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

Udhëzues për qeverisjen e mirë me sigurinë kibernetike

Përmbajtja

HYRJE E PËRGJITHSHME		4
KAPITULLI 1	PARAQITJA E QEVERISJES SË MIRË TË SEKTORIT TË SIGURIS	5
KAPITULLI 2	SI LIDHEN HAPËSIRA KIBERNETIKE DHE SIGURIA KIBERNETIKE ME QEVERISJEN E MIRË TË SEKTORIT TË SIGURISË	25
KAPITULLI 3	KORNIZAT JURIDIKE NDËRKOMBËTARE DHE RAJONALE NË HAPËSIRËN KIBERNETIKE	39
KAPITULLI 4	ZBATIMI I NORMAVE DHE STANDARDEVE NDËRKOMBËTARE DHE RAJONALE NË NJË KONTEKST KOMBËTAR	57
KAPITULLI 5	STRATEGJITË KOMBËTARE TË SIGURISË KIBERNETIKE	69
KAPITULLI 6	LLOGARITET SE 15% E PUNËTORËVE SI NË SEKTORIN SHTETËROR ASHTU EDHE ATË PRIVAT HUMBËN VENDET E TYRE TË PUNËS NË 2009-2010	87

Hyrje e përgjithshme

Aksesi gjithnjë e më i madh i njerëzve në hapësirën kibernetike dhe burimet e saj, ndikon në jetën tonë të përditshme dhe ka një ndikim të konsiderueshëm në shoqëritë tona. Ajo tashmë ka transformuar thellësisht mënyrën se si jetojmë, punojmë dhe bashkëveprojmë. Hapësira kibernetike ofron mundësi të panumërta për zhvillimin ekonomik, ndërveprimin shoqëror dhe shkëmbimet politike. Ajo ka siguruar mjete për të kryer mbikëqyrje të paligjshme, për të mbledhur të dhëna personale, për të ndikuar në proceset demokratike, për të kryer krime dhe për të ndryshuar mjetet dhe metodat e luftës.

Këto sfida kërkojnë përgjigje të shumta dhe qeveritë, sektori privat dhe shoqëria civile duhet të bashkohen për të adresuar sfidat e qeverisjes së sigurisë kibernetike. Për më tepër, kornizat ligjore dhe të politikave do të duhet të përshtaten për respektimin dhe zbatimin më të mirë të normave ndërkombëtare të të drejtave të njeriut, ndërsa luftojnë në mënyrë efektive krimin kibernetik, veprimet keqdashëse kibernetike, sulmet kibernetike si dhe përdorimin e internetit për qëllime terroriste dhe promovimin e ekstremizmit të dhunshëm. Vetëm veprimi i fuqishëm në këtë drejtim do të promovojë një hapësirë kibernetike të sigurt, të qëndrueshme dhe të hapur.

Në këtë kontekst Drejtoria e Bashkëpunimit të Sigurisë dhe Mbrojtjes (DCSD) e Ministrisë Franceze për Evropën dhe Punët e Jashtme dhe Qendra për Qeverisjen e Sektorit të Sigurisë, Gjenevë (DCAF) filluan në 2018 hartimin e këtij udhëzuesi për praktikat e mira për promovimin e qeverisjes së mirë në hapësirën kibernetike. Në vitin 2020, ky udhëzues u përkthye në serbisht, shqip, maqedonisht dhe anglisht si pjesë e projektit DCAF Përmirësimi i Qeverisjes së Sigurisë Kibernetike në Ballkanin Perëndimor me mbështetjen e Zyrës së Jashtme, të Komonuelthit dhe Zhvillimit të Mbretërisë së Bashkuar.

Ky Udhëzues është shkruar për politikëbërësit, ekspertët teknikë, shoqërinë civile dhe të gjithë ata që janë të interesuar për praktikat më të mira të qeverisjes së sigurisë kibernetike. Ai mbështetet në përvojën e DCAF në promovimin e qeverisjes së mirë në sektorin e sigurisë.

Ky libër përbëhet nga gjashtë kapituj që shpjegojnë se si të zbatohen parimet e qeverisjes së mirë për sigurinë kibernetike. Kapitujt përqendrohen në temat vijuese:

- qeverisja e mirë e sektorit të sigurisë dhe zbatimi i tij në hapësirën kibernetike;
- lidhja midis hapësirës kibernetike, sigurisë kibernetike dhe qeverisjes së sektorit të sigurisë;
- kornizat ligjore ndërkombëtare dhe rajonale të zbatueshme në hapësirën kibernetike;
- zbatimi i standardeve ndërkombëtare dhe rajonale;
- strategjitë kombëtare të sigurisë kibernetike;
- promovimin i bashkëpunimit efektiv midis sektorit publik dhe privat në hapësirën kibernetike.

KAPITULLI 1
PARAQITJA E QEVERISJES SË MIRË TË SEKTORIT TË SIGURISË

OBJEKTIVAT

Ky kapitull synon të rrisë njohurinë dhe kuptimin e përdoruesve për termat kryesorë në lidhje me qeverisjen e mirë të sektorit të sigurisë; me synimin për t'i vendosur ata brenda kontekstit të hapësirës kibernetike. Për këtë qëllim, ky kapitull synon të përqendrohet në tre përbërës thelbësorë të qeverisjes së mirë të sektorit të sigurisë që janë gjithashtu të rëndësishëm në hapësirën kibernetike:

- a. Llogaridhënia,
- b. Transparenca, dhe
- c. Sundimi i ligjit

Pas prezantimit të këtyre koncepteve, sfidat specifike në lidhje me promovimin e këtyre parimeve të qeverisjes së mirë në hapësirën kibernetike do të paraqiten edhe praktika e mira të identifikuara.

Objektivat e nxënies së këtij kapitulli janë si më poshtë:

- Rritja e ndërgjegjësimit për termat dhe përkufizimet kryesore në lidhje me qeverisjen, qeverisjen e sektorit të sigurisë dhe qeverisjen e mirë të sektorit të sigurisë.
- Kuptimi i shtuar për konceptin themelor të parimeve të qeverisjes së mirë, siç janë llogaridhënia, transparenca dhe sundimi i ligjit.
- Rritja e njohurive në lidhje me parimet themelore të qeverisjes së mirë të sektorit të sigurisë.
- Rritja e të kuptuarit mbi rëndësinë e promovimit të parimit të qeverisjes së mirë në hapësirën kibernetike.

1. Hyrje

Qeverisja, Qeverisja e sektorit të sigurisë dhe Qeverisja e mirë e sektorit të sigurisë

Qeverisja përshkruan 'ushtrimin e pushtetit dhe autoritetit'. Si një koncept i përgjithshëm, qeverisja mund të përdoret për të përshkruar rregullat me të cilat drejtohet çdo organizatë, duke përfshirë subjektet tregtare private dhe jofitimprurëse. Brenda sektorit të sigurisë, "qeverisja" përdoret për të përshkruar të gjitha vendimet formale dhe joformale, proceset dhe aktorët që ndikojnë në sigurimin e të mirave publike, të tilla si shëndetësia, arsimi ose siguria.

Qeverisja e sektorit të sigurisë (QSS) përshkruan 'ushtrimin e pushtetit dhe autoritetit në kontekstin e një sektori të veçantë të sigurisë kombëtare'.[1] Është një koncept analitik që nuk bazohet në një përkushtim ndaj normave ose vlerave specifike.

> Qeverisja e mirë e sektorit të sigurisë përqendrohet posaçërisht në zbatimin e parimeve të qeverisjes së mirë për sigurimin, menaxhimin dhe mbikëqyrjen e sigurisë në mjedisin kombëtar.

Koncepti i QSS-së së përshkruan mirë se si ta bëjmë sektorin e sigurisë së një shteti më efektiv dhe të përgjegjshëm brenda një kornize të kontrollit civil demokratik, respektimit të të drejtave të njeriut dhe parimit të shtetit të së drejtës[2].

Për më tepër, QSS-ja e mirë bazohet mbi idenë se sektori i sigurisë duhet të mbahet në të njëjtat standarde të larta të ofrimit të shërbimeve publike si ofruesit e tjerë të sektorit publik. Prandaj, një sektor i sigurisë që nuk përputhet me këto standarde mund të sfidojë stabilitetin politik, ekonomik dhe shoqëror në një kontekst kombëtar (i përshkruar gjithashtu si 'QSS e dobët').

1 Dokument informues i DCAF-it për reformën e sektorit të sigurisë (shih. Bibliografinë).
2 Ibid.

Çfarë është sektori i sigurisë?

Në përgjithësi, një sektor i sigurisë përbëhet nga të gjitha strukturat, institucionet dhe personeli përgjegjës për sigurimin, menaxhimin dhe mbikëqyrjen e sigurisë në nivelet kombëtare dhe lokale.[3]

Prandaj, sektori i sigurisë në një shtet nuk duhet të veprojë si ofruesi i vetëm i sigurisë dhe drejtësisë. Vetë njerëzit shpesh ofrojnë siguri dhe drejtësi në shtëpitë dhe komunitetet e tyre, pavarësisht se a vepron shteti për të përmbushur këto nevoja apo jo. Veçanërisht, njerëzit mund të organizohen dhe të ofrojnë siguri në mënyra të ndryshme, duke përfshirë rojëmbajtje në lagje, grupe të grave ose ofrimit komercial të sigurimit.

Për më tepër, rolet zakonore të figurave të rëndësishme të komunitetit në sigurinë dhe vendimmarrjen në drejtësi, mekanizmat alternativë të zgjidhjes së mosmarrëveshjeve, traditat dhe rregullat joformale mund të formojnë sigurinë dhe ofrimin e drejtësisë brenda një komuniteti. Si pasojë, këto grupe të komunitetit janë gjithashtu pjesë e sektorit të sigurisë dhe drejtësisë në kuptimin e gjerë.

Sektori i sigurisë përbëhet nga të gjitha strukturat, institucionet dhe personeli përgjegjës për sigurimin, menaxhimin dhe mbikëqyrjen e sigurisë në nivel kombëtar dhe lokal, duke përfshirë:

- Ofruesit e sigurisë , siç janë forcat e armatosura, policia, rojet e kufirit, shërbimet e inteligjencës, institucionet penale dhe korrigjuese dhe ofruesit joshtetërorë të sigurisë;
- Organet e menaxhimit dhe mbikëqyrjes së sigurisë , siç janë ministritë e qeverisë, parlamenti, institucionet e posaçme të mbikëqyrjes ligjore, pjesë të sektorit të drejtësisë dhe aktorët e shoqërisë civile me një interes në standardet e larta të ofrimit të sigurisë publike, duke përfshirë organizatat e grave dhe mediat.

Duhet theksuar se reforma e sektorit të sigurisë (RSS) bazohet në një kuptim të gjerë të sektorit të sigurisë. RSS-ja është një proces qëllimi përfundimtar i të cilit është arritja e qeverisjes së mirë të sektorit të sigurisë për të promovuar sigurinë e njeriut dhe shtetit.

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

3 Ibid.

Ofruesit joshtetërorë të shërbimeve të sigurisë dhe drejtësisë përfshihen në përkufizimin më të gjerë të sektorit të sigurisë për shkak të efektit të tyre të drejtpërdrejtë në qeverisjen e sektorit të sigurisë. Në dy dekadat e fundit, ofruesit privatë të sigurisë janë vendosur, gjithnjë e më shumë, për të ofruar siguri dhe shërbime në mbrojtjen e njerëzve dhe pronës. Në veçanti, kompanitë private ushtarake dhe të sigurisë që veprojnë mbi baza komerciale janë bërë një aktor i rëndësishëm i sigurisë.

Çfarë është reforma në sektorin e sigurisë?

Një sektor i sigurisë që nuk është as efektiv dhe as i përgjegjshëm nuk mund të japë siguri për të gjithë sepse nuk mund të kryejë me besueshmëri detyrat e tij, siç janë mbrojtja kombëtare, zbatimi i ligjit ose ndihma publike. Një sektor joefikas i sigurisë ka të ngjarë të harxhojë burime publike; devijimin e fondeve nga shërbimet e tjera thelbësore publike.[4]

Reforma e sektorit të sigurisë (RSS) është procesi politik dhe teknik i përmirësimit të sigurisë njerëzore dhe shtetërore duke i bërë dispozitat e sigurisë, menaxhimit dhe mbikëqyrjes më efektive dhe të përgjegjshme brenda një kornize të kontrollit civil demokratik, shtetit të së drejtës dhe respektimit të të drejtave të njeriut[5] .

Praktikë e mirë: Të njohin që individët dhe komunitetet kanë nevoja të diferencuara të sigurisë, këtu përfshihet edhe hapësira kibernetike

Çdo person që përdor hapësirën kibernetike ka nevoja individuale të sigurisë. Në hapësirën kibernetike, gratë dhe vajzat preken në mënyrë disproporcionale nga fanatizmi, urrejtja dhe fjalimet e urrejtjes. Njohja e këtij fakti dhe rrjedhimisht sigurimi i mekanizmave efektivë për të raportuar incidentet dhe për të filluar hetimet penale mund të kontribuojë në rritjen e sigurisë së grupeve vulnerabile të prekura.

4 Ibid.

5 Dokumenti informues i DCAF-it për RSS, f. 2 në dispozicion në https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_2_Security%20Sector%20Reform.pdf

SHEMBUJ TË PRAKTIKËS SË MIRË

Benini ka nisur një fushatë vjetore të sigurisë kibernetike si pjesë e përpjekjes kombëtare për të rritur ndërgjegjësimin mbi sigurinë kibernetike në të gjithë vendin. Fushata përqendrohet tek të rinjtë e vendit dhe do të kodifikohet në dokumentin kombëtar të strategjisë së sigurisë kibernetike.

Si pjesë e lëvizjes së gjuhës pa urrejtje, shtetet anëtare të Këshillit të Evropës filluan fushata kombëtare si dhe vendosën organe kombëtare raportuese për të futur procedurat dhe mekanizmat kombëtarë të raportimit për gjuhën e urrejtjes, krimin e urrejtjes dhe ngacmimin në internet.

Në Austri, Ministria e Brendshme drejton një mekanizëm raportimi për videot ekstremiste të dhunshme dhe radikale në mënyrë që të sigurojë platformat nga fjalimet e urrejtjes.

(Burimi: Ministria Federale e Brendshme e Austrisë, http://bvt.bmi.gv.at/601/)

Policia ukrainase vendosi një pikë kontakti për të raportuar raste të ngacmimit në internet dhe të gjuhës së urrejtjes, për t'u mundësuar individëve të prekur të paraqesin ankesë.

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

Në Senegal, Shkolla Kombëtare e Sigurisë Kibernetike (Ecole Nationale en Cybersécurité à Vocation Régionale - ENVR) u krijua me mbështetjen franceze në nëntor 2018 për të forcuar mbrojtjen e Afrikës Perëndimore kundër piratëve kompjuterikë dhe përdorimin e internetit për financimin dhe propagandën e terrorizmit. Shkolla do të ofrojë trajnim për shërbimet e sigurisë, gjyqësorin dhe ndërmarrjet private për luftimin e krimit kibernetik dhe do të ketë një "rol profesional rajonal" për të ndihmuar vendet e tjera në Afrikën Perëndimore.

(Burimi: 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. Qeverisja e mirë e sektorit të sigurisë në hapësirën kibernetike

Çfarë është qeverisja e mirë e sektorit të sigurisë?

QSS-ja e mirë ka të bëjë me zbatimin e parimeve të qeverisjes së mirë për sigurinë, menaxhimin dhe mbikëqyrjen e sigurisë në një mjedis kombëtar. Shtatë parimet e qeverisjes së mirë janë:

- **Llogaridhënia**: ka pritje të qarta për ofrimin e sigurisë dhe autoritetet e pavarura mbikëqyrin nëse këto pritje përmbushen dhe vendosin sanksione nëse ato pritje nuk plotësohen.

- **Transparenca:** informacioni është lirisht i disponueshëm dhe i arritshëm për ata që do të preken nga vendimet dhe zbatimi i tyre.

- **Shteti i ligjit:** të gjithë personat dhe institucionet, duke përfshirë edhe shtetin, u nënshtrohen ligjeve që njihen publikisht, zbatohen në mënyrë të paanshme dhe në përputhje me normat dhe standardet ndërkombëtare dhe kombëtare të të drejtave të njeriut.

- **Pjesëmarrja:** të gjitha gratë dhe burrat nga të gjitha prejardhjet kanë mundësinë të marrin pjesë në vendimmarrje dhe ofrimin e shërbimeve mbi një bazë të lirë, të drejtë dhe gjithëpërfshirëse, qoftë drejtpërdrejt ose nëpërmjet institucioneve legjitime përfaqësuese.

- **Përgjigja:** institucionet janë të ndjeshme ndaj nevojave të ndryshme të sigurisë për të gjitha pjesët e popullsisë dhe kryejnë misionet e tyre në frymën e një kulture të shërbimit.

- **Efektiviteti:** institucionet përmbushin rolet, përgjegjësitë dhe misionet e tyre përkatëse me një standard të lartë profesional.

- **Efikasiteti:** institucionet përdorin sa më mirë burimet publike në përmbushjen e roleve, përgjegjësive dhe misioneve të tyre përkatëse.

Zbatimi i parimeve të qeverisjes së mirë në hapësirën kibernetike

Nëse hapësira kibernetike do të ishte një vend, do të ishte më i madhi dhe më i populluari në botë. Sidoqoftë, nuk do të kishte një organ ligjvënës ose përfaqësues tjetër të vendimmarrjes, as nuk do të kishte një mekanizëm të caktuar të zbatimit të ligjit ose një mekanizëm për të mbrojtur të drejtat e njeriut të qytetarëve të saj, sepse nuk ka asnjë subjekt që ushtron autoritet dhe kontroll ekskluziv mbi të gjithë hapësirën digjitale.[6]

Qeverisja e hapësirës kibernetike karakterizohet nga një mori aktorësh të ndryshëm që kanë role dhe përgjegjësi të ndryshme duke ndikuar në vendimet politike dhe rregullatore.

Aktorët joshtetërorë në hapësirën kibernetike përfshijnë shoqërinë civile, ku përfshihen organizatat joqeveritare; grupet kërkimore akademike dhe mediat; sektori privat, në veçanti kompanitë private dhe organet industriale; dhe organizatat ndërkombëtare dhe rajonale.

Për shkak të numrit të madh të aktorëve të përfshirë në zhvillimin dhe zbatimin e politikave dhe për shkak të kornizave rregullatore në hapësirën kibernetike, këto procese shpesh janë të vështira, komplekse dhe/ose joefektive.

Kjo, së bashku me mungesën e njohurive se si të zbatohen në mënyrë efektive parimet e qeverisjes së mirë në hapësirën kibernetike mund të rezultojë në qeverisje të dobët, ku sektori i sigurisë në përgjithësi është joefektiv në mbështetjen e sigurisë njerëzore dhe shtetërore. Seksionet e mëposhtme hedhin një vështrim më të afërt të tre parimeve të qeverisjes së mirë: llogaridhënia, transparenca dhe sundimi i ligjit.

6 Anja Mihr (2014): Good Cyber Governance, Human Rights and Multi-stakeholder Approach, Georgetown Journal of International Affairs, gjendet në https://www.jstor.org/stable/43773646

STUDIM I RASTIT: PROGRAMI I MBIKËQYRJES I AGJENCISË AMERIKANE TË SIGURISË KOMBËTARE

Në vitin 2013, Eduard Snouden, punonjës i CIA-s, lëshoi dokumente tepër sekrete që zbuluan se agjencitë amerikane dhe britanike të inteligjencës kishin zhvilluar programe të mbikëqyrjes masive në të gjithë botën, duke përfshirë, por pa u kufizuar në përgjimin e trafikut të internetit dhe telefonit duke kaluar përmes kabllove me fibra optike nënujore të dhëna nga llogaritë e përdoruesve të Google dhe Yahoo dhe të dhënat e telefonit celular, spiunimi i qeverive të huaja, pirateria dhe infektimi i kompjuterëve me malware.

Veçanërisht, kompanitë morën urdhër publik nga Gjykata e Mbikëqyrjes së Inteligjencës së Jashtme të SHBA (FISA) për të dorëzuar të dhënat e klientëve të tyre. Për më tepër, u zbuluan raste të mëdha të shpërndarjes së inteligjencës midis anëtarëve të 'Aleancës me Pesë Sy' dhe vendeve të tjera. Megjithëse ish-Presidenti Obama u përgjigj me reformimin e programeve të mbikëqyrjes së NSA-së dhe Gjykatës FISA për të rritur transparencën, Kongresi i SHBA-së është ende në një ngërç për të krijuar një sistem që do të siguronte mbrojtje kritike për privatësinë, duke ruajtur aftësitë hetimore.

(Burimi: ACLU, gjendet në 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. Zhvillimi i normave dhe institucioneve që kontribuojnë dhe forcojnë llogaridhënien e sektorit të sigurisë në hapësirën kibernetike.

Kontrolli demokratik dhe civil është i nevojshëm për një llogaridhënie efektive. Mund të ushtrohet nga parlamentet nacionale si dhe më gjerësisht nga shoqëria civile. Kjo formë e mbikëqyrjes është thelbësore për të siguruar llogaridhënien e sektorit të sigurisë. Sidoqoftë, në hapësirën kibernetike, kontrolli demokratik dhe civil i sektorit të sigurisë shpesh cenohet për disa arsye.

Mbikëqyrja demokratike përballet shpesh me pengesat e mëposhtme[7]:

- **Kompleksiteti i rrjetit të internetit**

Së pari, sfidat e mbikëqyrjes ndërlikohen nga kompleksiteti i rrjetit. Një numër i madh dhe i larmishëm shtetesh, aktorë privatë, ndërkombëtarë dhe të tjerë jo-shtetërorë janë të përfshirë në sigurinë kibernetike. Në mënyrë të ngjashme, një grup i larmishëm aktorësh marrin pjesë në ato që ne mund t'i quajmë gjerësisht 'sulme kibernetike'. Kompleksiteti teknik i rrjetit e bën të vështirë për organet mbikëqyrëse, siç janë komisionet parlamentare - me kapacitet shpesh të kufizuar - të ndjekin aktorët përkatës, të njoftohen për ekzistencën dhe aktivitetet e tyre apo edhe të marrin një mandat ligjor për ta bërë këtë.

7 Shih Buckland, B., F. Schreier, and Th. H. Winkler, op. cit., pp. 18-19., gjendet në https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf

- **Njohuritë teknike të kërkuara për hartimin dhe zbatimin e rregullores efektive**

Së dyti, sfidat e mbikëqyrjes përkeqësohen nga natyra tepër teknike e hapësirës kibernetike. Si rezultat, organeve të mbikëqyrjes siç janë parlamentet shpesh u mungon ekspertiza e nevojshme për ta kuptuar atë në mënyrë adekuate dhe si rrjedhimi për të hartuar legjislacionin që mund të rregullojë në mënyrë efektive aktivitetet në hapësirën kibernetike. Bashkëpunimi publik-privat mund të ndërlikohet më tej nga ndarja midis ekspertëve teknikë të paguar shumë dhe të sofistikuar të përfshirë në zhvillimin dhe zbatimin e rregullores efektive dhe aktorëve qeveritarë shpesh të paguar dhe më pak të informuar, të ngarkuar me mbikëqyrjen e tyre.

- **Kompleksitetet ligjore të natyrshme në hapësirën kibernetike, siç janë juridiksioni dhe atribuimi**

Së treti, sfidat e mbikëqyrjes përkeqësohen nga kompleksiteti ligjor. Natyra e ndërlidhur, "pa kufij" e hapësirës kibernetike sjell sfida reale për kornizat tradicionale territoriale të zbatimit të ligjit. Të dhënat dhe aktivitetet kibernetike mund të zhvendosen nga serverët e vendosur nga një juridiksion në tjetër, me shpejtësinë e dritës. Për më tepër, ndërsa shpesh thuhet se të njëjtat ligje jashtë linje duhet të zbatohen edhe për aktivitetet në internet, shpesh nuk është e qartë se çfarë do të thotë kjo në praktikë. Siguria kibernetike shtron pyetje komplekse ligjore, të lidhura, ndër të tjera, me të drejtën për privatësi dhe lirinë e shprehjes. Ky kompleksitet më pas zmadhohet nga bashkëpunimi publik-privat dhe pyetjet përkatëse ligjore që lidhen me përgjegjësinë dhe kontrollin.

- **Natyra e larmishme e aktorëve të përfshirë që ngatërrojnë linjat tradicionale të përgjegjësisë dhe mbikëqyrjes**

KSë katërti, sfidat e mbikëqyrjes përkeqësohen nga natyra e larmishme e aktorëve të përfshirë. Në shumicën e rasteve, institucionet kombëtare të mbikëqyrjes janë të organizuara përgjatë linjave të agjencisë ose ato funksionale. Për shembull, një komision parlamentar mund të mbikëqyrë shërbimet e inteligjencës, forcat e armatosura ose institucionet e drejtësisë. Bashkëpunimi privat publik i përfshirë në sigurinë kibernetike, megjithatë, tejkalon kufijtë e agjencisë dhe kështu në të gjithë fushat e ekspertizës dhe mandatit të mbikëqyrjes. Si rezultat i kësaj kemi një numër të madh të zonave në të cilat ka mbikëqyrje joadekuate ose nuk ka fare.

Për sa i përket thyerjes së linjave të përgjegjësisë dhe kontrollit, veprimet e çdo agjenti qeveritar lidhen në një zinxhir ose përgjegjësi nga drejtori deri te agjenti. Për shembull, një oficer policie i Parisit është i lidhur nëpërmjet hierarkisë me prefektin e policisë (shefi i caktuar politikisht) dhe në fund, me ministrinë e brendshme dhe ekzekutivin. Prandaj, ekziston një lidhje e përgjegjësisë dhe mbikëqyrjes midis institucioneve të qeverisjes demokratike (si parlamenti) dhe individëve ose agjencive që zbatojnë urdhrat qeveritare. Këto lidhje mund të ndërpriten me përfshirjen e aktorëve privatë dhe krijimin e mekanizmave të bashkëpunimit privat-publik. Ndërsa një firmë IT e kontraktuar nga një agjenci publike mund të duket se vepron si një agjent i thjeshtë i shtetit, marrëdhënia është përgjithësisht shumë më komplekse dhe mjegullohet nga asimetri të shumta informacioni që zvogëlojnë transparencën dhe parandalojnë që mekanizmat e mbikëqyrjes të funksionojnë në mënyrë efektive.

Kuptimi i mandatit nga vetë organi mbikëqyrës

Në përgjithësi, organet e mbikëqyrjes qeveritare kanë të bëjnë me agjencitë qeveritare mbi të cilat ata kanë përgjegjësi të drejtpërdrejtë. Kjo mund të lërë partnerët privatë të agjencive të tilla jashtë fushëveprimit të mbikëqyrjes, edhe në rastet kur ato financohen drejtpërdrejt nga, ose punojnë në bashkëpunim të ngushtë me agjenci të tilla.

STUDIM I RASTIT: BUNDESTAGU GJERMAN, HETIM PËR SHITJEN E TEKNOLOGJIVE MBIKQYRËSE QEVERIVE TË HUAJA

Në vitin 2014, deputetët gjerman zhvilluan një hetim mbi shitjen e teknologjive të mbikëqyrjes tek qeveritë e huaja. Si përgjigje, qeveria gjermane deklaroi se gjatë dekadës së kaluar, ajo u ka dhënë kompanive gjermane licenca për të eksportuar teknologji të mbikëqyrjes në të paktën 25 vende, shumë prej të cilave kanë histori të gjatë të abuzimeve të të drejtave të njeriut.

Si pasojë e këtij hetimi, qeveria gjermane deklaroi se do të lobojë më tej për të rregulluar teknologjitë e mbikëqyrjes që dëmtojnë të drejtat e njeriut.

(Burim: EDRi Protecting Digital Freedom, gjendet në:: https://edri.org/germany-exports-surveillance-technologies-to-human-rights-violators/)

Kompleksiteti teknik i hapësirës kibernetike përkeqëson edhe më tepër vështirësitë tradicionale me të cilat përballen parlamentarët në mbikëqyrjen e sektorit të sigurisë. Kjo mund të cenojë llogaridhënien efektive. Kjo së bashku me vështirësinë për t'i atribuuar në mënyrë të besueshme një aktori të caktuar, shkeljet e ligjit në hapësirën kibernetike, mund ta bëjnë të vështirë, nëse jo të pamundur, për autoritetet civile të mbajnë përgjegjës sektorin e sigurisë, duke kontribuar kështu në një kulturë të mosndëshkimit.

Sektori i drejtësisë luan një rol thelbësor në mbikëqyrjen e veprimeve nga sektori i sigurisë. Për shembull, sektori i drejtësisë mund të autorizojë kompetenca të veçanta për zbatimin e ligjit dhe për agjencitë e shërbimit të inteligjencës duke lëshuar urdhra kërkimi. Kjo mund të jetë veçanërisht e rëndësishme në kontekstin e përgjimit të komunikimit. Sidoqoftë, kontrolli gjyqësor shpesh anashkalohet ose kufizohet për arsye të sigurisë kombëtare dhe gjendjes së jashtëzakonshme

STUDIM I RASTIT: MBIKEQYRJA PARLAMENTARE E SIGURISË NË SUEDI: SFIDAT KRYESORE DHE PRAKTIKAT E MIRA

Parlamenti suedez ka pesëmbëdhjetë komisione. Këto komisione parlamentare kanë role të ndryshme. Ata, për shembull, mund të kryejnë dëgjime publike për të fituar njohuri mbi çështje specifike që do të duhej të ligjësonin. Ndërsa është e paqartë se cili komision parlamentar ka detyrën vetëm të mbikëqyrë qeverisjen e sigurisë kibernetike, ka të ngjarë që komisione të ndryshme të kenë një rol në varësi të kontekstit. Për shembull, Komisioni i Mbrojtjes mund të ngarkohet me çështje që lidhen me sigurinë kibernetike.

