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

Водич за добро управување со кибербезбедноста

Содржина

Општ вовед

LCè поголемиот пристап на луѓето до киберпросторот и неговите ресурси, влијае врз нашите секојдневни животи, а значително влијае и врз нашите општества. Веќе суштински се промени начинот на кој живееме, работиме и комуницираме. Киберпросторот нуди безбројни можности за економски развој, социјална интеракција и политички комуникации. Но, тој истовремено дава и алатки за вршење на незаконско следење, собирање на лични податоци, влијание врз демократските процеси, за вршење на кривични дела и менување на средствата и методите за војување.

Поради овие предизвици потребни се и различни реакции, при што државите, приватниот и граѓанскиот сектор мора заеднички да работат на решавање на предизвиците поврзани со управувањето со киберпросторот. Покрај тоа, ќе мора да се приспособат правната и стратешката рамка за подобро да се почитуваат и спроведуваат меѓународните норми за човекови права додека ефективно се справуваме со киберкриминалот, злонамерните дела и нападите во киберпосторот, како и со употребата на интернетот за терористички цели и поттикнување на насилен екстремизам. Само жестоки активности во оваа насока ќе овозможат безбеден, стабилен и отворен киберпростор.

Во овој контекст, Управата за соработка во областа на безбедноста и одбраната (DCSD) на Министерството за Европа и надворешни работи на Франција и Центарот за управување во безбедносниот сектор од Женева (DCAF) во 2018 година започнаа со подготовката на овој Водич кој содржи добри практики за унапредување на управувањето со кибербезбедноста. Во 2020 година, Водичот беше преведен на српски, албански, македонски и англиски јазик како дел од проектот на DCAF Подобрување на управувањето со кибербезбедноста на Западен Балкан кој се спроведува со поддршка од Канцеларијата на Обединетото Кралство за надворешни работи, Комонвелт и развој.

Овој Водич треба да им користи на носителите на политики, техничките експерти, граѓанскиот сектор и на сите оние што се заинтересирани за најдобрите практики во управувањето со кибербезбедноста. Тој се заснова врз искуството на DCAF за поттикнување на добро управување во безбедносниот сектор.

Оваа книга се состои од шест поглавја во кои се објаснува како да се применат начелата на добро управување врз кибербезбедноста. Поглавјата се фокусираат на следните теми:

- Добро управување во безбедносниот сектор и неговата примена во киберпросторот;
- Врската меѓу киберпросторот, кибербезбедноста и управувањето во безбедносниот сектор;
- Меѓународна и регионална правна рамка применлива на киберпросторот;
- Примена на меѓународни и регионални стандарди;
- Национални стратегии за кибербезбедност;
- Поттикнување на ефективна соработка меѓу јавниот и приватниот сектор во киберпросторот.

ПОГЛАВЈЕ 1
ВОВЕДУВАЊЕ ДОБРО УПРАВУВАЊЕ СО БЕЗБЕДНОСНИОТ СЕКТОР

ЦЕЛИ

Целта на ова поглавје е да се подобрат знаењето и разбирањето на корисниците на клучните термини поврзани со доброто управување со безбедносниот сектор; целта е тие да се стават во контекст на киберпросторот. Заради тоа, ова поглавје се фокусира на три суштински елементи на доброто управување со безбедносниот сектор кои, исто така, се однесуваат и на киберпросторот:

- а. Отчетноста;
- б. Транспарентноста; и
- в. Владеењето на правото.

Откако ќе ги претставиме овие концепти, ќе бидат претставени и конкретни предизвици кои се поврзани со промовирањето на овие концепти на добро управување во киберпросторот, по што ќе следуваат добри практики што се идентификувани досега.

Целите за учење за ова поглавје се следните:

- Да се подобри информираноста за главните термини и дефиниции во однос на управувањето со безбедносниот сектор, а особено доброто управување со секторот.
- Подобро разбирање на основните концепти и начела на доброто управување, како што се отчетноста, транспарентноста и владеењето на правото.
- Подобрено знаење во врска со основните начела на добро управување со безбедносниот сектор.
- Подобро разбирање на важноста од промовирање на начелото на добро управување во киберпростор.

1. Вовед

Управување, управување со безбедносниот сектор и добро управување со безбедносниот сектор

Управувањето се опишува како „остварување надлежности и овластувања“. Како општ концепт, управувањето може да се искористи за да се опишат правилата според кои се управува со некоја организација, меѓу другото и со приватни комерцијални или непрофитни субјекти. Во безбедносниот сектор, терминот „управување“ се користи да се опишат сите формални и неформални одлуки, процеси и чинители кои влијаат врз обезбедувањето на јавните добра и услуги, како што се здравството, образованието или безбедноста.

Управувањето со безбедносниот сектор (УБС) практично значи „остварување на надлежности и овластувања во контекст на еден конкретен национален безбедносен сектор.“[1] Тоа е аналитички концепт кој не се заснова врз посветеност на специфични норми или вредности.

Доброто управување со безбедносниот сектор се фокусира особено врз примена на начелата за добро управување врз обезбедувањето, управувањето и надзорот над безбедноста во национален контекст.

Концептот на доброто УБС опишува како безбедносниот сектор во една држава да стане поефективен и отчетен во согласност со начелата за демократска цивилна контрола, почитување на човековите права и владеење на правото[2].

Покрај тоа, доброто УБС се заснова врз идејата дека безбедносниот сектор треба да се придржува до истите стандарди за обезбедување на јавни услуги како и давателите на услуги во другите сектори. Поради тоа, безбедносниот сектор кој не ги исполнува овие стандарди може негативно да влијае врз политичката, економската и социјалната стабилност во една држава (ова се нарекува уште и „лошо УБС“).

1 Информативен документ на DCAF за реформата во безбедносниот сектор (види Библиографија).
2 Ibid.

Што претставува безбедносниот сектор?

Генерално, безбедносниот сектор се состои од сите структури, институции и лица одговорни за обезбедување, управување и надзор над безбедноста на национално и на локално ниво.[3]

Поради тоа, безбедносниот сектор не мора да биде ограничен на една држава како единствен обезбедувач на безбедност и правда. И самите граѓани честопати обезбедуваат безбедност и правда во своите домови и заедници, без оглед на тоа дали државата дејствува за да ги исполни овие потреби или не. Имено, луѓето може да се организираат за да обезбедат безбедност на различни начини, меѓу другото, и преку маалски патроли, здруженија на жени или преку ангажирање приватно обезбедување.

Покрај тоа, вообичаените улоги на важни лица од заедницата во однос на одлучувањето за безбедноста и правдата, механизмите за алтернативно решавање на спорови, традициите и неформалните правила може да влијаат врз безбедноста и правдата во една заедница. Поради тоа, овие групи во заедницата се, исто така, дел од безбедносниот и правосудниот сектор во поширока смисла на зборот.

Безбедносниот сектор се состои од сите структури, институции и лица одговорни за обезбедување, управување и надзор над безбедноста на национално и на локално ниво, меѓу кои се и:

- Давателите на услуги за обезбедување, како што се вооружените сили, полицијата, граничната полиција, разузнавачките служби, казнено-поправните установи и комерцијалните и други чинители кои не се дел од државата;
- Органи за управување и надзор над безбедноста, како што се министерствата, собранието, посебните законски институции за надзор, делови од правосудниот сектор и чинители од граѓанскиот сектор кои имаат удел во одржување високи стандарди во јавниот сектор, меѓу кои и женските организации и медиумите.

Исто така, важно е да се наведе дека реформата во безбедносниот сектор (РБС) се заснова врз поширок разбирање на безбедносниот сектор. РБС е процес чија крајна цел е да се постигне добро управување со безбедносниот сектор со цел подобрување на безбедноста на луѓето и државата.

Извор: Информативен документ на DCAF за реформата во безбедносниот сектор (види Библиографија)

3 Ibid.

Актерите во безбедносниот и во правосудниот сектор се вклучени во поширокаата дефиниција на безбедносниот сектор бидејќи директно влијаат врз неговото управување. Во последните две децении давателите на услуги за приватно обезбедување сè повеќе се користат за обезбедување заштита на лица и имот. Особено приватните воени и безбедносни компании кои работат врз комерцијална основа станаа важен чинител во безбедносниот сектор.

Што претставува реформата во безбедносниот сектор?

Безбедносниот сектор кој не е ниту ефективен ниту отчетен, не може да овозможи безбедност за сите, бидејќи не може уверливо да ги врши своите задолженија, како што се одбрана на државата, полициско работење и помагање на граѓаните. Неефикасниот безбедносен сектор веројатно залудно ќе троши јавни средства, поради што тие нема да може да се користат за други суштински јавни услуги.[4]

Реформата на безбедносниот сектор е политички и технички процес за подобрување на човековата и на државната безбедност преку зголемување на ефективноста и отчетноста на обезбедувањето, управувањето и надзорот над безбедноста во рамки на демократската цивилна контрола, владеењето на правото и почитувањето на човековите права[5] .

Добри практики: Да се согледа дека поединците и заедниците имаат различни безбедносни потреби, вклучително и во киберпросторот.

Секое лице кое го користи киберпросторот има индивидуални безбедносни потреби. На Интернет жените и децата се непропорционално погодени од објавите со предрасуди, омраза и мизогинија. Согледувањето на ова, и соодветно на тоа, обезбедувањето ефективни механизми за пријавување инциденти и започнување на кривични истраги може да придонесе за поголема безбедност на погодените ранливи групи.

4 Ibid.

5 Информативниот документ на DCAF за РБС, стр. 2. Достапен на: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_2_Security%20Sector%20Reform.pdf

ПРИМЕРИ ЗА ДОБРИ ПРАКТИКИ

Бенин започна годишна кампања за безбедност на Интернет како дел од напорите за подобрување на информираноста за безбедноста на Интернет во целата држава. Кампањата се фокусира на младите во државата, а ќе се регулира и со националната стратегија за кибербезбедност.

