engl. OAS) je 2017.godine preko svog Programa sajber bezbednosti i na zahtev Vlade Meksika okupila komisiju sastavljenu od međunarodnih stručnjaka kako bi podelili najbolje prakse sa meksičkim pravnim licima i stekli uvid u trenutno stanje u oblasti sajber bezbednosti u Meksiku i kako bi odredili nivo trenutne zrelosti sajber bezbednosti i unapredili njene nacionalne okvire.

Ovi stručnjaci su došli iz privatnog sektora, drugih vlada, tehničke zajednice, međunarodnih organizacija i civilnog društva.

(Izvor: http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-049/17 and http://www.oas.org/documents/eng/press/Recommendations-for-the-Development-of-the-National-Cybersecurity-Strategy.pdf)

Dobra praksa 2: Proces pisanja nacionalne strategije sajber bezbednosti trebalo bi da vodi glavni predstavnik vlasti i tom prilikom uključi široki spektar interesnih strana i učesnika.

Kako bi se započelo sa pisanjem NCSS-a, potrebno je da se odredi glavni predstavnik vlasti. On može da bude neko već postojeće pravno lice ili novo uspostavljena agencija. Jedna od ključnih obaveza ovog vodećeg predstavnika trebalo bi da bude koordinacija procesa na neutralan način. On bi trebalo da bude odgovoran za određivanje ključnih interesnih grupa i učesnika u procesu koji će biti uključeni u razvoj NCSS-a, kao i za omogućavanje neprestane razmene između učesnika kako bi se neophodna znanja i ekspertize koristile na najbolji mogući način u procesu pisanja NCSS-a. Ovaj glavni predstavnik trebalo bi dodatno da bude odgovoran i za jasno određivanje uloga i odgovornosti ovih interesnih strana.

STUDIJA SLUČAJA: ČILENASKI MEĐUMINISTARSKI ODBOR

Međuministarski odbor u Čileu rukovodi procesom pisanja nacionalne strategije bezbednosti, a u njemu sede predstavnici Ministarstva unutrašnjih poslova i javne bezbednosti i Ministarstva odbrane.

Ovaj međuministarski odbor organizuje i koordinira sastanke radnih grupa na teme koje su definisane nacionalnom strategijom sajber bezbednosti. Radne grupe su se bavile raznim temama, kao što su informativna infrastruktura, prevencija i sankcije, obrazovanje i podizanje svesnosti, saradnja i međunarodni odnosi, institucionalizacija. Stalni članovi ovih radnih grupa bili su državni sekretari Ministarstva unutrašnjih poslova, odbrane, pravde, privrede, telekomunikacija, predstavništva i državne obaveštajne agencije.

(Izvor: http://www.ciberseguridad.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADtica-Nacional-sobre-Ciberseguridad.pdf)

Iako je opštepoznato da privatni sektor ima posebnu ulogu u oblasti sajber bezbednosti, saradnja između javnog i privatnog sektora još uvek nije institucionalizovana.

Javno-privatna saradnja je dodatno važna kod zaštite kritične infrastrukture s obzirom na to da su privatna lica vlasnici ili lica koja upravljaju najvažnijim infrastrukturama. Oni bi zato trebalo da budu aktivno uključeni u proces planiranja zaštite nacionalne kritične infrastrukture od sajber pretnji.

Od suštinske je važnosti da u proces razvijanja NCSS-a bude uključen što veći broj interesnih strana kako bi se imalo pravo svojine nad ovom strategijom. Pravo svojine je izuzetno važno u fazi primene. Kao dodatak tome, uključivanje svih odgovarajućih strana može dalje da nam bude garancija da će oni biti aktivni učesnici i da će dati doprinos svojim stručnim znanjima u postizanju više stope uspešnosti.

PRIMERI DOBRE PRAKSE

U UK-u postoji otvoren proces konsultacija dostupan na sajtu svima koji žele da daju povratnu informaciju po pitanju ove strategije u cilju postizanja optimalnog ishoda svoje NCSS-a.

Izvor: https://www.gov.uk/government/consultations/developing-the-uk-cyber-security-profession

Kanadska vlada započela je proces onlajn javnih konsultacija koji pita Kanađane za mišljenje, privatni sektor, univerzitet i druge informisane interesne strane o sajber bezbednosti u Kanadi. Izveštaj o ovom procesu revizije je nakon toga bio objavljen i dostupan onlajn.

Izvor: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-cybr-rvw-cnslttns-rprt/index-en.aspx

Britanska strategija sajber bezbednosti kaže da je neophodno da svi rade zajedno (privatni sektor, pojedinci i vlade) kako bi se dostigao cilj sigurnog i bezbednog interneta. Svi imamo koristi od korišćenja sajber prostora, ali i obavezu da pomognemo da se on zaštiti.

Javno-privatna partnerstva su najčešći oblik institucionalne saradnje između javnog i privatnog sektora, koja imaju svoje probleme. Ovo se posebno odnosi na mandat javno-privatnog partnerstva, nedostatak jasno određenih uloga i odgovornosti, nepoverenje među interesnim stranama, prepreke kod deljenja informacija, nedostatak podstreka za zajednički rad kao odsustvo uspešnog nadzora, a samim tim i odgovornosti.

Tipični mehanizmi koji uključuju različite interesne strane mogu da budu odbori, okrugli stolovi, radionice, razgovori sa stručnjacima, konsultacije i dr.

STUDIJA SLUČAJA: ODREĐIVANJE ODGOVARAJUĆIH INTERSNIH STRANA

Iako nije neophodno da sve interesne strane budu uključene u svaku raspravu, važno je da odredimo koje su to odgovarajuće interesne strane koje imaju direktni interes i stručna znanja i koje kao takve mogu da daju svoj doprinos diskusijama.

Sledi spisak odgovarajućih interesnih strana koje učestvuju u razvijanju NCSS-a. Ovo nije konačna lista, ali može da da dobar pregled uključenih interesnih strana.

- **Vlada:** odgovarajuća ministarstva (IKT, privrede, komunikacija, itd.), regulatorne agencije, sudstvo i unutrašnji poslovi, odbrana i bezbednosne službe.
- **Privatni sektor:** IKT kompanije, kompanije za informativnu bezbednost, poslovna udruženja.
- **Civilno društvo:** grupe rukovođene određenim interesom (kao što su ljudska prava ili zaštita dece onlajn), grupe na osnovu identifikovanja (vera, manjine, ženska prava), mreže organizacija civilnog društva.
- **Univerzitet:** univerziteti, istraživači, trust mozgova, nezavisni istraživači.

- **Tehnička zajednica:** CERT, timovi za reagovanje na bezbednosne incidente (engl. CSIRT), organizacije za sistem standardizacije imena domena.
- **Međunarodne org.:** regionalne i međunarodne organizacije (kao što su, na engleskom AU, OSCE, OAS, CoE), međunarodne institucije (npr. Svetska banka, ITU).

Izvor: https://www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf

Dobra praksa 3: Proces pisanja nacionalne strategije sajber bezbednosti bi trebalo da obuhvati što više prednosti i mana sajber bezbednosti zemlje.