Strategjia kombëtare e sigurisë kibernetike e Suedisë 2016 adreson një gamë të tërë të subjekteve; nga rregullimi i ofruesve të TIK-ut deri te mbrojtja e infrastrukturës kritike. Sidoqoftë, duket se nuk ka komisione ose nënkomisione të ngarkuara posaçërisht për sigurinë kibernetike. Një çështje e tillë shpesh nënkupton përgjigje ndërqeveritare dhe duket se ky është rasti në Suedi. Kjo mund të komplikohet më tej nga fakti që një pjesë e rëndësishme e mbrojtjes kibernetike sigurohet nga aktorë privatë dhe komisionet parlamentare nuk kanë një mandat adekuat për të shqyrtuar me kujdes këtë veprimtari. Sidoqoftë, ndryshe nga disa strategji kombëtare të sigurisë kibernetike, strategjia suedeze përcakton parimet strategjike dhe një plan veprimi, i cili mund të ndihmojë parlamentin të kërkojë llogari nga aktorët.

Përveç funksioneve të kontrollit parlamentar dhe gjyqësor, shoqëria civile luan një rol thelbësor në mbikëqyrjen e sektorit të sigurisë. Shoqëria civile mund të kontribuojë në sigurimin e këshillave të politikave, si dhe ekspertizë teknike dhe mund të lehtësojë dialogun dhe negociatat në rolin e tyre si vëzhgues publik.

Shoqëria civile kontribuon më tej në rritjen e ndërgjegjësimit për çështje të ndryshme dhe mund të drejtojë krijimin e politikave. Sidomos, media mund të hetojë dhe mbështesë qasjen në informacion duke analizuar më thellë çështjet shqetësuese.

STUDIM I RASTIT: ROLI I NDËRMARRJEVE PRIVATE NË SHITJEN E TEKNOLOGJISË SË MBIKËQYRJES QEVERIVE

Kompanitë private, si kompania italiane "Hacking Team", kanë shitur sisteme të ndërhyrjeve në distanca në vende të ndryshme, duke përfshirë Egjiptin, Nigerinë, Uzbekistanin, Turqinë, Marokun dhe Kolumbinë. Kjo tendencë në rritje ka nxitur diskutime mbi përdorimin e mundshëm të këtyre teknologjive si mjete të shtypjes dhe shkeljeve të të drejtave të njeriut.

Mbikëqyrja masive përbën një sfidë në zhvillim dhe kompanitë private vazhdojnë të shesin mjete dhe teknologji vëzhgimi në vende të ndryshme. Ndërsa organizatat e shoqërisë civile janë duke rritur ndërgjegjësimin në lidhje me këtë praktikë biznesi, dhe madje kanë lëshuar një bazë të dhënash të kërkueshme për më shumë se 520 kompani survejimi që shesin mjetet e tyre qeverive në të gjithë botën, kjo çështje mbetet shumë e parregulluar.

2.2. Zhvillimi i normave dhe institucioneve që promovojnë dhe forcojnë transparencën dhe e bëjnë informacionin lirisht të disponueshëm dhe të arritshëm

Arritja e qeverisjes së mirë të sektorit të sigurisë është proces dhe qëllim i reformës në sektorin e sigurisë.

Transparenca zakonisht mund të konsiderohet se i shërben një qëllimi të dyfishtë: të lejojë shkëmbimin e informacionit që nxit efektivitetin e institucioneve të sektorit të sigurisë, si dhe të jetë një parakusht për përgjegjësinë e tyre. Për më tepër, teknologjitë e informacionit dhe komunikimit (TIK) janë vetë një mjet për të promovuar dhe forcuar transparencën, duke e bërë informacionin të arritshëm për qytetarët.

Sidoqoftë, transparenca absolute është e parealizueshme dhe nuk rekomandohet domosdoshmërish në varësi nga konteksti i sektorit të sigurisë.

Është e rëndësishme të kuptohet kjo 'dilemë transparence' në lidhje me promovimin e një kulture të besimit dhe hapjes ndërmjet ofruesve të sigurisë publike dhe private. Transparenca, megjithatë, duhet të jetë rregulli, dhe kufizimi i transparencës duhet të jetë përjashtim dhe i përcaktuar qartë në legjislacionin kombëtar.[8]

Transparenca gjithashtu rrit kuptimin e rreziqeve të sigurisë kibernetike dhe inkurajon qeveritë, kompanitë private dhe shoqërinë civile për të koordinuar dhe bashkëpunuar në mënyrë më efektive për të parandaluar dhe përgjigjur këtyre rreziqeve të sigurisë kibernetike.

Kuptimi i këtyre rreziqeve kibernetike mund të kontribuojë në vendimmarrjen e informuar nga përdoruesit individualë. Kjo është thelbësore, pasi përdoruesit individualë të teknologjive shpesh konsiderohen si hallka më e dobët në zinxhirin e sigurisë (kibernetike). Kanalet e përmirësuara të informacionit mund të mbështesin sjellje më të mirë në internet (referuar gjithashtu si 'higjiena kibernetike' e mirë), e cila nga ana tjetër ka të ngjarë të zvogëlojë shkallën e suksesit në pjesën më të madhe të aktiviteteve dashakeqe.

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

Në këtë drejtim, qasjet me shumë aktorë mund të kontribuojnë, gjithashtu, në nxitjen e transparencës dhe mund të rrisin vetëdijen për rreziqet e sigurisë kibernetike..

SHEMBUJ TË PRAKTIKËS SË MIRË

Organizata për Sigurinë dhe Bashkëpunimin në Evropë (OSBE) në vitin 2014 miratoi Marrëveshje mbi masat e ndërtimit të besimit. Masat vullnetare përfshijnë sigurimin e pikëpamjeve kombëtare mbi doktrinën, strategjinë dhe kërcënimet kibernetike. Anëtarët e OSBE-së, mandej, ranë dakord të shkëmbejnë informacione mbi organizatat, programet ose strategjitë kombëtare të rëndësishme për sigurinë kibernetike, të identifikojnë një pikë kontakti për të lehtësuar komunikimin dhe dialogun mbi çështjet e sigurisë së TIK-ut.

El Salvador ka miratuar ligje për mbrojtjen e të dhënave dhe qasjen në informacionin publik, të cilat përcaktojnë norma për transparencën dhe lirinë e informacionit.

(Burimi: https://publications.iadb.org/handle/11319/7449, f. 74)

Organizata e Shteteve Amerikane publikoi një raport mbi ekipet e përgjigjes ndaj incidenteve të sigurisë kompjuterike (CSIRT) që identifikon mënyra të ndryshme për të rritur bashkëpunimin midis CSIRT-ve për ndarjen e informacionit.

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

Stimulimi i krijimit të partneritetit publik-privat mund të kontribuojë për një mjedis të të favorshëm për shkëmbimin e informacionit dhe qasjen në informacion.

2.3. Forcimi i parimit të sundimit të ligjit në hapësirën kibernetike.

Hapësira kibernetike krijon gjithashtu një fushë të re për sjellje të paligjshme, për shembull përhapjen e gjuhës së urrejtjes, pornografinë e fëmijëve, nxitjen e dhunës, shkeljet e të drejtës së autorit, mashtrimin, vjedhjen e identitetit, pastrimin e parave ose sulmet "DoS".[9] Këto veprime kriminale janë gjithnjë e më transnacionale.

"Mjedisi digjital nga natyra e tij mund të shkatërrojë privatësinë dhe të drejtat e tjera themelore dhe të cenojë vendimmarrjen e përgjegjshme."[10] Si pasojë, ekziston një potencial në rritje që parimi i shtetit të së drejtës të cenohet duke shkelur të drejtat e privatësisë dhe liritë e tjera themelore, siç është liria e shprehjes.

9 Këshilli i Evropës, Sundimi i ligjit në internet dhe në botën e gjerë dixhitale, dokument i botuar nga Komisioneri i Këshillit të Evropës për të Drejtat e Njeriut, Përmbledhje Ekzekutive dhe rekomandimet e Komisionerit, 2014, gjendet në: http://www.statewatch.org/news/2014/dec/coe-hr-comm-rule-of-law-on-the%20internet-summary.pdf

10 Ibid. f. 6.

Parimi i sundimit të ligjit është interpretuar më tej nga gjykatat ndërkombëtare, siç është Gjykata Evropiane e të Drejtave të Njeriut (GJEDNJ). GJEDNJ zhvilloi një test të sundimit të ligjit ku "të gjitha kufizimet mbi të drejtat themelore duhet të bazohen në rregulla ligjore të qarta, precize, të arritshme dhe të parashikueshme dhe duhet të shërbejnë qartë për qëllime legjitime; ato duhet të jenë "të domosdoshme" dhe "proporcionale" me qëllimin përkatës legjitim [...] dhe duhet të ketë një zgjidhje "efektive [mundësisht gjyqësore]" në dispozicion.[11]

Qeveritë u kanë bërë thirrje kompanive private që zotërojnë platforma të mediave sociale, të sigurojnë që shërbimet e tyre të mos rrëmbehen nga ekstremizmi i dhunshëm dhe terrorizmi.

Sekretari i Përgjithshëm i Kombeve të Bashkuara shpjegoi konceptin e sundimit të ligjit në mënyrën vijuese:

Për Kombet e Bashkuara, sundimi i ligjit i referohet një parimi të qeverisjes në të cilin të gjithë personat, institucionet dhe subjektet, publike dhe private, përfshirë vetë Shtetin, janë përgjegjës ndaj ligjeve që dekretohen publikisht, zbatohen në mënyrë të barabartë dhe gjykohen në mënyrë të pavarur, si dhe që janë në përputhje me normat dhe standardet ndërkombëtare të të drejtave të njeriut. Kjo kërkon gjithashtu, masa për të siguruar respektimin e parimeve të epërsisë së ligjit, barazinë para ligjit, përgjegjësinë ndaj ligjit, drejtësinë në zbatimin e ligjit, ndarjen e pushteteve, pjesëmarrjen në vendimmarrje, sigurinë ligjore, shmangien ose arbitraritetin dhe transparencën procedurale dhe ligjore.

(Burimi Raporti i Sekretarit të Përgjithshëm të KB "Sundimi i ligjit dhe drejtësia tranzicionale në shoqëritë e konfliktit dhe postkonfliktit", S / 2004/616 (23 gusht 2004), para 6., gjendet në: https://www.un.org/ruleoflaw/files/2004%20report.pdf.

Për të përmbushur këto kërkesa të qeverisë, kompanitë private - veçanërisht kompanitë e mediave sociale si (Fejsbuk) Facebook, (Gugëll) Google dhe (Tuiter) Twitter - kanë zhvilluar kushtet e shërbimit dhe kodet e sjelljes për të rregulluar përmbajtjen e pritur në këto platforma të mediave sociale - de facto krijimi i normave në internet. Sidoqoftë, këto kushte të shërbimit dhe kodet e sjelljes nuk janë të njëjta në platforma të ndryshme - duke krijuar paqartësi dhe pasiguri ligjore se çfarë përmbajtjeje është e ndaluar në cilën platformë.

11 Ibid, f. 8

STUDIM I RASTIT: ROLI I KOMPANIVE TË MEDIAVE SOCIALE NË KONTROLLIN E PLATFORMAVE TË TYRE

Ndërsa është e pakontestueshme që kompanitë e mediave sociale duhet të kenë të drejtë të kontrollojnë platformat e tyre dhe të identifikojnë standardet e komunitetit, kur bëhet fjalë për terrorizmin, kompanitë e mediave sociale de facto veprojnë si rregullatorë që mund të kufizojnë fjalën e lirë në platformat e tyre - pa pasur detyrime sipas të drejtës ndërkombëtare të të drejtave të njeriut. Për më tepër, kompanitë e mediave sociale po përjetojnë gjithashtu një presion të shtuar nga shtetet për të moslejuar në platformat e tyre asnjë lloj fjalimi të dhunshëm që nxit, madhëron ose arsyeton terrorizmin.

Si pasojë, këto kompani të mediave sociale kanë përditësuar standardet e tyre të për të adresuar këtë kërkesë të ngutshme nga shtetet - që shpesh çon drejt rregulloreve ambivalente.

Fejsbuku (Facebook) për shembull nuk lejon asnjë organizatë ose individ që është i përfshirë në aktivitet terrorist të ketë prani në Fejsbuk. Aktiviteti terrorist përcaktohet nga organizatat terroriste si "çdo organizatë joqeveritare që përfshihet në veprime të paramenduara dhune kundër personave ose pasurisë për të frikësuar një popullatë civile, qeveri ose organizatë ndërkombëtare për të arritur një qëllim politik, fetar ose ideologjik. Akti terrorist përcaktohet si një akt i paramenduar i dhunës ndaj personave ose pasurisë i kryer nga një aktor joqeveritar për të frikësuar një popullatë civile, qeveri ose organizatë ndërkombëtare për të arritur një qëllim politik, fetar ose ideologjik.

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

Ndërsa Tuiteri (Twitter) nuk i referohet terrorizmit në Rregullat e Tuiterit. Tuiteri ndalon përmbajtjen e urrejtjes që nxit dhunën ose sulmon drejtpërdrejt ose kërcënon njerëz të tjerë bazuar në racë, përkatësi etnike, origjinë kombëtare, orientim seksual, gjini, identifikim gjinor, përkatësi fetare, moshë, paaftësi ose sëmundje serioze. Përveç kësaj, Tuiteri ndalon glorifikimin e dhunës në platformat e tij si dhe kërcënimet e dhunshme. Shembuj të glorifikimit të dhunës mund të përfshijnë vrasje masive, sulme terroriste, përdhunime dhe sulme seksuale.

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

Zbulimet e Snoudenit demonstruan se agjencitë e inteligjencës përgjojnë rregullisht komunikimet private dhe i ndjekin ato nga "dera e pasme". Me fjalë të tjera, në lidhje me sigurinë kombëtare, nuk ka asnjë gur themeli të vërtetë për të mbështetur sundimin e ligjit, megjithëse - edhe pse ka të paktën parime themelore që mund të formojnë themelin e një pjese kaq thelbësore të ngrehinës universale të të drejtave të njeriut. Duke pasur parasysh partneritetet e rritura midis agjencive të zbatimit të ligjit dhe inteligjencës dhe sigurisë, dobësimi i shtetit të së drejtës kërcënon të përhapet në policë dhe prokurorë. Mungesa e kornizave të qarta ligjore në këtë drejtim, brenda dhe ndërkombëtarisht, është një kërcënim i mëtejshëm për shtetin e së drejtës në internet dhe në mjedisin global digjital.

Parimi i shtetit të së drejtës është gjithashtu i sfiduar në kontekstin e së drejtës ndërkombëtare, pasi ekziston një tendencë për të shkuar drejt rregullave vullnetare, jo-detyruese dhe më tepër ad-hoc dhe kornizave rregullatore që rregullojnë sjelljen e aktorëve të sektorit të sigurisë në hapësirën kibernetike. (Për një përmbledhje të kornizës ligjore ekzistuese ndërkombëtare dhe rajonale shih Kapitullin 3).

STUDIM I RASTIT:ORGANE TË PRIVATIZUARA TË ZBATIMIT TË LIGJIT NË HAPSIRËN KIBERNETIKE

Fakti që interneti dhe mjedisi global digjital kontrollohen kryesisht nga subjekte private (veçanërisht, por jo vetëm korporatat amerikane) gjithashtu paraqet një kërcënim për shtetin e së drejtës. Subjekte të tilla private mund të vendosin (dhe të "inkurajohen" të imponojnë) kufizime në qasjen në informacion pa u nënshtruar kufizimeve kushtetuese ose të së drejtës ndërkombëtare që zbatohen për kufizimet shtetërore të së drejtës së lirisë së shprehjes. Këto subjekte private mund të urdhërohen gjithashtu nga gjykatat vendase, duke vepruar me kërkesë të subjekteve të tjerë privatë, për të kryer analiza shumë ndërhyrëse të të dhënave të tyre për të zbuluar shkelje të ngjashme (ose thjesht të mundshme) të të drejtave të pronës private, shpesh të drejta të pronës intelektuale.

Ata mund të urdhërohen të "tërheqin" të dhëna, duke përfshirë të dhëna qeveritare, komerciale dhe personale, nga serverët në vendet e tjera, për qëllime të zbatimit të ligjit ose të sigurisë kombëtare, pa marrë pëlqimin e vendit tjetër - ose pëlqimin e kompanive ose subjekteve të të dhënave në vendin tjetër - duke shkelur sovranitetin e vendit tjetër, konfidencialitetin tregtar për të cilin kanë të drejtë kompanitë dhe të drejtat e njeriut e subjekteve të të dhënave.

Përgjegjësia e kompanive të mediave sociale ("përgjegjësia ndërmjetësuese") duhet të interpretohet shumë ngushtë. E thënë ndryshe, nëse dhe kur platformat si Goolge, Facebook, YouTube mbahen përgjegjës për përmbajtjen që përdoruesit e tyre postojnë në platformat e tyre duhet të vlerësohen me shumë kujdes, pasi kjo mund të ketë një efekt të drejtpërdrejtë në lirinë e shprehjes dhe të drejtat e tjera të njeriut. Sidoqoftë, qeveritë në të gjithë botën gjithnjë e më shumë i kanë bërë presion këtyre kompanive për të imponuar kontroll më të rreptë të përmbajtjes, duke inkurajuar një klimë të 'vetëcensurës'.

SHEMBUJ TË PRAKTIKËS SË MIRË

Parimet e Manilës mbi Përgjegjësinë e Ndërmjetësimit përcaktojnë se "ndërmjetësuesve nuk u kërkohet të kufizojnë përmbajtjen nëse nuk është lëshuar një urdhër nga një autoritet gjyqësor i pavarur dhe i paanshëm që ka përcaktuar që materiali në fjalë është i paligjshëm". Parimet e Manilës avokojnë më tej se "provat e mjaftueshme për të dokumentuar bazën ligjore të urdhrit" sigurohen përpara se çdo përmbajtje të kufizohet nga një ndërmjetës. Parimet e Manilës theksojnë më tej rëndësinë e ndërtimit të transparencës dhe llogaridhënies në ligje, duke theksuar se qeveritë nuk duhet të përdorin masa jashtëgjyqësore për të kufizuar përmbajtjen, e cila përfshin presione kolaterale për të detyruar ndryshime në terma të shërbimit, për të promovuar ose zbatuar të ashtuquajturat praktika "vullnetare" dhe për të siguruar marrëveshje në frenimin e tregtisë ose në frenimin e shpërndarjes publike të përmbajtjes.

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

Projektligji i Argjentinës për përgjegjësinë ndërmjetësuese thotë se "ofruesit e shërbimeve të internetit nuk do të jenë përgjegjës për përmbajtjen e krijuar nga palë të treta, përveç kur janë njoftuar siç duhet për një urdhër gjykate për heqjen ose bllokimin e përmbajtjes".

(Burimi: 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/)

GJETJET KRYESORE

- Siguria duhet të shihet nëpërmjet prizmit të qeverisjes sepse tregon se si një larmi aktorësh shtetërorë dhe joshtetërorë ushtrojnë pushtet dhe autoritet mbi sigurinë, zyrtarisht dhe jozyrtarisht dhe në nivele ndërkombëtare, kombëtare dhe lokale.
- Qeverisja është një term ombrellë që mund të zbatohet mbi sigurinë në përgjithësi për të shpjeguar se si aktorët ndërkombëtarë, kombëtarë dhe vendorë luajnë të gjithë një rol në formësimin e vendimeve për sigurinë dhe zbatimin e tyre.
- Parimet e QSS-së së mirë janë: përgjegjësia, transparenca, sundimi i ligjit, pjesëmarrja, përgjegjësia, efektiviteti dhe efikasiteti.
- Për më tepër, QSS-ja e mirë bazohet në idenë se sektori i sigurisë duhet të mbahet në të njëjtat standarde të larta të ofrimit të shërbimeve publike si ofruesit e tjerë të sektorit publik.
- QSS-ja e mirë është një sërë parimesh dhe për këtë arsye, të njëjtat parime thelbësore të qeverisjes së mirë zbatohen ndryshe në secilin sektor të sigurisë.
- Themelimi i QSS-së së mirë është çështje e rregullimit të vazhdueshëm ndërsa kërcënimet e sigurisë vazhdimisht zhvillohen.
- RSS-ja e përmirëson aftësinë e sektorit të sigurisë për të ofruar siguri për shtetin dhe qytetarët e tij.
- RSS-ja e bën përdorimin e burimeve publike në sektorin e sigurisë më efikas.
- RSS-ja i zvogëlon mundësitë për korrupsion duke përmirësuar mbikëqyrjen dhe profesionalizmin
- RSS-ja mbron pavarësinë profesionale të personelit të sigurisë që ata të mund të përmbushin në mënyrë efektive detyrat e tyre legjitime dhe rritë standardet profesionale dhe forcon përgjegjësinë, duke zvogëluar abuzimin e popullatës.
- RSS-ja e promovon sigurimin gjithëpërfshirës të sigurisë dhe mundësitë e barabarta brenda sektorit të sigurisë.
- RSS-ja e parandalon konfliktin duke promovuar unitetin, neutralitetin politik, barazinë dhe profesionalizmin brenda sektorit të sigurisë.

BURIME

Dokument informues i DCAF për reformën e sektorit të sigurisë. Aplikimi i parimit të qeverisjes së mirë të sektorit të sigurisë, gjendet në: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_1_Security_Sector_Governance_EN.pdf

Dokument informues i DCAF për reformë e sektorit të sigurisë. Aplikimi i parimeve të qeverisjes së mirë të sektorit të sigurisë, gjendet në: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_2_Security%20Sector%20Reform.pdf

DCAF Ekipi Këshillëdhënës i Sektorit Ndërkombëtar të Sigurisë, RSS në me disa fjalë. Manual për trajnimin hyrës mbi reformën e Sektorit të Sigurisë, gjendet në: https://issat.dcaf.ch/download/2970/25352/ISSAT%20LEVEL%201%20TRAINING%20MANUAL%20-%20SSR%20IN%20A%20NUTSHELL%20-%205.3.pdf

DDCAF-ISSAT Hyrje në Reformën e Sektorit të Sigurisë. Një kurs falas i mësimit elektronik i disponueshëm në faqen e internetit të Komunitetit të praktikumit të DCAF-ISSAT: 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)

Forumi Global mbi Ekspertizën Kibernetike, Rritja e vetëdijes për sigurinë kibernetike duke ndërtuar besimin përmes transparencës, gjendet në 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), gjendet në https://onlinelibrary.wiley.com/doi/full/10.1111/capa.12243

KAPITULLI 2

SI LIDHEN HAPËSIRA KIBERNETIKE DHE SIGURIA KIBERNETIKE ME QEVERISJEN E MIRË TË SEKTORIT TË SIGURISË

OBJEKTIVAT

Ky kapitull synon t'u ofrojë pjesëmarrësve një vështrim më të afërt në hapësirën kibernetike dhe sigurinë kibernetike. Në mënyrë të veçantë, qëllimi i këtij kapitulli është të rrisë njohuritë e pjesëmarrësve mbi hapësirën kibernetike dhe sigurinë kibernetike dhe të nxjerrë në pah kompleksitetet në zbatimin e praktikave të mira të qeverisjes së sektorit të sigurisë (QSS) në këto fusha.

Objektivat e nxënies e këtij kapitulli janë si më poshtë:

- Rritja e njohurive për mediumin e hapësirës kibernetike mbi fushëveprimin, aktorët dhe rreziqet.
- Rritja e njohurive për sigurinë kibernetike dhe për ndikimin e saj mbi sigurinë njerëzore, sigurinë kombëtare dhe ofrimin e shërbimeve.
- Kuptimi i kufizimeve dhe mënyrës ku mund të zbatohen praktikat e QSS-së në kontekstin e hapësirës kibernetike.

1. 1. Hyrje

Siç u diskutua në kapitullin e mëparshëm, praktikat e mira të QSS-së janë thelbësore për të mbështetur një mjedis efektiv dhe të përgjegjshëm në të cilin respektohen të drejtat e njeriut dhe parimi i shtetit ligjor. Meqenëse sektori i sigurisë është i përbërë nga aktorë shtetërorë dhe joshtetërorë, parimet e QSS-së së mirë duhet të shtrihen përtej praktikave shtetërore.

QSS-ja e mirë brenda hapësirës kibernetike është koncept relativisht i ri që ka ndikime të thella si në qeveri ashtu edhe mbi qytetarët. Meqenëse hapësira kibernetike dhe aktivitetet dhe shërbimet brenda saj janë bërë një pjesë e integruar e jetës së përditshme, mbrojtja e të dhënave dhe informacionit brenda hapësirës kibernetike është thelbësore.

Përkundër kësaj, dhe ndoshta për shkak të përdorimeve të tij të larmishme, koncepti i hapësirës kibernetike dhe përbërësve të tij të ndryshëm nuk janë të përcaktuar mirë. Për t'iu qasur sa më mirë çështjeve të QSS-së së mirë brenda hapësirës kibernetike, nevojitet një kuptim më konciz i asaj që nënkuptohet me "hapësirë kibernetike" dhe "siguri kibernetike".

Çfarë është hapësira kibernetike?

Natyra e hapësirës kibernetike si një koncept abstrakt me sa duket i pabazuar në botën fizike, ka sjellë mungesë qartësie se çfarë nënkuptohet me këtë term.

Shpesh organizatat dhe kombet përcaktojnë hapësirën kibernetike në një mënyrë që i përshtatet më mirë qëllimit të tyre ose përdorimit të saj. Shpesh këto përkufizime përqendrohen te siguria, militarizimi ose dobësitë e pranishme brenda hapësirës kibernetike, në secilën organizatë, komb dhe grup duke theksuar aspekte të ndryshme. Sidoqoftë, ekziston një temë e zakonshme që gjendet në shumicën e përkufizimeve: hapësira kibernetike është një mjedis i krijuar nga të përbërësit fizikë dhe virtualë, ku të dhënat, informacioni ose komunikimi ruhen, modifikohen ose shkëmbehen.

Ndërsa interneti mund të jetë forma më e zakonshme dhe lehtësisht e arritshme e hapësirës kibernetike për një qytetar mesatar, ai është larg aspektit të tij të vetëm.[1] Hapësira kibernetike përfshin çdo sistem rrjeti të bazuar në kompjuter për qëllimet e lartpërmendura të ruajtjes, modifikimit ose shkëmbimit,[2] siç mund të gjenden në numrin e rritjes së orëve, pajisjeve dhe sendeve të tjera të lidhura në hapësirën kibernetike

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. Gjendet në:: https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf

(i njohur gjithashtu si Interneti i Gjërave - IoT). Të marra së bashku, këto flukse të ndryshme të të dhënave dhe informacionit përbëjnë konstruktin "virtual" që quhet hapësirë kibernetike.

Hapësira kibernetike është një fushë globale, plot burime, informacione dhe mundësi. Ajo është bërë aspekt i tillë integral i jetës së përditshme që Këshilli i Kombeve të Bashkuara për të Drejtat e Njeriut në vitin 2016 pohoi "se të njëjtat të drejta që njerëzit kanë jashtë internetit duhet të mbrohen edhe në internet, në veçanti liria e shprehjes, e cila është e zbatueshme pavarësisht nga kufijtë dhe nëpërmjet çfarëdo medie, në përputhje me nenet 19 të Deklaratës Universale të të Drejtave të Njeriut dhe të Paktit Ndërkombëtar për të Drejtat Civile dhe Politike[3]".

Hapësira kibernetike gjithashtu ka aspekte fizike, duke përfshirë desktopët dhe laptopët, tabletët dhe telefonat e mençur, dhe serverët dhe kabllot fizikë që krijojnë infrastrukturën e internetit. Hapësira kibernetike si medium lejon aktivitete që shpesh u ngjajnë aktiviteteve në botën fizike: njerëzit mbështeten në hapësirën kibernetike për të komunikuar me njëri-tjetrin, të merren me tregti, të kryejnë kërkime, të përfshihen në aktivitete rekreative dhe të marrin lajme të përditësuara. Sidoqoftë, jo të gjitha përdorimet e hapësirës kibernetike janë aq të pafajshme: i njëjti medium mund të shërbejë si hapësirë për veprimtari kriminale, sulme ushtarake dhe aktivitete të tjera qëllimkeqe.

3 Promovimi, mbrojtja dhe gëzimi i të drejtave të njeriut në internet. Sesioni i 32-të i Këshillit për të Drejtat e Njeriut (27 Qershor 2016), A / HRC / 32 / L.20

Përcaktimi i hapësirës kibernetike
Disa shembuj të përkufizimeve të hapësirës kibernetike që përdoren aktualisht:

Unioni Ndërkombëtar i Telekomunikacionit
Hapësira kibernetike është mjedisi në të cilin ndodh komunikimi midis rrjeteve kompjuterike. Dhe pothuajse të gjithë në një mënyrë ose në një tjetër lidhen me të.