Како дел од движењето за борба против говорот на омраза, државите членки на Советот на Европа започнаа кампањи и формираа национални тела за известување со цел да се воведат процедури и механизми за пријавување говор на омраза, кривични дела сторени од омраза и малтретирање на Интернет.

Во Австрија, Министерството за внатрешни работи е одговорно за механизмот за пријавување насилен екстремизам и радикални видеозаписи со цел онлајн платформите да се безбедни и ослободени од говор на омраза.

(Извор: Сојузно министерство за внатрешни работи на Австрија, http://bvt.bmi.gv.at/601/)

Украинската полиција назначи лице кај кое ќе се пријавуваат предмети поврзани со малтретирање на Интернет и говор на омраза, со цел засегнатите да може да го пријават тоа.

(Извор: Совет на Европа, https://www.coe.int/en/web/no-hate-campaign/reporting-to-national-bodies#{%2237117314%22:[8]}}

Во ноември 2018 година во Сенегал беше отворена Национална школа за кибербезбедност (Ecole Nationale en Cybersécurité à Vocation Régionale - ENVR), со поддршка од Франција, со цел да се подобри одбраната на Западна Африка од компјутерски хакери и злоупотреба на Интернет за финансирање и поттикнување тероризам. Во школата ќе се организираат обуки за безбедносните институции, правосудството и за приватни претпријатија за борба против киберкриминалот. Таа ќе има и регионална улога и ќе им помага и на другите држави во Западна Африка.

(Извор: 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. Добро управување со безбедносниот сектор во киберпросторот

Што значи добро управување со безбедносниот сектор?

Доброто управување со безбедносниот сектор значи примена на начелата на добро управување врз обезбедувањето, управувањето и надзорот над безбедноста во национален контекст. Постојат седум начела за добро управување. Тие се:

- **Отчетност**: постојат јасни очекувања за безбедноста, и постојат независни органи кои вршат надзор дали тие очекувања се исполнети, а изрекуваат санкции доколку не е така.
- **Транспарентност:** постојат бесплатни и достапни информации за лицата кои се засегнати од одлуките и од нивното спроведување.
- **Владеење на правото:** сите лица и институции, вклучувајќи ја и државата, подлежат на законите кои се јавно познати, непристрасно се спроведуваат и се во согласност со меѓународните и националните норми и стандарди за човекови права.
- **Учество:** сите жени и мажи од сите средини имаат можност да учествуваат во одлучувањето и обезбедувањето услуги врз слободна, правична и инклузивна основа, било директно или преку законските институции кои ги претставуваат.
- **Одговорност:** институциите се свесни за различните безбедносни потреби на сите делови од населението и својата мисија ја вршат во духот на култура на опслужување.
- **Ефективност:** институциите ги вршат своите задолженија, одговорности и мисии согласно високи професионални стандарди.
- **Ефикасност:** институциите ги користат јавните ресурси најдобро што можат и ги исполнуваат своите задолженија, одговорности и мисии.

Примена на начелата за добро управување во киберпросторот

Доколку киберпросторот е држава, таа ќе беше најголемата и најнаселената држава во светот. Сепак, таа нема да има законодавна власт или друг орган кој ќе одлучува и ќе ги застапува граѓаните, ниту пак ќе има друг механизам за спроведување на законот или за заштита на човековите права на граѓаните, бидејќи нема таков субјект кој има исклучиви овластувања и контрола над целиот дигитален простор.[6]

Спротивно на ова, управувањето со киберпросторот се карактеризира со голем број различни чинители кои имаат различни улоги и одговорности и кои влијаат врз стратешките одлуки и дискусиите за регулативите.

Недржавните чинители во киберпросторот се граѓанскиот сектор, меѓу кои се и невладините организации, научните истражувачки групи и медиумите; приватниот сектор, а особено приватните компании и индустриски тела; и меѓународните и регионалните организации.

Поради големиот број чинители вклучени во изработката и спроведувањето на политиките и регулативите во киберпросторот, овие процеси честопати се гломазни, сложени и/или не даваат резултати.

Ова, заедно со немањето знаење за тоа како ефективно да се спроведат начелата за добро управување во киберпросторот, може да доведе до лошо управување и до ситуација кога безбедносниот сектор генерално нема да може успешно да ја одржува човековата и државната безбедност. Во наредните поглавја одблиску ќе ги погледнеме начелата за добро управување: отчетноста, транспарентноста и владеењето на правото.

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

СЛУЧАЈ ЗА АНАЛИЗА: ПРОГРАМАТА ЗА НАДЗОР НА АГЕНЦИЈАТА ЗА НАЦИОНАЛНА БЕЗБЕДНОСТ НА СОЕДИНЕТИТЕ АМЕРИКАНСКИ ДРЖАВИ

Во 2013 година, Едвард Сноуден, вработен во ЦИА, извлекол документи кои се државна тајна во кои се открива дека разузнавачките агенции на САД и Обединетото Кралство спроведуваат програми за масовно следење насекаде во светот, меѓу кои и пресретнување на телефонскиот сообраќај и на сообраќајот на Интернет кој поминува преку оптичките кабли под океанот, дека собираат податоци за корисниците на „Гугл“ и „Јаху“ од нивните кориснички налози, ги шпионираат странските влади, ги хакираат и заразуваат компјутерите со злонамерен софтвер.

Имано, компаниите добиваат наредби издадени од Судот за следење на странски разузнавачки информации (FISA) да ги предадат податоците за нивните корисници. Покрај тоа, беа откриени и обемни споделувања на разузнавачки информации меѓу државите членки на Алијансата „Пет очи“, како и со други држави. Иако поранешниот претседател Обама на сето ова одговори со реформирање на програмите за следење на NSA и на Судот FISA со цел да се зголеми транспарентноста, Конгресот на САД сè уште не може да одобри воспоставување систем кој би обезбедил критична заштита на приватноста, а истовремено овозможувајќи истрага кога е потребно.

(Извор: ACLU. Достапно на 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. Развивање норми и институции кои ќе придонесат и ќе ја зајакнат отчетноста на безбедносниот сектор во киберпросторот

За ефективна отчетност потребна е демократска и цивилна контрола. Таквата контрола може да ја спроведуваат националните собранија, како и поопшто граѓанскиот сектор. Оваа форма на надзор има основно значење за да се гарантира отчетноста на безбедносниот сектор. Сепак, во киберпросторот, демократската и цивилна контрола на безбедносниот сектор честопати не е на завидно ниво, и тоа од неколку причини.

Демократскиот надзор честопати се соочува со следните пречки[7]:

Сложеност на онлајн мрежата

Прво, проблемите со надзорот се комплицираат поради сложеноста на мрежата. Многу држави, многу приватни, меѓународни и други недржавни чинители се вклучени во кибербезбедноста. Слично на ова, разновидна група чинители учествуваат во она што општо може да го именуваме како „кибернапади“. Техничката сложеност на мрежата им отежнува на надзорните тела, како што се собраниските комисии – кои честопати имаат и ограничен капацитет – да ги следат релевантните чинители, да

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

се информираат за нивното постоење и активности, па дури и да добијат правен мандат да го прават тоа.

- **Техничкото знаење кое е потребно за да се подготват и спроведат ефективни регулативи**

Како второ, проблемите со надзорот се влошуваат поради екстремно техничката природа на киберпросторот. Како резултат на ова, телата за надзор, какви што се собранијата, честопати ја немаат потребната стручност соодветно да го разберат киберпросторот, а со тоа и не можат да подготват законски текстови кои ефективно ќе ги регулираат активностите во него. Соработката меѓу јавниот и приватниот сектор може дополнително да се комплицира поради поделеноста меѓу високо платените и софистицирани технички експерти кои се вклучени во развивање и спроведување ефективни регулативи, од една страна, и честопати недоволно платените и понеинформирани владини чинители кои се задолжени за надзор, од друга страна.

- **Законската сложеност својствена за киберпросторот, како што се надлежноста и доделување на правата**

Како трето, проблемите со надзорот се влошуваат поради правната сложеност. Меѓусебната поврзаност и „безграничната“ природа на киберпросторот носи вистински предизвици за традиционалните територијални рамки за спроведување на законите. Податоците и киберактивностите може да се преместуваат од сервери лоцирани во една држава на други сервери во други држави буквално со брзина на светлината. Покрај тоа, иако се вели дека треба истите закони да се применуваат и на онлајн активностите, честопати не е јасно што тоа точно значи во практика. Кибербезбедноста наметнува сложени правни прашања кои се поврзани, меѓу другото, и со правото на приватност и слободата на изразување. Оваа сложеност потоа е зголемена поради соработката на јавниот и приватниот сектор, и придружните правни прашања во однос на одговорноста и контролата.

- **Различната природа на вклучените чинители што ги попречува традиционалните линии на одговорност и надзор**

Како четврто, предизвиците со надзорот се влошуваат поради различната природа на вклучените чинители. Во најголем дел од случаите, националните институции за надзор се организирани во рамките на институциите или согласно функцијата. На пример, собраниска комисија може да врши надзор над разузнавачките служби, вооружените сили и над правосудните институции. Сепак, соработката меѓу јавниот и приватниот сектор кој е вклучен во кибербезбедноста ги надминува границите на институциите, а со тоа и знаењата и мандатот на институциите за надзор. Поради тоа, има голем број области во кои нема надзор или тој не е соодветен.

Во однос на прекинување на линиите на одговорност и контрола, активностите на секоја владина институција се поврзани во синџир или одговорности од налогодавач до вршител. На пример, еден полицаец во Париз преку хиерархијата во полицијата е поврзан со раководителот на полициската служба во Париз (политички назначено лице) и на крајот, секако, со министерот за внатрешни работи и извршната власт. Поради тоа, има поврзаност од аспект на одговорноста и надзорот меѓу институциите за демократско владеење (како што е собранието) и поединци или институции кои ги

спроведуваат владините насоки. Овие врски може да се пресечат со воведувањето на приватни чинители и создавањето механизми за соработка меѓу приватниот и јавниот сектор. Иако некоја компанија за ИТ која е ангажирана од јавна институција може да изгледа дека дејствува како едноставен вршител ангажиран од државата, односот генерално е многу посложен и заматен од многуте асиметрии во однос на информациите кои ја намалуваат транспарентноста и спречуваат механизмите за надзор ефективно да функционираат.