U sledećoj fazi procesa razvijanja NCSS-a važno je da se proceni i analizira sajber bezbednost određene zemlje kako bi se utvrdile prednosti i mane sajber bezbednosti date zemlje. Sastavni deo ovog prikupljanja podataka i analize je mapiranje i tumačenje nacionalnog regulatornog okvira (uključujući zakone, politike i programe koji se odnose na sajber bezbednost), nacionalna kritična infrastruktura i javno-privatna partnerstva, kao i tehnički i institucionalni kapaciteti u cilju sprečavanja rizika sajber bezbednosti (kao što su CERT-ovi) i zaštite od istih (kao što su službenici zaduženi za zaštitu podataka).

Proces prikupljanja podataka i analize procenjuje nivo zrelosti sajbera jedne zemlje kako bi dalje bili sigurni da je NCSS usklađena sa stvarnim potrebama date zemlje.

STUDIJA SLUČAJA: MODEL ZRELOSTI KAPACITETA SAJBER BEZBEDNOSTI, MINISTARSTVO KOMUNIKACIJA GANE

Model zrelosti sajbera je napravljen u cilju pružanja podrške procesu pregleda kapaciteta sajber bezbednosti Gane u odnosu na sledećih pet dimenzija:

- politike i strategije sajber bezbednosti;
- sajber kulturu i društvo;
- obrazovanje, obuku i veštine iz oblasti sajber bezbednosti;
- zakonske i regulatorne okvire;
- standarde, organizacije i tehnologije.

Ova procena imala je za cilj da pruži Vladi Gane bolje razumevanje prednosti i mana sajber bezbednosti, kao i da u skladu sa time poveća ulaganja u izgradnju kapaciteta.

Izvor: https://moc.gov.gh/cybersecurity-capacity-maturity-model-assessment-held

NCSS može nakon ove procene da bude razvijena pod rukovodstvom nekog predstavnika vlasti i uz aktivno učešće što većeg broja ključnih interesnih strana. Idealno je da se odrede radne grupe koje se bave pisanjem određenih delova NCSS-u u zavisnosti od njene stručnosti. Dobrom praksom se smatra postojanje procesa revizije NCSS-a pre njenog usvajanja u obliku konsultacija ili radionica između većeg broja interesnih strana. Na ovaj način osiguravamo da se NCSS zasniva na zajedničkoj viziji.

U zavisnosti od konkretnog procesa usvajanja, parlament ili vlada imaju ovlašćenje da usvoje NCSS. Usvojena NCSS bi trebalo da bude objavljena u Službenom glasniku ili na sajtu ministarstva kako bi bili sigurni da je javnost upoznata sa njenim postojanjem i sadržajem, kao i prioritetima vlade po pitanju sajber bezbednosti kako bi mogli aktivno da doprinesu postizanju strateških prioriteta koji su navedeni u datoj strategiji.

Ne postoji samo jedan pristup oblikovanju procesa pisanja NCSS-a. Dobre prakse se razlikuju i zavise od delokruga NCSS-a, broja uključenih interesnih strana, kao i dostupnih tehničkih zahteva.
U Čileu, Keniji i Meksiku i nacrt NCSS-a je bio objavljen onlajn kako bi omogućili različitim interesnim stranama da daju svoje komentare i na taj način postanu njeni 'vlasnici'.

Dobra praksa 4: NCSS sadrži sledeće strateške prioritete: poboljšanje koordinacije procesa kreiranja politika vladinih predstavnika na operativnom nivou, jačanje javno-privatne saradnje, unapređenje međunarodne saradnje i poštovanje osnovnih prava.

Velika većina NCSS-a ističe važnost međunarodne saradnje u cilju promovisanja sajber bezbednosti i potrebu za sklapanjem delotvornijih saveza i partnerstava među sličnim zemljama, uključujući izgradnju kapaciteta. Dodatno, najveći broj NCSS-a prepoznaje važnost poštovanja osnovnih prava, a posebno prava na privatnost i slobodu izražavanja i mišljenja, kao i slobodan protok informacija kao nešto bez čega ne može da postoji bezbedan sajber prostor.

Većina NCSS-a sadrže i prevenciju sajber kriminala kao strateški prioritet.

PRIMERI DOBRE PRAKSE

Kanadska nacionalna strategija sajber bezbednosti predstavlja odraz kanadskih vrednosti, kao što su vladavina prava, odgovornost i pravo na privatnost.

(Izvor: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/canadas-cyber-security-strategy/@@download_version/5a41f8f967154454a13d71acc40a8f28/file_en)

Nacionalna strategija informacionih i komunikacionih tehnologija Malavija ističe da će vlada nastaviti da obezbeđuje povoljnu klimu za učešće, kako javnog, tako i privatnog sektora, u procesu razvoja, primene i upotrebe IKT--a u gradskim i ruralnim sredinama.

(Izvor: https://www.macra.org.mw/?wpdmpro=malawi-ict-policy-2013)

Dobra praksa 5: Određivanje nacionalne kritične infrastrukture kako bi bila obuhvaćena NCSS-om.

Neophodno je da odredimo nacionalnu kritičnu infrastrukturu u cilju razvijanja politika njihove zaštite od sajber pretnji. Bez jasne definicije i spiska šta čini kritičnu infrastrukturu biće teško da se ona zaštiti od sajber pretnji.

Sve veći deo kritične infrastrukture zavisi od informaciono-komunikacionih tehnologija kako bi mogle da rade i funkcionišu. Zaštita nacionalne kritične infrastrukture od sajber pretnji je od suštinske važnosti s obzirom na to da može imati stvarne posledice, pa se upravo iz ovog razloga veoma često uzima kao jedan od prioriteta nacionalnih strategija sajber bezbednosti mnogih država.

Stoga sve veći broj država određuje svoju nacionalnu kritičnu infrastrukturu, a za većinu su to vodovod, elektrane i bolnice.

Direktiva Saveta EU-a 2008/114/EC od 8.decembra 2008.godine o određivanju i imenovanju evropske kritične infrastrukture i proceni potrebe za njihovom zaštitom je važan dokument. Ova Direktiva Evropske unije posebno se osvrće na kritičnu infrastrukturu i definiše je kao „imovinu, sistem ili njegov deo na teritoriji država članica koji je od suštinske važnosti za održavanje životnih, društvenih funkcija, zdravlja, sigurnosti, bezbednosti, ekonomskog ili društvenog blagostanja ljudi, a čiji bi prekid rada ili uništenje imalo značajan uticaj na državu članicu kao posledicu prekida rada ovih funkcija ”.

PRIMERI DOBRE PRAKSE

Član 17. južnoafričkog Zakona o zaštiti kritične infrastrukture navodi spisak faktora koji bi trebalo da se uzmu u obzir kada se proglašava kritična infrastruktura. Ovi faktori su, na primer: sektor u okviru koga se sprovode primarne funkcije ove infrastrukture; strateška važnost, uključujući i mogući uticaj uništenja, ometanja rada, kvara ili degradacije jedne ovakve infrastrukture ili prekid u radu koji utiče na normalno funkcionisanje Republike Južne Afrike; neometano funkcionisanje rada osnovnih javnih službi ili održavanje zakona i reda; rizične kategorije ove infrastrukture, resursi koji su na raspolaganju osobi koja kontroliše infrastrukturu; posledice ili rizici uništenja, ometanja, kvara ili degradacije jedne ovakve infrastrukture; veličina i lokacija bilo koje ugrožene populacije; istorijski primeri uništavanja, nivo rizika ili pretnji kojima je ova infrastruktura izložena; posebne osobine ili odlike ove infrastrukture; mera u kojoj će proglašavanje nečega kritičnom infrastrukturom da promoviše javne interese; kao i bilo koji drugi faktori koje odredi nadležni ministar.