Organizata Ndërkombëtare për Standardizim
Mjedisi kompleks që rezulton nga ndërveprimi i njerëzve, programeve dhe shërbimeve në internet me anë të pajisjeve teknologjike dhe rrjeteve të lidhura me të, e cila nuk ekziston në asnjë formë fizike.

Bashkimi Evropian
Hapësira kibernetike është një grup asetesh materiale dhe jo-materiale të varura nga koha, të cilat ruajnë dhe / ose transferojnë informacionet elektronike.

Afrika e Jugut
"Hapësira kibernetike" do të thotë një terren fizik dhe jofizik i krijuar dhe / ose i përbërë nga disa ose të gjitha gjërave në vijim: kompjuterë, sisteme kompjuterike, rrjete dhe programet e tyre kompjuterike, të dhëna kompjuterike, të dhëna përmbajtjeje, të dhëna trafiku dhe përdorues.

(Burime: CCDCOE, gjendet në: https://ccdcoe.org/; ENISA, ENISA pregled sajber bezbednosti i povezane terminologije, verzija 1. Evropska unija, septembar, 2017. e aksesuesshme në: 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.)

SHEMBULL I PRAKTIKËS SË MIRË

Në fillim të shekullit 21, Franca kishte një nga nivelet më të ulëta të depërtimit të internetit dhe kompjuterit brenda Bashkimit Evropian. Sidoqoftë, sot një shumicë e madhe e popullsisë merr pjesë në hapësirën kibernetike. Për të rritur më tej aksesin dhe lehtësinë e përdorimit të hapësirës kibernetike, Franca ka nisur iniciativën e re "Très Haut Débit", për të promovuar akses me shpejtësi të lartë në internet, veçanërisht për komunitetet rurale dhe që kanë lidhje të ulët. Nëpërmjet partneritetit me grupe publike dhe private, Franca synon të shohë mbulimin 100% në lidhjen e internetit me shpejtësi të lartë dhe t'u japë qasje digjitale të gjithë qytetarëve deri në vitin 2022.

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

Megjithëse ka disa gjëra të përbashkëta midis përkufizimeve të ndryshme institucionale të hapësirës kibernetike, natyra e pasaktë e të gjitha këtyre përkufizimeve u siguron aktorëve në hapësirën kibernetike aftësinë për të përshtatur përkufizimet më mirë nevojave të tyre dhe për të justifikuar veprimet e tyre. Kjo është parë veçanërisht kur përshkruhet se si të shfrytëzohet ose mbrohet më së miri mediumi. Përkufizimet gjithashtu tregojnë për mënyrën në të cilën shtetet e shohin hapësirën kibernetike, si një mjet për ushtrinë, një platformë nga e cila shpërndajnë shërbimet, ose një arenë për tregti dhe komunikim.

Për qëllimet tona, hapësira kibernetike do të përkufizohet si: mjedisi global, i rrjetëzuar në të cilin shkëmbehen, ruhen dhe modifikohen të dhënat dhe informacionet, dhe i cili është i qasshëm nga aktorët shtetërorë dhe joshtetërorë.

Përdorimi dhe autoriteti në hapësirën kibernetike

Duke pasur parasysh karakterin e gjerë të hapësirës kibernetike, është logjike që përdorimet, dhe përdoruesit, të jenë po aq të larmishme sa vetë mediumi. Aktorët përfshijnë aktorë shtetërorë dhe joshtetërorë. Shtetet përdorin hapësirën kibernetike për të mbajtur zgjedhje dhe për të ofruar shërbime për popullsinë e tyre, si dhe një mjet për të mbrojtur sigurinë kombëtare dhe interesat jetike kombëtare.[4] Aktorët joshtetërorë shkojnë nga ndërmarrjet te qytetarët, të gjithë shfrytëzojnë hapësirën kibernetike për qëllime të ndryshme. Të gjithë këta aktorë kontribuojnë në ndikimin dhe formësimin e hapësirës kibernetike.

Natyra globale e hapësirës kibernetike gjithashtu vë kufizime për qeveritë në lidhje me rregullimin dhe qeverisjen e saj. Megjithëse forcimi i sigurisë kibernetike si pjesë e politikës së sigurisë kombëtare është i rëndësishëm, mbështetja e QSS-së së mirë në hapësirën kibernetike do të ketë gjithashtu efekte të rëndësishme si në sigurinë ekonomike ashtu edhe në atë njerëzore.[5] Ndërsa bota bëhet më e varur nga shërbimet dhe liria e të dhënë nga hapësira kibernetike, bëhet gjithnjë e më e domosdoshme që të mbrohen të drejtat e njeriut dhe siguria njerëzore[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, f. 9. E aksesuesshme në: https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf

STUDIM I RASTIT SIGURIMI I PËRBËRËSIT FIZIK

Kohëve të fundit ka pasur një shtytje për të rritur sigurinë e pajisjeve të bazuara në kompjuter, si laptopët, tabletët dhe smartfonët (smartphone). Bashkimi Evropian dhe vendet anëtare si dhe Shtetet e Bashkuara kanë filluar të bëjnë presion mbi prodhuesit e teknologjisë për të siguruar sigurinë e produkteve të tyre.

Departamenti i Sigurisë Kombëtare të Shteteve të Bashkuara të Amerikës lëshoi një numër parimesh strategjike në 2016 që synojnë sigurimin e Internetit të Gjërave (Internet of Things). Faza e parë e kësaj qasjeje është sigurimi i pajisjeve gjatë prodhimit të tyre, pastaj ruajtja e sigurisë përmes azhurnimeve dhe menaxhimit të cenueshmërisë.

Mbretëria e Bashkuar krijoi një "kod sigurie të praktikës" për prodhuesit për t'i inkurajuar ata që të rrisin sigurinë e pajisjeve ndërsa janë në fazën e zhvillimit. Për të rritur sigurinë e vetë pajisjeve, kodi kërkon që pajisjet e Internetit të Gjërave të kenë kërkesa më unike për fjalëkalim, si dhe një nxitje për transparencë më të madhe në shkeljet e sigurisë duke inkurajuar zbulimin publik të çdo dobësie në pajisjet. Aktualisht ky kod është vetëm mbi një bazë vullnetare, por Britania e Madhe nuk ka përjashtuar mundësinë e bërjes së tij të detyrueshme për pajisjet e prodhuara në vend.

Megjithëse qasja e BE për rritjen e sigurisë së pajisjes është ende duke u hartuar, ajo do të krijojë një proces certifikimi për pajisjet IoT në një shkallë të gjerë të BE-së.

Të gjitha këto qasje përpiqen të inkurajojnë vendet e tjera të zhvillojnë qasjet dhe politikat e tyre me qëllim që të sigurojnë pajisje të lidhura me hapësirën kibernetike.

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

Siguria Kibernetike

Me përhapjen e përdorimit të hapësirës kibernetike nga qeveritë, si dhe individët dhe kompanitë, sasia e të dhënave dhe informacioneve të ndjeshme brenda hapësirës kibernetike po rritet në mënyrë eksponenciale ndërsa rritet edhe numri i dobësive të reja që ndryshojnë në vazhdimësi.[7] Mbrojtja efektive e këtij informacioni është thelbësore për krijimin e një ambienti të sigurt brenda dhe jashtë hapësirës kibernetike. Siguria kibernetike, siç do të sugjeronte emri, konsiston në praktikat dhe metodat e sigurimit të të dhënave, informacionit dhe integritetit të përbërësve të ndryshëm të hapësirës kibernetike, duke përfshirë por pa u kufizuar në aspektet fizike të mediumit.[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

Megjithëse siguria kibernetike shoqërohet shpesh me strategji të sigurisë kombëtare, është e rëndësishme të shikojmë përdorimet më të gjera të termit. ITU përshkruan sigurinë kibernetike si mjete, udhëzime dhe qasje të tjera për të mbrojtur integritetin dhe natyrën konfidenciale të hapësirës kibernetike për organizatat private, qeverinë dhe shoqërinë civile[9] .

Në përputhje me rëndësinë në rritje të hapësirës kibernetike për aktivitete profesionale, rekreative dhe politike, siguria kibernetike është një fushë në zhvillim në sektorin e sigurisë dhe qeverisjes së mirë të sektorit të sigurisë. Normat në lidhje me sigurinë në hapësirën kibernetike kanë evoluar për t'iu përgjigjur zgjerimit të shpejtë të praktikave dhe teknikave të sigurisë kibernetike dhe aktorëve gjithnjë në ndryshim në këtë fushë.[10] Ndërsa kombet hartojnë qasje kombëtare për të siguruar një mjedis më të sigurt të hapësirës kibernetike brenda vendit të tyre, po shfaqen disa norma në lidhje me shtrirjen e fuqisë së tyre mbi hapësirën kibernetike, si dhe mënyrën në të cilën shtetet mund të ushtrojnë pushtet mbi hapësirën kibernetike[11] .

Matja e Sigurisë Kibernetike

Duke pasur parasysh përkufizimet e gjera dhe konkurruese të hapësirës kibernetike dhe sigurisë kibernetike, analizimi i sigurisë kibernetike nuk është një gjë e lehtë. ITU krijoi Indeksin Global të Sigurisë Kibernetike për të përcaktuar përkushtimin e vendeve anëtare të tyre për forcimin e sigurisë kibernetike. Ky Indeks vlerëson pesë aspekte të ndryshme të sigurisë kibernetike, juridike, teknologjike, organizative, ndërtimit të kapaciteteve dhe bashkëpunimit, për të parë përkushtimin e një kombi.
Ndërsa ky është një mjet i mirë për të vendosur reagimin dhe veprimet e qeverisë ndaj qeverisjes së hapësirës kibernetike, ai neglizhon rolin e aktorit jo-shtetëror si në hapësirën kibernetike ashtu edhe në sigurinë kibernetike. Meqenëse vlerëson politikat dhe jo praktikat, nuk merr në konsideratë ndikimet praktike ose efikasitetin e këtyre angazhimeve.

9 ITU vodič za razvoj NCSS, 13.

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

11 Ibid.

2. QSS në hapësirën kibernetike

Hapësira kibernetike paraqet një sërë lirish, kufizimesh dhe kompleksitetesh unike për natyrën e vetë mediumit. Duke pasur parasysh grupin e larmishëm të aktorëve brenda hapësirës kibernetike dhe mënyrën në të cilën ajo mund të shfrytëzohet ose abuzohet, krijimi i një kornize për praktikat e mira të QSS-së përballet me grupe të ndryshme pengesash nga siguria më tradicionale 'territoriale'. Disa nga këto pengesa u shqyrtuan në kapitullin e fundit, kryesisht ato që dobësojnë sundimin e ligjit, transparencën dhe llogaridhënien.

Gjatë shikimit të QSS-së nëpërmjet prizmit të hapësirës kibernetike, është e rëndësishme të merren parasysh aktorët e ndryshëm në këtë sferë, të vlerësohet se cili ka kontroll mbi aspektet e hapësirës kibernetike dhe si të ndikojmë ose stimulojmë më mirë sjelljet dhe praktikat që në fund të fundit do të forcojnë QSS-në në arenën e hapësirës kibernetike. Renditja e larmishme e aktorëve në hapësirën kibernetike dhe sigurinë kibernetike krijon një paradigmë interesante për t'u eksploruar nga politikëbërësit, pasi shteti nuk është në gjendje të sigurojë në mënyrë të njëanshme sigurinë dhe rregullimin efektiv të mediumit.

Praktikë e mirë: Zbatoni një qasje të sigurisë kibernetike që përfshin aktorë nga sektorët publikë dhe privatë në hapësirën kibernetike.

Meqenëse hapësira kibernetike është një platformë për aktorët privatë dhe ata publikë, krijimi dhe zbatimi i politikave të ndryshme që ndikojnë në QSS duhet të përfshijë subjekte që ekzistojnë jashtë sferës publike. Njohja e rolit të kompanive të teknologjive të informacionit dhe komunikimit (TIK) dhe korporatat private të sigurisë kibernetike luajnë në formimin dhe mbrojtjen e të drejtave dhe sigurisë së përdoruesve është një hap i rëndësishëm për krijimin e një mjedisi kibernetik më të sigurt.

SHEMBUJ TË PRAKTIKËS SË MIRË

Qeveria e Kamerunit punon me disa partnerë të sektorit privat mbi çështje që kanë të bëjnë me sigurinë kibernetike dhe ka krijuar marrëdhënie pune me vendet e tjera kur menaxhon dhe u përgjigjet kërcënimeve kibernetike. Vlen të veçohet rasti kur pas një mashtrimi në internet që përfshinte një kompani farmaceutike, Kameruni hyri në partneritet me Republikën Çeke, INTERPOL-in dhe Nigerinë për të kryer hetime digjitale. Autoritetet kamerunase promovojnë disa masa të ndërtimit të besimit dhe marrëveshjeve të bashkëpunimit ndërkombëtar në hapësirën kibernetike duke shkëmbyer informacion mbi incidentet kibernetike dhe praktikat më të mira për sigurinë kibernetike.

Problemet aktuale me QSS-në në hapësirën kibernetike

Praktikat e mira të QSS-së në hapësirën kibernetike mund të ndihmojnë që siguria njerëzore, sundimi i ligjit dhe aspektet e tjera të qeverisjes së mirë të vëzhgohen dhe mbrohen më tej brenda hapësirës kibernetike.

Siç u përmend shkurtimisht në kapitullin e fundit, një nga sfidat me të cilat përballet qeverisja e sektorit të sigurisë në hapësirën kibernetike është mungesa e të kuptuarit se si të zbatohen parimet efektive të qeverisjes në hapësirën kibernetike, duke rezultuar në politika dhe rregullore të papërshtatshme, dhe krijimin e një mjedisi të mundshëm për veprimtari kriminale.[12] Mungesa e njohurive mund të ndikojë gjithashtu në rregullimin efektiv të shteteve mbi aktorët e sektorit privat, duke minuar aftësinë e shtetit për të miratuar praktika të mira të QSS-së në hapësirën kibernetike.

Aktualisht shumë shërbime të sigurisë në hapësirën kibernetike sigurohen nga subjekte tregtare private duke krijuar sfida për zbatimin efektiv të praktikave QSS brenda hapësirës kibernetike. Një aspekt i qeverisjes së mirë që po bëhet gjithnjë e më i vështirë për t'u zbatuar nga shtetet është transparenca. Si sfidë e parë, nuk është bërë ende përkufizimi i transparencës në hapësirën kibernetike nga një perspektivë e QSS së mirë. Sidoqoftë, gjithnjë e më shumë nocioni i transparencës në këtë kontekst shoqërohet me zbulimin se kur, dhe në çfarë mase, ka ndodhur një shkelje e sistemeve të informacionit.[13]

STUDIM I RASTIT MANDATIMI I TRANSPARENCËS

Australi

Në vitin 2017, Parlamenti Australian miratoi një ndryshim në Ligjin e Privatësisë 1998 që kërkon që organizatat qeveritare të Komonuelthit, organizatat e sektorit privat dhe organet e tjera të specifikuara të zbulojnë informacionin në lidhje me shkeljet e sigurisë kibernetike atyre që janë prekur nga shkeljet. Mosrespektimi i kësaj rregulloreje të re do të rezultojë me një kompensim monetar për ata që janë prekur nga shkelja, njohja publike dhe falja për mosrespektimin dhe ndëshkimet e mëdha civile për ata që përjetojnë raste të shumta të mosrespektimit.

Burimi: Ben Allen, "Australia: Cybercrime – New Mandatory Data Breach Reporting Requirements" mondaq, www.mondaq.com. E aksesuesshme në : http://www.mondaq.com/australia/x/573188/Security/Cybercrime+New+Mandatory+Data+Breach+Reporting+Requirements

Shtetet e Bashkuara të Amerikës

Komisioni i Letrave me Vlerë dhe Shkëmbim i Shteteve të Bashkuara shqiptoi një gjobë të madhe prej 35 milion USD për Jahu (Yahoo) si rezultat i mos zbulimit të një sulmi kibernetik që ndikoi mbi 500 milion llogari. Ky ishte rasti i parë i një kompanie që u ndëshkua për mosrespektimin e kërkesave për zbulim të mandatuara nga kompanitë e tregtuara publikisht.

Burimi: Kadhim Shubber, "Yahoo's $35m Fine Sends a Message" , Financial Times, www.ft.com. E aksesuesshme në: https://www.ft.com/content/4c0932f0-6d8a-11e8-8863-a9bb262c5f53

Inkurajimi ose mandatimi i aktorëve për të zbuluar shkeljet e sigurisë kibernetike është një mënyrë që një shtet të rrisë praktikat e mira QSS, pasi jo vetëm që rrit transparencën brenda hapësirës kibernetike, por gjithashtu siguron që të adresohen boshllëqet brenda praktikave aktuale të sigurisë kibernetike, duke ndihmuar në

12 Buzatu, SSG/SSR in Cyberspace, p. 7-8.

13 VShikoni, p.sh., ICANN Organization's Cybersecurity Transparency Guidelines (2018), available online at: https://www.icann.org/en/system/files/files/cybersecurity-transparency-guidelines-03aug18-en.pdf

ndalimin e përhapjes së sulmeve kibernetike dhe përmirësimin e praktikave të sigurisë në hapësirën kibernetike.[14] Mungesa e transparencës në lidhje me sulmet kibernetike cenon në masë të madhe sigurinë njerëzore brenda hapësirës kibernetike, pasi mund të lejojë sulmet dashakeqe kibernetike të dëmtojnë më shumë viktima.

Natyra transnacionale e hapësirës kibernetike krijon gjithashtu një dilemë për shtetet që të miratojnë praktika të mira të QSS-së brenda saj. Ndërsa qytetarët angazhohen në transaksione që kalojnë kufijtë ndërkombëtarë territorialë në mënyrë të vazhdueshme, aftësia e një shteti për të ushtruar autoritet mbi ato që ndikojnë në popullsinë e tyre zvogëlohet shumë. Në shumicën e rasteve, Shtetet duhet të mbështeten tek ndërmjetësit komercialë - siç janë platformat e mediave sociale - për të mbikëqyrur dhe rregulluar sjelljet në internet.[15] Kjo mund të minojë praktikat e mira të QSS-së, pasi shteti zakonisht nuk ka qasje për të parë se si filtrohet ose merret informacioni. Një sfidë tjetër është natyra transnacionale e informacionit në Internet, i cili mund të ruhet në një ose më shumë serverë të vendosur në juridiksione të shumëfishta. Mbështetja te shtetet e tjera në hetimin, përndjekjen dhe dënimin e kriminelëve në internet gjithashtu krijon një dinamikë tjetër. Në këtë mënyrë, hapësira kibernetike minon praktikat e mira të qeverisjes pasi ajo mbështetet jo vetëm tek aktorët brenda një juridiksioni të vetëm, por përkundrazi ndikon një grup aktorësh ndërkombëtarë.

STUDIM I RASTIT: HETIME NDËRKOMBËTARE

Hetimi ndërkombëtar dhe ndjekja penale në fushën e sigurisë kibernetike nuk është një fenomen i padëgjuar. Në prill 2018, një faqe në internet që shiste shërbime të shpërndarjes së mohimit të shërbimit (DDoS), Webstresser.org, ishte ngrirë dhe administratorët u akuzuan për krime kibernetike falë një aksioni për hetimin ndërkombëtar të Njësisë Kombëtare Holandeze të Krimit të Teknologjisë së Lartë dhe Agjencisë Kombëtare të Krimit të MB-së me mbështetjen e shumë organizatave të tjera. Operacioni "Pauer of" (Power Off) është vetëm një shembull se si aktorët ndërkombëtarë mund të punojnë së bashku për të krijuar një mjedis kibernetik më të sigurt për përdoruesit.

Burimi: Cal Jeffrey, Operation Power OFF pulls the plug on 'DDoS-for-hire' website, TechSpot www.techspot.com. 25.april 2018. Gjendet në: 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" Europol.europa.org. 25.april 2018. Gjendet në: https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down

Megjithëse mund të duket sikur ka shumë pengesa për të zbatuar praktika të mira QSS në hapësirën kibernetike, nuk është fare një detyre e pamundur. Disa korniza dhe norma ndërkombëtare që ofrojnë udhëzime se si të integrohen QSS-të në hapësirën kibernetike kanë filluar të konkretizohen. Ndërsa duhet të rishikohen praktikat dhe politikat për t'iu përshtatur kontekstit kombëtar, identifikimi i kornizave ndërkombëtare dhe rajonale që janë të rëndësishme për hapësirën kibernetike është një hap parësor drejt QSS-së së mirë në hapësirën kibernetike.

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

GJETJET KRYESORE

- Hapësira kibernetike ekziston si në nivelin fizik ashtu edhe në atë jo fizik dhe përbëhet nga çdo platformë mbi të cilën informacioni, të dhënat dhe komunikimet mund të transferohen, transformohen ose ndryshohen nga një kompjuter në tjetrin. Ai gjithashtu përfshin infrastrukturën fizike të Internetit që shtrihet në të gjithë globin.
- Qeveria, qytetarët dhe kompanitë po bëhen gjithnjë e më të varura nga burimet që hapësira kibernetike siguron në jetën e përditshme.
- Ekziston një gamë e gjerë aktorësh brenda hapësirës kibernetike dhe sigurisë kibernetike.
- Ekzistojnë pengesa të ndryshme për QSS në hapësirën kibernetike, duke filluar nga aktorë të shumtë që ndikojnë në aspekte të ndryshme të hapësirës kibernetike, deri te mungesa e përgjithshme e njohurive në lidhje me përdorimin e sigurt të hapësirës kibernetike.
- Megjithëse disa shtete kanë politika dhe korniza të vendosura për sigurinë kibernetike dhe qeverisjen e hapësirës kibernetike, një mungesë e përgjithshme e njohurive mbi këtë temë e bën të vështirë sigurimin e zbatimit të duhur të praktikave të QSS në hapësirën kibernetike.

Burime

Buckland, Benjamin, Fred Schreier, and Theodor H. Winkler, "Democratic Governance Challenges of Cybersecurity" DCAF Horizon 2015 Working Paper no. 1. Gjeneva: Kontrolli Demokratik i Forcave të Armatosura, 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, 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: Kontrolli Demokratik i Forcave të Armatosura, https://www.dcaf.ch/sites/default/files/publications/documents/Cyber2.pdf

Liaropoulos, Andrew N. 2017, Cyberspace Governance and State Sovereignty 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, 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. Atlanta: Georgia Institute of Technology. https://www.researchgate.net/publication/267971678

KAPITULLI 3

KORNIZAT JURIDIKE NDËRKOMBËTARE DHE RAJONALE NË HAPËSIRËN KIBERNETIKE

OBJEKTIVAT

Ky kapitull synon t'u ofrojë përdoruesve një përmbledhje të kornizave ligjore ndërkombëtare dhe rajonale të zbatueshme në hapësirën kibernetike dhe thekson qasjet dhe iniciativat interesante dhe inovative.

Objektivat e nxënies së këtij kapitulli janë si më poshtë:

- Rritja e njohurive të organizatave të ndryshme ndërkombëtare dhe rajonale që adresojnë hapësirën kibernetike dhe sigurinë kibernetike.
- Rritja e ndërgjegjësimit për burimet e disponueshme që mbështetesin zbatimin e kornizave ligjore ndërkombëtare dhe rajonale në një nivel kombëtar.
- Rritja e njohurive mbi krimin kibernetik, terrorizmin kibernetik dhe përdorimin terrorist të internetit.

Hyrje

Kornizat ligjore efektive - në nivelet ndërkombëtare, rajonale dhe kombëtare - janë një nga shtyllat e qeverisjes së mirë dhe përbëjnë një parakusht për parimin e sundimit të ligjit. Në përgjithësi, kornizat ligjore janë thelbësore për të rregulluar sjelljen e ligjshme dhe për të ndaluar ose penalizuar veprimtari të paligjshme. Kornizat ligjore në hapësirën kibernetike janë gjithashtu të rëndësishme për të siguruar respektimin e të drejtave të njeriut.

Ka pasur shumë diskutime dhe konfuzion rreth asaj se si kornizat ligjore mund dhe zbatohen në hapësirën kibernetike. Për shkak të natyrës së tij ndërkufitar dhe duke pasur informacionin në qendër të saj, hapësira kibernetike përbën sfidë për qeverisjen të përqendruar në shtetin. Nga njëra anë, infrastruktura fizike që përbën hapësirën kibernetike i nënshtrohet juridiksionit dhe autoritetit kombëtar. Nga ana tjetër, rrjedha e të dhënave dhe informacionit nëpër atë infrastrukturë vazhdimisht kalon nëpër juridiksione territoriale (të shumta), duke e bërë të vështirë për një juridiksion ligjor të ushtrojë "kontroll efektiv" mbi këtë fluks informacioni. Kjo ka bërë që shumë njerëz të bëjnë thirrje për zhvillimin e regjimeve të reja normative për të rregulluar hapësirën kibernetike.

Këto ditë është e pakontestueshme që parimet e së drejtës ndërkombëtare janë të zbatueshme në hapësirën kibernetike. Ajo që është më pak e qartë është se si këto parime përkthehen në praktikë. Si pasojë, ky hendek midis politikës dhe praktikës çon në pasiguri ligjore dhe madje edhe në boshllëqe ligjore që mund të cenojnë mbrojtjen e të drejtave të njeriut të përdoruesve në Internet. Prandaj, organizatat ndërkombëtare dhe rajonale kanë ndërmarrë të fillojnë iniciativa që synojnë të identifikojnë dhe interpretojnë se si zbatohen parimet ekzistuese ligjore të së drejtës ndërkombëtare në hapësirën kibernetike.

1. Kuadri ligjor dhe rajonal ndërkombëtar

Nisma të shumta në nivelin ndërkombëtar dhe rajonal synojnë të promovojnë sjellje më të përgjegjshme në hapësirën kibernetike dhe të zhvillojnë kornizat rregullatore dhe masat e ndërtimit të besimit në hapësirën kibernetike. Më poshtë jepet një përmbledhje e këtyre nismave.

Kombet e Bashkuara

Aktualisht nuk ka asnjë instrument ligjërisht të detyrueshëm në nivelin ndërkombëtar që rregullon sjelljen në hapësirën kibernetike. Sidoqoftë, ekzistojnë një numër iniciativash "të buta" (të cilat ligjërisht nuk janë detyruese) që identifikojnë normat në hapësirën kibernetike dhe ofrojnë udhëzime për shtetet në lidhje me zbatimin e këtyre normave.

Këto ditë është përgjithësisht e pakontestueshme që e drejta ndërkombëtare - në veçanti Karta e Kombeve të Bashkuara, e drejta ndërkombëtare e të drejtave të njeriut dhe e drejta ndërkombëtare humanitare - zbatohet në hapësirën kibernetike.

STUDIM I RASTIT: RAPORTI I OKB NGA GRUPI I EKSPERTËVE QEVERITARË

Raporti i vitit 2015 i OKB-së nga GEQ-ja rendit rekomandimet e mëposhtme për sjelljen e përgjegjshme të shteteve për të kontribuar në një hapësirë kibernetike të hapur, të sigurt, të qëndrueshme, të arritshme dhe paqësore:

Normat pozitive:

- Shtetet duhet të bashkëpunojnë për të rritur stabilitetin dhe sigurinë në përdorimin e TIK-ut dhe për të parandaluar praktikat e dëmshme të TIK-ut.
- Shtetet duhet të marrin në konsideratë të gjithë informacionin përkatës në lidhje me atribuimin në mjedisin e TIK-ut;
- Shtetet duhet të marrin masat e duhura për të mbrojtur infrastrukturën kritike kombëtare nga kërcënimet e TIK-ut, si dhe t'u përgjigjen kërkesave për ndihmë nga një shtet tjetër;
- Shtetet duhet të ndërmarrin hapa të arsyeshëm për të siguruar integritetin e zinxhirit të furnizimit dhe duhet të parandalojnë përhapjen e mjeteve dhe teknikave dashakeqe të TIK-ut.
- Shtetet duhet të inkurajojnë raportimin e përgjegjshëm të dobësive të TIK-ut dhe të ndajnë informacionin përkatës.

Normat kufizuese:

- Shtetet nuk duhet të lejojnë që me vetëdije territori i tyre të përdoret për veprime të gabuara ndërkombëtarish duke përdorur TIK.
- Shtetet duhet t'i përmbahen rezolutave të Asamblesë së Përgjithshme të Kombeve të Bashkuara për të drejtat e njeriut.
- Shtetet nuk duhet me vetëdije të kryejnë veprimtari në mbështetje të TIK-ut që janë në kundërshtim me detyrimet e tyre sipas ligjit ndërkombëtar.
- Shtetet nuk duhet të kryejnë ose mbështesin me vetëdije veprimtari për të dëmtuar sistemet e informacionit të ekipeve të autorizuara të reagimit në rast emergjence.

Kombet e Bashkuara, për shembull, që nga viti 2004 kanë krijuar gjashtë grupe të ekspertëve qeveritarë (UN GGE) - bazuar në "shpërndarjen e drejtë gjeografike" dhe duke përfshirë "fuqitë kryesore kibernetike" siç janë Shtetet e Bashkuara të Amerikës, Kinën, Rusinë, Francën, Mbretërinë e Bashkuar dhe Gjermaninë - me qëllim që të propozojnë norma të sjelljes së përgjegjshme në hapësirën kibernetike.