Разбирање на мандатот од страна на самото тело за надзор

Генерално, телата за надзор на државата се занимаваат со државните институции над кои имаат директна одговорност. Поради ова, приватните партнери на таквите институции може да се надвор од опсегот на надзорот, дури и во случаи кога тие се директно финансирани од таквите институции или остваруваат тесна соработка со нив.

СЛУЧАЈ ЗА АНАЛИЗА: ГЕРМАНСКИ БУНДЕСТАГ, ИСТРАГА ЗА ПРОДАЖБАТА НА ТЕХНОЛОГИЈА ЗА НАДЗОР НА СТРАНСКИ ВЛАДИ

Во 2014 година, германскиот парламент спроведе истрага за продажбата на технологии за надзор на странски влади. Како одговор на тоа, германската влада изјави дека во текот на минатата деценија им дала лиценци на германски компании да извезуваат технологија за надзор во 25 држави, од кои многу земји имаат долга историја на злоупотреба на човековите права.

Како последица на оваа истрага, германската влада изјави дека понатаму ќе лобира да се регулираат технологиите за надзор кои им штетат на човековите права.

(Извор: EDRi Protecting Digital Freedom. Достапно на: https://edri.org/germany-exports-surveillance-technologies-to-human-rights-violators/)

Технолошката сложеност на киберпросторот дополнително ги влошува традиционалните проблеми со кои се соочуваат пратениците кога треба да вршат надзор над безбедносниот сектор. Ова може да ја поткопа ефективната отчетност. Ова, во комбинација со тешкотиите да се утврди кој точно е одговорен за прекршување на законите во киберпросторот, може да ги отежне, ако не и да ги оневозможи цивилните власти да бараат одговорност од безбедносниот сектор, со што се придонесува за создавање култура на неказнивост.

Правосудниот сектор игра клучна улога во надзорот над активностите на безбедносниот сектор. На пример, правосудниот сектор може да додели посебни овластувања на полициските и на разузнавачките служби со издавање на наредби за претрес. Ова може да е особено релевантно во контекст на следење на комуникацијата. Сепак, правосудната контрола честопати се избегнува или се ограничува поради причини поврзани со националната безбедност и вонредна состојба.

СЛУЧАЈ ЗА АНАЛИЗА: ПАРЛАМЕНТАРЕН НАДЗОР НА КИБЕРБЕЗБЕДНОСТА ВО ШВЕДСКА – ГЛАВНИ ПРЕДИЗВИЦИ И ДОБРИ ПРАКТИКИ

Во парламентот на Шведска функционираат 15 комисии. Улогата на овие собранискиот комисии е различна. Тие, на пример, може да спроведуваат јавни расправи за да добијат информации за конкретни прашања за кои сметаат дека треба да се уредат. Иако не е јасно која собраниска комисија има исклучива надлежност да врши надзор над управувањето со кибербезбедноста, веројатно различни комисии имаат определени улоги, зависно од контекстот. На пример, Комисијата за одбрана може да добие задолженија поврзани со кибербезбедноста.

Стратегијата за кибербезбедност на Шведска од 2016 година се осврнува на различни теми, од регулирањето на давателите на услуги за ИКТ, па сè до заштита на клучната инфраструктура. Сепак, изгледа дека нема комисии или поткомисии конкретно задолжени за кибербезбедноста. Ова прашање многу често бара реакција од повеќе министерства, и тоа е изгледа и случајот во Шведска. Ова може дополнително да се комплицира со фактот што дел од киберзаштитата се обезбедува од страна на приватни чинители и собранискиите комисии немаат соодветен мандат да ги анализираат нивните активности. Сепак, за разлика од неколку други национални стратегии за кибербезбедност, шведската стратегија ги поставува стратегиските начела и дава акциски план, кој може да му помогне на собранието да бара одговорност од различните чинители.

Покрај контролните функции на собранието и на правосудната власт, граѓанскиот сектор игра многу важна улога во надзорот над безбедносниот сектор. Граѓанскиот сектор може да придонесе со давање совети за политики, како и со техничка стручност, а може и да ги олесни дијалогот и преговорите меѓу различните чинители, согласно неговата улога на чувар на интересите на јавноста.

Понатаму, граѓанскиот сектор придонесува за зголемување на информираноста за различни прашања и може да ги насочува политиките. Особено медиумите може да ги истражат и да овозможат пристап до информации преку навлегување подлабоко во темите кои предизвикуваат загриженост

СЛУЧАЈ ЗА АНАЛИЗА: УЛОГАТА НА ПРИВАТНИТЕ КОМПАНИИ ВО ПРОДАЖБАТА НА ТЕХНОЛОГИЈА ЗА НАДЗОР НА ВЛАДИТЕ

Приватните компании, како што е италијанската компанија „Hacking Team“, продала системи за далечински влез на различни држави, меѓу кои и Египет, Нигерија, Узбекистан, Турција, Мароко и Колумбија. Овој растечки тренд предизвика дискусии за можната употреба на овие технологии како средство за репресија и повреда на човековите права.

Масовниот надзор станува сè поголем предизвик и приватните компании продаваат алатки и технологии за надзор на различни држави. Иако граѓанските организации ја подигнуваат свесноста за овие деловни практики, дури и објавиле база низ која може да се пребаруваат повеќе од 520 компании кои им ги продаваат своите производи на државите во светот, ова прашање сè уште е во голема мера нерегулирано.

2.2. Развивање норми и институции кои ја поттикнуваат и зголемуваат транспарентноста и овозможуваат слободна достапност и пристап до информациите

Транспарентноста генерално има две функции: дозволува споделување информации, благодарение на што се поттикнува ефективноста на институциите во безбедносниот сектор, но, исто така, е и предуслов за нивната отчетност. Покрај тоа, информацискатa и комуникацискатa технологија (ИКТ) се алатки, сами по себе, за поттикнување и зголемување на транспарентноста, со тоа што овозможуваат информациите да им се достапни на граѓаните.

Постигнување добро управување со безбедносниот сектор е процес и цел на реформата во безбедносниот сектор

Сепак, апсолутната транспарентност не е ниту изводлива ниту пак се препорачува, зависно од контекстот на безбедносниот сектор.

Важно е да се разбере оваа „дилема околу транспарентноста“ во однос на поттикнување култура на доверба и отвореност меѓу јавноста и приватните даватели на услуги за обезбедување. Сепак, транспарентноста треба да биде правилото, а ограничувањето на транспарентноста да биде исклучокот, и тоа треба да биде јасно дефинирано во националните закони.[8]

Транспарентноста, исто така, го подобрува разбирањето на ризиците во полето на кибербезбедноста и ги поттикнува државите, приватните компании и граѓанскиот сектор поуспешно да се координираат и да соработуваат со цел да ги спречат и да реагираат на овие ризици во полето на кибербезбедноста.

Разбирањето на овие киберризици може да придонесе за индивидуалните корисници да одлучуваат врз база на добиени информации. Ова е клучно, бидејќи индивидуалните корисници на технологии честопати се сметаат за најслабата алка во (кибер) безбедносниот синџир. Подобрените канали за информирање поддржуваат подобро

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

однесување на Интернет (што се нарекува и добра „киберхигиена“), што, пак, веројатно ја намалува успешноста на голем број злонамерни активности.

Во оваа насока, пристапите со повеќе засегнати страни, исто така, може да придонесат за поттикнување на транспарентноста и може да ја зголемат свесноста за ризиците на Интернет..

ПРИМЕРИ ЗА ДОБРИ ПРАКТИКИ

Организацијата за безбедност и соработка во Европа (ОБСЕ) во 2014 година усвои договор за Мерки за градење доверба. Доброволните мерки вклучуваат обезбедување национални мислења во однос на кибердоктрина, стратегија и закани. Земјите членки на ОБСЕ понатаму се договорија да споделуваат информации за национални организации, програми и стратегии релевантни за кибербезбедноста, да идентификуваат лице за контакт заради олеснета комуникација и да водат дијалог за прашања од сферата на безбедноста на ИКТ.

Ел Салвадор има усвоено закони за заштита на податоци и пристап до јавни информации, коишто утврдуваат норми за транспарентност и слобода на информации

(Извор: https://publications.iadb.org/handle/11319/7449, p 74)

Организацијата на американските држави објави извештај за тимовите за одговор при безбедносни компјутерски инциденти (CSIRT), во кој се идентификувани различни начини за подобрување на соработката меѓу тимовите за споделување информации.

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

Поттикнувањето на јавно-приватните партнерства може да придонесе за поволна средина за споделување информации и пристап до информации.

2.3. Зајакнување на начелото на владеење на правото во киберпросторот.

Киберпросторот, исто така, создава ново поле за незаконско дејствување, како на пример, ширење говор на омраза, детска порнографија, поттикнување насилство, повреда на авторски права, измама, кражба на идентитет, перење пари или напади за блокирање на услуга.[9] Овие кривични дејства се сè почесто транснационални.

„Дигиталната средина со самата своја природа може да ги еродира приватноста и другите основни права, како и да го поткопа одговорното носење одлуки“.[10] Следствено на тоа, се зголемува можноста начелото за владеење на правото да

9 Совет на Европа, Владеење на правото на Интернет и во поширокиот дигитален свет, документ издаден од комесарот за човекови права на Советот на Европа, Извршно резиме и препораки на комесарот, 2014 година. Достапно на http://www.statewatch.org/news/2014/dec/coe-hr-comm-rule-of-law-on-the%20internet-summary.pdf

10 Ibid. стр. 6.

биде поткопано преку еродирање на правата на приватност и на другите основни слободи, како што е слободата на изразување.