Izvor: https://pmg.org.za/bill/644/

Nemačka Strategija nacionalne kritične infrastrukture (2009) definiše kritičnu infrastrukturu kao „organizacionu ili fizičku strukturu i objekte od takvog vitalnog značaja za društvo i privredu jedne zemlje da bi njen kvar ili uništenje dovelo do ozbiljnih nestašica u snabdevanju, značajnog ometanja javne sigurnosti i bezbednosti, kao i drugih dramatičnih posledica".

Izvor: https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=1

Francuska definiše kritičnu infrastrukturu kao „institucije, strukture ili objekte koji obezbeđuju neophodnu robu i usluge i time čine okosnicu francuskog društva i njegovog načina života". Sami operateri su sačinili spisak kritične infrastrukture na kojem se nalaze centri za proizvodnju, kontrolni centri mreže ili baze podataka.

Izvor: http://www.sgdsn.gouv.fr/uploads/2016/10/plaquette-saiv.pdf

Švajcarska je uključila sledeće sektore u deo kritične infrastrukture: predstavnike vlasti, energetiku, odlaganje otpada, finansije, vodoprivredu, zdravstvo i prehranu, informacije i komunikaciju, transport i javnu bezbednost.

Izvor: https://www.babs.admin.ch/fr/aufgabenbabs/ski.html

Dobra praksa 6: Nacionalna strategija sajber bezbednosti obezbeđuje plan sprovođenja, istraživanja i razvoja.

NCSS je uspešna onoliko koliko i njeno sprovođenje. Stoga uspešno sprovođenje NCSS-a zavisi od usvojenog plana sprovođenja (koji se ponekad naziva i akcioni plan) kako bi strategija postala konkretan niz akcija i politika putem koordinisanja snaga i resursa.

Glavni deo plana sprovođenja je razvijanje ključnih indikatora kontrole i procene uspešnosti NCSS-a. U procesu kontrole vlade bi trebalo da se postaraju da se NCSS sprovodi u skladu sa njenim akcionim planom. U fazi procene trebalo bi da se oceni da li je NCSS i dalje odraz svojih ciljeva i prioriteta, a ukoliko nije da se oni ponovo procene.[2]

Plan sprovođenja bi dalje trebalo da sadrži mehanizme za prijavljivanje incidenata i načine na koje možemo da podignemo svest ljudi po pitanju rizika i pretnji u sajber prostoru. Prijavljivanje kompjuterskih bezbednosnih incidenata igra veoma važnu ulogu kod unapređivanja nacionalne sajber bezbednosti u celini. Ovakva vrsta prijavljivanja pomaže da se prilagodi i oblikuje spisak mera za sajber bezbednost u odnosu na prirodu stalno promenljivih rizika. Saradnja između javnog i privatnog sektora je neophodan preduslov za proces prijavljivanja. Stoga su pouzdanost i poverenje od suštinske važnosti za ohrabrivanje otvorenog deljenja informacija kada govorimo o rizicima i pretnjama u sajber prostoru. Osnivanje timova za reagovanje na kompjuterske incidente (engl. CSIRT) smatra se okosnicom uspešnog koordinisanja upravljanjem incidentima.

Da bi plan sprovođenja bio delotvoran, potrebno je da se sprovode inicijative za podizanje svesti pojedinačnih korisnika i njegovog/njenog znanja o pretnjama i ranjivostima sajber bezbednosti. Ovo je jako važno kako bismo bili sigurni da ovaj korisnik zna kako da se zaštiti od rizika u sajber prostoru koji bi mogli da utiču na nacionalnu sajber bezbednost cele zemlje.

Ulaganje i jačanje istraživanja i razvoja (engl. R&D) je isto tako neophodno za razvoj alatki za odvraćanje od sajber pretnji, zaštitu i prilagođavanje svim vrstama sajber pretnji.

2 ITU Vodič za razvoj strategije sajber bezbednosti, str. 26

PRIMERI DOBRE PRAKSE

NCSS Kenije ističe sledeće ciljeve: „Vlada Kenije je posvećena sigurnosti, bezbednosti i napretku naše nacije i njenih partnera. Za nas je sajber bezbednost ključna komponenta s obzirom na to da ona uliva organizacijama i pojedincima veće poverenje u onlajn i mobilne transakcije; ohrabruje veće strane investicije i otvara jedan širi dijapazon trgovinskih mogućnosti na globalom tržištu. Uspešna primena ove strategije će dalje omogućiti Keniji da dostigne svoje ekonomske i društvene ciljeve tako što će obezbediti bezbedno onlajn okruženje za građane, privredu i strane partnere i njihovo poslovanje." (strana 4)

Nacionalna strategija sajber bezbednosti Nigerije kaže da je pojedinačni korisnik najslabija karika u lancu sajber bezbednosti. Stoga ova strategija predlaže „inicijative i mere koje će pomoći da se zaštite pojedinačni internet korisnici, pripadnici šire javnosti, tako što će im obezbediti materijale i alatke koje će im pomoći da zaštite građane Nigerije od sajber pretnji i ranjivosti." .

(Izvor: Nigerija, Nacionalna strategija sajber bezbednosti, Poglavlje 11)

Nacionalna IKT politika Malavija sadrži detaljnu Strategiju za sprovođenje, kontrolu i ocenu pomoću koje se kontroliše i ocenjuje uspešnost i pogodnost, jednom godišnje ili češće, po potrebi. (Izvor: Malavi, Nacionalna politika IKT--a, 2013, strana 11)

Nacionalna strategija sajber bezbednosti Mauritanije sadrži u sebi detaljni plan primene same politike. (Izvor: Maurétanie, Stratégie Nationale de Modernisation de l'Administration et des TICs 2012-2016. (Mauritanija, Nacionalna strategija modernizacije javne uprave i IKT-a)

Poljska nacionalna strategija sajber bezbednosti ističe da je najvažniji zadatak strategije podizanje svesti korisnika o metodama i merama bezbednosti u sajber prostoru. (Poljska, Nacionalna strategija sajber bezbednosti, 2013)

Tunis, Južna Afrika i Kenija osnovale su funkcionalne nacionalne CERT-ove.

Dobra praksa 7: Obezbediti dovoljno resursa za pokretanje kampanja podizanja svesti o sajber bezbednosti za širu javnost u okviru sprovođenja NCSS-a.

Svi na Internetu, od zvaničnika vlade, poslovnih ljudi, finansijskog i trgovinskog sektora do šire javnosti, uključujući i decu, osetljivi su i podložni pretnjama sajber bezbednosti.

Uopšteno govoreći, svi shvataju da sajber bezbednost nije odgovornost samo jedne agencije, pravnog lica ili pojedinca, već zajednička odgovornost svih koji su na Internetu ili koriste aplikacije koje su povezane u ovom onlajn carstvu.