STUDIM I RASTIT: NDËRHYRJET ZGJEDHORE NËPËRMJET FUSHATËS ONLAJN - RAST PËR TË DREJTËN NDËRKOMBËTARE

Ndërsa ndërhyrja në proceset politike midis mjeteve të fshehura ose të hapura nuk është asgjë e re në marrëdhëniet ndërkombëtare, që nga viti 2016, zyrtarët qeveritarë kryesisht në shtetet perëndimore shprehin shqetësime mbi ndërhyrjet në zgjedhje nëpërmjet operacioneve të synuara kibernetike dhe fushatave të keqinformimit.

Në vitin 2014, operacionet CyberBerkut e vunë në shënjestër Komisionin Qendror të Zgjedhjeve të Ukrainës, duke sulmuar një pjesë të rrjeteve të Komisionit për gati njëzet orë dhe duke shpallur një fitues të rremë në ditën e zgjedhjeve. Në vitin 2016, njësia e piraterisë "Fancy Bear" sulmoi sistemet e Bundestagut Gjerman, Ministrive të Jashtme dhe të Financave të Gjermanisë dhe të Bashkimit Demokristian. Në vitin 2017, operacionet kibernetike që synonin të mbjellin maluer (malware) në faqen e internetit të një fushate, vunë në shënjestër fushatën e Emanuel Makron për Presidencën Franceze.

Sipas detyrimeve të së drejtës ndërkombëtare, ka të ngjarë që këto të përbëjnë shkelje të sovranitetit të një shteti. Sovraniteti është konsideruar gjerësisht si parim dhe rregull parësor i së drejtës ndërkombëtare - që gjithashtu u përfshi nga raporti i KB GGE 2015

"Sovraniteti i shteteve dhe normat dhe parimet ndërkombëtare që rrjedhin nga sovraniteti zbatohen në miratimin aktiviteteve të shteteve që lidhen me TIK dhe për juridiksionin e tyre mbi infrastrukturën e TIK-ut brenda territorit të tyre."

Në përgjithësi, parimi i objektit dhe qëllimit të sovranitetit është "t'u ofrojë shteteve kontroll të plotë mbi hyrjen dhe aktivitetet në territorin e tyre".

Çfarë do të thotë kjo në ndërhyrjen e zgjedhje nëpërmjet operacioneve kibernetike?

Ekspertët argumentojnë se pika kritike për të vlerësuar nëse një veprim i tillë përbën një shkelje të parimit të sovranitetit nuk është "se kishte një lidhje midis sistemit të synuar dhe zgjedhjeve, por thjesht sepse operacioni rezultoi me një dëmtim përkatës - humbje e funksionalitetit." Sipas Manualit të Talinit 2.0 veprimet që mund të cilësohen si shkelje të sovranitetit janë: operacioni kibernetik që bën që infrastruktura kibernetike ose programet të funksionojnë ndryshe; ndryshimi ose fshirja e të dhënave të ruajtura në infrastrukturën kibernetike pa shkaktuar pasoja fizike ose funksionale, siç përshkruhet më sipër; vendosja e maluer (malware) në një sistem; instalimi i dyerve të pasme; dhe duke shkaktuar një humbje të përkohshme, por të konsiderueshme, të funksionalitetit, si në rastin e një veprimi të madh të shpërndarjes së mohimit të shërbimit.

Përparim i madh u arrit në vitin 2013, kur GGE-ja e KB-së që përbëhej nga vetëm pesëmbëdhjetë anëtarë miratoi raportin e tij të konsensus që afirmonte zbatimin e së drejtës ndërkombëtare në hapësirën kibernetike. Raporti i konsensusit i UN GGE 2015 e riafirmoi këtë deklaratë dhe specifikoi më tej kornizën normative për përdorimin e aftësive kibernetike nga shteti. Me interes të veçantë në këtë drejtim është seksioni që përqendrohet në "normat, rregullat dhe parimet për sjelljen e përgjegjshme të shteteve".

Fatkeqësisht, UN GGE 2016-2017 nuk ishte i suksesshëm në miratimin e një raporti konsensusi, duke e hedhur komunitetin ndërkombëtar në një çrregullim në lidhje me mënyrën e qasjes më të mirë të së drejtës ndërkombëtare në hapësirën kibernetike. Sidoqoftë, në tetor 2018, Asambleja e Përgjithshme e OKB-së (UNGA) miratoi rezolutën / C.1 / 73 / L.37 për të krijuar një GGE tjetër në 2019, duke ngarkuar grupin të raportonte përsëri në 2021 në seancën e 76-të të UNGA. Paralelisht, përmes rezolutës A / C.1 / 73 / L.27 / Rev.1, UNGA gjithashtu krijoi një grup punues të hapur që do të thirret në qershor 2019 në mënyrë që të zhvillojë rregullat, normat dhe parimet e sjelljes së përgjegjshme të shtetit në hapësirën kibernetike, si dhe të marrin në konsideratë zbatimin praktik të tyre.

INFOBOX: ANONIMITETI NË INTERNET

Anonimiteti është thelbësor për të mbrojtur të drejtat e njeriut. Me ardhjen e internetit, është bërë e qartë se rëndësia e anonimitetit nuk mund të kufizohet vetëm në lirinë e individëve për të komunikuar me njëri-tjetrin, për të shkëmbyer informacione dhe ide, por edhe për të mbrojtur individët nga vëzhgimi i panevojshëm dhe i padrejtë.
Sidoqoftë, e drejta për anonimitet në internet deri më tani ka marrë njohje të kufizuar sipas ligjit ndërkombëtar. Tradicionalisht, mbrojtja e anonimatit në internet ka qenë e lidhur me mbrojtjen e të drejtës për privatësi dhe të dhëna personale (shih nenin 12 UDHR, 17 ICCPR).
Për më tepër, anonimiteti është një koncept kryesor në mbrojtjen e lirisë së shprehjes, si dhe të së drejtës për privatësi. Në mënyrën më të thjeshtë, anonimati është fakti i mos identifikimit dhe, në këtë kuptim, është pjesë e përvojës së zakonshme të shumicës së njerëzve në baza ditore, p.sh. të ecësh si pjesë e një turme ose të qëndrosh në një radhë të huajsh. Në këtë mënyrë, një aktivitet mund të jetë anonim duke qenë publik.

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

Në përgjithësi është pranuar se korniza ndërkombëtare e ligjit për të drejtat e njeriut, duke përfshirë edhe Deklaratën Universale për të Drejtat e Njeriut dhe Paktin Ndërkombëtar për të Drejtat Civile dhe Politike, të zbatohen në hapësirën digjitale. Këtë e pohoi Këshilli i të Drejtave të Njeriut (KDNJ) në rezolutën A / HRC / 20 / L.13 që vë në dukje se "të njëjtat të drejta që njerëzit kanë jashtë internetit duhet të mbrohen gjithashtu në internet".[1] Kjo rezolutë ka një rëndësi të veçantë pasi ishte hera e parë që organi ndërkombëtar deklaroi në mënyrë të qartë se të drejtat e njeriut zbatohen gjithashtu në hapësirën kibernetike.

Pas zbulimeve të Snoudenit, në vitin 2015[2] UNGA vendosi të emërojë një Raportues të ri special për të drejtën e privatësisë në mënyrë që të adresojë më mirë privatësinë në epokën digjitale dhe për të krijuar një mjedis digjital më të sigurt në 2015. Raportuesi special për të drejtën e privatësisë është i mandatuar të vizitojë shtete, të bëjë rekomandime dhe të pranojë ankesa nga individë.

Një rezolutë tjetër e rëndësishme e UNGA-s është A / RES / 57/239 mbi krijimin e një kulture globale të sigurisë kibernetike që njeh krimin kibernetik si një sfidë të madhe për sigurinë kibernetike.[3]

Një instrument tjetër i OKB-së që është i rëndësishëm për identifikimin e normave në hapësirën kibernetike janë Parimet udhëzuese të Kombeve të Bashkuara mbi biznesin dhe të drejtat e njeriut[4] (të njohura edhe si 'Parimet Ruggie') që u miratuan në 2011 dhe

1 Asambleja e Përgjithshme e Kombeve të Bashkuara, Këshilli i të Drejtave të Njeriut për promovimin, mbrojtjen dhe gëzimin e të drejtave të njeriut në internet, A / HRC / 20 / L.13, 29 qershor 2012

2 The Guardian, The NSA files, gjendet në 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, gjendet në https://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf

që ofrojnë udhëzime për shtetet si dhe për bizneset në lidhje me mbrojtjen e të drejtave të njeriut. Parimet Ruggie bazohen në kornizën e OKB-së "Respekto, mbro dhe zgjidh". Në pjesën hyrëse të këtyre parimeve udhëzuese përcaktohet se "roli i ndërmarrjeve të biznesit si organe të specializuara të shoqërisë që kryejnë funksione të specializuara, kërkohet të respektojnë të gjitha ligjet në fuqi dhe të respektojnë të drejtat e njeriut". [5]

Në kontekstin e rregullimit të llojeve të caktuara të fjalës së paligjshme në internet, në veçanti të gjuhës së urrejtjes, raporti nga Komisioneri i Lartë i OKB-së për të drejtat e njeriut dhe miratuar nga Këshilli i të Drejtave të Njeriut në 2013 (i njohur gjithashtu si 'Planveprimi i Rabatit') përcakton kritere që shërbejnë për të identifikuar gjuhën e urrejtjes dhe mund të japë udhëzime edhe në sferën onlajn [6].

STUDIM I RASTIT: PLANVEPRIMI I RABATIT

Planveprimi i Rabatit identifikon një test gjashtë pjesësh për të vlerësuar ashpërsinë e shprehjes që mund të konsiderohet si vepër penale. Këto gjashtë kritere janë: konteksti, folësi; qëllimi, përmbajtja dhe forma, shtrirja e aktit të fjalës, gjasat, pashmangshmërinë.

Për sa i përket elementit të 'kontekstit', Planveprimi i Rabatit konkretizon se konteksti ka një "rëndësi të madhe kur vlerëson nëse deklarata të veçanta ka të ngjarë të nxisin diskriminim, armiqësi ose dhunë ndaj grupit të synuar, dhe ai mund të ketë lidhje të drejtpërdrejtë si me qëllimet ashtu edhe me shkakësinë. Analiza e kontekstit duhet ta vendosë aktin e të folurit brenda kontekstit shoqëror dhe politik të përhapur në kohën kur është bërë dhe shpërndarë fjalimi ".

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

Agjenci dhe zyra të tjera të ndryshme të OKB-së, si Instituti i OKB-së për Kërkimin e Çarmatimit (UNIDIR), Instituti Ndërkombëtar i OKB-së për Krimin dhe Drejtësinë dhe Zyra e OKB-së për Drogat dhe Krimin (UNODC) adresojnë çështje që lidhen me sigurinë kibernetike, si dhe Grupi Punues për Luftën kundër Përdorimit të Internetit për Qëllime Terroriste i cili vepron nën Task-Forcën e OKB-së për Zbatimin e Luftës kundër Terrorizmit.[7]

Unioni Ndërkombëtar i Telekomunikimeve (ITU), një agjenci e OKB-së e specializuar në telekomunikacion, merret me sigurinë kibernetike si pjesë e mandatit të saj. Për këtë qëllim, ITU harton ligje modele dhe profile të sigurisë kibernetike të vendeve që janë në dispozicion të publikut dhe i mbështet shtetet anëtare të OKB-së në zhvillimin e kornizave efektive normative për hapësirën kibernetike

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

6 OHCHR, Rabat Plan of action, gjendet në https://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf

7 Zyra e Kombeve të Bashkuara për Drogat dhe Krimin (2012): The use of the Internet for terrorist purposes, gjendet në https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

STUDIM I RASTIT: PROJEKTI NDËRKOBËTAR I UNIONIT TË TELEKOMUNIKIMIT PËR TË MBËSHTETUR PËRAFRIMIN E POLITIKAVE TË TIK NË AFRIKËN SUBSAHARIANE (HIPSSA)

HIPSSA u iniciua si rezultat i kërkesës së bërë nga organizatat e integrimit ekonomik në Afrikë, si dhe shoqatat e rregullatorëve rajonalë, ITU dhe Komisionit Evropian për ndihmë në përafrimin e politikave dhe legjislacioneve të TIK në Afrikën Subsahariane.

HIPSSA u bë një bllok i rëndësishëm ndërtimi në krijimin e politikave dhe kornizave të harmonizuara panafrikane globale.

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

Këshilli i Evropës

Këshilli i Evropës (KE) përbëhet nga 47 Shtete Anëtare. Konventa e saj mbi krimin kibernetik (e njohur edhe si "Konventa e Budapestit")[8] konsiderohet - për momentin - instrumenti ligjor më i rëndësishëm ndërkombëtar që siguron kuadrin ligjor për të adresuar krimin kibernetik. Si shtetet anëtare ashtu edhe ato joanëtare të KE-së mund të aderojnë në Konventën e Budapestit. Deri më sot, Konventa e Budapestit është ratifikuar nga 61 shtete.[9] Konventa e Budapestit plotësohet me Protokollin e saj mbi ksenofobinë dhe racizmin të kryer nëpërmjet sistemeve kompjuterike. .[10]

Me rëndësi është të theksohet se Konventa e Budapestit u siguron shteteve (i) kriminalizimin e një liste sulmesh kundër dhe me anë të kompjuterëve, (ii) mjete ligjore të procedurave për ta bërë hetimin e krimit kibernetik dhe sigurimin e provave elektronike në lidhje me ndonjë krim më efektiv dhe subjekt i masave mbrojtëse të sundimit të ligjit, dhe (iii) bashkëpunimi ndërkombëtar policor dhe gjyqësor mbi krimin kibernetik dhe provat elektronike.

Për më tepër, KE-ja hartoi Konventën për Mbrojtjen e Individëve gjatë Përpunimit Automatik të të Dhënave Personale (Konventa nr. CETS 108),[11] që ka për qëllim të "mbrojë çdo individ, pavarësisht nga kombësia ose vendbanimi i tij, në lidhje me përpunimin e të dhënave të tyre personale, duke kontribuar kështu në respektimin e të drejtave të tij dhe të njeriut dhe liritë themelore, dhe veçanërisht të drejtën për privatësi ".[12]

Kjo Konventë ishte instrumenti i parë ndërkombëtar i detyrueshëm ligjërisht në fushën e mbrojtjes së të dhënave. Sipas kësaj Konvente, palëve u kërkohet të ndërmarrin hapat e nevojshëm në legjislacionet e tyre përkatëse kombëtare për të zbatuar parimet në mënyrë që të sigurojnë respektimin në territorin e tyre për të drejtat themelore të njeriut

8 CKëshilli i Evropës, Konventa për Krimin Kibernetik, CETS Nr. 185, në dispozicion në https://www.coe.int/en/web/cybercrime/the-budapest-convention

9 Senegali është palë në Konventën e Budapestit. Tunizia dhe Maroku janë në proces të nënshkrimit dhe ratifikimit të Konventës së Budapestit.

10 Këshilli i Evropës, Protokolli shtesë i Konventës mbi Krimin Kibernetik, në lidhje me kriminalizimin e akteve të natyrës raciste dhe ksenofobike të kryera nëpërmjet sistemeve kompjuterike, ETS Nr. 189, i disponueshëm në https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

11 Këshilli i Evropës, Konventa për Mbrojtjen e Individëve gjatë Përpunimit të të Dhënave Personale, CETS Nr. 180, gjendet në: https://www.coe.int/en/web/data-protection/home

12 CKëshilli i Evropës, Konventa e Modernizuar për Mbrojtjen e Individëve në lidhje me Përpunimin e të Dhënave Personale, gjendet në: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8

të të gjithë individëve në lidhje me përpunimin e të dhënave personale. Konventa nr. 108 është përditësuar në maj 2018 për të kapur zhvillimet e fundit në fushën e teknologjive të reja dhe mbrojtjen e të dhënave. Deri më sot, Konventa është ratifikuar nga 53 shtete anëtare dhe joanëtare të KE-së.[13]

Përveç kësaj, KE-ja jep udhëzime për interpretimin e konventave dhe programeve të ndryshme të ndërtimit të kapaciteteve, si për shembull me programin e saj GLACY + që mbështet shtetet në zhvillimin e legjislacionit efektiv për hapësirën kibernetike.[14] .

Ndërsa Konventa e Budapestit është e vetmja kornizë ligjore ndërkombëtare për rregullimin e krimit kibernetik, mbrojtësit e të drejtave të njeriut thekson veçanërisht faktin se Konventa e Budapestit bazohet në supozimin e shteteve që kanë mekanizma mbrojtës të të drejtave e njeriut.
Sidoqoftë, shtetet që nuk janë anëtare të Këshillit të Evropës nuk kanë domosdoshmërish të njëjtat masa mbrojtëse të të drejtave të njeriut

Bashkimi Afrikan

Në vitin 2014, Bashkimi Afrikan miratoi Konventën për sigurinë kibernetike dhe mbrojtjen e të dhënave personale (e njohur edhe si "Konventa Malabo").[15] Sidoqoftë, konventa nuk ka hyrë në fuqi akoma, pasi është miratuar nga vetëm pesë Shtete Anëtare të Bashkimit Afrikan (Senegal, Mauritius, Guineja, Namibia dhe Gana) dhe e kanë nënshkruar nëntë shtete anëtare. Neni 25 (1) i tij thotë se "Çdo shtet palë do të miratojë masa të tilla legjislative dhe / ose rregullatore që i konsideron efektive duke i konsideruar si vepra penale materiale veprimet që ndikojnë në konfidencialitetin, integritetin, disponueshmërinë dhe mbijetesën e sistemeve të teknologjisë së informacionit dhe komunikimit, të dhënat që ato i përpunojnë dhe infrastrukturën themelore të rrjetit, si dhe masa efektive procedurale për të ndjekur penalisht shkelësit. Shtetet palë do të marrin në konsideratë zgjedhjen e gjuhës që përdoret në praktikat më të mira ndërkombëtare".

STUDIM I RASTIT: KONVENTA E BASHKIMIT AFRIKAN MBI SIGURINË KIBERNETIKE DHE KONVENTA E BUDAPESTIT

Konventa e Budapestit është aktualisht e vetmja kornizë ligjore ndërkombëtare e detyrueshme juridikisht në temën e sigurisë kibernetike, hapësirës kibernetike dhe rolit të shtetit në këtë fushë. Edhe pse vetëm një pjesë e vogël e kombeve afrikane e kanë nënshkruar atë drejtpërdrejt ose janë ftuar të aderojnë, ajo është përdorur si një kornizë udhëzuese për krijimin e Konventës së Bashkimit Afrikan mbi Sigurinë Kibernetike. Ky është një shembull i mënyrës në të cilën normat më të gjera ndërkombëtare mund të përshtaten dhe miratohen në një kontekst specifik për rajonin.

Burimi: "Comparative Analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime", Global Action on Cybercrime Extended. 20 (November 2016), 3-5.

Bashkimi Ekonomik i Shteteve të Afrikës Perëndimore

Bashkimi Ekonomik i Shteteve të Afrikës Perëndimore (ECOWAS) miratoi Aktin shtesë për mbrojtjen e të dhënave personale brenda ECOWAS në vitin 2010,[16] i cili është i ndikuar nga Direktivat e BE-së për mbrojtjen e të dhënave, duke specifikuar përmbajtjen e kërkuar të ligjeve të privatësisë së të dhënave dhe detyron vendet anëtare të krijojnë autoritetin e mbrojtjes.

13 Konventa Nr. 108 u ratifikua nga Kepi i Gjelbër, Mauritius, Senegal dhe Tunizi.

14 Këshilli i Evropës, Veprimi Global mbi Krimin Kibernetik (GLACY), gjendet në: https://www.coe.int/en/web/cybercrime/glacyplus

15 Konventa e Bashkimit Afrikan për Sigurinë Kibernetike dhe Mbrojtjen e të Dhënave Personale, 27 qershor 2014, gjendet në: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

16 ECOWAS, Akti Shtesë për Mbrojtjen e të Dhënave Personale, Shih: http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

ECOWAS gjithashtu miratoi një Direktivë për luftimin e krimit kibernetik (2011) dhe Aktin plotësues për transaksionet elektronike brenda ECOWAS[17] .

Organizata për Siguri dhe Bashkëpunim në Evropë

Organizata për Sigurinë dhe Bashkëpunimin në Evropë (OSBE) adreson çështjet e sigurisë kibernetike / TIK, veçanërisht në dritën e kundërterrorizmit dhe krimit kibernetik. Në 2013, OSBE-ja miratoi masa për ndërtimin e besimit (MNB) për hapësirën kibernetike nëpërmjet Vendimit të Këshillit të Përhershëm Nr. 1106, 3 dhjetor 2013.[18] Këto MNB synojnë zvogëlimin e konfliktit që buron nga përdorimi i teknologjive të informacionit dhe komunikimit.

MNB-të e identifikuara nga OSBE-ja përfshijnë: shkëmbimin e informacionit mbi kërcënimet kibernetike, sigurinë dhe përdorimin e TIK-ut, organizimin kombëtar, strategjitë dhe terminologjinë, mbajtjen e konsultave për të zvogëluar rreziqet e keqperceptimit dhe të shfaqjes së mundshme të tensionit, ndarjen e informacionit mbi masat e marra për të siguruar një internet të hapur dhe të sigurt, shkëmbimi i pikave të kontaktit dhe përdorimi i OSBE-së si një platformë për dialog.

Sidoqoftë, MNB-të bazohen në një qasje vullnetare dhe për këtë arsye janë një instrument që nuk është i detyrueshëm me ligj.

Organizata e Shteteve Amerikane

Organizata e Shteteve Amerikane (OSHA) krijoi një Grup punues mbi krimin kibernetik që në vitin 1999, si forumi kryesor për "forcimin e bashkëpunimit ndërkombëtar në parandalimin, hetimin dhe ndjekjen penale të krimit kibernetik, lehtësimin e shkëmbimit të informacionit dhe përvojave midis anëtarëve të saj, dhe të bëjë rekomandimet e nevojshme për të rritur dhe siguruar përpjekjet për të luftuar këto krime".[19] Grupi i punës takohet çdo dy vjet, duke ofruar rekomandime për shtetet anëtare.

OSHA merret, gjithashtu, edhe me sigurinë kibernetike në një kuptim më të gjerë. Në vitin 2004, Asambleja e Përgjithshme e OSHA-s siguroi një mandat me rezolutën AG / RES.2004 (XXXIV-O / 04), me titull "Strategjia integruese ndëramerikane për të luftuar kërcënimet ndaj sigurisë kibernetike" për Sekretariatin e Komitetit Interamerikan të OSHA-s kundër terrorizmit. Detyrat kryesore e këtij Sekretariati janë të ndihmojë në krijimin e ekipeve kombëtare të reagimit ndaj incidenteve të sigurisë kompjuterike (CSIRT), krijimin e një rrjeti të përbërë nga këto CSIRT dhe mbështetjen e zhvillimit të strategjive kombëtare të sigurisë kibernetike. Që nga viti 2007, Sekretariati është përpjekur të krijojë një program gjithëpërfshirës për ndërtimin e kapaciteteve nëpërmjet seminareve, kurseve teknike, diskutimeve mbi politikat në tryezë të rrumbullakët, ushtrimeve të menaxhimit të krizave dhe shkëmbimin e praktikave më të mira.

17 EECOWAS, Komuniteti Ekonomik i Shteteve të Afrikës Perëndimore (ECOWAS), Direktiva C / DIR.1 / 08/11 për Luftimin e Krimit Kibernetik brenda ECOWAS, 2011, në dispozicion në http://www.osiris.sn/Directive-C-DIR-1-08-11-du-19-aout.html and Supplementary Act A/SA.2/01/10 on Electronic Transactions within ECOWAS, 2010, gjendet në http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Electronic-Transaction-Act.pdf

18 OVendimi i OSBE-së Nr. 1202, Masat e Ndërtimit të Besimit të OSBE-së për të Ulur Rreziqet e Konflikteve që rrjedhin nga Përdorimi i Teknologjive të Informacionit dhe Komunikimit, PC.DEC / 1202, 10 Mars 2016, gjendet në: https://www.osce.org/pc/227281?download=true

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

Organizata e Bashkëpunimit e Shangait

Organizata e Bashkëpunimit e Shangait (OBSH), organizatë ndërkombëtare me gjashtë shtete anëtare (domethënë Kina, Kazakistani, Kirgistani, Rusia, Taxhikistani dhe Uzbekistani) miratoi në 2009 një Marrëveshje midis qeverive të shteteve anëtare të OBSH-së për bashkëpunim në fushën e sigurisë së informacionit ndërkombëtar.[20] Në vitin 2011, katër shtete anëtare të OBSH-së i paraqitën Asamblesë së Përgjithshme të OKB-së një Kod ndërkombëtar të sjelljes për sigurinë e informacionit. Në vitin 2015, në Asamblenë e Përgjithshme të OKB-së, u paraqit një Kod i ri ndërkombëtar i sjelljes[21].

STUDIM I RASTIT: PROPOZIM-KODI NDËRKOMBËTAR I SJELLJES I OSHB, 2015

Sipas sponsorëve të këtij propozim-kodi - përkatësisht, shtetet anëtare të OSHB-së - drafti i kodit ka për qëllim "të shtyjë përpara debatin ndërkombëtar mbi normat ndërkombëtare mbi sigurinë e informacionit dhe të ndihmojë në krijimin e një konsensusi të hershëm mbi këtë çështje".

Sipas disa analistëve, draft-kodi i thekson sovranitetin dhe territorialitetin e shtetit në hapësirën kibernetike dhe merret shumë me imperativat e inteligjencës, sigurisë kombëtare dhe stabilitetit të regjimit dhe i mungon mbrojtja thelbësore e të drejtave të njeriut dhe adreson kryesisht kufizimet në lirinë e shprehjes në dispozicion të shteteve sipas ligjit. Vlen të përmendet, gjithashtu, se drafti i kodit nuk i referohet aspak të drejtës së privatësisë.

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

Bashkëpunimi ekonomik aziatik-paqësor

Bashkëpunimi ekonomik aziatik-paqësor (APEK) në 2002 nxori Strategjinë e sigurisë kibernetike APEK që përmban rekomandime në fushën e legjislacionit për krimin kibernetik, udhëzimet e sigurisë dhe teknike, ndërgjegjësimin e publikut dhe trajnimin dhe edukimin.[22] Deklarata e Limas (2005) synon të përmirësojë infrastrukturën e informacionit për të avancuar shoqërinë e informacionit.[23] Deklarata adreson gjithashtu sigurinë e rrjetit dhe rëndësinë e krijimit të ekipeve kompjuterike të reagimit ndaj emergjencave (CERT). Strategjia e APEK-ut për të siguruar një mjedis të besueshëm, të sigurt dhe të qëndrueshëm në internet synon të ofrojë informacion dhe siguri të rrjetit, të harmonizojë kornizat për sigurimin e transaksioneve dhe komunikimeve dhe të luftojë krimin kibernetik. Gjithnjë e më shumë, kjo përfshinë bashkëpunimin e ngushtë me sektorin privat dhe me organizata të tjera ndërkombëtare. Planveprimi strategjik

20 Marrëveshja midis Qeverive të Shteteve Anëtare të SCO-së për Bashkëpunim në Fushën e Garantimit të Sigurisë Ndërkombëtare të Informacionit, 2009, gjendet në https://unidir.org/cpp/en/organization-pdf-export/eyJvcmdhbml6YXRpb25fZ3JvdXBfaWQiOiIxMiJ9

21 Organizata e Bashkëpunimit e Shangait, Projekt Kodi Ndërkombëtar i Sjelljes, Letër e datës 9 Janar 2015 për Asamblenë e Përgjithshme të Kombeve të Bashkuara, A / 69/723, gjendet në: https://digitallibrary.un.org/record/786846?ln=en

22 Strategjia e Sigurisë Kibernetike e APEC, gjendet në: https://www.ccdcoe.org/uploads/2018/10/APEC-020823-CyberSecurityStrategy.pdf

23 AAPEC, Deklarata e Limas, 2005, gjendet në: https://www.apec.org/Meeting-Papers/Sectoral-Ministerial-Meetings/Telecommunications-and-Information/2005_tel

i TEL APEK 2010 - 2015 synon të "promovojë një mjedis të sigurt, të rezistueshëm dhe të besuar të TIK-ut", duke përfshirë fushat kryesore në vijim: përmirësimi i qëndrueshmërisë së infrastrukturës kritike të brendshme, siguria dhe menaxhimi i rrezikut, ndërtimi i kapaciteteve të sigurisë kibernetike, ngritja e kibernetikës ndërgjegjësimi për sigurinë, iniciativat e sigurisë kibernetike me industrinë, aktivitetet për promovimin e mjediseve të sigurta në internet për grupet në nevojë, dhe ekonomia e internetit[24].