Начелото на владеење на правото беше дополнително толкувано од меѓународни судови, како што е Европскиот суд за човекови права (ЕСЧП). ЕСЧП изработи тест за владеење на правото според кој „сите ограничувања на основните права мора да се засноваат врз јасни, прецизни, достапни и предвидливи законски правила, и мора јасно да служат за легитимни цели; тие мора да бидат „неопходни“ и „сразмерни“ со релевантната легитимна цел […] и мора да стои на располагање „ефективен [по можност судски] правен лек“.[11]

Владите бараа од приватните компании кои поседуваат платформи на социјални медиуми да се погрижат нивните услуги да не бидат преземени од насилен екстремизам и тероризам.

Генералниот секретар на Обединетите нации го објасни концептот на владеење на правото на следниов начин:

За Обединетите нации, владеењето на правото се однесува на начело на управување според кое сите лица, институции и субјекти, јавни и приватни, вклучително и самата држава, одговараат пред законите кои се јавно прогласени, еднакво спроведувани и самостојно арбитрирани, и коишто се доследни со меѓународните норми и стандарди за човекови права. Исто така, неопходни се мерки преку кои ќе се обезбеди придржувањето до начелата за надмоќ на правото, еднаквост пред законот, одговорност пред законот, правичност во примената на законот, поделба на власта, учество во носењето одлуки, правна сигурност, избегнување арбитрарност и процедурална и правна транспарентност.

(Извор: Извештај на Генералниот секретар на ОН „Владеењето на правото и транзициска правда во конфликтни и постконфликтни општества“, S/2004/616 (23 август 2004 г.), став 6. Достапно на: https://www.un.org/ruleoflaw/files/2004%20report.pdf.

За да се исполнат овие владини барања, приватните компании – особено социјалните медиуми, како што се „Фејсбук“, „Гугл“ и „Твитер“ – изработија услови за користење на услугите и кодекси на однесување со цел да ја регулираат содржината што се поставува на овие платформи на социјални медиуми – со што де факто се создаваат норми на Интернет. Меѓутоа, овие услови за користење на услугите и кодекси на однесување не се исти на различните платформи и со тоа создаваат нејасност и правна несигурност во однос на тоа која содржина е забранета на која платформа.

11 Ibid, стр. 8

СЛУЧАЈ ЗА АНАЛИЗА: УЛОГАТА НА КОМПАНИИТЕ-СОЦИЈАЛНИ МЕДИУМИ ВО ОДРЖУВАЊЕ РЕД НА НИВНИТЕ ПЛАТФОРМИ

Иако е неоспорно дека комапаниите-социјални медиуми треба да имаат право да одржуваат ред на своите платформи и да утврдат стандарди на заедницата, кога станува збор за тероризам, социјалните медиуми де факто постапуваат како регулатори коишто може да го ограничат слободниот говор на нивните платформи без да имаат обврски согласно меѓународното право за човекови права. Освен тоа, социјалните медиуми се изложени и на растечки притисок од државите да го отстранат од своите платформи секој насилен говор што поттикнува, велича или брани тероризам.

Следствено на тоа, овие социјални медиуми ги ажурираа стандардите на заедницата за да ги исполнат овие итни барања на државите, што честопати доведува до двосмислени прописи.

„Фејсбук“, на пример, не дозволува ниту една организација или поединец коишто се замешани во терористичка активност да бидат присутни на „Фејсбук“. Терористичките организации се дефинираат како „кои било организации што не се дел од државниот систем и кои учествуваат во планирани насилни акти насочени против лицата или имотот со цел да се заплашат цивилното население, владата или меѓународните организации за да се постигнат политички, религиски или идеолошки цели. Терористичките акти се дефинираат како планирани насилни акти насочени против лицата или имотот, извршени од чинител,кој не е дел од државниот систем со цел да се заплашат цивилното население, владата или меѓународните организации за да се постигнат политички, религиски или идеолошки цели.

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

Наспроти ова, „Твитер“ во своите правила не се осврнува на тероризмот. „Твитер“ забранува содржина со омраза која промовира насилство или директно ги напаѓа или им се заканува на други луѓе врз основа на раса, етничка припадност, национално потекло, сексуална ориентација, род, родов идентитет, религиска припадност, возраст, попреченост или сериозна болест. Освен тоа, „Твитер“ забранува величање насилство на неговата платформа, како и насилни закани. Примери за величање насилство се масовни убиства, терористички напади, силувања и сексуални напади.

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

Откритијата на Сноуден покажаа дека агенциите за разузнавање рутински се приклучуваат на приватна комуникација и ја следат незаконски. Со други зборови, кога станува збор за националната безбедност, нема вистинска основа која ќе го поддржи владеењето на правото, иако сепак постојат барем основни начела кои би можеле да бидат основа на тој суштински дел од универзалниот систем на човекови права. Со оглед на зголемената соработка меѓу органите за спроведување на законот и службите за разузнавање и безбедносните служби, ова слабеење на владеењето на правото се заканува да се прошири кај полициските службеници и обвинителите. Отсуството

на јасни законски рамки во оваа сфера, како на национално така и на меѓународно ниво, претставува дополнителна закана за владеењето на правото на Интернет и во глобалната дигитална средина.

Начелото на владеење на правото наидува на предизвици и во контекст на меѓународното право, затоа што постои тенденција на придвижување кон доброволни, необврзувачки и ад хок правила и регулациски рамки според кои се раководи однесувањето на чинителите од безбедносниот сектор во рамки на киберпросторот. (За преглед на постојните меѓународни и регионални правни рамки видете во Поглавје 3.).

СЛУЧАЈ ЗА АНАЛИЗА: ПРИВАТИЗИРАНО СПРОВЕДУВАЊЕ НА ЗАКОНОТ ВО КИБЕРПРОСТОРОТ

Фактот дека Интернет и глобалната дигитална средина се во голема мера контролирани од приватни субјекти (особено, но не исклучиво корпорации од САД), исто така претставува закана за владеењето на правото. Таквите приватни субјекти може да наметнат (и да бидат „поттикнати“ да наметнат) ограничувања на пристапот до информации без да подлежат на ограничувањата од уставот или од меѓународното право кои важат за ограничувањата на државата врз правото на слобода на изразување. На овие приватни субјекти може да им биде наложено од страна на домашните судови, кои постапуваат по барање на други приватни субјекти, да вршат високоинтрузивни анализи на нивните податоци за да најдат веројатни (или можни) повреди на правата на приватна сопственост, честопати правата на интелектуална сопственост.

Ним може да им биде наложено да „извлечат“ податоци, вклучително државни, деловни и лични податоци, од сервери во други земји, за целите на спроведување на законот или за целите на националната безбедност, без да се добие согласност од другата земја, или од компаниите или субјектите на податоци во другата земја, што претставува повреда на суверенитетот на другата земја, повреда на деловната тајна на која имаат право компаниите и повреда на човековите права на субјектите на податоци.

Одговорноста на компаниите-социјални медиуми („посредничка одговорност“) треба да се толкува мошне тесно. Со други зборови, треба многу внимателно да се оценува дали и кога платформите, како што се „Гугл“, „Фејсбук“ и „Јутуб“, ќе одговараат за содржината што нивните корисници ја поставуваат на нивните платформи, затоа што тоа може да има директен ефект врз слободата на изразување и другите човекови права. Меѓутоа, државите низ светот сè повеќе ги притискаат овие компании да наметнат построга контрола над содржината, со што се поттикнува клима на „самоцензура“.

ПРИМЕРИ ЗА ДОБРИ ПРАКТИКИ

Принципите од Манила за посредничка одговорност предвидуваат дека „од посредниците не смее да се бара да ја ограничат содржината, освен во случај кога е издаден налог од независен и непристрасен судски орган којшто утврдил дека предметниот материјал е незаконски“. Принципите од Манила, исто така, се залагаат да бидат обезбедени „докази доволни за да се документира правната основа на налогот“ пред која било содржина да биде ограничена од посредникот. Понатаму, Принципите од Манила ја истакнуваат важноста на вградувањето транспарентност и отчетност во законите, при што се напоменува дека државите не смеат да користат вонсудски мерки за ограничување на содржината, што вклучува паралелен притисок за правење промени во условите за користење на услугата, за промовирање или спроведување на таканаречени „доброволни“ практики и за обезбедување договори за ограничување на трговијата или за ограничување на јавното ширење на содржината.

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

Во аргентинскиот Нацрт-закон за посредничка одговорност е пропишано дека „давателите на интернет-услуги нема да одговараат за содржина создадена од трети лица, освен во случај кога биле уредно известени со судски налог дека треба да отстранат или блокираат одредена содржина“.

(Извор: 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/)

ГЛАВНИ НАОДИ

- Пристапувањето кон безбедноста од аспект на управувањето е корисно затоа што истакнува како низа државни и недржавни чинители ги остваруваат своите овластувања и надлежности во однос на безбедноста, формално и неформално, како и на меѓународно, национално и локално ниво.
- Управувањето е сеопфатен термин којшто генерално може да се примени кај безбедноста за да се објасни како меѓународните, националните и локалните чинители играат улога во обликувањето на решенијата за безбедноста и во нивното спроведување.
- Начелата за добро УБС се: отчетност, транспарентност, владеење на правото, учество, одговорност, ефективност и ефикасност.
- Покрај тоа, доброто УБС се заснова врз идејата дека безбедносниот сектор треба да се придружува до истите стандарди за обезбедување јавни услуги како и давателите на услуги во другите сектори.
- Доброто УБС е збир на начела, па затоа, истите основни начела на добро управување се применуваат различно во секој безбедносен сектор.
- Воспоставувањето добро УБС е прашање на постојано приспособување, затоа што безбедносните закани континуирано се менуваат.
- УБС ја подобрува способноста на безбедносниот сектор за обезбедување безбедност на државата и на нејзините граѓани.
- УБС ја прави поефикасна употребата на јавни ресурси во безбедносниот сектор.
- УБС ја намалува можноста за корупција преку подобрување на надзорот и професионализмот.
- УБС ја штити професионалната независност на вработените во безбедноста за да можат тие успешно да ги исполнуваат своите легитимни задачи, ги подигнува професионалните стандарди, ја зголемува отчетноста и ја намалува злоупотребата на населението.
- УБС промовира обезбедување инклузивна безбедност и еднакви можности во рамки на безбедносниот сектор.
- УБС спречува конфликти преку промовирање единство, политичка неутралност, еднаквост и професионализам во рамки на безбедносниот сектор.