Po Organizaciji američkih država (engl. OAS) „sajber kriminal nastaje kao posledica velikog broja različitih ponašanja i primenjenih tehnika, uključujući krađu identiteta, eksploataciju dece, sajber maltretiranje, pretnje upadima, slanje lažnih mejlova s ciljem izvlačenja informacija (engl. phishing), kao i mnogi drugi, i protiv toga se moramo boriti."[3].

Neophodno je obrazovati javnost o rizicima i pretnjama u sajber prostoru s obzirom na to da svako može da bude žrtva više različitih vrsta sajber kriminala.

STUDIJA SLUČAJA: SET ALATA KAMPANJE ZA PODIZANJE SVESTI O SAJBER BEZBEDNOSTI OAS-A – SITUACIONA ANALIZA

Dobro razumevanje sadašnjeg konteksta pretnji sajber bezbednosti je od suštinske važnosti za osmišljavanje uspešnih kampanja podizanja svesti.

OAS je stoga razvio neka pitanja koje služe kao smernice i pomažu pri analiziranju trenutne situacije,a to su:

- U kojoj meri je vaša zemlja povezana?
- Gde i kako se ljudi povezuju na Internet?
- Ko je onlajn?
- Kojom vrstom uređaja?
- Koje operativne sisteme i kanale komunikacija koriste?
- Za koju vrstu proizvoda i usluga?
- Kako se Internet koristi za posao?
- Koji je raspon ovih poslova (npr. vlasništvo, poljoprivredna saradnja, mala i srednja preduzeća, laka industrija)?
- Sa kojim sajber bezbednosnim pretnjama se vaša zemlja suočava?
- Sa kojom vrstom sajber kriminala se vaši kupci i klijenti suočavaju?
- Sa kojom vrstom sajber kriminala se susrećete prilikom obavljanja vaših poslova?
- Da li se ove vrste sajber kriminala razlikuju po grupama?
- Koji su rizici za kritičnu infrastrukturu?
- Da li je bilo u skorije vreme nekih većih prekršaja, bilo za vladu ili za komercijalni sektor?
- Da li postoje pretnje i rizici od većih prekršaja u budućnosti?
- Koji su mogući ekonomski gubici od sajber pretnji?

3 Set alata za podizanje svesti o sajber bezbednosti, strana 8, OAS (2016), dostupno na https://thegfce.org/wp-content/uploads/2020/06/2015-oas-cyber-security-awareness-campaign-toolkit-english-1.pdf

Izvor: Set alata kampanje za podizanje svesti o sajber bezbednosti, OAS, 2016, dostupno na https://thegfce.org/wp-content/uploads/2020/06/2015-oas-cyber-security-awareness-campaign-toolkit-english-1.pdf

Uspešna kampanja podizanja svesti prenosi poruke koje se lako razumeju, precizne su, planirane i razvijene u razgovoru sa više interesnih strana, uključujući predstavnike vlade, privatne kompanije (internet provajderi, telekomunikacione kompanije), predstavnike civilnog društva, nevladine organizacije, medije i univerzitet.

PRIMERI DOBRE PRAKSE

Jordan je 2015.godine usvojio Zakon o borbi protiv sajber kriminala i osnovao specijalizovanu jedinicu „Jedinicu za sajber kriminal". Ova jedinica koja radi uz podršku Kancelarije UN-a za drogu i kriminal snimila je jedan video u cilju podizanja svesti o rizicima, tipovima i pravnim posledicama sajber kriminala.

Izvor: https://www.unodc.org/middleeastandnorthafrica/en/web-stories/jordan_-releasing-a-video-on-cyber-security-awareness-raising.html

Kampanja 'Budi Bezbedan Onlajn' (engl. Stay Safe Online) kojom rukovodi Nacionalna alijansa sajber bezbednosti promoviše kulturu sajber bezbednosti. Na svom sajtu je u tu svrhu objavila infografski prikaz kako bismo bili sigurni da svi u jednom domaćinstvu, uključujući decu i starije ukućane, znaju da koriste Internet na bezbedan i odgovoran način.

Izvor: https://staysafeonline.org/wp-content/uploads/2018/09/NCSAM-2018-Week1.pdf

ZAKLJUČAK

- Države su u obavezi da neprestano kontrolišu i usaglašavaju svoje nacionalne strategije sajber bezbednosti sa nizom pretnji koje se usložnjavaju kako bi bile u stanju da idu u korak sa sadašnjim i nekim novim sajber pretnjama.
- Da bi nacionalne strategije sajber bezbednosti bile uspešne, neophodno je postaviti određene ciljeve i strateške prioritete.
- Strategije sajber bezbednosti bi trebalo da uzmu u obzir poštovanje osnovnih prava, kao što su privatnost i sloboda izražavanja i veroispovesti, kao i slobodni protok informacija, kako bi mogle da promovišu slobodan i otvoren sajber prostor.
- Sajber bezbednost je problem koji zahvata različite sektore i utiče na odgovornosti većeg broja državnih agencija. Stoga je bliska saradnja između svih tela vlade, kao i saradnja sa privatnim sektorom, važna potpora uspešne primene nacionalne strategije sajber bezbednosti.
- Vlade bi trebalo da ulože više resursa u istraživanje i razvoj (engl. R&D) kako bi mogle da razviju nove alate za odvraćanje, zaštitu, otkrivanje i prilagođavanje novim vrstama sajber pretnji.
- Važno je da prvo definišemo šta se smatra 'nacionalnom kritičnom infrastrukturom' u datom kontekstu kako bismo mogli da je zaštitimo od sajber pretnji.

IZVORI

ITU Guide to National Cybersecurity Strategies (ITU Vodič za nacionalne strategije sajber bezbednosti), dostupno na https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018

https://www.enisa.europa.eu/publications/ncss-good-practice-guide

Microsoft, Developing a National Strategy for Cybersecurity: Foundations for Security, Growth and Innovation (Majkrosoft, Razvoj nacionalne strategije sajber bezbednosti: Temelji bezbednosti, rasta i inovacije), dostupno na https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVoNi

Global Partners Digital: Multistakeholder Approaches to National Cybersecurity Strategy Development, (Pristupi razvoju nacionalne strategije sajber bezbednosti koji obuhvataju više interesnih strana), jun, 2018, dostupno na https://www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf

Organization for American States, Cybersecurity Awareness Campaign Toolkit, (Organizacija američkih država, Uputstva za kampanju podizanja svesti o sajber bezbednosti), 2016, dostupno na https://thegfce.org/wp-content/uploads/2020/06/2015-oas-cyber-security-awareness-campaign-toolkit-english-1.pdf

POGLAVLJE 6
USPEŠNA SARADNJA JAVNOG I PRIVATNOG SEKTORA U SAJBER PROSTORU

CILJEVI

Ovo poglavlje pruža korisnicima pregled dobrih i loših strana privatno- -javnih partnerstava u oblasti sajber prostora, a posebno između agencija koje sprovode zakon i privatnih kompanija prilikom istraživanja kriminalnih radnji i nezakonitog sadržaja na Internetu.

Šta ćemo naučiti ovom poglavlju?