Pakti i Vendeve të Azisë Juglindore

OSHA i referohet konceptit të "sigurisë ndërkombëtare të informacionit", duke nënvizuar rëndësinë e përmbajtjes si një burim për një kërcënim të mundshëm të sigurisë

Pakti i Vendeve të Azisë Juglindore (ASEAN) e përbërë nga dhjetë shtete anëtare (Brunei, Kamboxhia, Indonezia, Laosi, Malajzia, Birmania, Filipinet, Singapori, Tailanda dhe Vietnami), lëshoi një Deklaratë nga ministrat e punëve të jashtme mbi bashkëpunimin në garantimin e sigurisë kibernetike dhe diskutoi mbi sigurinë kibernetike në kontekstin e antiterrorizmit dhe krimit ndërkombëtar.[25]

Komonuelthi i Kombeve

Bashkësia e Kombeve përbëhet nga 53 Shtete Anëtare dhe përqendrohet në ndërtimin e kapaciteteve, shkëmbimin e informacionit dhe sigurimin e ndihmës për shtetet anëtare të Komonuelthit në zbatimin e kornizave ligjore që i përgjigjen krimit kibernetik. Brenda Komonuelthit të Kombeve ekzistojnë dy platforma: Forumi i sigurisë kibernetike dhe Iniciativa e sigurisë kibernetike që veprojnë nën Organizatën e Telekomunikacionit të Komonuelthit. Ky i fundit ka miratuar Modelin e bashkëpunimit kibernetik,[26] i cili u miratua në Deklaratën e Abuxhas në tetor 2013 dhe u lansua gjatë Forumit të sigurisë kibernetike të Komonuelthit në Londër në 2014.[27]

Modeli i Komonuelthit Modeli i qeverisjes kibernetike[28] ofron një draft të të gjitha parimeve për shqyrtim për të kontribuar për një hapësirë të sigurt dhe efektive globale në internet; të mbështesë zhvillimin më të gjerë ekonomik dhe shoqëror; të veprojë individualisht dhe kolektivisht për të luftuar krimin kibernetik; për të ushtruar të drejtat dhe për të përmbushur përgjegjësitë në hapësirën kibernetike.

Bashkimi Evropian

Dokumentet e miratuara nga Bashkimi Evropian (BE) dhe më të rëndësishmet për sigurinë kibernetike janë ose dokumente juridikisht jodetyruese (si komunikimet) ose lloje të ndryshme të akteve ligjërisht të detyrueshme që vendosin detyrime ndaj Shteteve Anëtare ose subjekteve specifike.

Në vitin 2013, BE-ja publikoi dokumentin e tij të parë gjithëpërfshirës - Strategjinë e Sigurisë Kibernetike - duke trajtuar një gamë të gjerë të kërcënimeve kibernetike. Në

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 Modeli i Qeverisjes Kibernetike i Komonuelthit, gjendet në: https://ccdcoe.org/uploads/2018/11/CommW-140304-CommonwealthCybergovernanceModel.pdf

27 CForumi i Sigurisë Kibernetike i Komonuelthit në Londër në 2014, gjendet në: https://ccdcoe.org/uploads/2018/11/CommW-140304-CommonwealthCybergovernanceModel.pdf

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

vitin 2016, BE-ja e miratoi Direktivën për sigurinë e rrjetit dhe sistemeve të informacionit (Direktiva NIS).[29] Strategjia përshkruan vizionin, rolet, përgjegjësitë dhe veprimet e kërkuara për BE në fushën e sigurisë kibernetike. Duhet theksuar se dokumenti nënvizon se në kontekstin e sigurisë kibernetike, nuk mjafton mbikëqyrja e centralizuar e BE-së, dhe se qeveritë nacionale duhet të mbeten njësitë kryesore që organizojnë parandalimin dhe reagimin ndaj incidenteve kibernetike në nivelin kombëtar.

Si një nga objektivat e saj, Strategjia e sigurisë kibernetike e BE-së identifikon hartimin e politikave dhe aftësive të mbrojtjes kibernetike në lidhje me kornizën e Politikës së përbashkët të sigurisë dhe Mbrojtjes dhe përshkruan një listë të veprimeve të parashikuara për bashkëpunimin e Agjencisë Evropiane të Mbrojtjes dhe Shteteve Anëtare.

Veprimet e lidhura me sigurinë kibernetike janë përfshirë më tej në Agjendën digjitale të BE-së, e cila e konsideron besimin dhe sigurinë në Internet si jetike për një shoqëri të gjallë digjitale. Veçanërisht, Agjenda evropiane për sigurinë i jep përparësi krimit kibernetik si një nga kërcënimet më të rëndësishme të shfaqura.

Strategjia e sigurisë kibernetike e BE-së përcakton se një "incident ose sulm i rëndë kibernetik mund të përbëjë një hapësirë të mjaftueshme për një shtet anëtar për të aplikuar klauzolën solidare të BE-së (neni 222 i Traktatit për funksionimin e Bashkimit Evropian).

Më 25 maj 2015 hyri në fuqi Rregullorja e përgjithshme e BE-së për mbrojtjen e të dhënave (GDPR).[30] Kjo rregullore ndryshon në mënyrë thelbësore mënyrën se si merren të dhënat në të gjithë sektorët, nga kujdesi shëndetësor deri te bankat dhe më gjerë. E rëndësishme është që GDPR-ja jo vetëm që zbatohet për organizatat brenda BE-së por edhe për organizatat jashtë BE-së nëse ato ofrojnë mallra dhe shërbime për, ose monitorojnë sjelljen e subjekteve të të dhënave të BE-së.

Organizata e Traktatit Veri-Atlantik

Politika e parë e mbrojtjes kibernetike e Organizatës së Traktatit të Atlantikut të Veriut (NATO) u përgatit në vitin 2008. Në Samitin e Lisbonës në 2010, mbrojtja kibernetike u përfshi në Konceptin Strategjik të NATO-s dhe deklarata e Samitit përshpejtoi azhurnimin e politikës së mbrojtjes kibernetike në 2011 dhe krijimin e një Planveprimi shoqërues në 2012.

Një politikë e re e zgjeruar e mbrojtjes kibernetike u miratua në Samitin e Uellsit, i cili thotë se "një sulm i madh digjital ndaj një vendi anëtar mund të mbulohet nga neni 5" [i Traktatit të Atlantikut të Veriut].[31]

29 Bashkimi Evropian, Direktiva për sigurinë e rrjeteve dhe sistemeve të informacionit, në gjendet 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 Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave të Bashkimit Evropian, gjendet në https://eugdpr.org/the-regulation/gdpr-faqs/

31 Traktati i Atlantikut të Veriut, 1949, gjendet në: https://www.nato.int/cps/ie/natohq/official_texts_17120.htm

Sa i përket mbrojtjes së të dhënave personale, vetëm 16 nga 55 vende në Afrikë kanë miratuar legjislacionin gjithëpërfshirës për mbrojtjen e të dhënave personale, përkatësisht: Angola, Benini, Burkina Faso, Kepi i Gjelbër, Gabon, Ganë, Bregu i Fildishtë, Lesoto, Madagaskar, Mali, Mauricius, Marok, Senegal, Sejshellet, Afrika e Jugut, Tunizia.

GDPR zbatohet për të gjitha kompanitë që përpunojnë dhe mbajnë të dhënat personale të subjekteve në BE banojnë në BE, pavarësisht nga vendndodhja e ndërmarrjes.

Politika më tej kërkon të përmirësojë shkëmbimin e informacionit dhe ndihmën e ndërsjellë midis aleatëve, të përmirësojë trajnimet dhe ushtrimet dhe bashkëpunimin e mëtejshëm me industrinë. Në Samitin e Varshavës në 2016, NATO njohu hapësirën kibernetike si një fushë operacionesh dhe u zotua të zhvillojë më tej bashkëpunimin e mbrojtjes kibernetike NATO-BE dhe të angazhojë më shumë burime për të rritur kapacitetet e mbrojtjes kibernetike. Në 2018, ministrat e mbrojtjes të shteteve anëtare të NATO-s ranë dakord mbi krijimin e një qendre të re operacionesh kibernetike në SHAPE për të ndihmuar integrimin e kibernetikës në planifikimin dhe operacionet e NATO-s në të gjitha nivelet.

NATO-ja ka një Komitet të Mbrojtjes Kibernetike (CDC), i njohur më parë si Komiteti i Politikave të Mbrojtjes dhe Planifikimit (Mbrojtja Kibernetike). Ky Komitet është organ i lartë këshillimor dhe ofron konsultime për shtetet anëtare të NATO-s dhe ushtron qeverisjen e përgjithshme të mbrojtjes së brendshme kibernetike të NATO-s. Për më tepër, ekziston një Bord i Menaxhimit të Mbrojtjes Kibernetike (CDMB) që operon nën kujdesin e Divizionit të Sfidave të Sigurisë në Zhvillim të Selisë së NATO-s dhe përbëhet nga përfaqësues të të gjithë aktorëve kryesorë të sigurisë kibernetike brenda NATO-s. Veçanërisht, CDMB-ja bën planifikimin strategjik dhe drejtimin ekzekutiv në lidhje me rrjetet e NATO-s, si dhe nënshkruan Memorandum mirëkuptimi me shtetet anëtare për të lehtësuar shkëmbimin e informacionit dhe për të koordinuar ndihmën.

Për më tepër, Bordi i Konsultimit, Kontrollit dhe Komandës së NATO-s (NC3) përbën komitetin kryesor për konsultim mbi aspektet teknike dhe të zbatimit të mbrojtjes kibernetike.

Grupi i Shtatë (G7)

G7 është grup joformal i shtatë shteteve (Kanadaja, Franca, Gjermania, Italia, Japonia, Mbretëria e Bashkuar dhe Shtetet e Bashkuara të Amerikës me BE-në që kanë statusin e vëzhguesit) që takohen rregullisht për të diskutuar çështje të rëndësishme politike dhe ekonomike. Që nga viti 2016, G7 ka përpiluar një numër dokumentesh në lidhje me sigurinë kibernetike dhe duke e bërë atë një nga temat kryesore në deklaratat e ndryshme të samitit[32].

INFOBOX: UDHËZUES PËR MBROJTJEN E TË DHËNAVE PERSONALE PËR AFRIKËN

Në maj 2018, Udhëzimet për mbrojtjen e të dhënave personale për Afrikën u nisën nga Shoqëria e Internetit dhe Komisioni i Bashkimit Afrikan në Samitin afrikan për internetin në Dakar, Senegal.
Udhëzimet përmbajnë 18 rekomandime të përqendruara në tri çështje:

1. Rekomandime për të krijuar besim, privatësi dhe përdorim të përgjegjshëm të të dhënave personale
2. Rekomandime për veprimet që duhen ndërmarrë nga qeveritë dhe politikëbërësit, autoritetet për mbrojtjen e të dhënave, dhe kontrolluesit e të dhënave dhe përpunuesit e të dhënave
3. Rekomandime për zgjidhje me shumë aktorë, mirëqenien e qytetarit digjital dhe masat e mundshme dhe mbështetëse
4. .

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

2. Nisma nga aktorë joshtetërorë

Për shkak se shtetet kanë hezituar të shprehin opinioni iuris dhe praktikën e tyre shtetërore në hapësirën kibernetike, nuk ka ndonjë marrëveshje të përbashkët për mënyrën se si zbatohet e drejta ndërkombëtare në hapësirën kibernetike, e cila ka bërë që aktorët joshtetërorë të fillojnë të plotësojnë këtë boshllëk. Kompanitë private të TIK-ut dhe organizatat e shoqërisë civile në veçanti kanë qenë proaktive në propozimin e normave kibernetike në përputhje me të drejtat e njeriut që synojnë të kontribuojnë për një internet më të sigurt dhe më të besueshëm.

Një grup akademikësh dhe ekspertësh të së drejtës ndërkombëtare humanitare hartuan Manualin e Talinit mbi zbatimin e së drejtës humanitare ndërkombëtare në operacionet kibernetike.[33] Ndërsa ky dokument është mjaft akademik, ai riafirmon parimet themelore të së drejtës ndërkombëtare humanitare, siç janë parimi i dallimit, proporcionalitetit dhe domosdoshmërisë në hapësirën kibernetike. Për më tepër, ky grup ekspertësh botoi Manualin e Talinit 2.0 që adreson ligjin e zbatueshëm në kohë paqeje në hapësirën kibernetike[34].

32 Grupi i 7, Komunikata e Samitit Charlevoix G7, gjendet në: https://www.consilium.europa.eu/en/press/press-releases/2018/06/09/the-charlevoix-g7-summit-communique/

33 Manuali i Talinit, në dispozicion në https://ccdcoe.org/research/tallinn-manual/

34 Fleta e Fakteve e Manualit të Talinit, gjendet në: https://www.almendron.com/tribuna/wp-content/uploads/2018/03/ccdcoe-tallinn-manual-onepager-web.pdf

STUDIM I RASTIT: NOCIONET E "SULMIT TË ARMATOSUR" DHE "PËRDORIMIT TË FORCËS" NË HAPËSIRËN KIBERNETIKE - TEJKALIMI I DILEMAVE GJUHËSORE NËPËRMJET KOMUNITETIT LIGJOR, POLITIK DHE TEKNIK

Duhet të bëhet dallimi i dy regjimeve në të drejtën ndërkombëtare: (i) ius ad bellum (kur shteti mund të përdorë forcën si një instrument të politikës së tij kombëtare), dhe (ii) ius in bello (e drejta ndërkombëtare humanitare që përcakton rregullat se si mund të kryhen operacionet gjatë një sulmi të armatosur).

Në kontekstin e ius ad bellum, sipas nenit 51 të Kartës së OKB-së, një sulm i armatosur mund të nxisë vetëmbrojtje. Prandaj, pyetja që kërkon përgjigje të shpejtë është kur një operacion kibernetik përbën një sulm të armatosur ku një shtet ligjërisht mund të meritojë një përgjigje ose me veprime kibernetike ose kinetike në nivelin e përdorimit të forcës. Rëndësia këtu është te nocioni i "armatosur", sepse Gjykata Ndërkombëtare e Drejtësisë në Aktgjykimin e Nikaraguas thotë se ekzistojnë "masa që nuk përbëjnë një sulm të armatosur, por sidoqoftë mund të përfshijnë përdorimin e forcës". Si pasojë, shtetet mund të përballen me një operacion kibernetik që përbën një përdorim të forcës, por duke e lënë shtetin të paaftë për të mbrojtur veten pasi operacionet kibernetike nuk kualifikohen si një sulm i armatosur. Për të adresuar këtë dilemë, një numër studiuesish të së drejtës ndërkombëtare kanë tendencën të interpretojnë "sulmin e armatosur" në hapësirën kibernetike si çdo veprim që rezulton me pasoja analoge me ato të shkaktuara nga veprimet kinetike (pasoja fizike).

Në kontekstin ius in bello, para se të zbatohet DNH-ja, duhet të ketë një sulm (që përcaktohet nëpërmjet një qasjeje të bazuar në pasoja kur interpretohet 'sulmi').

Microsoft, një korporatë private transnacionale, propozoi në shkurt 2017 që shtetet të miratojnë "Konventën Digjitale të Gjenevës" që përcakton normat për hapësirën kibernetike, në kohë paqeje. Mikrosofti (Microsoft) boton rregullisht dokumente politikash dhe nxjerrë postime në blog që synojnë të kontribuojnë në besimin dhe ndërtimin e besimit midis palëve të ndryshme të interesit në hapësirën kibernetike. Sidoqoftë, ndërsa shtetet në përgjithësi po i mirëpresin iniciativat proaktive nga aktorë joshtetërorë, ka ende skepticizëm ndaj perspektivës së suksesit.[35]

Në të njëjtën kohë, kompanitë e TIK-ut i nxisin gjithnjë e më shumë shtetet të rregullojnë disa sjellje të dëmshme në hapësirën kibernetike. Për shembull, Mikrosofti e nxiti Kongresin e Shteteve të Bashkuara të Amerikës të miratojë rregullore për të kufizuar përdorimin e teknologjisë së njohjes së fytyrës[36].

35 Dokumenti i politikës Microsoft, Konventa Dixhitale e Gjenevës për të mbrojtur hapësirën kibernetike, gjendet në: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH ; shih gjithashtu udhëzimet për sigurinë kibernetike të Microsoft, gjendet në: https://www.microsoft.com/en-us/cybersecurity/default.aspx

36 Natasha Singer, The New York Times (13 korrik 2018): Microsoft Urges Congress to Regulate Use of Facial Recognition, gjendet në: https://www.nytimes.com/2018/07/13/technology/microsoft-facial-recognition.html

Gjithashtu janë hartuar mjete të tjera ligjore të buta, siç janë Parimet e Manilës mbi përgjegjësinë e ndërmjetësimit,[37] që ofrojnë udhëzime për shtetet në lidhje me politikat që rregullojnë përgjegjësinë ligjore të ndërmjetësve për përmbajtjen e postuar në platformat e tyre. Aktorët joshtetërorë, në veçanti kompanitë e TIK-ut dhe organizatat e shoqërisë civile, janë bërë më proaktivë në propozimin e normave të zbatueshme në hapësirën kibernetike. Veçanërisht Mikrosofti ka qenë një pararendës këto vitet e fundit[38].

Organizatat e shoqërisë civile gjithashtu, janë bërë më aktive duke mbushur vakumin e lënë nga shtetet në hapësirën kibernetike, duke propozuar norma që synojnë promovimin e të drejtave të njeriut në hapësirën kibernetike. Për shembull, neni 19 (organizatë jo-qeveritare me seli në Londër me disa OJQ të tjera mbështet Parimet e Kamdenit mbi lirinë e shprehjes dhe barazinë në internet.[39] Përveç kësaj, instrumentet e ligjit të butë siç janë Parimet e Manilës mbi përgjegjësinë e ndërmjetësimit janë miratuar.

Nisma e Rrjetit Global është një nismë shumëpalëshe që zhvillon standardet globale për internet. Parimet e tij mbi lirinë e shprehjes dhe privatësinë ofrojnë drejtime dhe udhëzime për industrinë e TIK-ut dhe palët e interesit në mbrojtjen dhe avancimin e gëzimit të të drejtave të njeriut në të gjithë botën[40].

Në lidhje me parandalimin e ekstremizmit të dhunshëm në internet, një koalicion i kompanive të mediave sociale, përkatësisht Facebook, Twitter, Youtube dhe Microsoft, u bashkuan në një Forum Global të Internetit Kundër Terrorizmit,[41] ku këta gjigantë të internetit zhvillojnë standarde normative për të rregulluar ekstremizmin e dhunshëm në platformat e tyre përkatëse.

Në përgjithësi, kompanitë private të TIK-ut duhet të ndërmarrin kujdesin e duhur efektiv, proaktiv dhe gjithëpërfshirës për të drejtat e njeriut, që përfshin angazhim kuptimplotë me individë, të drejtat e të cilëve mund të ndikohen nga ndërmarrjet private të TIK-ut.

Parimet udhëzuese të biznesit dhe të drejtave të njeriut (GPBHR) thonë se korporata ka përgjegjësinë të respektojë të drejtat e njeriut. Për kompanitë e TIK-ut kjo nënkupton marrjen parasysh të çështjeve specifike të industrisë, siç janë liria e shprehjes, privatësia dhe siguria. Duhet theksuar se disa nga çështjet më të ngutshme të kujdesit të duhur lindin nga përdorimi i produkteve të kompanisë, shërbimit, teknologjive dhe aplikacioneve nga përdoruesit dhe nga përpjekjet e qeverive për të kufizuar të drejtat e përdoruesve.

INFOBOX: PËRGJEGJËSIA E NDËRMJETME

Të gjitha komunikimet që përfshijnë internetin lehtësohen nga ndërmjetësuesit. Duke pasur parasysh kompleksitetin e internetit, ekzistojnë disa lloje të ndryshme të ndërmjetësve:

- Ofruesit e shërbimeve në Internet (ISP) u referohet ofruesve të aksesit në internet
- Ofrues të mbajtjes së faqeve në internet ('host') zakonisht i referohen çdo personi ose kompanie që kontrollon një faqe në internet ose një faqe në internet e cila lejon çdo palë të tretë të postojë dhe ngarkojë përmbajtje.
- Platformat e mediave sociale si Facebook, Twitter, Youtube, etj., që inkurajojnë individët të lidhen dhe të ndërveprojnë me përdoruesit e tjerë dhe të ndajnë përmbajtje.
- Motorët e kërkimit, siç është Google, janë programe softuerësh që përdorin algoritme për të marrë të dhëna, skedarë ose dokumente në përgjigje të një pyetjeje.

Këto janë ofruesit e aksesit në internet, rrjetet sociale dhe motorët e kërkimit. Përgjegjësia ndërmjetësuese nënkupton politikat që rregullojnë përgjegjësinë ligjore të ndërmjetësve për përmbajtjen e këtyre komunikimeve.
Burimi: 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

37 Parimet e Manilas mbi përgjegjësinë e ndërmjetësimit, gjendet në: https://www.manilaprinciples.org/

38 Dokumenti i politikave të Mikrosoftit, Një Konventë dixhitale e Gjenevës për të mbrojtur hapësirën kibernetike, në dispozicion në https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace

39 Neni 19, Parimet e Kamdenit mbi Lirinë e Shprehjes dhe Barazisë, gjendet në: https://www.article19.org/data/files/pdfs/standards/the-camden-principles-on-freedom-of-expression-and-equality.pdf

40 Më shumë informacion në lidhje me Nismën e Rrjetit Global do të gjeni në: https://globalnetworkinitiative.org/

41 GPolitika publike e Gugëllit, përditësim i Forumit global të internetit për luftën kundër terrorizmit, 4 dhjetor 2017, gjendet në: https://www.blog.google/around-the-globe/google-europe/update-global-internet-forum-counter-terrorism/

Gjetjet kryesore

- Boshllëqet e kriminalizimit në çdo vend mund të krijojnë hapësirë për shkelësit me potencial për të ndikuar në vendet e tjera globalisht.
- Dallimet e kriminalizimit paraqesin sfida për bashkëpunimin ndërkombëtar në çështjet penale që përfshijnë krimin kibernetik, veçanërisht në lidhje me parimin e kriminalitetit të dyfishtë.
- Një analizë krahasuese e veprave të krimit kibernetik është në gjendje të eksplorojë praktikat e mira që shtetet mund të përdorin në hartimin e ligjeve kombëtare, në përputhje me standardet e reja ndërkombëtare në këtë fushë.

Burimet

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

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

KAPITULLI 4

ZBATIMI I NORMAVE DHE STANDARDEVE NDËRKOMBËTARE DHE RAJONALE NË NJË KONTEKST KOMBËTAR

OBJEKTIVAT

Ky kapitull do të shqyrtojë se si kornizat ligjore ndërkombëtare dhe rajonale nga kapitulli paraprak, si dhe normat e tjera brenda hapësirës kibernetike, mund të zbatohen në një nivel kombëtar, veçanërisht nëpërmjet legjislacionit, politikave dhe strategjive përkatëse.

Objektivat e nxënies së këtij kapitulli janë si më poshtë:

- Kuptim i mëtejshëm i kornizave dhe normave të tjera në hapësirën kibernetike dhe zbatueshmëria e tyre në një kontekst kombëtar.
- Rritja e kuptimit të nevojës për legjislacionin kombëtar, politikat dhe strategjitë në hapësirën kibernetike.
- Rritja e njohurive se si të krijohen ose ndryshohet legjislacioni kombëtar, politikat dhe strategjitë bazuar në hapësirën kibernetike, bazuar në praktikat e mira të QSS-së.

Hyrje

Përdorimi i hapësirës kibernetike është gjithnjë e më i përhapur midis njerëzve, qeverive dhe kompanive, si për konsumin e informacionit, sigurimin dhe marrjen e shërbimeve publike dhe private ashtu edhe për mbështetjen e proceseve të punës. Kjo rritje do të thotë që të gjithë këta aktorë janë potencialisht të ndjeshëm ndaj shkeljeve dhe sulmeve në internet, një cenueshmëri që kërcënon të drejtat e njeriut si dhe sigurinë kombëtare dhe njerëzore.

Ndërsa disa norma për praktikat e sigurta në hapësirën kibernetike dhe një kornizë e përgjithshme e pritjeve ligjore të të drejtave brenda hapësirës kibernetike janë krijuar në nivele ndërkombëtare dhe rajonale, tani ka një përqendrim të shtuar të nevojës për qasje koherente dhe holistike kombëtare ndaj sfidave të hapësirës kibernetike. Mbështetja e vazhdueshme në hapësirën kibernetike do të thotë se legjislacioni, politikat dhe strategjitë e efektshme kombëtare janë më se të nevojshme për të mbrojtur të dhënat, informacionin dhe njohuritë që transmetohen dhe përdoren në hapësirën kibernetike, si dhe për të rritur sigurinë e qytetarëve në të.

Kornizat ndërkombëtare ose rajonale të shqyrtuar në kapitullin e fundit - të përbërë nga rezoluta, raporte, konventa dhe marrëveshje mbi të drejtat e njeriut dhe rregullimin e hapësirës kibernetike - kanë krijuar një sërë normash që vendet duhet t'i respektojnë kur ndryshojnë hapësirën e tyre kibernetike dhe legjislacionin, politikat dhe strategjitë e sigurisë kibernetike, dhe mund t'i ndihmojë ato në hartimin ose azhurnimin e politikave dhe strategjive kombëtare mbi hapësirën kibernetike dhe sigurinë kibernetike. Përveç kësaj, kompanitë private dhe organizatat joqeveritare janë përpjekur të zgjerojnë kornizat dhe normat e lartpërmendura për të detajuar qasjet mbizotëruese të sigurisë kibernetike. Shtetet mund të mbështeten në këta elementë të ndryshëm për të krijuar një hapësirë të plotë kibernetike dhe qeverisje të sigurisë kibernetike që bazohet në parimet e qeverisjes së mirë të sektorit të sigurisë.

Praktikat e mira të mëposhtme nxjerrin në pah aspektet kryesore rregullatore që shtetet duhet t'i adresojnë dhe përforcojnë kur krijojnë ose ndryshojnë një strategji kombëtare të sigurisë kibernetike.[1]

Për më tepër, politikat dhe strategjitë kombëtare duhet të përfshijnë një vështrim ndërkombëtar ose të plotësohen me politika dhe strategji që përqendrohen në mënyrë specifike në bashkëpunimin ndërkombëtar, në mënyrë që rregullimi kibernetik dhe siguria kibernetike të mos ndalen në kufijtë kombëtarë.

1 Praktikat e mira bazohen në: Cybersecurity Policy Framework. A Practical guide to the development of national cybersecurity policy. Microsoft (2018).

Praktika e mirë 1: Qeveritë duhet të zhvillojnë dhe miratojnë ligje, politika dhe strategji kombëtare për rregullimin e hapësirës kibernetike.

Megjithëse hapësira kibernetike është në praktikë një medium global, duke folur ligjërisht detyra e rregullimit të tij dhe sigurimit të qeverisjes së mirë bie mbi shtetet pasi nuk ka një strukturë ndërkombëtare të qeverisjes.[2] Gjithashtu, është e rëndësishme të përmendet se "të njëjtat të drejta që njerëzit kanë jashtë internetit duhet të mbrohen edhe në internet".[3] Kështu, lejimi i ndërmarrjeve të TIK-ut të veprojnë pa një kornizë të mjaftueshme rregullatore mund të rezultojë me praktika të shkëputura nga interesi publik dhe potencialisht me shkeljen e të drejtave të njeriut.[4] Prandaj, shtetet si mbartës kryesorë të detyrimeve të të drejtave të njeriut dhe mbrojtës të interesit publik do të pasqyrojnë zhvillimet më të fundit në teknologji në përpjekjet e tyre legjislative për të kufizuar hapësirën për pasoja të mundshme të padëshiruara të veprimeve të sektorit privat. Legjislacioni kombëtar, politikat dhe strategjitë, si dhe roli i sektorit të sigurisë në rregullimin e hapësirës kibernetike dhe sigurimin e sigurisë kibernetike, janë thelbësore për të siguruar praktika të mira qeverisjeje.

Për më tepër, kornizat dhe normat ndërkombëtare dhe rajonale janë të një natyre më të përgjithshme, ndërsa legjislacioni kombëtar, politikat dhe strategjitë lejojnë adresimin e nevojave dhe specifikave kombëtare mbi hapësirën kibernetike dhe sigurinë kibernetike.

Në fund, duke u mbështetur vetëm në kornizat dhe normat e vendosura në nivelin ndërkombëtar dhe rajonal nuk sigurohet një garanci se shtetet e tjera nuk do të shkelin këto parime jodetyruese, dhe as nuk sigurohet se aktorët privatë dhe publikë brenda një shteti të vetëm do të respektojnë normat.[5] Mandej, krijimi ose ndryshimi i legjislacionit, politikave dhe strategjive të hapësirës kibernetike dhe të sigurisë kibernetike, për hapësirën kibernetike dhe qeverisjen e sigurisë kibernetike mund të shërbejnë si një mënyrë më gjithëpërfshirëse dhe kohezive për të siguruar respektimin e ligjeve dhe të drejtave të njeriut në hapësirën kibernetike brenda një shteti përkatës.

Legjislacioni për krimin kibernetik duhet të hartohet duke pasur parasysh kërkesat e mëposhtme:

- Duhet të jetë neutral sa duhet nga aspekti teknologjik për t'u kujdesur për evolucionin e vazhdueshëm të teknologjisë dhe krimit pasi përndryshe rrezikon të vjetërsohet tashmë në kohën kur ai hyn në fuqi.

- Kompetencat e zbatimit të ligjit duhet t'i nënshtrohen masave mbrojtëse për të siguruar përmbushjen e kërkesave të shtetit ligjor dhe të drejtave të njeriut.