БИБЛИОГРАФИЈА

Информативен документ на DCAF за реформата во безбедносниот сектор. Примена на начелата за добро управување во безбедносниот сектор. Достапно на https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_1_Security_Sector_Governance_EN.pdf

Информативен документ на DCAF за реформата во безбедносниот сектор. Примена на начелата за добро управување во безбедносниот сектор. Достапно на https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_2_Security%20Sector%20Reform.pdf

DCAF. Меѓународен советодавен тим во безбедносниот сектор, Реформа на безбедносниот сектор во кратки црти. Прирачник за воведна обука за реформа на безбедносниот сектор. Достапно на: https://issat.dcaf.ch/download/2970/25352/ISSAT%20LEVEL%201%20TRAINING%20MANUAL%20-%20SSR%20IN%20A%20NUTSHELL%20-%205.3.pdf

DCAF-ISSAT. Вовед во реформа на безбедносниот сектор, Бесплатен курс за е-учење достапен на веб-страницата на Заедницата за практикување на DCAF-ISSAT: http://issat.dcaf.ch

HHeiner 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).

Глобален форум за киберекспертиза, Подигнување на свеста за кибербезбедноста со градење доверба преку транспарентност. Достапно на: 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), Достапно на: https://onlinelibrary.wiley.com/doi/full/10.1111/capa.12243

ПОГЛАВЈЕ 2

КАКО КИБЕРПРОСТОРОТ И КИБЕРБЕЗБЕДНОСТА СЕ ПОВРЗАНИ СО ДОБРОТО УПРАВУВАЊЕ СО БЕЗБЕДНОСНИОТ СЕКТОР

ЦЕЛИ

Целта на ова поглавје е учесниците подобро да се запознаат со поимите киберпростор и кибербезбедност. Поточно, поглавјето има цел да го зголеми знаењето на учесниците за киберпросторот и за кибербезбедноста, како и да ја истакне комплексноста на спроведувањето практики за добро управување со безбедносниот сектор (УБС) во овие полиња.

Целите за учење за ова поглавје се следните:

- Зголемено знаење за киберпросторот како медиум од аспект на опсегот, чинителите и ризиците.
- Зголемено знаење за кибербезбедноста и нејзиното влијание врз човековата безбедност, националната безбедност и врз обезбедувањето услуги.
- Создавање разбирање за ограничувањата и начинот на кој практиките на УБС може да се спроведуваат во контекст на киберпросторот.

1. Вовед

Како што е наведено во претходното поглавје, добрите практики на УБС имаат суштинско значење за промовирање ефективна и одговорна средина во која се почитуваат човековите права и владеењето на правото. Со оглед на тоа дека безбедносниот сектор го сочинуваат истовремено државни и недржавни чинители, начелата за добро УБС треба да се протегаат и надвор од она што се исклучиво државни практики.

Доброто УБС во рамки на киберпросторот претставува релативно нов концепт кој има длабоко влијание, како врз владите така и врз обичните граѓани. Бидејќи киберпросторот и активностите и услугите во него станаа составен дел од секојдневниот живот, заштитата на податоците и на информациите во неговите рамки има витално значење.

И покрај тоа, а можеби и поради неговата разновидна употреба, концептот на киберпростор и разните негови компоненти не се добро дефинирани. За да му се пристапи најдобро на прашањето на доброто УБС во рамки на киберпросторот, неопходно е поконцизно сфаќање за тоа што се подразбира под „киберпростор“ и „кибербезбедност“.

Што е киберпростор?

Природата на киберпросторот како апстрактен концепт, кој навидум не е заснован врз физичкиот свет, доведе до нејаснотии во однос на тоа што се подразбира под овој поим.

Честопати организациите и државите го дефинираат киберпросторот на начин којшто најмногу им одговара на целта или на намената за која се користи. Често овие дефиниции се насочени кон безбедноста, милитаризацијата или ранливостите присутни во рамки на киберпросторот, при што секоја организација, нација и група истакнува различни аспекти. Меѓутоа, има заедничка тема што се провлекува низ повеќето дефиниции: киберпросторот е средина создадена истовремено од физички и од виртуелни компоненти, каде се складираат, менуваат или разменуваат податоци, информации или комуникација.

Додека Интернет е можеби најчестата и најлесно пристапната форма на киберпростор за обичниот граѓанин, тој е далеку од негов единствен аспект.[1] Киберпросторот ги вклучува сите компјутерски базирани мрежни системи за горенаведените цели

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

на складирање, менување или разменување[2], како оние што може да се најдат кај сè повеќе часовници, апарати и други предмети поврзани во киберпросторот (познат и како „Интернет на нешта“ – IoT). Земени заедно, овие различни текови на податоци и информации ја сочинуваат „виртуелната“ структура што се нарекува киберпростор.

Киберпросторот е глобално поле, исполнето со ресурси, информации и можности. Тоа прерасна во составен дел од секојдневниот живот во таа мера што во 2016 година Советот за човекови права на Обединетите нации изјави „дека истите права што луѓето ги имаат офлајн, мора да се заштитат и онлајн, особено слободата на изразување, која се применува без оглед на границите и во рамки на сите медиуми по сопствен избор, во согласност со членовите 19 од Универзалната декларација за човекови права и Меѓународниот пакт за граѓанските и политичките права“ [3].

Киберпросторот има и свои физички аспекти, како што се статичните и преносните компјутери, таблетите и паметните телефони, како и серверите и физичките кабли што ја сочинуваат инфраструктурата на Интернет. Киберпросторот како медиум овозможува активности кои честопати наликуваат на активностите од физичкиот свет: луѓето го користат киберпросторот за комуникација едни со други, за трговија, истражување, рекреативни активности, како и за да бидат во тек со најновите случувања. Меѓутоа, секое користење на киберпросторот не е толку наивно: овој ист медиум може да послужи како простор за криминални активности, воени напади и за други злонамерни дејства

.

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. Достапно на: https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf

3 Унапредување, заштита и уживање на човековите права на Интернет. 32-ра сесија на Советот за човекови права (27 јуни 2016 г.), A/HRC/32/L.20.

Дефинирање на поимот киберпростор
Некои примери на дефиниции за киберпростор кои моментално се користат:

Меѓународна унија за телекомуникации
Киберпросторот е средина во која се одвива комуникација преку компјутерски мрежи. И скоро сите на еден или друг начин се поврзани на нив.

Меѓународна организација за стандардизација
Комплексна средина што се јавува како резултат на интеракција на луѓе, софтвер и услуги на Интернет со помош на технолошки уреди и мрежи поврзани на него, којашто не постои во никаков физички облик.

Европска Унија
Киберпросторот е временски зависен збир од опипливи и неопипливи средства со кои се складираат и/или пренесуваат електронски информации.

Јужна Африка
„Киберпростор“ подразбира физички и нефизички простор создаден и/или сочинет од некои, или пак од сите следни компоненти: компјутери, компјутерски системи, мрежи и нивни компјутерски програми, компјутерски податоци, содржински податоци, податоци за сообраќај и корисници.

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

ПРИМЕР ЗА ДОБРА ПРАКТИКА

На почетокот на 21 век Франција ја имаше една од најниските стапки на влез на Интернетот и компјутерите од сите земји на Европската Унија. Но денес најголем дел од населението учествува во киберпросторот. Со цел понатамошно зголемување на пристапноста и лесното користење на киберпросторот, Франција ја активираше „Très Haut Débit“, нова иницијатива за промовирање пристап до Интернет со голема брзина, особено за руралните средини и оние средини кои не се доволно поврзани. Преку партнерства со јавни и приватни групации, Франција се стреми да достигне 100 % покриеност со брз Интернет и да им обезбеди дигитален пристап на сите граѓани до 2022 година.

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

Иако постојат некои заеднички елементи во различните институционални дефиниции за киберпростор, непрецизната природа на сите овие дефиниции им овозможува на чинителите во рамки на киберпросторот да ги обликуваат аспектите на дефиницијата на начин што најмногу им одговара на нивните потреби и којшто најдобро ги оправдува нивните постапки. Тоа особено може да се забележи кога се опишува како најдобро да се искористи или заштити медиумот. Дефинициите, исто така, укажуваат на начинот на кој државите гледаат на киберпросторот, односно како алатка за воени цели, платформа од која се дистрибуираат услуги или пак како арена за трговија и комуникација.

За нашите цели, киберпросторот ќе го дефинираме како: глобална вмрежена средина во која се разменуваат, складираат и менуваат податоци и информации и до која имаат пристап државни и недржавни чинители.

Користење и авторитет во киберпросторот

Со оглед на разноликиот карактер на киберпросторот, сосем е логично намената и корисниците да бидат еднакво разновидни како и самиот медиум. Како актери истовремено се вклучени државни и недржавни чинители. Државите го користат киберпросторот за организирање избори и за обезбедување услуги на своите граѓани, но и како алатка за заштита на националната безбедност и на националните витални интереси.[4] Групата недржавни чинители опфаќа од компании, па сè до граѓани, при што сите го користат киберпросторот за различни цели. Сите овие чинители придонесуваат за влијание и обликување на киберпросторот.

Глобалната природа на киберпросторот, исто така, создава ограничувања за владите во однос на неговата регулација и управувањето. Иако зголемувањето на кибербезбедноста како дел од националната безбедносна политика е важно, поддршката за добро УБС во киберпросторот ќе има значителни ефекти и врз економската и човековата безбедност.[5] Како што светот станува позависен од услугите и слободата што се даваат во киберпросторот, заштитата на човековите права и на човековата безбедност, како и на националната безбедност, станува сè поголем императив[6] .