- Upoznaćemo bolje koncepte inicijativa koji uključuju više interesnih strana i javno-privatna partnerstva.
- Postaćemo svesniji saradnje između agencija koje sprovode zakon i privatnih kompanija.
- Bolje ćemo razumeti koji su to elementi neophodni za stvaranje uspešnih pristupa sajber bezbednosti, a obuhvataju više interesnih strana.

Uvod

Sajber bezbednost pokriva više oblasti i zajednički je cilj svake Strategije nacionalne bezbednosti (engl. NCSS). Upravo iz ovog razloga je saradnja između javnih i privatnih sajber aktera neophodna kako bi se unapredila sajber bezbednost. Pristupi sajber prostoru i sajber bezbednosti koji obuhvataju više interesnih grupa (javno-privatna partnerstva; engl. PPP), postaju sve važniji kod upravljanja sajber bezbednošću, kako zbog veoma velike uloge koju imaju privatne kompanije, tako i zbog transnacionalne odlike sajber prostora. Uspešna saradnja između svih interesnih strana (vlade, sektor IKT-a, fakulteta i civilnog društva) postala je jedan od osnovnih elemenata za primenu međunarodnih standarda i normi delotvorne NCSS-a.

Ulaganje sve većih napora u sajber bezbednost, koji kombinuju javne, javno-privatne i privatne mehanizme, postalo je odlika veoma važne promene načina obavljanja poslova na globalnom nivou. U skladu sa ovim trendom, saradnja između velikog broja različitih interesnih strana (država, biznisa i civilnog društva) može da se posmatra kao pragmatičan odgovor koji služi da popuni jaz prilikom primene tradicionalnih regulatornih pristupa u upravljanju. Zaista ovakve inicijative imaju za cilj da pruže podršku uspešnom rukovođenju tako što obezbeđuju komercijalnim akterima da rade u okvirima poštovanja vladavine prava i poštovanja ljudskih prava. Grupe koje se sastoje od različitih interesnih strana mogu zajedno da osmisle bolje pristupe i rešenja nego što bi to učinila samo jedna grupa.

1. Šta su javno-privatna partnerstva?

Pregled

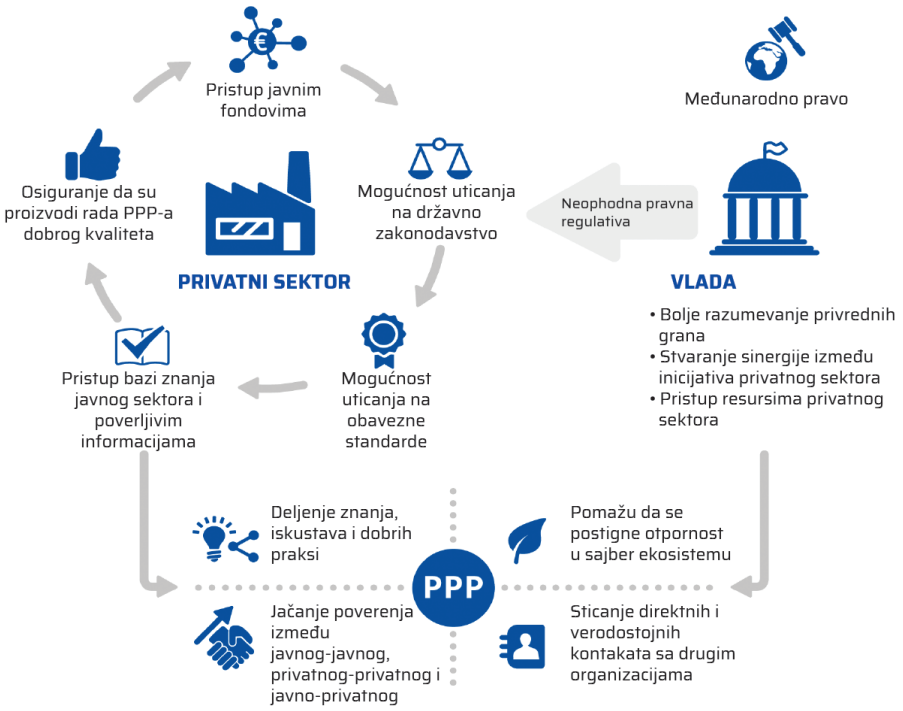
Javno-privatna partnerstva uključuju deljenje resursa (oprema, veštine, stručna znanja i finansije), rizika i nagrada između interesnih grupa. U oblasti sajber bezbednosti PPP označava saradnju između vlada i javnih institucija, sa jedne strane, i IKT-a, fakulteta i civilnog društva, sa druge strane, kako bi se proširila svest o sajber bezbednosti, ublažili rizici sajber bezbednosti i stvorili snažni kapaciteti za nju. Ova saradnja se odvija na više polja i može da obuhvati unapređenje kapaciteta za sajber odbranu i deljenje informacija. Ekonomski interesi, regulatorni zahtevi i odnosi s javnošću mogu takođe da budu vodeća sila PPP-a. U zemljama u razvoju PPP-ovi iz oblasti sajber bezbednosti se bave širenjem svesti o sajber bezbednosti ili obezbeđivanjem snažnih nacionalnih kapaciteta za sajber bezbednost.

Za sajber bezbednost PPP-ovi mogu da budu korisni iz više razloga:

- u mogućnosti su da podrže širenje svesti o sajber bezbednosti i razumevanje širom organizacija i društva;
- u mogućnosti su da unaprede nacionalnu bazu sajber veština putem pokretanja inicijativa koje su tako osmišljene da otkriju, inspirišu i osposobe više ljudi da postanu profesionalci iz oblasti sajber bezbednosti;
- u mogućnosti su da nagrade profesionalce iz sajber bezbednosti odgovarajućim finansijskim i tehničkim resursima preko odgovarajućih inicijativa;
- u mogućnosti su da podstaknu istraživanja i razvoj u sferi sajber bezbednosti;
- u mogućnosti su da spreče kriminal i prijave prevare;
- u mogućnosti su da izdaju sertifikat i akreditaciju iz sajber bezbednosti;
- u mogućnosti su da povežu i ojačaju saradnju između javnih i privatnih lica koja se bave sajber bezbednošću.

PPP-ovi u oblasti sajber bezbednosti mogu da budu podeljeni na četiri tipa:

- institucionalni PPP-ovi koji su formirani u okviru jednog pravnog dokumenta i koji su u vezi sa zaštitom kritične infrastrukture, a zajednička sredstva saradnje su radne grupe, grupe za brzo reagovanje i dugoročne zajednice;
- PPP-ovi sa određenim ciljem koji su napravljeni kako bi se izgradila kultura sajber bezbednosti preko platformi ili saveta koji okuplja privatni i javni sektor da bi pritom razmenili znanja i dobre prakse, a koje je usmereno na jednu temu ili jedan specifičan cilj;
- spoljni saradnici koji su angažovani za usluge iz oblasti sajber bezbednosti, a osnovani su u trenutku kada vlade ne mogu uspešno da odgovore na određene potrebe privatnog sektora i kada se PPP ponaša kao nezavisna treća strana, ali pruža aktivnu podršku potrebama privrede i vladama pri donošenju politika ili kod njihove primene;
- hibridni PPP-ovi, a to su timovi Centra za bezbednost informaciono- -komunikacionih sistema (engl. Computer Emergency Response Teams (CERT)) koji funkcionišu pod jednim okvirom PPP-a, a vlade im dodeljuju zadatke sprovođenja usluga CERT-a u okviru državne administracije ili cele zemlje.