- Duhet të jetë i harmonizuar sa duhet ose së paku i pajtueshëm me ligjet e vendeve të tjera për të lejuar bashkëpunimin ndërkombëtar, për shembull, për të përmbushur kushtin e kriminalitetit të dyfishtë.

2 ITU National Cybersecurity Strategy Guide 26.

3 Këshilli i Kombeve të Bashkuara për të Drejtat e Njeriut, Rezoluta mbi promovimin, mbrojtjen dhe gëzimin e të drejtave të njeriut në internet, A / HRC / 20 / L.13, 29 qershor 2012, para. 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.

SHEMBULL I PRAKTIKËS SË MIRË

Krimi në internet është një fushë ku legjislacioni dhe politikat kombëtare kanë një rëndësi kritike. Shtetet afrikane që hartojnë legjislacionin për krimin kibernetik mund të mbështeten në udhëzime, në veçanti, nga Konventa e Bashkimit Afrikan për Sigurinë Kibernetike dhe Mbrojtjen e të Dhënave Personale të miratuar në Malabo në qershor 2014.[6]

Që nga viti 1997, Algjeria në mënyrë progresive ka fituar mjete për të luftuar krimin kibernetik. Rezultati është legjislacion i cili është i përshtatur kryesisht për luftën kundër krimit në përputhje me shumë parime themelore, megjithëse dobësitë vazhdojnë në të dy aspektet. Ligji algjerian përfshin shumicën e dispozitave të Konventës së Budapestit, në disa raste me formulime alternative. Ai përfshin veprat e mëposhtme: aksesi dhe mbajtja mashtruese në një sistem; kapja e komunikimeve dhe fjalëve të folura në mënyrë private ose konfidenciale; fshirja ose modifikimi i të dhënave që përmbahen në sistem pas aksesit ose mbajtjes mashtruese; ndryshimi i funksionimit të një sistemi pas aksesit ose mbajtjes mashtruese; keqpërdorimi i pajisjeve elektronike; pornografia e fëmijëve; dhe shkeljet në lidhje me shkeljet e pronës intelektuale dhe të drejtat e përkatëse.

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

Praktika e mirë 2: Qeveritë duhet të përditësojnë legjislacionin kombëtar në lidhje me sfidat aktuale të hapësirës kibernetike.

Gjatë hartimit dhe miratimit të legjislacionit kombëtar mbi hapësirën kibernetike dhe sigurinë kibernetike (qoftë me përditësimin e legjislacionit ekzistues apo krijimin e një legjislacioni të ri), politikëbërësit dhe ligjet duhet të kenë parasysh disa sfida aktuale.

Së pari, përparimi i inovacionit në hapësirën kibernetike është shumë më i shpejtë sesa proceset legjislative kombëtare. Prandaj, edhe pjesët më moderne të legjislacionit kibernetik mund - dhe me gjasë - do të mbeten prapa teknologjive të fundit. Së dyti, legjislacioni mbi hapësirën kibernetike kërkon njohuri dhe ekspertizë thelbësore të TI-së, të cilat janë të rralla në sektorin publik, pasi shpërblehen shumë më mirë në sferën private. Së treti, edhe nëse një ligjvënës i shtetit arrin të miratojë ligje përkatëse për rregullimin e hapësirës kibernetike, karakteri ndërkombëtar i çështjeve të lidhura me internetin e bën të ndërlikuar dhe nganjëherë të pamundur zbatimin e ligjeve të brendshme.

Përparimi i shpejtë në inovacionin e teknologjisë qëndron në kontrast të plotë me proceset e ngadalta dhe shpesh të zgjatura legjislative të vendit.[7] Për këtë arsye, shumë teknologji dhe mjete kibernetike po përdoren pa rregullimin e nevojshëm. Një shembull tipik i një vakumi të tillë rregullator është përdorimi i inteligjencës artificiale (IA). Ndërsa një shumicë e madhe e shteteve nuk ka arritur të miratojë legjislacionin e duhur për

6 African Union Commission and Symantec, Cyber crime and cyber security trends in Africa Report (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, (2019): 18, (https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf).

rregullimin e përmbajtjes nga kompanitë e mediave sociale që punësojnë moderatorë të përmbajtjes njerëzore, mjetet e mundësuara nga IA tashmë janë vendosur për të zëvendësuar njerëzit në këtë punë[8].

Sidoqoftë, shtetet do të shmangin legjislacionin në një mënyrë të shpejtë dhe të pakoordinuar. Megjithëse shqetësimet e publikut në lidhje me progresin e shpejtë teknologjik mund të jenë nxitje politike për të miratuar legjislacionin në mënyrë që të demonstrojë kompetencën dhe reagimin e institucioneve shtetërore, një numër i madh i normave të miratuara me shpejtësi mund të jetë më përçarës sesa lejimi i ndërmarrjeve private të veprojnë pa rregullim të plotë ndërsa teknologjitë e reja janë duke u testuar. Për këtë arsye, shtetet duhet të vëzhgojnë teknologjitë e reja dhe të identifikojnë rrjedhat e reja, por të hartojnë ligjin vetëm pas një procesi të kujdesshëm diskutimi që i përfshin të gjithë aktorët e interesuar, duke përfshirë sektorin privat dhe shoqërinë civile.

Për më tepër, kur miratojnë legjislacionin për këtë çështje, shtetet do të shmangin dhënien e tepërt të rekomandimeve, pasi kjo mund të pengojë procesin e inovacionit dhe kërkimit, si dhe të dekurajojnë ndërmarrjet më të vogla të TIK-ut në treg, të cilat mund të mos jenë në gjendje të përmbushin standardet e larta të legjislacionit të tillë. Por kur vendosin nëse duhet të ligjërojnë për një çështje specifike mbi internetin, shtetet do të marrin në konsideratë opsione të tjera përtej legjislacionit: për shembull, ndonjëherë miratimi i kodeve të sjelljes vullnetare ose një grup parimesh udhëzuese jodetyruese mund të përmbushin një objektiv të dëshiruar rregullator. Gjithashtu, instrumente të tilla të ligjit të butë janë më të lehta për t'u ndryshuar dhe kështu më të prira për të pasqyruar tendencat e fundit në teknologji.

8 Asambleja e Përgjithshme e Kombeve të Bashkuara, "Raporti i Raportuesit Special mbi promovimin dhe mbrojtjen e të drejtës për lirinë e mendimit dhe shprehjes", A / 73/348, 29 gusht 2018, para. 18.

SHEMBUJ TË PRAKTIKËS SË MIRË

Në Ganë, rregulloret specifike për institucionet bankare dhe financiare - të cilat formojnë sektorin më të prekur nga krimi kibernetik - u miratuan nga një Direktivë e sigurisë kibernetike 2018 për institucionet financiare të Bankës së Ganës. Direktiva kërkon përfshirje aktive të drejtuesve të lartë dhe bordit për të forcuar sigurinë kibernetike. Të gjitha bankave në vend u kërkohet të caktojnë një zyrtar të sigurisë kibernetike dhe të informacionit (CISO) i cili do të këshillonte menaxhmentin e lartë dhe bordin për çështjet e sigurisë kibernetike, dhe gjithashtu të formulonte masa adekuate për të menaxhuar rreziqet e sigurisë kibernetike dhe të informacionit.

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

Shumë ekonomi afrikane kanë forcuar masat e zbatimit. Në Afrikën e Jugut, Akti i mbrojtjes së informacionit personal (POPI) i vitit 2013 krijoi Rregullatorin e Informacionit për të siguruar privatësinë e të dhënave. Në vitin 2017, Rregullatori i Informacionit filloi hetimin e shkeljes më të madhe të të dhënave të atij viti në vend, në të cilin u vodhën më shumë se 30 milion të dhëna personale. Agjencia gjithashtu u bëri kërkesa zyrtare kompanive të interesuara për të dhënë shpjegime.

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

Praktika e mirë 3: Qeveritë duhet të rrisin ekspertizën kibernetike.

Mungesa e ekspertizës dhe njohurive të IT-së në sektorin publik është një pengesë tjetër serioze për shtetet në miratimin e legjislacionit për çështjet e lidhura me internetin.[9] Zgjidhja e vetme për këtë problem është që shtetet të gjejnë mënyra për të grumbulluar më shumë ekspertizë të lëndës. Ka shumë mënyra sesi mund të arrihet ky objektiv, gjëja më e drejtpërdrejtë është që shteti të punësojë numrin e nevojshëm të stafit me ekspertizë të IT-së. Sidoqoftë, shtetet kanë tendencë të kenë burime financiare dhe të tjera shumë më të kufizuara sesa kompanitë private të TIK-ut dhe mund të përballen me probleme në tërheqjen dhe mbajtjen e ekspertëve për çështje të tilla të profilit të lartë si siguria kibernetike, IA dhe analiza e të dhënave.

Një zgjidhje e pjesshme mund të jetë nëpërmjet skemave alternative rregullatore, të cilat do të ofronin qasje në ekspertizën e sektorit privat duke e lënë atë të marrë pjesë në një farë mase në procesin rregullator, por pa hequr përgjegjësinë e përgjithshme të shtetit. Duke pasur parasysh që kompanitë private kanë ekspertizë të nivelit të lartë dhe njohuri të nevojshme teknike mbi çështjet që kanë të bëjnë me hapësirën kibernetike, rregullat e miratuara në bashkëpunim me sektorin privat mund të kapërcejnë hendekun tradicional midis përparimit të teknologjisë dhe nivelit të legjislacionit kombëtar. Gjithashtu, skema të tilla bashkë-rregulluese mund të jenë shumë më pak të politizuara sesa vetëm proceset legjislative kombëtare.

9 Raymond, Mark. "Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot." Strategic Studies Quarterly10, no. 4 (2016): 137, (http://www.jstor.org/stable/26271532).

SHEMBUJ TË PRAKTIKËS SË MIRË

Ekspertiza kombëtare kibernetike është zmadhuar në koordinim me sektorin privat dhe kompanitë e huaja shumëkombëshe[10].

Në Kenia, iniciativat e sektorit privat të sigurisë kibernetike çuan në krijimin e një Qendre të Zhytjes Kibernetike në Najrobi në mars 2018 nga Serianu, një kompani panafrikane e sigurisë kibernetike dhe e konsulencës afariste. Qendra ofron një mjedis për firmat për të eksperimentuar dhe testuar aftësitë e tyre të sigurisë kibernetike. Ajo gjithashtu siguron lehtësi edukative për të zhvilluar profesionistë të sigurisë kibernetike. Një qendër e ngjashme u hap në Mauricius nga mesi i vitit 2017.

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

Në Nigeri, Mikrosofti (Microsoft) u bashkua me Paradigm Initiative Nigeria (PIN) për të edukuar nigerianët mbi krimet kibernetike dhe për të krijuar mundësi ekonomike. Komisioni i Krimeve Ekonomike dhe Financiare të vendit (EFCC) njoftoi në tetor 2009 se mbylli rreth 800 faqe në internet të lidhura me krime kibernetike dhe arrestoi 18 banda të krimit kibernetik. EFCC vuri në dukje se kishte ndihmuar "teknologjia inteligjente" e siguruar nga Mikrosofti.

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

Praktika e mirë 4: Qeveritë duhet të zhvillojnë dhe të përditësojnë ligjet që mbrojnë privatësinë dhe të dhënat personale.

Mbrojtja e privatësisë dhe e të dhënave personale është thelbësore për sigurinë kibernetike dhe është një fushë ku është bërë përparim konkret në drejtim të zbatimit të të drejtës së privatësisë dhe mbrojtjes së të dhënave personale, veçanërisht në BE. Rregullorja e përgjithshme e BE-së për mbrojtjen e të dhënave (GDPR - shih Kapitullin 3), e cila hyri në fuqi në maj 2018, krijoi një regjim rregullator rajonal me objektivat e dhënies së kontrollit individëve mbi të dhënat e tyre personale. Rregullorja ka rezultuar edhe me disa ligje të privatësisë dhe mbrojtjes së të dhënave në nivelin kombëtar.

Në vitin 2014, Bashkimi Afrikan miratoi Konventën Malabo mbi sigurinë kibernetike dhe mbrojtjen e të dhënave personale (shih Kapitullin 3). Konventa nuk ka hyrë në fuqi akoma. Si e tillë, Konventa e Budapestit është aktualisht e vetmja kornizë ligjore ndërkombëtare e detyrueshme juridikisht mbi temën e sigurisë kibernetike, hapësirës kibernetike dhe rolit të shtetit në këtë fushë. Edhe pse vetëm një pjesë e vogël e kombeve afrikane e kanë nënshkruar atë drejtpërdrejt ose janë ftuar të aderojnë, ajo është përdorur si një kornizë udhëzuese për krijimin e Konventës së Bashkimit Afrikan mbi Sigurinë Kibernetike.

10 Nir Kshetri (2019) Cybercrime and Cybersecurity in Africa, Journal of Global Information Technology Management, 22:2, 77-81, DOI: 10.1080/1097198X.2019.1603527

SHEMBUJ TË PRAKTIKËS SË MIRË

Në Kenia, një projekt-ligj i ri për mbrojtjen e të dhënave u paraqit për shqyrtim në Parlament në nëntor 2018. Projekt-ligji përfshin shumë elementë të Rregullores së përgjithshme të mbrojtjes së të dhënave të Evropës (GDPR). Për shembull, projektligji kërkon që organizatat t'i informojnë përdoruesit se pse janë mbledhur të dhënat e tyre, për çfarë qëllimi përdoren ato të dhëna dhe për sa kohë organizata do t'i ruajë të dhënat. Projekt-ligji përfshin gjithashtu një dispozitë e cila u jep konsumatorëve të drejtën të kërkojnë nga organizatat të fshijnë të dhënat e tyre. Përveç kësaj, u kërkon organizatave të kenë një nivel të caktuar të standardeve të sigurisë për ruajtjen e të dhënave.

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

Franca miratoi Loi relative à la protection des données personnelles në qershor 2018 në mënyrë që të përafrojë ligjin kombëtar francez me Rregulloren e përgjithshme të mbrojtjes së të dhënave të BE-së (GDPR). Duke u bazuar në Aktin francez të mbrojtjes së të dhënave të janarit 1978, Ligji 2018 zgjeron autoritetin për mbrojtjen e të dhënave të Komisionit Kombëtar të Informatave dhe Lirive (CNIL), duke e fuqizuar nëpërmjet këtyre mënyrave:

• Rritja e autoritetit rregullator për të zbatuar rregulloret e sigurisë, kodet e sjelljes dhe zhvillimin e dokumenteve dhe rekomandimeve të referencës. Për më tepër, CNIL do të ketë fuqinë për të aprovuar organet certifikuese si dhe autoritetin për të certifikuar në përputhje me GDPR dhe produktet e ligjit kombëtar francez, personat dhe procedurat.

• Fuqitë e mbikëqyrjes janë forcuar, duke lejuar agjentët e CNIL-së të bëjnë kërkesa për çdo dokument që nuk mbrohet nga privilegji ligjor. Agjentët e CNIL-së mund të përdorin, madje edhe lloje të reja sanksionesh, kurse tarifat administrative janë rritur dukshëm. Në rast se një kompani nuk arrin të mbrojë të dhënat personale, tarifat mund të shkojnë nga 10 milion euro ose 2% të të ardhurave të saj globale në 20 milion euro ose 4% të të ardhurave të saj globale (çfarëdo që është më e lartë) për shkeljet më të rënda.

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

Praktika e mirë 5: Vlade bi trebalo da razviju i ažuriraju zakone koji štite kritičnu infrastrukturu.

Instalimet të infrastrukturës kritike, të njohura edhe si IIK, janë thelbësore për mirëqenien e popullatës së përgjithshme. IIK-të janë pasuri, sisteme, rrjete (si fizike ashtu edhe virtuale) që janë thelbësore për funksionet vitale shoqërore, përfshirë shëndetin, sigurinë dhe mirëqenien ekonomike dhe shoqërore, dhe prishja ose

shkatërrimi i të cilave do të kishte një ndikim të rëndësishëm negativ në popullatë.

Shembuj të instalimeve të infrastrukturës kritike përfshijnë:

- Termocentralet
- Furnizimet me ujë dhe ushqim
- Sigurinë Publike: forcat e sigurisë, organizatat e emergjencës, mbrojtja civile
- Shëndetin Publik: spitalet dhe kujdesi mjekësor, laboratorët
- Administratën Publike
- Transportin (p.sh. transporti rrugor, hekurudhor dhe ajror)
- Deponimin e mbeturinave (mbeturinave dhe ujërave të zeza)
- Shërbimet financiare (p.sh., bankat, kompanitë e sigurimeve)
- Rrjetet e teknologjive të informacionit dhe komunikimit

Një pjesë e konsiderueshme e instalimeve kritike të infrastrukturës (IKI) kanë përfshirë teknologji të reja për të mbështetur operacionet e tyre. Ndërsa ky modernizim ka ndihmuar për ta bërë këtë infrastrukturë më efikase në shpërndarjen e të mirave publike tek popullata, ajo gjithashtu i ka ekspozuar ato ndaj dobësive që mund të kenë efekte shkatërruese mbi popullatën lokale.

Shtetet kanë për detyrë të mbrojnë nga IIK-të e sulmeve kibernetike brenda kufijve të tyre. Mbrojtja e IIK-ve nga sulmi kibernetik duhet të jetë një përparësi në strategjinë e sigurisë kibernetike të një shteti. Për këtë qëllim, shtetet duhet të zhvillojnë dhe zbatojnë masa të mbrojtjes kibernetike që mbrojnë zonat e prekshme në sistemet e informacionit IIK. Këto masa duhet të jenë në gjendje të zbulojnë, mbrohen dhe neutralizojnë sulmet kibernetike.

SHEMBUJ TË PRAKTIKËS SË MIRË

Parlamenti i Afrikës së Jugut, në mars 2019, miratoi legjislacionin e IIK-ve i cili synon, ndër të tjera, të parashikojë identifikimin dhe deklarimin e infrastrukturës si infrastrukturë kritike; të sigurojë udhëzime dhe faktorë që duhet të merren parasysh për të siguruar identifikimin dhe deklarimin transparent të infrastrukturës kritike; dhe të parashikojë masa që duhen vendosur për mbrojtjen, ruajtjen dhe qëndrueshmërinë e infrastrukturës kritike. Legjislacioni gjithashtu përcakton Këshillin Kritik të Infrastrukturës dhe i jep ministrit të Policisë diskrecionin për të deklaruar instalime të caktuara të infrastrukturës kritike dhe përshkruan se si këto mbrohen në interes të sigurisë kombëtare.

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

GJETJET KRYESORE

- Kornizat ndërkombëtare ose rajonale ofrojnë një sërë normash për zhvillimin, miratimin dhe ndryshimin e legjislacionit, politikave dhe strategjive të sigurisë kibernetike.
- Qeveritë kanë rolin kryesor në sigurimin e qeverisjes së mirë të sigurisë kibernetike.
- Qeveritë duhet të zhvillojnë, miratojnë dhe përditësojnë ligjet, politikat dhe strategjitë kombëtare për të rregulluar hapësirën kibernetike dhe për të përmbushur sfidat aktuale në hapësirën kibernetike, përfshirë fushat e privatësisë dhe mbrojtjen e të dhënave personale, dhe mbrojtjen e infrastrukturës kritike.
- Rritja e ekspertizës së hapësirës kibernetike përmes arsimit dhe ndarjes së njohurive, veçanërisht nëpërmjet Partneriteteve Privat-Publike (PPP), është thelbësore për qeverisjen e mirë të sigurisë kibernetike.

Burime

The Rule of Law Checklist. Venice Commission of the Council of Europe, 2016.

Cybersecurity Policy Framework. A Practical guide to the development of national cybersecurity policy. Microsoft (2018).

International Cybersecurity Norms: Reducing Conflict in an Internet-dependent World. Microsoft (2014).

African Union Commission and Symantec, Cyber crime and cyber security trends in Africa Report (2017). https://thegfce.org/wp-content/uploads/2020/06/CybersecuritytrendsreportAfrica-en-2-1.pdf

KAPITULLI 5

STRATEGJITË KOMBËTARE TË SIGURISË KIBERNETIKE

OBJEKTIVAT

Ky kapitull synon t'u sigurojë përdoruesve të këtij udhëzuesi një hyrje në strategjitë kombëtare të sigurisë kibernetike (SKSK). Në veçanti, ai synon të rrisë njohuritë e përdoruesve në lidhje me elementet kryesore të një SKSK dhe të ofrojë shembuj të praktikave të mira.

Objektivat e nxënies së këtij kapitulli janë si më poshtë:

- Rritja e njohurive në lidhje me strategjitë kombëtare të sigurisë kibernetike në përgjithësi.
- Rritja e njohurive në lidhje me elementët kryesorë të një strategjie kombëtare të sigurisë kibernetike.
- Rritja e ndërgjegjësimit në lidhje me burimet e disponueshme që mund të mbështesin ligjvënësit dhe politikëbërësit kombëtar në zhvillimin e strategjive kombëtare të sigurisë kibernetike

Hyrje

Që nga paraqitja e saj, hapësira kibernetike ka siguruar një larmi mundësish për zhvillimin ekonomik, teknologjik dhe shoqëror. Sidoqoftë, në të njëjtën kohë kërcënimet transnacionale - të tilla si spiunazhi kibernetik i sponsorizuar nga shteti, aktivitete kibernetike ushtarake, krimi kibernetik, terrorizmi kibernetik dhe përdorim terrorist i internetit - kanë qenë në rritje. Kur këto rreziqe të sigurisë të shoqëruara ose të lehtësuara nëpërmjet hapësirës kibernetike nuk janë ekuilibruar si duhet me strategjitë dhe planet e veprimit gjithëpërfshirës, shtetet nuk do të jenë në gjendje të mbrojnë sigurinë kombëtare dhe njerëzore ose të ruajnë rritjen ekonomike.

Si përgjigje, shtetet në të gjithë botën zhvillojnë dhe përshtatin strategji për të adresuar këtë peizazh të rrezikut të sigurisë në zhvillim, duke miratuar politika të reja ekzistuese ose duke ndryshuar politikat ekzistuese të sigurisë kombëtare. Politikat e sigurisë kombëtare që përqendrohen në peizazhin e kërcënimeve në hapësirën kibernetike quhen strategji kombëtare të sigurisë kibernetike (SKSK).

SKSK-ja mund të marrë forma të ndryshme dhe, varësisht nga gatishmëria kibernetike e një vendi, ndryshon në hollësi. Për shkak se SKSK-të janë specifike për kontekstin, nuk është e mundur të kemi një plan për një SKSK efektive. Sidoqoftë, ka mundësi të identifikohen një sërë prioritetesh strategjike që përmbahen në shumicën e SKSK-ve. Këto janë kornizat rregullatore, mbrojtja e infrastrukturës kritike, bashkëpunimi ndërkombëtar dhe bashkëpunimi publik-privat, si dhe kërkimi dhe zhvillimi.

Ndërsa nuk ka një përkufizim të rënë dakord për SKSK, Bashkimi Ndërkombëtar i Telekomunikacionit (ITU), përcakton një strategji kombëtare të sigurisë kibernetike si:

- Një shprehje e vizionit, objektivave, parimeve dhe përparësive të nivelit të lartë që drejtojnë një vend në adresimin e kërcënimeve kibernetike.

- Një përmbledhje e aktorëve të ngarkuar me detyrën për të përmirësuar sigurinë kibernetike të kombit dhe rolet dhe përgjegjësitë e tyre përkatëse.

- Një përshkrim i hapave, programeve dhe iniciativave që një vend do të ndërmarrë për të mbrojtur infrastrukturën e tij kombëtare kibernetike dhe, në proces e sipër, të rrisë sigurinë dhe qëndrueshmërinë e saj.[1]

Ndërsa kërcënimet kibernetike po evoluojnë me një ritëm të shpejtë, edhe fusha e SKSK-së ka evoluar: nga mbrojtja e individëve dhe organizatave si aktorë të veçantë deri te mbrojtja e shoqërisë në tërësi.

1 ITU, Udhëzues për hartimin e një strategjie kombëtare të sigurisë kibernetike, 2018, f. 13

Në thelb, një SKSK kërkon të arrijë dy objektiva të ndërlidhur:

- 1. Forcimin e sigurisë kibernetike për ekonominë e internetit për të nxitur më tej prosperitetin ekonomik dhe shoqëror, dhe
- 2. Mbrojtjen e shoqërive që mbështeten në internetin nga kërcënimet kibernetike.

Siguria kibernetike është një sfidë komplekse që përfshin aspekte të ndryshme të qeverisjes, politikave, aspekteve operacionale, teknike dhe ligjore. Politikat kombëtare përgjithësisht përcaktojnë metodologjinë dhe përcaktojnë qëllimet për arritjen e përparësive kombëtare.

Praktika e mirë 1: Një Strategji kombëtare e sigurisë kibernetike është përfshirë në politikën më të gjerë të sigurisë kombëtare të një qeverie.

Një SKSK duhet të shihet si një mjet shtesë për të arritur prioritetet strategjike kombëtare. Prandaj, është e rëndësishme që një vend të konsiderojë SKSK-në si pjesë të strategjisë së tij të përgjithshme të sigurisë. Kjo më tej kontribuon në një qasje gjithëpërfshirëse të sigurisë kombëtare.

Përfshirja e sigurisë kibernetike si një element i rëndësishëm në një strategji të sigurisë kombëtare dhe anasjelltas demonstron kuptimin e një qeverie se hapësira kibernetike është një pjesë kritike, praktikisht, për çdo aspekt të sigurisë kombëtare.

SHEMBUJ TË PRAKTIKËS SË MIRË

Strategjia suedeze e sigurisë kibernetike thotë se strategjia e saj "bazohet në objektivat për sigurinë e Suedisë: mbrojtjen e jetës dhe shëndetit të popullatës, funksionimin e shoqërisë dhe aftësinë tonë [suedeze] për të mbështetur vlerat themelore si demokracia, shteti i ligjit dhe të drejtave dhe lirive të njeriut."

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

Finlanda për zbatimin e strategjisë së saj kombëtare të sigurisë kibernetike ndjek parimet dhe procedurat e vendosura në Strategjinë e sigurisë për shoqërinë.

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

Kur hartohet një SKSK gjithëpërfshirëse, është e rëndësishme të përkthehet vizioni dhe objektivat e një vendi në veprime konkrete që në fund të fundit kontribuojnë në arritjen e qëllimeve dhe objektivave të identifikuara në radhë të parë.

Cikli jetësor i mëposhtëm, i zhvilluar nga ITU, i një SKSK-je synon të ndihmojë për të drejtuar mendimin strategjik të përdoruesit në një nivel kombëtar:

Figura 1: Cikli i jetesës i SKSK-së së bazuar në Udhëzuesin ITU për zhvillimin e një strategjie kombëtare të sigurisë kibernetike

Para zhvillimit të një SKSK-je, është thelbësore që një Qeveri të identifikojë objektivat dhe qëllimin e një strategjie të tillë dhe të artikulojë qartë vizionin e saj në kontekstin e sigurisë kibernetike.

STUDIM I RASTIT: MISIONI I ASISTENCËS TEKNIKE I OSHA PËR MEKSIKËN

Në vitin 2017, Organizata e Shteteve Amerikane (OSHA), nëpërmjet Programit të saj të sigurisë kibernetike, dhe me kërkesë të Qeverisë së Meksikës, thirri një komision të ekspertëve ndërkombëtarë për të shkëmbyer praktikat më të mira me subjektet meksikane për të kuptuar gjendjen aktuale të sigurisë kibernetike në Meksikë, për të identifikuar gjendjen aktuale të pjekurisë së sigurisë kibernetike, si dhe për të avancuar një kornizë kombëtare të sigurisë kibernetike.

Ekspertët në komision u përshëndetën nga sektori privat, qeveritë e tjera, komuniteti teknik, organizatat ndërkombëtare dhe shoqëria civile.

(Burimi: 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)

Praktika e mirë 2: Procesi i hartimit të një strategjie kombëtare të sigurisë kibernetike duhet të drejtohet nga një autoritet kryesor dhe të përfshijë një grup të gjerë të palëve të interesuara.

Për të filluar procesin e zhvillimit të një SKSK-je, duhet të identifikohet një autoritet kryesor. Ky mund të jetë ose një subjekt paraekzistues ose një agjenci e krijuar rishtazi. Një nga përgjegjësitë kryesore të këtij autoriteti kryesor duhet të jetë koordinimi i procesit në mënyrë neutrale. Ajo duhet të jetë përgjegjëse për identifikimin e palëve

kryesore të interesit që duhet të përfshihen në zhvillimin e SKSK-së dhe për sigurimin e shkëmbimeve të vazhdueshme me palët e interesit për të siguruar që njohuritë dhe ekspertiza përkatëse të përdoren në procesin e hartimit të SKSK-së. Për më tepër, autoriteti udhëheqës duhet të jetë, gjithashtu, përgjegjës për përcaktimin e qartë të roleve dhe përgjegjësive të aktorëve kryesorë.

STUDIM I RASTIT : KOMITETI NDËRMINISTROR I KILIT

Në Kili, një komitet ndërministror i përbërë nga Ministria e Brendshme dhe Siguria Publike dhe Ministria e Mbrojtjes Kombëtare drejtoi procesin e zhvillimit të një strategjie kombëtare të sigurisë kibernetike.