4 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.

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

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

СЛУЧАЈ ЗА АНАЛИЗА: ОБЕЗБЕДУВАЊЕ НА ФИЗИЧКАТА КОМПОНЕНТА

Неодамна беа направени напори за зголемување на безбедноста на компјутерските уреди, како што се лаптопите, таблетите и паметните телефони. Европската Унија и нејзините земји членки, како и САД, започнаа да вршат притисок врз технолошките производители за обезбедување безбедност на нивните производи.

Во 2016 година Министерството за внатрешна безбедност на САД објави неколку стратегиски начела насочени кон обезбедување на Интернетот на нешта. Првата фаза од овој пристап е да се обезбедат уредите при нивното производство, а потоа безбедноста да се одржува преку ажурирања и управување со ранливоста.

Обединетото Кралство создаде „кодекс на безбедносни практики“ за производителите, за да ги охрабри да ја зголемат безбедноста на уредите во фазата на нивната изработка. За да се зголеми безбедноста на самите уреди, кодексот повикува уредите кои се дел од Интернетот на нешта да имаат поуникатни барања во однос на лозинката, како и да се стремат кон поголема транспарентност во случај на повреда на безбедноста преку поттикнување на јавно објавување на сите ранливости на уредите. Моментално овој кодекс е врз доброволна основа, но Обединетото Кралство не ја отфрла можноста да го направи да биде задолжителен за уредите произведени во земјата.

Иако пристапот на ЕУ кон зголемување на безбедноста на уредите сè уште е во изработка, тој ќе предвидува процес на сертификација на уредите од Интернетот на нешта на ниво на ЕУ.

Сите овие пристапи имаат цел да ги охрабрат другите држави да развијат свои сопствени пристапи и политики за обезбедување на уредите поврзани во киберпросторот.

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

Кибербезбедност

Со сè помасовното користење на киберпросторот од страна на владите, поединците и компаниите, количеството чувствителни податоци и информации во рамки на киберпросторот експоненцијално расте и е изложено на нови ранливости кои постојано се менуваат.[7] Ефективната заштита на овие информации има суштинско значење заради создавање безбедна средина во рамки на киберпросторот и надвор од него. Кибербезбедноста, како што кажува и самото име, се состои од практики и методи за обезбедување на податоците, информациите и на целокупноста

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

на различните компоненти од киберпросторот, кои ги вклучуваат, но не се ограничени на физичките аспекти на медиумот.[8]

Иако кибербезбедноста честопати се поврзува со стратегии за национална безбедност, важно е да се гледа поширокатa примена на поимот. Меѓународната унија за телекомуникации (ITU) ја опишува кибербезбедноста како алатка, насоки и други пристапи за заштита на целосноста и на доверливата природа на киберпросторот за приватните организации, владата и за граѓанското општество[9].

Во согласност со растечката важност на киберпросторот за професионалните, рекреативните и политичките активности, кибербезбедноста е развојно поле во доменот на безбедноста и доброто управување со безбедносниот сектор. Нормите поврзани со безбедноста во киберпросторот постепено се развиваат со цел да одговорат на брзото ширење на практики и техники во полето на кибербезбедноста, како и на чинителите во ова поле кои постојано се менуваат.[10] Додека државите изработуваат национални пристапи за обезбедување посигурен киберпростор во рамките на својата територија, се јавуваат одредени норми во однос на обемот на нивните овластувања врз киберпросторот, како и во однос на начинот на кој државите може да остваруваат надлежност врз киберпросторот[11] .

Мерење на кибербезбедноста

Со оглед на големиот број конкурентни дефиниции за киберпростор и кибербезбедност, анализирањето на кибербезбедноста не е лесен потфат. Меѓународната унија за телекомуникации го создаде Глобалниот индекс на кибербезбедност за да ја утврди посветеноста на нејзините земји членки кон зголемување на кибербезбедноста. Со овој индекс се оценуваат пет различни аспекти на кибербезбедноста, имено правниот, технолошкиот, организацискиот, оној за градење капацитети и оној за соработка, за да се увиди посветеноста на секоја земја.
Иако ова е добра алатка за утврдување на одговорот и на активностите на државата во однос на управувањето со киберпросторот, таа ја занемарува улогата на недржавните чинители, како во киберпросторот така и во кибербезбедноста. Бидејќи оценува политики, а не практики, таа не ги зема предвид практичните влијанија или ефикасноста на овие заложби.

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

9 ITU vodič za razvoj NCSS, 13.

10 M“International Cybersecurity Norms”, Microsoft Policy Papers Microsoft. Достапно на: https://www.microsoft.com/en-us/cybersecurity/content-hub/international-cybersecurity-norms-overview

11 IBID.

2. УБС во киберпросторот

Киберпросторот претставува збир на слободи, ограничувања и комплексности кои се уникатни за природата на медиумот како таков. Со оглед на широкиот дијапазон на чинители во рамки на киберпросторот и начинот на кој тој може да биде искористен или злоупотребен, процесот на создавање рамка на добри практики за УБС наидува на најразлични пречки од потрадиционалната „територијална“ безбедност. Некои од овие пречки беа анализирани во последното поглавје, особено оние поврзани со слабеење на владеењето на правото, транспарентноста и отчетноста.

При разгледување на УБС низ призмата на киберпросторот, важно е да се имаат предвид различните чинители во областа, да се оцени кој има контрола врз кои аспекти од киберпросторот, и како најдобро да се влијае или да се поттикнат поведенија и практики кои, во крајна линија, би го зајакнале доброто УБС во доменот на киберпросторот. Широкиот дијапазон на чинители во киберпросторот и во кибербезбедноста создава интересна парадигма која творците на политики треба да ја истражуваат, затоа што државата не е во можност едностранo да обезбеди ефективна безбедност и регулација на медиумот.

Добра практика: Спроведувајте пристап кон кибербезбедноста што ќе вклучува чинители и од јавните и од приватните сектори во киберпросторот

Бидејќи киберпросторот е платформа, како за јавни така и за приватни чинители, создавањето и спроведувањето различни политики што влијаат врз УБС треба да вклучуваат субјекти кои постојат надвор од јавната сфера. Важен чекор кон создавање побезбедна киберсредина е препознавањето на улогата што компаниите за информациски и комуникациски технологии и приватните корпорации за кибербезбедност ја имаат во формирањето и заштитата на правата и безбедноста на корисниците.

ПРИМЕРИ ЗА ДОБРИ ПРАКТИКИ

Владата на Камерун работи со повеќе партнери од приватниот сектор на прашања поврзани со кибербезбедноста и има воспоставено работни односи со други земји за управување и одговор на киберзакани. Како најистакнат пример, во случајот на една онлајн измама која вклучуваше фармацевтска компанија, заедно со Чешката Република, ИНТЕРПОЛ и Нигерија, Камерун спроведе дигитални истраги. Камерунските власти промовираат неколку мерки за градење доверба и договори за меѓународна соработка во киберпросторот преку размена на информации за киберинциденти и најдобри практики за кибербезбедност.

Trenutni problemi sa USB u sajber prostoru

Добрите практики на УБС во киберпросторот може да помогнат за понатамошно почитување и заштита на човековата безбедност, владеењето на правото и другите аспекти на добро управување во рамки на киберпросторот.

Како што накратко беше споменато во последното поглавје, еден од предизвиците со кои се соочува полето на управување со безбедносниот сектор во киберпросторот е недостигот на разбирање за тоа како да се воспостават начела за ефективно управување во киберпросторот, што резултира со несоодветни политики и несоодветна регулација, како и со создавање поволна средина за криминални активности.[12] ОНедостигот на знаење може да влијае и врз ефективното регулирање на чинителите од приватниот сектор од страна на државата, на тој начин поткопувајќи ја способноста на државата да усвои добри практики за УБС во киберпросторот.

Моментално голем број безбедносни услуги во киберпросторот се обезбедуваат од приватни комерцијални субјекти, со што се создаваат предизвици за ефективно спроведување практики на УБС во киберпросторот. Еден од аспектите на доброто управување кој на државите им е сè потешко да го спроведат, е транспарентноста. Како прв предизвик, дефиницијата за транспарентност во киберпросторот од аспект на доброто УБС не е усогласена. Меѓутоа, концептот на транспарентност во овој контекст сè повеќе се поврзува со обелоденување на тоа кога и во кој обем имало упад во информациските системи[13]

СЛУЧАЈ ЗА АНАЛИЗА: НАЛОЖУВАЊЕ ТРАНСПАРЕНТНОСТ

Австралија

Во 2017 година, австралискиот парламент донесе измена на Законот за приватност од 1998 година, со која им се наложува на владините служби од Комонвелтот, на организациите од приватниот сектор и на други утврдени тела да споделуваат информации за случаи на повреда на кибербезбедноста со оние кои биле засегнати од таквата повреда. Непочитувањето на овој нов пропис би резултирало со обврска за исплата на паричен надомест на оние кои биле погодени од таквата повреда, јавно признавање и извинување за непочитувањето и големи граѓански казни за оние кои имале повеќе случаи на непочитување на овој пропис.

Извор: BBen Allen, “Australia: Cybercrime – New Mandatory Data Breach Reporting Requirements” mondaq www.mondaq.com. Достапно на: http://www.mondaq.com/australia/x/573188/Security/Cybercrime+New+Mandatory+Data+Breach+Reporting+Requirements

Соединети Американски Држави

Комисијата за хартии од вредност и берза на САД му изрече висока парична казна од 35 милиони американски долари на „Jaxy“ поради необелоденување информации за кибернапад со кој биле засегнати над 500 милиони сметки. Ова е прв случај да ѝ се изрече парична казна на компанија поради непочитување на обврските за обелоденување информации кои важат за компании котирани на официјалниот пазар.