Razlozi i motivacija za stvaranje javno-privatnih partnerstava

Izvor: Javno-privatna partnerstva u sajber prostoru, ENISA, novembar, 2017, strana 14

2. Uloga vlada i drugih interesnih strana

Ključna uloga javnih institucija prilikom saradnje više interesnih strana

Vlade imaju glavnu ulogu prilikom razvijanja jedne uspešne NCSS-a. Donosioci zakona i politika su odgovorni za kreiranje adekvatnih okvira, u skladu sa obavezama države prema međunarodnom pravu, kao i nacionalnim zakonima. Vlade sarađuju sa privatnim akterima kao što su IKT kompanije kako bi bile sigurne da je i zajednička regulativa i samoregulativa usklađena sa međunarodnim i nacionalnim zakonima za zaštitu ljudskih prava.

Osim ovog čisto pravnog pristupa, države mogu da igraju važnu ulogu prilikom koordinisanja i saradnje sa sektorom IKT-a i civilnim društvom tako što će napraviti i pružati podršku platformama za saradnju. Ovo je naročito važno za nacionalne jedinice za upućivanje koje traže i skreću pažnju na sumnjive onlajn kontakte i zahtevaju uklanjanje sadržaja putem procesa upućivanja upozorenja IKT kompanijama. Platforme za saradnju mogu da obezbede vrednosne informacije vlada i doprinesu ojačanju inkluzivnijeg procesa donošenja odluka. Otvoreni kanali komunikacije između odgovarajućih interesnih strana mogu da pomognu da se otkriju i popune kritične praznine kod sajber bezbednosti, kao i da se spreči mogući sukob interesa. Napori koji su koordinisani i institucionalizovani takođe su u mogućnosti da promovišu komplementarne aktivnosti i da usmeravaju ljudske i finansijske resurse između različitih interesnih strana.

STUDIJA SLUČAJA: CERT-OVI

CERT-ovi su jedinice stručnjaka koje imaju za zadatak da pomognu pojedincima ili institucijama, žrtvama sajber napada. Njihov glavni zadatak je da otkriju zlonamerni malver i spreče njegovo dalje širenje preko mreže dok istovremeno rešavaju posledice napada. Ovakve jedinice se često nalaze pri privatnim kompanijama ili državnim institucijama, ali mogu da postoje i na nacionalnom nivou kao odvojena vladina agencija koja nudi pomoć širokom spektru privatnih i javnih pravnih lica.

Iako su nacionalni CERT-ovi državne agencije, one predstavljaju dobar primer javno- -privatne saradnje. Osnovna funkcija svakog CERT-a je da pruži informacije o nedavno otkrivenim sajber ranjivostima uključujući i odgovarajuće ažuriranje softvera i takozvanih zakrpa. Većini nacionalnih CERT-ova možemo da se obratimo i prijavimo sajber rizike ili sajber incidente putem onlajn javno dostupnog formulara. Neki nacionalni CERT-ovi čak imaju mobilne timove koje mogu da pošalju u neku instituciju kojoj je potrebna pomoć u slučaju sajber napada.

Saradnja između privatnog i javnog sektora je od suštinske važnosti za održavanje i obezbeđivanje sajber okruženja. Javne institucije ne mogu same da čuvaju sajber prostor iz dva glavna razloga. Prvo, privatni sektor je taj koji upravlja inovacijama na ovom polju i kontroliše najveći deo sajber prostora. Drugo, čak i one kritične infrastrukture koje su u vlasništvu države i pod njenom kontrolom se u velikoj meri oslanjaju na proizvode i usluge privatnih kompanija kako bi se zaštitile.

Štaviše, vlade su u obavezi da poštuju i štite ljudska prava svojih građana onlajn i zato moraju da se postaraju da nijedna aktivnost od strane privatnih kompanija i nacionalnih CERT-ova ne krši ljudska prava, a posebno pravo na privatnost i slobodu izražavanja. Kako bi ispunili ovaj cilj, CERT-ovi bi trebalo da budu oslobođeni političkog uticaja i ne bi trebalo da budu instrumenti vlada koje bi ih koristile za upade u kompjuterske sisteme i narušavale privatnost mreže ili poverljivost komunikacija.

Pri uspostavljanju nacionalnih CERT-ova vlade bi trebalo da imaju na umu ljudsku dimenziju sajber bezbednosti, sa osvrtom na sva tri aspekta: poverljivost, dostupnost i integritet. Stoga moramo da shvatimo da se sajber bezbednost u svojoj osnovi ne odnosi samo na obezbeđivanje mreže, već i na poboljšanje bezbednosti ljudi. Ako govorimo o zaštiti poverljivosti informacija, trebalo bi da se vodimo načelom prava na privatnost kao vodećim standardom za sve operacije zaštite i unapređivanja poverljivosti podataka. Što se tiče dostupnosti podataka važno je da se poštuje i štiti sloboda izražavanja i informacija.

Izvor: https://www.africacert.org/african-csirts/

STUDIJA SLUČAJA: ISTRAŽNA INTERNET JEDINICA EVROPSKE UNIJE I NACIONALNI NIVO

Istražna internet jedinica (engl. Internet Referral Unit (IRU)) Evropske unije je deo Evropol- -ovog Evropskog centra za borbu protiv terorizma i sastoji se od tima stručnjaka za terorizam koji je podstaknut verskim razlozima, zatim jezičke, informacione i komunikacione tehnologije i agencija specijalizovanih za borbu protiv terorizma[1] koje sprovode zakon. Počela je sa radom 2015. godine i mandatom:

- Spružanja podrške odgovarajućim telima Evropske unije putem obezbeđivanja strateških i operativnih analiza;
- upozorenja na teroristički i nasilno ekstremistički onlajn sadržaj i podele saznanja sa odgovarajućim partnerima;
- otkrivanja i zahtevanja uklanjanja internet sadržaja koje koriste mreže za trgovinu ljudi kako bi privukle migrante i izbeglice;
- pružanja brze podrške i reagovanja na proces prijavljivanja prekršaja ili sumnjivih sadržaja, blisko sarađujući sa industrijom[2].