Ky komitet ndërministror organizoi dhe koordinoi sesione të grupeve të punës që korrespondojnë me temat e identifikuara për strategjinë kombëtare të sigurisë kibernetike. Subjektet e ndryshme të grupeve të punës ishin: infrastruktura e informacionit, parandalimi dhe sanksionet, edukimi dhe ndërgjegjësimi, bashkëpunimi dhe marrëdhëniet ndërkombëtare, institucionalizimi. Anëtarët e përhershëm të këtyre grupeve të punës ishin sekretaritë për punë të brendshme, mbrojtjen, presidencën e përgjithshme, drejtësinë, ekonominë, telekomunikacionin dhe agjencinë kombëtare të inteligjencës.

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

Ndërsa është e vërtetë se sektori privat ka një rol të veçantë në garantimin e sigurisë kibernetike, bashkëpunimi midis sektorit publik dhe privat nuk është gjithnjë i institucionalizuar.

Bashkëpunimi publik-privat është gjithashtu i rëndësishëm për mbrojtjen e infrastrukturës kritike, pasi që infrastruktura më kritike është në pronësi dhe operohet nga subjekte private. Prandaj, këto duhet të përfshihen në mënyrë aktive në planifikimin për mbrojtjen e infrastrukturës kritike kombëtare kundër kërcënimeve kibernetike.

Përfshirja e sa më shumë aktorëve në procesin e zhvillimit të një SKSK-je është thelbësore për të promovuar pronësinë e strategjisë. Pronësia është kritike për fazën e implementimit. Për më tepër, përfshirja e të gjithë aktorëve relevantë siguron që këta aktorë të kontribuojnë me njohuritë e tyre eksperte për të arritur një shkallë më të lartë suksesi.

SHEMBUJ TË PRAKTIKËS SË MIRË

Në mënyrë që të sigurojë rezultatin optimal të SKSK-së së saj, Mbretëria e Bashkuar kishte një proces të hapur konsultimi të disponueshëm në faqen e saj të internetit për të gjithë për të siguruar reagime mbi strategjinë.

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

Qeveria Kanadeze filloi një proces të konsultimit publik në internet që kërkonte pikëpamjet e kanadezëve, sektorit privat, akademisë dhe aktorëve të tjerë të interesuar mbi peizazhin e sigurisë kibernetike në Kanada. Një raport i këtij procesi të rishikimit është botuar në përputhje me rrethanat dhe është bërë i disponueshëm në internet.

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

Strategjia e sigurisë kibernetike e MB-së thotë se arritja e qëllimit të një interneti të sigurt do të kërkojë nga të gjithë, sektori privat, individët dhe qeveria të punojnë së bashku. Ashtu si të gjithë përfitojmë nga përdorimi i hapësirës kibernetike, kështu që të gjithë kemi përgjegjësinë të ndihmojmë në mbrojtjen e tij.

Ndërsa partneritetet publike-private janë formati më i zakonshëm i institucionalizimit të bashkëpunimit midis sektorit publik dhe privat, sfidat mbeten. Veçanërisht në lidhje me mandatin e partneritetit publik-privat, mungesa e qartësisë në lidhje me rolet dhe përgjegjësitë, mosbesimi midis palëve të interesuara, pengesat në ndarjen e informacionit, mungesa e stimujve për të punuar së bashku, dhe mungesa e mbikëqyrjes efektive dhe rrjedhimisht e përgjegjësisë.

STUDIM I RASTIT: IDENTIFIKIMI I AKTORËVE RELEVANTË

Ndërsa jo të gjithë aktorët duhet të përfshihen në çdo diskutim, është e rëndësishme të identifikoni aktorët përkatës që kanë një interes dhe ekspertizë të drejtpërdrejtë dhe kështu mund të kontribuojnë në diskutime.

Më poshtë jepet një listë e palëve të interesuara përkatëse në zhvillimin e një SKSK-je. Megjithëse lista nuk është gjithëpërfshirëse, ajo gjithsesi duhet të sigurojë një pasqyrë të mirë të aktorëve përkatës.

- **Qeveria:** ministritë përkatëse (TIK, Ekonomi, Komunikime, etj.), agjencitë rregullatore, gjyqësori dhe organet e zbatimit të ligjit, shërbime të mbrojtjes dhe sigurisë
- **Sektori privat:** kompanitë e TIK-ut, kompanitë e sigurisë së informacionit, shoqata e biznesit

- **Shoqëria civile:** grupe të drejtuara nga interesi (të tilla si të drejtat e njeriut ose mbrojtja e fëmijëve në internet), grupe të bazuara në identitetin (besimi, pakica, të drejtat e grave), rrjetet e organizatave të shoqërisë civile.
- **Qarqet akademike:** universitete, subjekte kërkimore, grupe studimore, studiues të pavarur
- **Komuniteti teknik:** Ekipet e përgjigjes ndaj emergjencave kompjuterike, ekipet e përgjigjes ndaj incidenteve të sigurisë kompjuterike, organizatat e standardizimit të sistemit të emrave të domenit.
- **ON:** organizata rajonale dhe ndërkombëtare (të tilla si UA, OSBE, OSHA, KE), institucionet ndërkombëtare (p.sh. Banka Botërore, ITU)

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

Praktika e mirë 3: Procesi i hartimit të një strategjie kombëtare të sigurisë kibernetike duhet të bëjë një vlerësim të gjerë të anëve të forta dhe të dobëta të sigurisë kibernetike në vendi

Si fazë tjetër në procesin e zhvillimit të SKSK, është e rëndësishme që peizazhi i sigurisë kibernetike në një vend specifik të vlerësohet dhe analizohet për të identifikuar pikat e forta dhe të dobëta të sigurisë kibernetike të një vendi. Si pjesë e kësaj përpjekje për vlerësimin dhe analizën, kuadri rregullator kombëtar (përfshirë ligjet, rregulloret, politikat dhe programet në lidhje me sigurinë kibernetike), infrastruktura kritike kombëtare dhe partneritetet publiko-privat, si dhe aftësitë teknike dhe institucionale për të parandaluar rreziqet e sigurisë kibernetike (siç janë ekipet e reagimit të emergjencave kompjuterike) dhe duhet të mbrohen nga kërcënimet e sigurisë kibernetike (siç janë nëpunësit e mbrojtjes së të dhënave) dhe të analizohen.

Një proces i mbledhjes dhe analizimit vlerëson nivelin e pjekurisë kibernetike të një vendi për të siguruar më tej që një SKSK të jetë përshtatur me nevojat aktuale të të njëjtit vend.

STUDIM I RASTIT: MODELI I PJEKURISË TË KAPACITETIT TË SIGURISË KIBERNETIKE, MINISTRIA E KOMUNIKIMEVE E GANËS

Kapaciteti i sigurisë kibernetike i Ganës u vlerësua nëpërmjet modelit të pjekurisë kibernetike të zhvilluar për të mbështetur rishikimin e kapaciteteve të sigurisë kibernetike në Gana në lidhje me pesë dimensionet:

- Politika dhe strategjia e sigurisë kibernetike
- Kultura dhe shoqëria kibernetike
- Edukimi, trajnimi dhe aftësitë e sigurisë kibernetike
- Kornizat ligjore dhe rregullatore
- Standardet, organizatat dhe teknologjitë.

Objektivi i këtij vlerësimi ishte që të lejojë Qeverinë e Ganës të fitojë një kuptim më të mirë të pikave të përparësive dhe dobësive në lidhje me sigurinë kibernetike, dhe për pasojë të rrisë investimet efektive në ndërtimin e kapaciteteve.

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

Duke u bazuar në këtë vlerësim, një SKSK mund të zhvillohet nën drejtimin e një autoriteti të përkushtuar dhe me angazhim të gjerë të palëve kryesore të interesit. Në mënyrë ideale, grupet e punës janë krijuar për të hartuar seksione specifike të SKSK-së, subjekt i ekspertizës përkatëse të grupit të punës. Si praktikë e mirë shihet që para miratimit të SKSK-së, të ketë një proces rishikimi të SKSK-së, në formën e konsultimit onlajn ose seminareve, midis një larmie të madhe të palëve të interesuara. Kjo kontribuon për të siguruar që SKSK-ja të bazohet në një vizion të përbashkët.

Në varësi të procesit konkret të miratimit, parlamenti ose qeveria janë të autorizuar të miratojnë një SKSK. SKSK-ja e miratuar duhet të botohet në Fletoren Zyrtare ose në faqen e internetit të një ministrie, për të siguruar që popullata të njihet me ekzistencën dhe përmbajtjen e saj, si dhe përparësitë e Qeverisë në lidhje me sigurinë kibernetike, dhe mund të kontribuojë në mënyrë aktive në arritjen e prioriteteve strategjike të përcaktuara në strategjinë.

Nuk ka një qasje të vetme kur bëhet fjalë për strukturimin e procesit të hartimit të një SKSK-je. Praktikat e mira do të ndryshojnë në varësi të fushës së SKSK-së, gamës së palëve të interesuara të përfshira dhe kërkesave teknike të disponueshme.
Në Kili, Kenia dhe Meksikë, versioni draft i SKSK-së u botua gjithashtu në internet për të lejuar palë të ndryshme të interesit të japin komente për të dhe të krijojnë pronësinë

Praktikë e mirë 4: Një SKSK përfshin përparësitë strategjike të mëposhtme: koordinimi i zgjeruar qeveritar në nivelet e politikave dhe operacionale, bashkëpunimi i përforcuar publik-privat, bashkëpunimi i përmirësuar ndërkombëtar dhe respektimi i të drejtave themelore.

Shumica e SKSK-ve nënvizojnë rëndësinë e bashkëpunimit ndërkombëtar për promovimin e sigurisë kibernetike dhe nevojën për aleanca dhe partneritete më efektive me vendet me të njëjtin mendim, përfshirë ndërtimin e kapaciteteve. Përveç kësaj, shumica e SKSK-ve njohin respektimin e të drejtave themelore, veçanërisht të drejtën për privatësi dhe liritë e shprehjes dhe mendimit, si dhe rrjedhën e lirë të informacionit, si të domosdoshme për një hapësirë të sigurt kibernetike.

Për më tepër, shumica e SKSK-ve kanë parandalimin e krimit kibernetik si një përparësi strategjike të përfshirë në strategjitë e tyre.

SHEMBUJ TË PRAKTIKËS SË MIRË

Strategjia kombëtare e sigurisë kibernetike e Kanadasë pasqyron vlerat kanadeze si sundimi i ligjit, llogaridhënia dhe privatësia.

(Burimi: 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)

Strategjia kombëtare e teknologjisë së informacionit dhe komunikimit të Malavit nënvizon se Qeveria do të vazhdojë të sigurojë një mjedis të përshtatshëm për pjesëmarrjen e sektorit publik dhe privat në zhvillimin, vendosjen dhe përdorimin e TIK-ut si në bashkësitë urbane ashtu edhe ato rurale.

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

Praktika e mirë 5: Identifikoni infrastrukturën kritike kombëtare për t'u përfshirë në SKSK.

Identifikimi i infrastrukturës kritike kombëtare është thelbësore për zhvillimin e politikave për t'i mbrojtur ato nga kërcënimet kibernetike. Pa një përkufizim dhe listë të qartë të asaj që përbën infrastrukturën kritike, është e vështirë të sigurohen këto pasuri kritike kundër rreziqeve kibernetike.

Një përqindje në rritje e infrastrukturës kritike varet nga teknologjia e komunikimit të informacionit që të operojë dhe funksionojë. Mbrojtja e infrastrukturës kritike kombëtare nga kërcënimet kibernetike është jetike sepse mund të ketë efekte në botën reale - si pasojë, zakonisht përfshihet si përparësi në strategjitë kombëtare të sigurisë kibernetike të shumë shteteve.

Një numër gjithnjë e në rritje i shteteve identifikojnë infrastrukturën e tyre kritike kombëtare. Shumica identifikon ujin, energjinë elektrike, spitalet, si infrastrukturë kritike kombëtare.

Direktiva e Këshillit të BE 2008/114 / EC e 8 dhjetorit 2008 mbi identifikimin dhe përcaktimin e infrastrukturës kritike evropiane dhe vlerësimin e nevojës për përmirësimin e mbrojtjes së tyre përbën një dokument të rëndësishëm në këtë drejtim. Në veçanti, kjo Direktivë e Bashkimit Evropian përcakton infrastrukturën kritike si "një aset, sistem ose pjesë e tij e vendosur në shtetet anëtare që është thelbësore për mirëmbajtjen e funksioneve jetësore shoqërore, shëndetit, sigurisë, mirëqenies ekonomike ose sociale të njerëzve dhe prishja ose shkatërrimi i të cilave do të kishte një ndikim të rëndësishëm në një shtet anëtar si rezultat i dështimit për të ruajtur ato funksione ".

SHEMBUJ TË PRAKTIKËS SË MIRË

Neni 17 i Projektligjit për mbrojtjen e infrastrukturës kritike në Afrikën e Jugut i rendit faktorët që duhet të merren parasysh në deklarimin e infrastrukturës kritike. Këta faktorë janë për shembull: sektori në të cilin ndodhin funksionet kryesore të një infrastrukture të tillë; rëndësia strategjike, duke përfshirë edhe ndikimin e mundshëm të shkatërrimit, prishjes, dështimit ose degradimit të një infrastrukture të tillë ose ndërprerjes së një shërbimi që mund të ndikojë në aftësinë e Republikës së Afrikës së Jugut për të funksionuar, ofruar shërbime themelore publike ose për të ruajtur rendin dhe ligjin; kategorinë e rrezikut të një infrastrukture të tillë; burimet në dispozicion të personit që kontrollon infrastrukturën; efektet ose rrezikun e shkatërrimit, përçarjes, dështimit ose degradimit të një infrastrukture të tillë; madhësinë dhe vendndodhjen e çdo popullate në rrezik; incidentet historike të shkatërrimit; nivelin e rrezikut ose kërcënimeve ndaj të cilave ekspozohet një infrastrukturë e tillë; karakteristikat e veçanta ose atributet e një infrastrukture të tillë; shkallën në të cilën shpallja si infrastrukturë kritike do të promovojë interesat e publikut; dhe çdo faktor tjetër që mund të përcaktohet nga ministri.

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

Strategjia e Gjermanisë për infrastrukturën kritike kombëtare (2009) e përcakton infrastrukturën kritike si "strukturat organizative dhe fizike dhe objektet e një rëndësie të tillë jetësore për shoqërinë dhe ekonominë e një kombi ku dështimi ose degradimi i tyre do të rezultojë me mungesa të qëndrueshme të furnizimit, prishje të konsiderueshme të sigurisë publike ose pasoja të tjera dramatike ".

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

Franca e përcakton infrastrukturën kritike si "institucione, struktura ose objekte që ofrojnë mallra dhe shërbime thelbësore duke formuar shtyllën kurrizore të shoqërisë franceze dhe mënyrën e saj të jetës". Vetë operatorët hartojnë listën e infrastrukturave kritike, të cilat mund të jenë vendet e prodhimit, qendrat e kontrollit, nyjat e rrjetit ose qendrat e të dhënave për shembull.

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

Zvicra përfshin sektorët e mëposhtëm si pjesë të infrastrukturës kritike:

autoritetet, energjinë, hedhjen e mbeturinave, financat, shëndetësinë, ujin dhe ushqimin, informacionin dhe komunikimin, transportin, sigurinë publike.

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

Praktika e mirë 6: Një strategji kombëtare e sigurisë kibernetike parashikon një plan zbatimi, për kërkimin dhe zhvillimin.

Një SKSK është efektive vetëm nëse zbatimi i saj është i tillë. Prandaj, zbatimi efektiv i një SKSK-je varet nga miratimi i një plani të zbatimit (ndonjëherë i referuar edhe si plan veprimi) për ta kthyer strategjinë në veprime dhe politika konkrete, duke koordinuar përpjekjet dhe burimet.

Një pjesë thelbësore e një plani të zbatimit është zhvillimi i treguesve kryesorë për të monitoruar dhe vlerësuar suksesin e SKSK-së. Në procesin e monitorimit, qeveria duhet të sigurojë që SKSK-ja të zbatohet në përputhje me planin e saj të veprimit. Në fazën e vlerësimit, ajo duhet të vlerësojë nëse SKSK-ja po i reflekton ende objektivat dhe përparësitë e saj - dhe nëse jo, për t'i rivlerësuar këto.[2]

Një plan zbatimi duhet të përfshijë më tej krijimin e një mekanizmi raportimi të incidenteve dhe si të rritet ndërgjegjësimi i njerëzve në lidhje me rreziqet dhe kërcënimet në hapësirën kibernetike. Raportimi i incidenteve të sigurisë kompjuterike luan një rol esencial në rritjen e sigurisë kombëtare kibernetike në përgjithësi. Një raportim i tillë kontribuon në rregullimin dhe përshtatjen e listës së masave të sigurisë kibernetike në ndryshimin e peizazhit të kërcënimeve. Një parakusht i domosdoshëm për raportimin është bashkëpunimi midis sektorit publik dhe privat. Prandaj, besimi është jetik për të mbështetur ndarjen e informacionit të hapur në lidhje me rreziqet dhe kërcënimet në hapësirën kibernetike. Krijimi i një ekipi kompjuterik për reagimin ndaj incidenteve (CSIRT) shihet si gur themeli i koordinimit efektiv të menaxhimit të incidenteve.

Në mënyrë që një plan zbatimi të jetë efektiv, duhet të ketë iniciativa për rritjen e ndërgjegjësimit në lidhje me përdoruesin individual dhe njohuritë e tij / saj në lidhje me kërcënimet dhe dobësitë e sigurisë kibernetike. Kjo është e domosdoshme për të siguruar që një përdorues individual të dijë si të mbrojë veten nga rreziqet në hapësirën kibernetike që mund të ndikojnë në sigurinë kombëtare kibernetike të një vendi.

Investimi dhe nxitja e kërkimit dhe zhvillimit (R&D) janë gjithashtu thelbësore për zhvillimin e mjeteve të reja për parandalimin, mbrojtjen, zbulimin dhe përshtatjen ndaj dhe kundër të gjitha llojeve të kërcënimeve kibernetike.

2 Udhëzuesi i ITU për zhvillimin e një strategjie të sigurisë kibernetike, f. 26

SHEMBUJ TË PRAKTIKËS SË MIRË

SKSK-ja e Kenisë përcakton objektivin e mëposhtëm "Qeveria e Kenisë është e angazhuar për sigurinë dhe prosperitetin e kombit tonë dhe partnerëve të tij. Ne e shohim sigurinë kibernetike si një komponent kryesor në atë angazhim, duke u siguruar organizatave dhe individëve besim të shtuar në transaksione në internet dhe celular, duke inkurajuar investime më të mëdha të huaja dhe duke hapur një grup më të gjerë të mundësive të tregtisë brenda tregut global. Zbatimi i suksesshëm i strategjisë do t'i mundësojë Kenisë më tej arritjen e qëllimeve të saj ekonomike dhe shoqërore nëpërmjet një mjedisi të sigurt në internet për qytetarët, industrinë dhe partnerët e huaj për të kryer punën. " (f. 4)

Strategjia kombëtare e sigurisë kibernetike e Nigerisë identifikon përdoruesin individual si hallkën më të dobët brenda zinxhirit të sigurisë kibernetike. Prandaj, strategjia siguron "iniciativa dhe masa që ndihmojnë në mbrojtjen e përdoruesve të përgjithshëm të internetit, sigurimin e materialeve dhe lehtësimin e mjeteve për të ndihmuar në mbrojtjen e qytetarëve nigerianë nga kërcënimet dhe vulnerabiliteti kibernetik".

(Burimi: Nigeria, Strategjia kombëtare e sigurisë kibernetike, Kapitulli i njëmbëdhjetë)

Politika kombëtare e TIK-ut e Malavit shoqërohet nga një Strategji e hollësishme e zbatimit, monitorimit dhe vlerësimit ndërsa zbatimi i politikës së TIK-ut monitorohet dhe vlerësohet, gjithashtu, për efektivitetin dhe përgjigjen mbi baza vjetore ose sipas nevojës. (Burimi: Malawi, Politika kombëtare e TIK-ut, 2013, f. 11)

Strategjia kombëtare e sigurisë kibernetike e Mauritanisë përfshin në politikë një plan të detajuar të zbatimit të vetë politikës. (Burimi: Maurétanie, Stratégie Nationale de Modernization de l'Administration et des TICs 2012-2016)

Strategjia kombëtare e sigurisë kibernetike e Polonisë identifikon rritjen e ndërgjegjësimit të përdoruesve për metodat dhe masat e sigurisë në hapësirën kibernetike si një komponent kritik i strategjisë së saj (Poloni, Strategjia kombëtare e sigurisë kibernetike, 2013)

Tunizia, Afrika e Jugut dhe Kenia kanë krijuar funksionimin e ekipeve kompjuterike të reagimit ndaj emergjencave (CERT).

Praktika e mirë 7: Siguron burime të mjaftueshme për të zhvilluar fushata të ndërgjegjësimit të sigurisë kibernetike për publikun e gjerë që shoqërojnë zbatimin e një SKSK-je.

Të gjithë të lidhur në internet - nga një zyrtar qeveritar, pronarë biznesi, sektori financiar dhe tregtar, deri te publiku i gjerë si dhe fëmijët - janë të prekshëm nga kërcënimet e sigurisë kibernetike.

Në përgjithësi, ekziston një mirëkuptim i përbashkët që siguria kibernetike nuk është përgjegjësi e një agjencie, subjekti ose individi të vetëm, por një përgjegjësi e përbashkët e të gjithëve të lidhur në internet ose duke përdorur aplikacione që janë të lidhura me këtë fushë në internet.

Sipas Organizatës së Shteteve Amerikane (OSHA) "krimet kibernetike përbëhen nga një gamë e gjerë sjelljesh dhe teknikash të ndryshme - përfshirë identifikimin e vjedhjeve, shfrytëzimin e fëmijëve, ngacmimin në internet, kërcënimet e brendshme, ishin dhe shumë e shumë të tjerë - që duhet të adresohen."[3].

Për shkak se të gjithë mund të preken nga lloje të ndryshme të krimit kibernetik, është e rëndësishme të edukohet publiku për rreziqet dhe kërcënimet në hapësirën kibernetike.

STUDIM I RASTIT: FUSHATA E NDËRGJEGJËSIMIT PËR SIGURINË KIBERNETIKE E OSHA - ANALIZË E GJENDJES

Për zhvillimin e një fushate të suksesshme sensibilizuese, me rëndësi është të kuptohet mirë kontekstit aktual në lidhje me peizazhin e kërcënimeve të sigurisë kibernetike.

Në këtë drejtim OSHA hartoi disa pyetje udhëzuese që synojnë të ndihmojnë për të analizuar një situatë aktuale:

- Sa i konektuar është vendi juaj?
- Ku dhe si po lidhen njerëzit në internet?
- Kush është në internet?
- Me çfarë lloj pajisjesh?
- Çfarë lloje të sistemeve operative dhe kanaleve të komunikimit?
- Për cilat lloje të produkteve dhe shërbimeve?
- Si po përdoret interneti për biznes?
- Cila është shkalla e këtyre bizneseve (p.sh. ndërmarrjet individuale, bashkëpunimi bujqësor, ndërmarrjet e vogla dhe të mesme, prodhimi i lehtë?)
- Cilat janë rreziqet e sigurisë kibernetike me të cilat përballet vendi juaj?
- Me cilat lloje të krimeve kompjuterike përballen konsumatorët me pakicë?
- Me çfarë lloj krimesh kibernetike në bizneset tuaja përballen?
- A ndahen këto krime kibernetike në grupe?
- Cilat janë rreziqet për infrastrukturën tuaj kritike?

3 OSHA (2016): Cybersecurity Awareness Raising Toolkit, p8, gjendet në https://thegfce.org/wp-content/uploads/2020/06/2015-oas-cyber-security-awareness-campaign-toolkit-english-1.pdf

- A ka pasur shkelje të mëdha - qeveritare ose komerciale - në të kaluarën e afërt?
- A ka rrezik për shkelje të mëdha në të ardhmen?
- Cilat janë humbjet ekonomike ose potenciali nga kërcënimet kibernetike?

Burimi: OAS, Cybersecurity Awareness Campaign Toolkit 2016, në dispozicion në https://thegfce.org/wp-content/uploads/2020/06/2015-oas-cyber-security-awareness-campaign-toolkit-english-1.pdf

Fushatat e suksesshme për ngritjen e vetëdijes përcjellin mesazhe të lehta për t'u kuptuar, të synuara dhe të planifikuara dhe të zhvilluara në një proces me shumë aktorë, që përfshin zyrtarë qeveritarë, kompani private siç janë ofruesit e shërbimeve të internetit, kompanitë e telekomunikacionit), si dhe përfaqësues të shoqërisë civile, si organizatat joqeveritare, media dhe qarqet akademike.

SHEMBUJ TË PRAKTIKËS SË MIRË

Në vitin 2015, Jordania miratoi një ligj për luftimin e krimeve kibernetike dhe u krijua një njësi e specializuar "Njësia e Krimit Kibernetik". Kjo Njësi e Krimit Kibernetik, e ndihmuar nga Zyra e Kombeve të Bashkuara për Drogat dhe Krimin, prodhoi një video sensibilizuese mbi rreziqet, llojet dhe pasojat ligjore të krimit kibernetik.

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

StaySafeOnline i cili mundësohet nga Aleanca Kombëtare e Sigurisë Kibernetike kërkon të inkurajojë një kulturë të sigurisë kibernetike. Për këtë qëllim, ajo publikoi në faqen e saj të internetit një infografik se si të sigurohet që të gjithë në një familje - duke përfshirë fëmijët dhe të moshuarit - të përdorin internetin në mënyrë të sigurt dhe me përgjegjësi.

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

GJETJET KRYESORE

- Në mënyrë që të adresojnë kërcënimet aktuale dhe ato në zhvillim të sigurisë kibernetike, shtetet duhet të monitorojnë dhe përshtatin vazhdimisht strategjitë e tyre kombëtare të sigurisë kibernetike në peizazhin e rrezikut në zhvillim.
- Duhet të vendosin doemos objektiva specifikë dhe prioritete strategjike që një strategji kombëtare e sigurisë kibernetike të jetë e suksesshme.
- Strategjitë e sigurisë kibernetike duhet të njohin respektimin e të drejtave themelore, të tilla si privatësia dhe liritë e shprehjes dhe besimit, si dhe rrjedhën e lirë të informacionit në mënyrë që të promovojnë një hapësirë të lirë dhe të hapur kibernetike.
- Siguria kibernetike është një çështje që përfshin sektorë të ndryshëm dhe përgjegjësi të agjencive të ndryshme publike. Prandaj, bashkëpunimi i ngushtë midis të gjitha autoriteteve qeveritare si dhe sektorit privat është një shtyllë e rëndësishme për zbatimin me sukses të një strategjie kombëtare të sigurisë kibernetike.
- Në mënyrë që të zhvillojnë mjete të reja për parandalimin, mbrojtjen, zbulimin dhe përshtatjen ndaj dhe kundër llojeve të reja të kërcënimeve kibernetike, qeveritë duhet të investojnë më shumë burime në Kërkim dhe Zhvillim.
- Për të mbrojtur infrastrukturën kritike kombëtare nga kërcënimet kibernetike, është e rëndësishme që së pari të përcaktohet ajo që konsiderohet “infrastruktura kritike kombëtare” në një kontekst të caktuar.

BURIMET

ITU Guide to National Cybersecurity Strategies, gjendet në 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, gjendet në https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVoNi

Global Partners Digital: Multistakeholder Approaches to National Cybersecurity Strategy Development, June 2018, në disopozicion në 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, 2016, gjendet në https://thegfce.org/wp-content/uploads/2020/06/2015-oas-cyber-security-awareness-campaign-toolkit-english-1.pdf

KAPITULLI 6

LLOGARITET SE 15% E PUNËTORËVE SI NË SEKTORIN SHTETËROR ASHTU EDHE ATË PRIVAT HUMBËN VENDET E TYRE TË PUNËS NË 2009-2010

OBJEKTIVAT

Ky kapitull synon t'u ofrojë përdoruesve një përmbledhje të pikave të forta dhe sfidave që lidhen me partneritetin privat-publik në hapësirën kibernetike, veçanërisht midis agjencive të zbatimit të ligjit dhe kompanive private kur hetojnë krime dhe përmbajtje të paligjshme në internet.

Objektivat e nxënjes së këtij kapitulli janë si më poshtë:

- Rritja e njohurive për konceptet e iniciativave me shumë aktorë dhe partneritete publike-private.
- Bashkëpunimi nëpërmjet agjencive për zbatimin e ligjit dhe sektorit financiar
- Kuptimi në rritje i elementëve për krijimin e qasjeve efektive të palëve të interesuara për sigurinë kibernetike.

Hyrje

Siguria kibernetike është një zonë ndërsektoriale dhe një objektiv i përbashkët i çdo Strategjie kombëtare të sigurisë kibernetike (SKSK) pra është bashkëpunimi midis aktorëve kibernetikë publikë dhe privatë për të rritur sigurinë kibernetike. Qasjet e shumë palëve të interesuara në hapësirën kibernetike dhe sigurinë kibernetike, të referuara gjithashtu si Partneritetet publiko-private (PPP), po bëhen gjithnjë e më vitale në qeverisjen e sigurisë kibernetike, pjesërisht për shkak të rolit të jashtëzakonshëm që luajnë kompanitë private dhe për shkak të karakteristikës transnacionale të hapësirës kibernetike. Bashkëpunimi efektiv midis të gjithë aktorëve të interesuar - veçanërisht qeverive, sektorit të TIK-ut, akademisë dhe shoqërisë civile - është bërë një element thelbësor i zbatimit të standardeve dhe normave ndërkombëtare dhe të SKSK-ve efektive.