Извор: Kadhim Shubber, “Yahoo’s $35m Fine Sends a Message”, Financial Times, www.ft.com. Достапно на: https://www.ft.com/content/4c0932f0-6d8a-11e8-8863-a9bb262c5f53

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

13 Види, на пр., ICANN Organization’s Cybersecurity Transparency Guidelines (2018). Достапно на: https://www.icann.org/en/system/files/files/cybersecurity-transparency-guidelines-03aug18-en.pdf

Поттикнувањето или наложувањето чинителите да ги обелоденуваат случаите на повреда на кибербезбедноста е еден од начините на кои државата може да ги зголеми практиките на добро УБС, затоа што со тоа не само што се зголемува транспарентноста во киберпросторот туку и се надополнуваат пропустите во актуелните практики на кибербезбедност. Со тоа, пак, се помага во спречување на ширењето кибернапади и се подобруваат безбедносните практики во киберпросторот. Недостигот на транспарентност во однос на кибернападите во голема мера ја поткопува човековата безбедност во рамки на киберпросторот, зашто може да предизвика поголем број жртви од злонамерните кибернапади.

Транснационалната природа на киберпросторот, исто така, создава дилема за државите од аспект на воспоставувањето практики на добро УБС во рамките на тој простор. Со оглед на тоа дека граѓаните учествуваат во трансакции кои постојано ги преминуваат меѓународните територијални граници, во голема мера се намалува способноста на државата да остварува надлежност врз она што го засега нејзиното население. Во најголем дел од случаите, државите мора да се потпираат на комерцијални посредници – како што се платформите на социјалните медиуми – за надгледување и регулирање на однесувањето онлајн.[14] Ова може да ги поткопа практиките на добро УБС, затоа што државата обично нема пристап да види како информациите се филтрираат или отстрануваат. Друг предизвик е транснационалната природа на информациите на Интернет, кои може да бидат складирани на еден или на повеќе сервери лоцирани во различни територии на судска надлежност. Потпирањето на други држави за истражување, судско гонење и осудување на киберкриминалците, исто така, создава различна динамика. На овој начин, киберпросторот ги поткопува практиките на добро управување затоа што се потпира не само на чинители во рамки на една територија на судска надлежност, туку влијае врз цела низа меѓународни чинители.

СЛУЧАЈ ЗА АНАЛИЗА: МЕЃУНАРОДНИ ИСТРАГИ

Меѓународните истраги и кривични гонења во полето на кибербезбедноста не се нешто нечуено. Во април 2018 година една веб-страница која продаваше услуги за Дистрибуиран напад заради блокирање на услуга (DDoS), Webstresser.org, беше замрзната, а нејзините администратори беа обвинети за киберкриминал благодарение на меѓународната истрага спроведена од холандското Национално одделение за високотехнолошки криминал и Националната агенција за борба против криминал на Обединетото Кралство, со поддршка на многу други организации. Операцијата „Power Off“ е само еден пример за тоа како меѓународните чинители може да соработуваат во насока на создавање побезбедна киберсредина за корисниците.

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

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

Иако може да се чини дека има голем број пречки во применувањето на практиките на добро УБС во киберпросторот, тоа не е нешто невозможно. Започнаа да се конкретизираат некои меѓународни рамки и норми кои даваат насоки за тоа како УБС да се интегрира во киберпросторот. Додека практиките и политиките мора да бидат изработени така за да одговараат на националниот контекст, идентификувањето на постојните меѓународни и регионални рамки кои се релевантни за киберпросторот е клучен чекор кон добро УБС во него.

ГЛАВНИ НАОДИ

- Киберпросторот постои истовремено во физичка и во нефизичка форма и се состои од платформа преку која може да се пренесуваат, трансформираат и менуваат информации, податоци и комуникации од еден компјутер до друг. Исто така, ја опфаќа физичката инфраструктура на Интернет која се протега низ целата планета.
- Владите, граѓаните и компаниите стануваат сè позависни од можностите што ги нуди киберпросторот во секојдневниот живот.
- Има широк дијапазон на чинители во киберпросторот и во полето на кибербезбедноста.
- Постојат разни пречки за УБС во киберпросторот, од разните чинители што влијаат врз различни негови аспекти, па сè до општиот недостиг на знаење во однос на безбедното користење на киберпросторот.
- Иако некои држави имаат воспоставено политики и рамки за управување со кибербезбедноста и киберпросторот, општото непознавање на темата го отежнува обезбедувањето на правилно спроведување на практиките за УБС во киберпросторот.

Библиографија

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

Elkin-Koren, Niva, and Eldar Haber, Governance by Proxy:Cyber Challenges to Civil Liberties, 82 Brook. L. Rev.105 (2016)

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, 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

ПОГЛАВЈЕ 3
МЕЃУНАРОДНИ И РЕГИОНАЛНИ ПРАВНИ РАМКИ ВО КИБЕРПРОСТОРОТ

ЦЕЛИ

Целта на ова поглавје е да им обезбеди на корисниците увид во меѓународните и регионалните правни рамки што се применуваат во киберпросторот, а истакнува интересни и иновативни пристапи и иницијативи.

Целите за учење за ова поглавје се следните:

- Зголемено знаење за различните меѓународни и регионални организации кои се занимаваат со киберпросторот и кибербезбедноста.
- Зголемена свесност за расположливите ресурси со кои се помага спроведувањето на меѓународните и регионалните правни рамки на национално ниво.
- Зголемено знаење за киберкриминалот, кибертероризмот и користењето на Интернет за терористички цели.

Вовед

Ефективните правни рамки – на меѓународно, регионално и на национално ниво – се еден од столбовите на доброто владеење и претставуваат предуслов за начелото на владеење на правото. Генерално, правните рамки имаат суштинско значење за уредување на законитото однесување и за забрана или криминализирање на незаконитите дејства. Правните рамки во киберпросторот се важни и за да се обезбеди почитување на човековите права.

Се разви голема дискусија и конфузија за тоа како правните рамки може да се применуваат и како се применуваат во киберпросторот. Поради својата прекугранична природа фокусирана на информации, киберпросторот создава предизвици за државноцентричните пристапи на владеење. Од една страна, физичката инфраструктура што го сочинува киберпросторот подлежи на национална јурисдикција и надлежност. Од друга страна, протокот на податоци и информации низ инфраструктурата постојано преминува низ (повеќе) територијални јурисдикции, што ја отежнува можноста една правна јурисдикција да врши „ефективна контрола“ врз овој проток на информации. Поради тоа, многумина повикуваат на изработка на нови нормативни режими за регулирање на киберпросторот.

Денес е неоспорно дека начелата на меѓународното право се применливи во киберпросторот. Она што не е толку јасно е како овие начела се преточуваат во практика. Следствено на тоа, овој јаз помеѓу политиката и практиката доведува до правни несигурности, па и до правни нејасности кои може да ја поткопаат заштитата на човековите права на корисниците на Интернет. Оттука, меѓународните и регионалните организации се заложија да започнат иницијативи преку кои ќе се идентификува и протолкува како постојните правни начела на меѓународното право се применуваат во киберпросторот.

1. Меѓународни правни и регионални рамки

Голем број иницијативи на меѓународно и регионално ниво имаат цел да промовираат поодговорно однесување во киберпросторот и да развијат регулациски рамки и мерки за градење доверба во киберпросторот. Во продолжение е даден преглед на голем дел од овие иницијативи.

Обединетите нации

Моментално не постои правно обврзувачки инструмент на меѓународно ниво со кој се уредува однесувањето во рамки на киберпросторот. Меѓутоа, има одреден

број иницијативи во форма на „меко право“ (кои правно не се обврзувачки) со кои се идентификуваат норми во киберпросторот и им се даваат насоки на државите во однос на примената на овие норми.

Денес е неоспорно дека меѓународното право – особено Повелбата на Обединетите нации, меѓународното право за човекови права и меѓународното хуманитарно право – се применуваат во киберпросторот.

СЛУЧАЈ ЗА АНАЛИЗА: ИЗВЕШТАЈ НА ГРУПА ВЛАДИНИ ЕКСПЕРТИ НА ОН

Извештајот од 2015 година на Групата владини експерти на ОН ги наведува следниве препораки за одговорно однесување на државите за да придонесат кон отворен, безбеден, стабилен, пристапен и мирољубив киберпростор:

Позитивни норми:

- Државите треба да соработуваат за да ги зголемат стабилноста и безбедноста во користењето на ИКТ и за да спречат штетни практики во полето на ИКТ.
- Државите треба да ги земат предвид сите релевантни информации во однос на атрибуција во средината на ИКТ.
- Државите треба да преземат соодветни мерки за заштита на националната критична инфраструктура од закани кон ИКТ, како и да одговорат на соодветните барања за помош од други држави.
- Државите треба да преземат разумни чекори за да обезбедат сигурност на синџирот на снабдување и треба да го спречат ширењето злонамерни алатки и техники на ИКТ.
- Државите треба да поттикнат одговорно известување за ранливостите на ИКТ и да споделуваат информации поврзани со тоа.

Ограничувачки норми:

- Државите не треба свесно да дозволат нивната територија да се користи за меѓународно противправни дејства со користење на ИКТ.
- Државите треба да се придржуваат до резолуциите на Генералното собрание на Обединетите нации поврзани со човекови права.
- Државите не треба да вршат или свесно да поддржуваат активност во полето на ИКТ која е спротивна на нивните обврски од меѓународното право.
- Државите не треба да вршат или свесно да поддржуваат активност со која им се наштетува на информациските системи на овластените тимови за одговор во итни ситуации.

Обединетите нации, на пример, од 2004 година имаат формирано шест последователни Групи владини експерти (UN GGE) – врз основа на „рамномерна географска распределба“ и со вклучување клучни „кибер-велесили“, какви што се Соединетите Американски Држави, Кина, Русија, Франција, Обединетото Кралство и Германија – со цел да се предложат норми за одговорно однесување во киберпросторот.

СЛУЧАЈ ЗА АНАЛИЗА: МЕШАЊЕ ВО ИЗБОРИТЕ ПРЕКУ ОНЛАЈН ИНФОРМАТИВНИ КАМПАЊИ – ПРЕДМЕТ ЗА МЕЃУНАРОДНО ПРАВО?