Na osnovu izveštaja EU IRU-a o transparentnosti iz 2017.godine „saradnja sa privatnim sektorom je od suštinske važnosti kod prevencije".[3] Od svog osnivanja, jula 2015.godine do decembra 2017, EU IRU je procenila da je bilo 46,392 terorističkih sadržaja koji su doveli do 44,807 odluka za opoziv, pri čemu je 92% sadržaja uklonjeno.[4]

Kao što je naglašeno u Izveštaju o transparentnosti i mandatu EU IRU-a, IRU je odgovoran za procenu onlajn sadržaja i skretanje pažnje odgovarajućim IKT kompanijama da uklone svoj sadržaj. Kao takva EU IRU se usredsređuje na sadržaj koji objavljuje Al Kaida, Daeš i njihove pristalice i vrši procenu ovog sadržaja u odnosu na mandat Evropol-a, a u skladu sa principima istaknutim u Direktivi EU-e o borbi protiv terorizma. Direktiva EU-e o borbi protiv terorizma obezbeđuje zaštitu po pitanju uklanjanja sadržaja, kao što je naznačeno u članu 21. (3):

„Mere za uklanjanje i blokiranje moraju da budu uspostavljene uz poštovanje sledećih transparentnih procedura u cilju obezbeđivanja adekvatne zaštite, sa posebnim naglaskom na ograničavanje mera na ono što je neophodno i proporcionalno, kao i na obaveštavanje korisnika o razlozima za preduzimanje tih mera. Uklanjanje ili blokiranje sadržaja mora da uzme u obzir mogućnost ulaganja pravnog leka.[5]

1 https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru
2 https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru
3 https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-transparency-report-2017
4 https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-transparency-report-2017
5 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32017L0541

U slučaju da ocenjeni sadržaj nije u okviru mandata Evropol-a, šalje se IKT kompaniji na čijoj je platformi otkriven. Sve u svemu, na kraju je na kompaniji i njenom diskrecionom pravu da odluči da li će da ukloni ili neće da ukloni pronađeni sadržaj nakon procene da li je to protivno njenim pravilima i uslovima. EU IRU nema pravno ovlašćenje da skine taj sadržaj.

Slične istražne jedinice postoje u UK-u, Francuskoj i Holandiji dok je Evropol objavio da su uspostavljeni paralelni mehanizmi i u Belgiji, Nemačkoj i Italiji.[6]

EU IRU dodatno organizuje takozvane zajedničke dane za akcije pod nazivom Referral Action Days sa IKT kompanijama poput Gugla, Tvitera i Telegrama. Ovi zajednički dani za akcije (engl. Referral Action Days) okupljaju specijalizovane jedinice za sprovođenje zakona iz raznih nacionalnih IRU-a kao i samu EU IRU i IKT kompanije. Specijalisti za sprovođenje zakona vrše procenu stotine hiljada potencijalnog terorističkog sadržaja na nekoj određenoj platformi kako bi otkrili način na koji teroristi i nasilne ekstremističke grupe koriste datu platformu. Oni dalje dele svoja saznanja sa odgovarajućom prisutnom IKT kompanijom koja pregleda i procenjuje sadržaj u odnosu na svoje uslove poslovanja. Kompanija donosi konačnu odluku o uklanjanju pronađenog sadržaja. Ovi zajednički dani za akcije promovišu koordinisani pristup između vlada i IKT kompanija kada je u pitanju rešavanje problema nasilnog ekstremističkog i terorističkog sadržaja na Internetu.[7]

Inicijative koje vode IKT industrije i civilno društvo

IKT kompanije se često suočavaju sa problemima zajedničke regulative i samoregulative njihovih platformi, a posebno po pitanju zaštite ljudskih prava kao što su sloboda govora i pravo na privatnost. Ove probleme usložnjava činjenica da su platforme društvenih medija postale jedna od osnovnih mesta na kojima građani razgovaraju, dele ili pronalaze informacije. Kao odgovor na to IKT industrija vodi inicijative za razmenu znanja i tehnologija među kompanijama, formira platforme za interaktivne alatke i resurse za ublažavanje sadržaja, vrši obuke za pristupe uklanjanju sadržaja koje vode veće kompanije za one manje, a sve to zajedno predstavlja jedno uspešno sredstvo za jačanje sajber bezbednosti.

6 Vidi https://www.europol.europa.eu/newsroom/news/referral-action-day-six-eu-member-states-and-telegram

7 Vidi https://www.europol.europa.eu/newsroom/news/eu-law-enforcement-and-google-take-terrorist-propaganda-in-latest-europol-referral-action-days; https://www.europol.europa.eu/newsroom/news/referral-action-day-six-eu-member-states-and-telegram

STUDIJA SLUČAJA: INHOPE

Međunarodna asocijacija internet tzv. vrućih linija (engl. International Association Of Internet Hotlines) prisutna je u 43 zemlje i daje svoj doprinos tako što osigurava da na internetu „nema seksualne zloupotrebe i eksploatacije dece."[8] Njena misija je da „pomogne međunarodnim inicijativama u borbi protiv bilo kakvog materijala koji podrazumeva seksualnu zloupotrebu dece."[9] Partneri INHOPE-a su predstavnici različitih interesnih grupa uključujući Interpol, Evropol, Tviter, Krisp, Majkrosoft, Gugl, Fejsbuk i Trend MICRO.

INHOPE se sastoji od 48 vrućih linija, koje javnosti obezbeđuju mehanizam za prijavljivanje onlajn sadržaja ili aktivnosti, za koji se sumnja da je protivzakonit. INHOPE deli nezakonite aktivnosti na dve različite kategorije: krivično nezakonite aktivnosti koje istražuju i gone organi za sprovođenje zakona, na koje se INHOPE vruće linije usredsređuju, i civilne nezakonite aktivnosti koje mogu da gone civilni organi.

INHOPE se najviše bavi seksualnom zloupotrebom dece, uključujući i onlajn prilaženje i udvaranje, ali se bavi i govorom mržnje i ksenofobičnim onlajn sadržajima. INHOPE daje određenu definiciju govora mržnje mada priznaje da je govor mržnje sam po sebi „izuzetno složena stvar" koja se često ne smatra nezakonitom po krivičnom zakonu. Stoga svaka prijava govora mržnje se procenjuje u odnosu na nacionalno zakonodavstvo, tj. tamo gde je pronađen dati sadržaj.[10]

Sav anonimno prijavljeni sadržaj pregleda analitičar za sadržaj vrućih linija (engl. Hotline Content Analyst) kako bi ocenio da li je nezakonit. Ukoliko analitičar smatra da je prijavljeni sadržaj nezakonit, pratiće njegovu lokaciju. Ukoliko se sadržaj nalazi u datoj zemlji, materijal se prijavljuje nadležnoj nacionalnoj agenciji za sprovođenje zakona i/ili IKT kompaniji da ga uklone. Ukoliko je materijal otkriven u nekoj drugoj zemlji, prosleđuje se njihovim vrućim linijama.

INHOPE je dalje razvio Pravila načina rada Internet hotlajn servera (engl. Code of Practice for Internet Hotline Providers) koja kažu da bi zemlje članice INHOPE-a trebalo redovno da konsultuju značajnije interesne strane, uključujući vlade, agencije za sprovođenje zakona, IKT industriju, institucije za brigu o deci, kao i da bi sve članice trebalo da poštuju principe transparentnosti, odgovornosti, preuzimanja dužnosti i pouzdanosti.

8 https://www.inhope.org/EN
9 https://www.inhope.org/EN/our-story
10 https://www.inhope.org/EN

INHOPE takođe ističe važnost dobrobiti zaposlenih, onih koji pregledaju prijavljene sadržaje, i prihvatanje psihološkog opterećenja pod kojim se oni nalaze prilikom gledanja sadržaja zloupotrebe dece i nasilnog ekstremizma ili terorizma. „Bela knjiga“ koju je napisao i objavio francuski hotlajn Point de Contact ima za cilj da razvije opšti skup najboljih praksi za operativni rad i obradu štetnog i potencijalno nezakonitog sadržaja koji može da ugrozi fizičku bezbednost, kao i psihološko stanje profesionalaca koji pregledaju date sadržaje[11].