Përpjekjet në rritje në lidhje me sigurinë kibernetike që ndërthur mekanizmat publik, publik-privat dhe privat tregojnë një ndryshim më thelbësor në mënyrën e kryerjes së biznesit në një shkallë globale. Në dritën e kësaj tendence, bashkëpunimi ndërmjet një sërë aktorësh të interesuar - shteteve, biznesit dhe shoqërisë civile - mund të shihet si një përgjigje pragmatike për të mbushur disa nga boshllëqet e qeverisjes të gjetura në qasjet rregullatore tradicionale. Të angazhuar për të përmirësuar sigurinë e shteteve dhe njerëzve brenda një kornize të qeverisjes demokratike, sundimit të ligjit dhe respektimit të të drejtave të njeriut. Grupet e përbëra nga palë të ndryshme të interesit së bashku mund të hartojnë mënyra dhe zgjidhje më të mira sesa do të rezultonin vetëm nga puna e një grupi të palëve të interesuara

.

1. 1. Kuptimi i partneritetit publik-privat

Përmbledhje

Partneritetet publiko-private përfshijnë ndarjen e burimeve (aseteve, aftësive, ekspertizës dhe financimit), rreziqeve dhe përfitimeve ndërmjet palëve të interesuara. Në fushën e sigurisë kibernetike, PPP-të nënkuptojnë bashkëpunim midis qeverisë dhe institucioneve publike nga njëra anë dhe industrisë së TIK-ut, akademisë dhe shoqërisë civile nga ana tjetër për të rritur ndërgjegjësimin e sigurisë kibernetike, për të zbutur rreziqet e sigurisë kibernetike dhe për të siguruar aftësi të forta kombëtare të sigurisë kibernetike. Ky bashkëpunim është shumëplanësh dhe mund të përfshijë rritjen e aftësive të mbrojtjes kibernetike dhe shkëmbimin e informacionit. Interesat ekonomikë, kërkesat rregullatore dhe marrëdhëniet me publikun gjithashtu mund të jenë forca shtytëse për PPP-të. Në vendet në zhvillim, PPP-të e sigurisë kibernetike

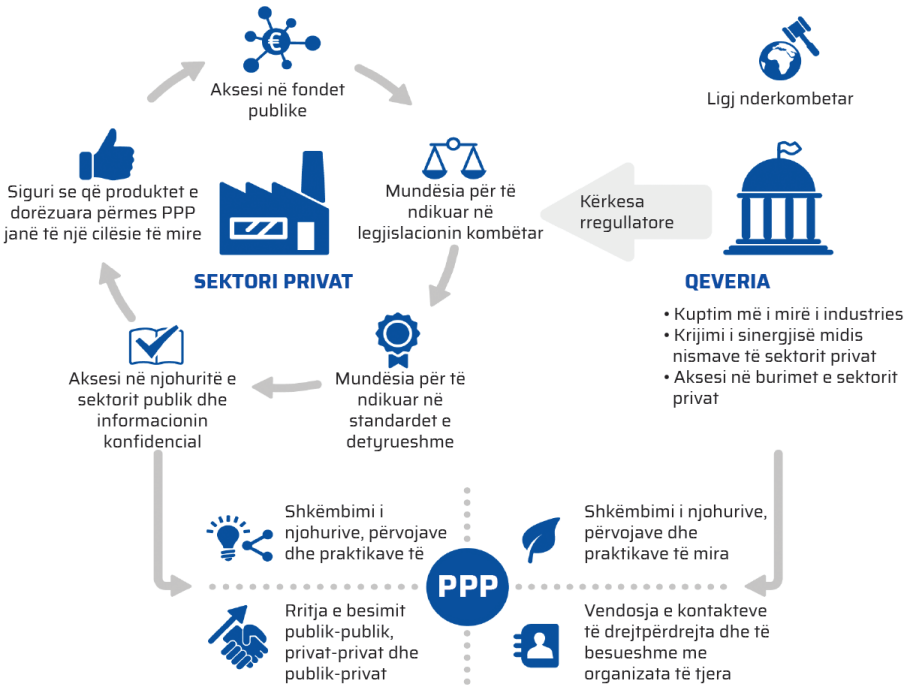
kanë të bëjnë kryesisht me rritjen e ndërgjegjësimit të sigurisë kibernetike ose sigurimin e aftësive të forta kombëtare të sigurisë kibernetike.

PPP-të mund të jenë të dobishme në sigurinë kibernetike për një numër arsyesh:

- Të inkurajojë përmirësimin e vetëdijes dhe kuptimin e drejtë të sigurisë kibernetike ndërmjet organizatave dhe gjithë shoqërisë.
- Për të përmirësuar grupin kombëtar të aftësive kibernetike nëpërmjet krijimit të iniciativave të dizajnuara për të identifikuar, frymëzuar dhe mundësuar më shumë njerëz që të bëhen profesionistë të sigurisë kibernetike;
- Të pajisë profesionistët e sigurisë kibernetike me burimet e kërkuara financiare dhe teknike, nëpërmjet iniciativave të dedikuara;
- Për kërkim dhe zhvillim në fushën e sigurisë kibernetike
- Për parandalimin e krimit dhe mashtrimin në veprim
- Për certifikimin dhe akreditimin në fushën e sigurisë kibernetike;
- Të lidhë dhe të nxisë bashkëpunimin midis subjekteve publike dhe private që punojnë në fushën e sigurisë kibernetike.

PPP-të në fushën e sigurisë kibernetike mund të kategorizohen sipas katër llojeve të në vazhdim:

- PPP-ja institucionale: e formuar në bazë të një akti ligjor të lidhur me mbrojtjen kritike të infrastrukturës. Mjetet e përbashkëta të bashkëpunimit janë grupet e punës, grupet me përgjigje të shpejtë dhe komunitetet afatgjata.
- PPP-ja e orientuar drejt qëllimit: i krijuar për të ndërtuar një kulturë të sigurisë kibernetike nëpërmjet një platforme ose këshilli që bashkon sektorin privat dhe publik për të shkëmbyer njohuri dhe praktika të mira. Përqendrohet në një temë ose qëllim specifik.
- Shërbime të jashtme të sigurisë kibernetike: të krijuara kur qeveritë nuk mund të adresojnë në mënyrë efektive nevojat e sektorit privat që i kanë identifikuar. PPP-të veprojnë si një palë e tretë autonome, por adresojnë në mënyrë aktive nevojat e industrisë dhe mbështesin qeverinë në hartimin e politikave ose zbatimin e tyre.
- PPP-ja hibride: Ekipet e reagimit të emergjencave kompjuterike (CERT) që veprojnë nën një kornizë PPP. Qeveritë u caktojnë këtyre PPP-ve detyrën e ofrimit të shërbimeve CERT në administratën publike ose në të gjithë vendin.



Arsyet dhe stimujt për Partneritet publiko-privat

Burimi: Public-Private Partnerships in Cyberspace, ENISA, November 2017, f. 14

2. Rolet e qeverive dhe aktorëve të tjerë

Roli kryesor për institucionet publike në bashkëpunimin me shumë aktorë

Qeveritë kanë përgjegjësinë kryesore për zhvillimin e një SKSK efektive. Ligjbërësit dhe politikëbërësit janë përgjegjës për krijimin e kornizave adekuate, në përputhje me detyrimet e shtetit sipas ligjit ndërkombëtar, si dhe në përputhje me ligjin e tij kombëtar. Qeveritë angazhohen me aktorë privatë siç janë kompanitë e TIK-ut për të siguruar që rregullimi i ndërsjellë dhe vetërregullimi të jenë në përputhje me ligjin ndërkombëtar për të drejtat e njeriut dhe ligjin kombëtar.

Përtej kësaj qasje thjesht legaliste, qeveritë mund të luajnë një rol të rëndësishëm në koordinimin dhe angazhimin me sektorin e TIK-ut dhe shoqërinë civile duke krijuar dhe mbështetur platforma bashkëpunuese. Këto janë me rëndësi të veçantë për njësitë kombëtare të referimit, të cilat kërkojnë dhe shënjojnë kontakte të dyshimta në internet dhe kërkojnë heqjen e përmbajtjes nëpërmjet proceseve të referimit me kompanitë e TIK-ut. Platformat bashkëpunuese mund të ofrojnë kontribut të vlefshëm për qeveritë

dhe të kontribuojnë në nxitjen e një procesi vendimmarrës më gjithëpërfshirës. Kanalet e hapura të komunikimit midis aktorëve relevantë gjithashtu ndihmojnë në identifikimin dhe plotësimin e boshllëqeve kritike në sigurinë kibernetike dhe zbutjen e konflikteve të mundshme të interesit. Përpjekjet e institucionalizuara dhe të koordinuara gjithashtu mund të promovojnë veprime plotësuese dhe kanalizimin e burimeve njerëzore dhe financiare ndërmjet palëve të ndryshme të interesit.

STUDIMI I RASTIT: EKIPET E REAGIMIT NDAJ EMERGJENCAVE KOMPJUTERIKE

Ekipet e reagimit ndaj emergjencave kompjuterike (CERT) janë njësi ekspertësh të ngarkuar për të ndihmuar individë ose institucione që bien viktima të një sulmi kibernetik. Detyrat e tyre kryesore janë të identifikojnë maluerin (malware) armiqësor dhe të parandalojnë përhapjen e tij më tej në rrjet duke zbutur pasojat e sulmit. Njësi të tilla përfshihen shpesh brenda ndërmarrjeve private ose institucioneve publike, por mund të ekzistojnë gjithashtu në nivel kombëtar si agjenci të veçanta qeveritare që ofrojnë ndihmën e tyre për një gamë të gjerë të subjekteve private dhe publike.

Megjithëse CERT-et kombëtare janë agjenci publike, ato përfaqësojnë një shembull të mirë të bashkëpunimit publik-privat. Funksioni themelor i çdo CERT-i është të sigurojë informacion në lidhje me dobësitë kibernetike të zbuluara së fundmi, duke përfshirë azhurnimet dhe rregullimet e programeve përkatëse. Shumica e CERT-ve kombëtare mund të informohen mbi rreziqet kibernetike ose incidentet kibernetike nëpërmjet një formulari publik onlajn. Përveç kësaj, disa CERT-e kombëtare ofrojnë ekipe mobile që mund të dërgohen në një institucion që kërkon ndihmë në rast sulmi kibernetik.

Bashkëpunimi midis sektorit privat dhe atij publik është thelbësor për ruajtjen e një ambienti të qëndrueshëm dhe të sigurt kibernetik. Institucionet publike nuk mund të sigurojnë hapësirën kibernetike më vete për dy arsye kryesore. Së pari, sektori privat drejton inovacionin në terren dhe kontrollon pjesën më të madhe të hapësirës kibernetike. Së dyti, edhe infrastruktura kritike kibernetike e zotëruar nga shteti dhe e kontrolluar nga shteti mbështetet shumë te produktet dhe shërbimet e ndërmarrjeve private për mbrojtjen e tyre.

Për më tepër, qeveritë janë të detyruara të respektojnë dhe mbrojnë të drejtat e njeriut të qytetarëve të tyre në internet dhe për këtë arsye duhet të sigurojnë se çdo veprim i ndërmarrjeve private dhe CERT-et kombëtare nuk i shkel të drejtat e njeriut, veçanërisht të drejtën për privatësi dhe shprehje të lirë. Për të përmbushur këtë qëllim, CERT-i duhet të jetë i pavarur nga ndikimi politik dhe të mos shërbejë si instrument qeveritar për të shkelur privatësinë e sistemit kompjuterik dhe të rrjetit ose privatësinë dhe fshehtësinë e komunikimit.

Kur vendosin CERT-et kombëtare, qeveritë duhet të kenë parasysh dimensionin njerëzor të sigurisë kibernetike në të tri aspektet e tij: konfidencialitetin, aksesin dhe integritetin. Kështu, duhet të kuptohet që siguria kibernetike është në thelbin e saj, jo për sigurimin e rrjeteve por

për rritjen e sigurisë njerëzore. Sa i përket mbrojtjes së konfidencialitetit të informacionit, e drejta për privatësi duhet të jetë një standard udhëzues për të gjitha operacionet që mbrojnë dhe rrisin konfidencialitetin e të dhënave. Sa i përket aksesit të të dhënave, është thelbësore që liria e shprehjes dhe informacionit të respektohet dhe mbrohet.

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

STUDIMI I RASTIT: NJËSITË E BRENDSHME TË REFERIMIT NË BE DHE NË NIVELIN KOMBËTAR

INjësia e Referimit të Internetit të Bashkimit Evropian (BE) (IRU) është pjesë e Qendrës Evropiane të Terrorizmit të EUROPOL-it dhe përbëhet nga një ekip ekspertësh nga fushat e terrorizmit të frymëzuar nga feja, ekspertë gjuhësorë, zhvillues të teknologjisë së informacionit dhe komunikimit dhe agjencive të zbatimit të ligjit të specializuar në luftën kundër terrorizmit[1] Filloi me punë në vitin 2015 dhe ka këtë mandat:

- Të mbështesë autoritetet kompetente të BE-së duke siguruar analiza strategjike dhe operacionale;
- Të shënjojë përmbajtjet terroriste dhe ekstremiste të dhunshme në internet dhe ta ndajë atë me partnerët përkatës;
- Të zbulojë dhe të kërkojë heqjen e përmbajtjes në internet të përdorur nga rrjetet e kontrabandës për të tërhequr migrantë dhe refugjatë;
- Të kryejë dhe mbështesë me shpejtësi procesin e referimit, në bashkëpunim të ngushtë me industrinë[2].

Sipas raportit të transparencës së IRU-së të BE-së në 2017, "bashkëpunimi me sektorin privat është thelbësor gjatë parandalimit".[3] Që nga themelimi i saj në korrik 2015 deri në dhjetor 2017, IRU e BE-së ka vlerësuar 46,392 pjesë të përmbajtjes terroriste që nxitën 44,807 vendime për referim me një normë 92 përqind të heqjes së përmbajtjes.[4]

Siç përshkruhet në raportin e transparencës dhe në mandatin e IRU-së së BE-së, IRU është përgjegjëse për vlerësimin e përmbajtjes në internet dhe referimin e saj te kompania përkatëse e TIK-ut që pret përmbajtjen për heqje. Si e tillë, IRU e BE-së përqendrohet në përmbajtjen e botuar nga Al-Kaeda dhe Daesh dhe grupet e lidhura me të dhe e vlerëson këtë përmbajtje sipas mandatit të EUROPOL, në përputhje me parimet e përcaktuara në Direktivën e BE-së për luftimin e terrorizmit. Direktiva e BE-së për luftimin e terrorizmit siguron masa mbrojtëse në lidhje me heqjen e përmbajtjes, të dhëna në nenin 21 (3):

Masat e heqjes dhe bllokimit duhet të përcaktohen duke ndjekur procedura transparente dhe duke siguruar masa adekuate mbrojtëse, veçanërisht për të siguruar që ato masa të jenë të kufizuara nga fakti se janë të nevojshme dhe proporcionale dhe që përdoruesit të informohen për arsyen e atyre

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

masave. Garancitë në lidhje me heqjen ose bllokimin do të përfshijnë gjithashtu mundësinë e dëmshpërblimit gjyqësor.[5]

Në rast se përmbajtja e vlerësuar shkel mandatin e EUROPOL, përmbajtja përkatëse i referohet kompanisë TIK në platformën e së cilës është zbuluar përmbajtja. Sidoqoftë, përfundimisht i lihet gjykimit të kompanisë që të heqë ose jo këtë përmbajtje të shënjuar, pasi ta vlerësojë atë përkundër kushteve përkatëse të shërbimit. IRU e BE-së nuk ka fuqi ligjore për të hequr përmbajtje.

Njësi të ngjashme referimi ekzistojnë në MB, Francë dhe Holandë, me deklarata nga EUROPOL që tregojnë se mekanizmat paralelë janë krijuar në Belgjikë, Gjermani dhe Itali.[6]

Përveç kësaj, IRU e BE-së organizon të ashtuquajturat Ditët e përbashkëta të veprimit të referimit me kompani TIK si Gugëll (Google), Tuiter (Twitter) dhe Telegram. Ditët e përbashkëta të veprimit të referimit bashkojnë njësi të specializuara të zbatimit të ligjit nga IRU të shumta kombëtare dhe kompanitë IRU dhe TIK të BE-së. Specialistët e zbatimit të ligjit vlerësojnë disa qindra pjesë të përmbajtjes potenciale terroriste në një platformë specifike dhe synojnë të zbulojnë modelet në përdorimin e platformës nga grupe terroriste dhe ekstremiste të dhunshme. Gjetjet më pas ndahen me pjesëmarrjen e kompanisë përkatëse të TIK-ut, e cila rishikon përmbajtjen e zbuluar sipas kushteve të saj. Kompania është ajo që merr vendimin përfundimtar për të hequr ndonjë përmbajtje. Ditët e përbashkëta të veprimit të referimit promovojnë një qasje të koordinuar midis qeverive dhe kompanive të TIK-ut në adresimin e përmbajtjes ekstremiste të dhunshme dhe terroriste në internet.[7]

Iniciativa të drejtuara nga industria e TIK-ut dhe nga Shoqëria Civile

Kompanitë e TIK-ut përballen shpesh me sfida të rregullimit të ndërsjellë dhe vetërregullimit në lidhje me platformat e tyre, veçanërisht kur bëhet fjalë për mbrojtjen e të drejtave të njeriut siç janë liria e fjalës dhe e drejta e privatësisë. Këto sfida përkeqësohen nga fakti që platformat e mediave sociale janë bërë mjete thelbësore për shoqërinë për të diskutuar, shkëmbyer dhe për t'iu qasur informacionit. Si përgjigje, iniciativat e drejtuara nga industria e TIK-ut, si shkëmbimi i njohurive dhe teknologjisë midis kompanive; krijimin e platformave për mjetet dhe burimet interaktive të moderimit të përmbajtjes; dhe seancat e trajnimit të drejtuara nga kompani më të mëdha për ato më të vogla mbi qasjet e heqjes së përmbajtjes, mund të jenë mjete efektive për forcimin e sigurisë kibernetike.

5 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32017L0541

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

7 Shih 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

STUDIMI I RASTIT: INHOPE

Shoqata Ndërkombëtare e Linjave të Nxehta në Internet (INHOPE) ka një prani globale në 43 vende dhe ka për qëllim të kontribuojë për një internet ku nuk do të ketë "abuzime dhe shfrytëzime seksuale të fëmijëve".[8] Misioni i saj është të "forcojë përpjekjet ndërkombëtare për të luftuar materialet e abuzimit seksual të fëmijëve".[9] Partnerët INHOPE me një sërë palësh të interesuara përfshirë Interpol, EUROPOL, Twitter, Crisp, Microsoft, Google, Facebook dhe Trend MICRO.

INHOPE përbëhet nga 48 linja telefonike që ofrojnë një mekanizëm për publikun për të raportuar përmbajtje ose aktivitet në internet që dyshohet se është i paligjshëm. INHOPE ndan aktivitetet e paligjshme në dy kategori të ndryshme: veprimtari kriminale ilegale që hetohet dhe ndiqet nga Zbatimi i Ligjit, në të cilën përqendrohen linjat e nxehta të INHOPE, dhe veprimtari të paligjshme civile që mund të ndiqen nga organet civile.

Fokusi kryesor i INHOPE është materiali i abuzimit seksual të fëmijëve, por gjithashtu përfshin edhe gjuhën e urrejtjes dhe përmbajtjet ksenofobike në internet. Ndërsa INHOPE ofron një përkufizim për gjuhën e urrejtjes, ajo pranon gjithashtu që gjuha e urrejtjes është një çështje "jashtëzakonisht komplekse" që shpesh nuk është e paligjshme sipas ligjit penal. Prandaj, secili raport në një linjë të nxehtë në lidhje me gjuhën e urrejtjes vlerësohet në kundërshtim me legjislacionin kombëtar, d.m.th. ku pritet përmbajtja përkatëse.[10]

E gjithë përmbajtja e raportuar në mënyrë anonime shqyrtohet nga një analist i përmbajtjes së linjës së nxehtë për të vlerësuar nëse materiali është i paligjshëm. Nëse analisti i përmbajtjes së linjës së nxehtë e konsideron përmbajtjen e raportuar të paligjshme, gjurmohet vendndodhja e kësaj përmbajtje. Nëse përmbajtja është vendosur në të njëjtin vend, materiali do të raportohet në agjencitë kombëtare të zbatimit të ligjit dhe / ose kompaninë e TIK-ut për t'u hequr. Nëse materiali organizohet në një vend të huaj, ai përcillet në linjën telefonike në vendin pritës.

INHOPE zhvilloi më tej një Kod të praktikës për ofruesit e linjave të nxehta të brendshme i cili përshkruan që anëtarët e INHOPE duhet të konsultohen rregullisht me aktorët kryesorë, duke përfshirë qeveritë, agjencitë e zbatimit të ligjit, industrinë e TIK-ut, institucionet e mirëqenies së fëmijëve dhe që anëtarët duhet të zbatojnë parimet e transparencës, llogaridhënies, përgjegjësisë dhe besueshmërisë.

INHOPE e thekson gjithashtu rëndësinë e mirëqenies së stafit për ata që rishikojnë përmbajtjen e raportuar dhe pranon rishikimin psikologjik të përmbajtjes së abuzimit të fëmijëve dhe përmbajtjes së dhunshme ekstremiste ose terroriste që mund të kenë tek rishikuesit. Një letër e bardhë, e hartuar dhe e botuar nga linja e nxehtë franceze Point de Contact, synon

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

të zhvillojë një grup të përbashkët të praktikave më të mira për trajtimin operativ dhe përpunimin e përmbajtjes së dëmshme dhe potencialisht të paligjshme që mund të rrezikojnë sigurinë fizike dhe mirëqenien psikologjike të recensuesve profesionistë të përmbajtjes[11].

3. Krijimi i PPP-ve të sigurisë kibernetike

Praktika e mirë 1: Duhet krijuar një mjedis i përshtatshëm si parakusht i domosdoshëm për krijimin e PPP-ve efektive.

Për krijimin e PPP-ve efektive nevojitet një mjedis mundësues. Kjo kërkon katër dimensione kryesore: formulimin e politikave, një kornizë ligjore dhe rregullatore, rregullimet institucionale dhe mbështetjen/investimet financiare. Për më tepër, Udhëzimet e BE-së e theksojnë rëndësinë e fleksibilitetit dhe transparencës nga të gjithë partnerët e përfshirë, si dhe njohjen reciproke të nevojave dhe objektivave të aktorëve të ndryshëm të përfshirë. [12]

Krijimi i një mjedisi mundësues duhet të përfshijë marrëveshje nga palët e interesit për bazën ligjore të PPP-ve. Institucionet publike duhet të marrin drejtimin në krijimin e PPP-ve ose planeve kombëtare të veprimit. Për ta bërë këtë, duhet të sigurohen burime të përshtatshme për koordinimin dhe bashkëpunimin e brendshëm të PPP-ve, dhe një qasje pragmatike e miratuar për zgjidhjen e sfidave në koordinim dhe bashkëpunim. Nxitja e pjesëmarrjes së sektorit privat, veçanërisht me ndërmarrjet e vogla dhe të mesme, është gjithashtu e rëndësishme për të siguruar krijimin e një mjedisi mundësues që promovon më tej bashkëpunimin midis palëve të interesuara përkatëse. Në fund, palët e interesuara të PPP-ve duhet të investojnë në komunikimin e hapur me publikun e gjerë.

Praktika e mirë 2: Duhen krijuar linja të qarta të përgjegjësisë dhe llogaridhënies për të mbrojtur të drejtat e njeriut.

Vendosja e linjave të qarta të përgjegjësisë dhe llogaridhënies së të gjithë palëve të interesuara është thelbësore për të siguruar që çështje të tilla si shkeljet e të drejtave të njeriut të mos ndodhin. Në kontekstin e KSKS-së, PPP-të mund të jenë problematike për disa arsye, duke përfshirë hezitimin e politikanëve për të marrë përgjegjësi për legjislacionin e rreptë të sigurisë kibernetike, e shoqëruar me rezistencën e sektorit privat për të pranuar përgjegjësi për sigurinë kombëtare, e cila lë partneritetin pa linja të qarta të përgjegjësisë ose llogaridhënies. Përfshirja e specifikimeve të qarta në

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

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

marrëveshjet e PPP-së të përgjegjësive dhe mekanizmat e llogaridhënies shkojnë dorë për dore me zbutjen e rreziqeve dhe për të siguruar që të gjithë palët e interesuara të kenë një kuptim adekuat të roleve dhe përgjegjësive të tyre.

Praktika e mirë 3: Besimi midis aktorëve të interesuar duhet të ndërtohet dhe mirëmbahet.

Ndërtimi dhe ruajtja e besimit midis njësive publike dhe private është një nga sfidat më të mëdha për PPP-të. Zhvillimi dhe ruajtja e besimit është një proces i vazhdueshëm që ka të bëjë me kulturën dhe me marrëdhëniet personale. Besimi nuk mund të arrihet pa një mjedis mundësues. Sfidat e tjera përfshijnë mungesën e burimeve njerëzore si në sektorin publik ashtu edhe në atë privat; buxheti dhe burimet e pamjaftueshme të sektorit publik që nuk përmbushin pritjet e sektorit privat; dhe kuptimi dhe dialogu i pamjaftueshëm midis sektorit publik dhe privat në lidhje me vetë konceptin e PPP-ve.

Agjencitë publike dhe subjektet private duhet të ndërtojnë besimin mbi hapjen, drejtësinë dhe respektin e ndërsjellë. Në rastin e PPP-ve, një test i rëndësishëm i besimit është shkëmbimi i informacionit. Pjesëmarrësit duhet të ndiejnë se marrin informacion shtesë të dobishëm duke qenë pjesë e partneritetit dhe, në të njëjtën kohë, se të dhënat e tyre janë të sigurta dhe të mbrojtura.

STUDIMI I RASTIT: FORUMI GLOBAL MBI EKSPERTIZËN KIBERNETIKE

Forumi global mbi ekspertizën kibernetike (GFCE) është një platformë për shtetet, organizatat ndërkombëtare dhe kompanitë private për të shkëmbyer praktikat dhe ekspertizat më të mira mbi ndërtimin e kapaciteteve kibernetike.

I formuar në prill të vitit 2015, qëllimi kryesor i GFCE-së është të sigurojë një platformë të përkushtuar, joformale për politikëbërësit, praktikuesit dhe ekspertët nga vende dhe rajone të ndryshme për të lehtësuar shkëmbimin e përvojës, ekspertizës dhe vlerësimeve mbi çështjet kyçe rajonale dhe tematike kibernetike. Që nga fillimi i tij, fokusi i GFCE-së është zhvendosur për t'u bërë një platformë koordinuese. Fushat fillestare të fokusit për ndërtimin e kapaciteteve dhe ekspertizës ishin siguria kibernetike, krimi kibernetik, mbrojtja e të dhënave dhe qeverisja elektronike. Në 2019, GFCE-ja u pozicionua për të lehtësuar dhe koordinuar ndarjen e njohurive dhe ekspertizës për zbatimin e ndërtimit të kapaciteteve kibernetike. Për më tepër, grupet e ndryshme të punës së GFCE-së po lëvizin drejt zhvillimit të një mekanizmi të kleringut.

Burimi: 'History', the GFCE

GJETJET KRYESORE

- Në hapësirën kibernetike dhe në sigurinë kibernetike, grupet e përbëra nga aktorë të ndryshëm kanë shpesh më shumë gjasa të jenë efektive sesa puna e vetëm një aktori të interesuar. Qasjet me shumë palë të interesuara, të referuara gjithashtu si partneritete publike-private (PPP), së bashku mund të krijojnë qasje dhe zgjidhje më të mira, dhe po bëhen gjithnjë e më vitale në qeverisjen e hapësirës kibernetike dhe adresimin e çështjeve të sigurisë kibernetike.
- Po vazhdojmë me krahasimin midis universiteteve publike e private në të dy vendet.
- Qeveritë mund të luajnë një rol të rëndësishëm në koordinimin dhe angazhimin me sektorin e TIK-ut dhe shoqërinë civile duke krijuar dhe mbështetur platforma bashkëpunuese.
- Aktorët privatë siç është industria e TIK-ut gjithashtu mund të drejtojnë iniciativa efektive me shumë aktorë për sigurinë kibernetike.
- Qeveritë duhet të investojnë në qasje pragmatike drejt ndërtimit të PPP-së që përfshijnë komunikim të hapur, pjesëmarrje gjithëpërfshirëse dhe motivim të rritjes së pjesëmarrjes së sektorit privat.

BURIMET

Public-Private Partnerships in Cyberspace, ENISA, November 2017, gjendet në https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models/at_download/fullReport

Public-private partnerships in national cyber-security strategies, gjendet në https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf

US National Council for Public Private Partnerships Definition of PPPs (2016)

Public Private Partnerships in the EU: Widespread shortcomings and limited benefits

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

African CERTs https://www.africacert.org/african-csirts/

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

www.dcaf.ch