3. Stvaranje javno-privatnih partnerstava u sajber bezbednosti

Dobra praksa 1: Preduslov za uspostavljanje uspešnih PPP-ijeva je okruženje koje omogućava njihov rad.

Stvaranje okruženja koje omogućava neometani rad je od suštinske važnosti za uspešnost PPP-ijeva. Ovo se odnosi na četiri ključne dimenzije: formulisanje politika, pravni i regulatorni okvir, institucionalne sporazume i finansijsku podršku/investicije. Smernice Evropske unije dodatno ističu važnost fleksibilnosti i transparentnosti svih partnera, kao i zajedničko priznavanje i prihvatanje potreba i ciljeva različitih uključenih strana.[12]

Stvaranje ovakvog okruženja trebalo bi da podrazumeva da uključene strane sklapaju sporazume koji predstavljaju pravnu osnovu PPP-ija. Državne institucije bi trebalo da rukovode procesom formiranja PPP-ijeva ili da to čine nacionalni akcioni planovi. Da bismo mogli to da učinimo, neophodno je da odgovarajući resursi budu obezbeđeni za internu koordinaciju i saradnju PPP-ijeva, kao i da se usvoje pragmatični pristupi rešavanja problema koordinacije i saradnje. Osnaživanje učešća privatnog sektora, a posebno malih i srednjih preduzeća, takođe je važno kako bismo obezbedili odgovarajuće okruženje koje će dalje da promoviše koordinaciju i saradnju između odgovarajućih strana. Na kraju, interesne strane u okviru privatno-javnih partnerstava bi trebalo da ulažu u otvorenu komunikaciju sa širom javnošću.

Dobra praksa 2: Jasno razgraničene odgovornosti u cilju zaštite ljudskih prava.

Uspostavljanje jasno razgraničenih odgovornosti svih interesnih strana je preduslov za sprečavanje kršenja ljudskih prava. U kontekstu NCSS-a, PPP može da predstavlja jedinstveni problem iz većeg broja razloga, uključujući nevoljnost političara da preuzmu odgovornost za donošenje strožeg zakonodavstva iz sajber bezbednosti, zajedno sa

11 https://www.pointdecontact.net/wp-content/uploads/2020/11/Livre_blanc_EN.pdf

12 EU smernice https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru

neprihvatanjem dužnosti ili odgovornosti privatnog sektora za nacionalnu bezbednost, što ostavlja ovo partnerstvo bez jasno razgraničenih odgovornosti. Stoga je neophodno da druge odrednice budu uključene u PPP sporazume po pitanju mehanizama preuzimanja odgovornosti kako bi se smanjili rizici i obezbedilo da sve interesne strane na odgovarajući način razumeju svoje uloge i zaduženja.

Dobra praksa 3: Poverenje između interesnih strana mora da se izgradi i održava.

Izgradnja i održavanje poverenja između javnih i privatnih pravnih lica je jedan od najvećih izazova PPP-a. Razvijanje i održavanje poverenja je proces koji traje i koji je specifičan za svaku kulturu, a zasniva se na izgradnji ličnih veza. Nema poverenja bez okruženja koje ga podržava. Drugi problemi su nedostatak ljudskih resursa, kako u javnom, tako i u privatnom sektoru, nedovoljno veliki budžet javnog sektora i manjak resursa koji ne može da ispuni očekivanja privatnog sektora, kao i nedovoljno razumevanje i nepostojanje dijaloga između javnog i privatnog sektora po pitanju samog koncepta PPP-a.

Državne agencije i privatna pravna lica moraju da grade poverenje na osnovama otvorenosti, pravičnosti i međusobnog poštovanja. U slučaju PPP-a deljenje informacija je odličan test poverenja. Učesnici bi trebalo da imaju osećaj da dobijaju dodatne korisne informacije i da su deo tog partnerstva, kao i da u isto vreme osećaju da su njihovi podaci bezbedni i sigurni.

STUDIJA SLUČAJA: GLOBALNI FORUM O SAJBER EKSPERTIZI

Globalni forum o sajber ekspertizi (engl. GFCE) je platforma na kojoj države, međunarodne organizacije i privatne kompanije mogu da razmene najbolje prakse i stručna znanja o izgradnji sajber kapaciteta.

GFCE je počeo sa radom aprila 2015.godine sa glavnim ciljem da bude posvećena, neformalna platforma za donosioce politika, za one koje ih sprovode i stručnjake iz različitih zemalja i regiona kako bi mogli da razmenjuju iskustva, stručna znanja i procene ključnih regionalnih i tematskih sajber problema. Od samog početka GFCE je postao pretežno platforma za koordinaciju. Glavne oblasti za izgradnju kapaciteta i stručnih znanja su bile sajber bezbednost, sajber kriminal, zaštita podataka i e-uprava. GFCE je 2019.godine postao platforma koja je omogućila i koordinisala razmenu znanja i ekspertize za primenu izgradnje sajber kapaciteta. Štaviše, različite radne grupe GFCE-a su počele da osnivaju mehanizme tzv. 'clearing house-a' (mesto na kome se prikupljaju i dele informacije).

Izvor: 'History', the GFCE (Istorijat GFCE-a)

ZAKLJUČAK

- U sajber prostoru veća je verovatnoća da grupe sastavljene od više interesnih strana budu uspešnije nego ukoliko svaka radi samostalno. Ovi pristupi koji uključuju više interesnih grupa, poznati pod nazivom javno-privatna partnerstva (engl. PPP), mogu zajedno da dođu do boljih pristupa i rešenja i tako postanu sve značajniji prilikom upravljanja sajber prostorom i rešavanja problema iz oblasti sajber bezbednosti.
- PPP-ijevi su uspostavljeni putem sporazuma o saradnji između javnih i privatnih institucija.
- Vlade mogu da imaju važnu ulogu u koordinaciji i saradnji sa IKT sektorom i civilnim društvom putem stvaranja i pružanja podrške platformama za saradnju.
- Privatni akteri (IKT grana privrede) mogu da vode uspešne inicijative koje uključuju više interesnih strana u oblasti sajber bezbednosti.
- Vlade bi trebalo da investiraju u pragmatične pristupe izgradnje PPP-ova koji podrazumevaju otvorenu komunikaciju, inkluzivno učešće i motivisanje učešća većeg broja predstavnika privatnog sektora.

IZVORI

Public-Private Partnerships in Cyberspace, ENISA, November 2017, (Javno-privatno partnerstvo u sajber prostoru, ENISA, novembar, 2017.) dostupno na https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models/at_download/fullReport

Public-private partnerships in national cyber-security strategies (Javno-privatna partnerstva u nacionalnim strategijama sajber bezbednosti) dostupno na https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf

US National Council for Public Private Partnerships Definition of PPPs (Američko nacionalno veće za javno privatna partnerstva, definicija PPP-a), 2016.

Public Private Partnerships in the EU: Widespread shortcomings and limited benefits (Javno privatna partnerstva u EU: Opšte poznati nedostaci i ograničene koristi)

http://publications.europa.eu/webpub/eca/special-reports/ppp-9-2018/en/

African CERTs (Afrički CERT-ovi) https://www.africacert.org/african-csirts/

EU IRU, dostupno na https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru

www.dcaf.ch