Додека мешањето во политичките процеси служејќи се со прикриени и неприкриени средства не е ништо ново во меѓународните односи, од 2016 година владите, првенствено во западните земји, изразуваат загриженост за мешањето во изборните процеси преку насочени кибероперации и кампањи за дезинформирање.

Во 2014 година, цел на операцијата „CyberBerkut“ беше украинската Централна изборна комисија, при што делови од мрежите на Комисијата беа соборени во период од скоро дваесет часа и беше прогласен лажен победник на денот на изборите. Во 2016 година, хакерската единица „Fancy Bear“ ги имаше за своја цел системите на германскиот Бундестаг, германските министерства за надворешни работи и за финансии, како и на Христијанско-демократската унија. Во 2017 година беше спроведена кибероперација чија цел беше вметнување злонамерен софтвер на веб-страницата на кампањата на Емануел Макрон за француските претседателски избори.

Согласно обврските од меѓународното право, веројатно е дека овие операции претставуваат повреда на суверенитетот на државата. Суверенитетот општоприфатено се сметаше за начело и за примарно правило на меѓународното право – што беше одразено и во Извештајот на Групата владини експерти на ОН од 2015 година.

„Државниот суверенитет и меѓународните норми и начела кои произлегуваат од суверенитетот важат за вршењето активности поврзани со ИКТ од страна на државите и за нивната јурисдикција над инфраструктурата за ИКТ во рамки на нивната територија“.

Генерално, целта и намената на начелото за суверенитет е „да им се овозможи на земјите целосна контрола врз пристапот и активностите на нивна територија“.

Што значи ова за мешањето во изборите преку кибероперации?

Експертите сметаат дека клучна точка при оценувањето дали таквото дејство претставува повреда на начелото на суверенитет „не е постоењето на врска помеѓу таргетираниот систем и изборите, туку самиот факт дека операцијата резултирала со оштетување на средството – губење на функционалност“. Според „Прирачникот од Талин 2.0“, дејства кои може

да се квалификуваат како повреда на суверенитетот се: кибероперација која предизвикува киберинфраструктурата или киберпрограмите да функционираат различно; менување или бришење податоци зачувани во киберинфраструктурата без да се предизвикаат физички или функционални последици, како што се опишани погоре; вметнување злонамерен софтвер во системот; поставување задни врати; и предизвикување привремена, но значителна загуба на функционалноста, како што е во случајот на поголема операција на дистрибуиран напад заради блокирање на услуга.

Важен напредок беше направен во 2013 година, кога Групата владини експерти на ОН, којашто тогаш се состоеше од само петнаесет члена, усвои консензуален извештај со кој се потврди применливоста на меѓународното право во киберпросторот. Консензуалниот извештај на Групата од 2015 година го реафирмираше тоа тврдење и дополнително ја прецизираше нормативната рамка за користењето на киберможностите од страна на државата. Од особен интерес во оваа насока е делот насочен кон „норми, правила и начела за одговорно однесување на државите“.

ИНФОРАМКА: АНОНИМНОСТ НА ИНТЕРНЕТ

Анонимноста е фундаментална за заштита на човековите права. Со создавањето на Интернет стана јасно дека важноста на анонимноста не може да се ограничи само на слободата на луѓето да комуницираат едни со други, да разменуваат информации и идеи, туку и да се заштитат луѓето од непотребна и несоодветна контрола. Меѓутоа, правото на онлајн анонимност досега доби само ограничено признание во рамки на меѓународното право. Традиционално, заштитата на анонимноста онлајн беше поврзана со заштитата на правото на приватност и лични податоци (види во член 12 од УДЧП, 17 од МПҐПП). Освен тоа, анонимноста е клучен концепт во заштитата на слободата на изразување, како и правото на приватност. Во својата најпроста форма, анонимноста подразбира да не бидеш идентификуван, и во таа смисла, таа е дел од секојдневните вообичаени искуства на повеќето луѓе, како на пример, да чекориш во толпа или да стоиш во редица со непознати. На тој начин, активноста може да биде анонимна иако е истовремено јавна.

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

За жал, Групата владини експерти на ОН за периодот 2016 – 2017 година не успеа да усвои консензуален извештај, што создаде неусогласеност во меѓународната заедница во однос на тоа како најдобро да му се пристапи на меѓународното право во киберпросторот. Меѓутоа, во октомври 2018 година Генералното собрание на ОН ја усвои Резолуцијата A/C.1/73/L.37 да формира нова Група владини експерти во 2019 година со задача да достави извештај во 2021 година, за време на 76-тото заседание на Генералното собрание на ОН. Истовремено, со резолуцијата A/C.1/73/L.27/Rev.1, Генералното собрание на ОН формираше и Отворена работна група која требаше да биде свикана во јуни 2019 година со цел да ги изработи правилата, нормите и начелата за одговорно однесување на државите во киберпросторот, како и да го разгледа нивното спроведување во практика.

Општо е прифатено дека рамката на меѓународното право за човекови права, вклучително Универзалната декларација за човекови права и Меѓународниот пакт за граѓански и политички права, се применуваат во дигиталниот простор. Тоа беше афирмирано од Советот за човекови права (HRC) во Резолуцијата A/HRC/20/L.13, каде е наведено дека „истите права што луѓето ги имаат офлајн мора да бидат заштитени и онлајн“.[1] Оваа Резолуција е особено важна затоа што првпат едно меѓународно тело експлицитно наведува дека човековите права важат и во киберпросторот.

1 Генерално собрание на Обединетите нации, Совет за човекови права за унапредување, заштита и уживање на човековите права на Интернет, A/HRC/20/L.13, 29 јуни 2012 година.

По разоткривањата на Сноуден[2] во 2015 година Генералното собрание на ОН одлучи да воспостави нов Специјален известувач за правото на приватност, со цел подобро да се осврне на приватноста во дигиталната доба и да создаде побезбедна дигитална средина. Специјалниот известувач за правото на приватност има мандат да остварува државни посети, да дава препораки и да прима индивидуални претставки.

Друга важна резолуција на Генералното собрание на ОН е Резолуцијата A/RES/57/239 за создавање глобална култура на кибербезбедност, којашто го препознава киберкриминалот како важен предизвик за кибербезбедноста.[3]

Друг инструмент на ОН којшто е релевантен за идентификување норми во киберпросторот се Насочувачките принципи за бизнис и човекови права на ОН[4] (познати и како Ruggie Principles), кои беа усвоени во 2011 година и коишто им даваат насоки на државите, како и на бизнис-заедницата, во однос на заштитата на човековите права. Насочувачките принципи се базирани врз рамката на ОН позната како „Почитувај, заштити и надомести“. Во воведниот дел на овие Насочувачки принципи се предвидува дека „улогата на деловните претпријатија како специјализирани органи на општеството кои извршуваат специјализирани функции, неопходно е да се придржуваат до сите применливи закони и да ги почитуваат човековите права“.[5]

Во контекст на регулирањето одредени видови незаконски говор на Интернет, особено говор на омраза, извештајот на Високиот комесар на ОН за човекови права усвоен од Советот за човекови права во 2013 година (познат и како „Акцискиот план од Рабат“) идентификува критериуми кои служат за препознавање говор на омраза, а може да даде насоки и во онлајн сферата.[6]

СЛУЧАЈ ЗА АНАЛИЗА: АКЦИСКИОТ ПЛАН ОД РАБАТ

Во Акцискиот план од Рабат има тест со прагови во шест дела за оценување на сериозноста на одредено изразување кое може да се смета за кривично дело. Овие шест критериуми се: контекст; говорител; намера; содржина и форма; обем на актот на говор; веројатност; вклучително неизбежност.

Во однос на елементот „контекст“, Акцискиот план од Рабат конкретизира дека контекстот е од „големо значење при оценување дали одредени изјави е веројатно да поттикнат дискриминација, непријателство или насилство кон целната група, и може да има директна поврзаност со намерата и/или причината. Анализата на контекстот треба да го смести актот на говор во рамки на социјалниот и политичкиот контекст кој бил актуелен во времето кога говорот бил извршен или раширен“.

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

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

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

4 Канцеларија на Високиот комесар за човекови права на ОН, Насочувачките принципи за бизнис и човекови права. Достапно на: https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

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

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

Разни други агенции и служби на ОН – како што се Институтот на ОН за истражување на разоружувањето (UNIDIR), Меѓурегионалниот истражен институт на ОН за криминал и правда, Канцеларијата на ОН за борба против дрога и криминал (UNODC) – се осврнуваат на прашања поврзани со кибербезбедноста, како и Работната група за борба против користењето на Интернет за терористички цели, којашто работи во рамки на Оперативната група на ОН за борба против тероризмот.[7]

Меѓународната унија за телекомуникации (ITU), агенција на ОН специјализирана за телекомуникации, се осврнува на кибербезбедноста во рамки на својот мандат. За таа цел, Меѓународната унија за телекомуникации изработува модели на закони и профили за кибербезбедност на земјите, коишто се јавно достапни, и им помага на земјите членки на ОН во изработката на ефективни нормативни рамки за киберпросторот.

СЛУЧАЈ ЗА АНАЛИЗА: ПРОЕКТ НА МЕЃУНАРОДНАТА УНИЈА ЗА ТЕЛЕКОМУНИКАЦИИ ЗА ПОДДРШКА НА УСОГЛАСУВАЊЕТО НА ПОЛИТИКИТЕ ЗА ИКТ ВО ПОТСАХАРСКА АФРИКА (HIPSSA)

Проектот HIPSSA беше иницира како резултат на барањето поднесено од организациите за економска интеграција во Африка, како и од регионалните регулаторни здруженија, до Меѓународната унија за телекомуникации и до Европската комисија за помош во усогласувањето на политиките и законодавството за ИКТ во Потсахарска Африка.

HIPSSA стана важен составен елемент во воспоставувањето глобални панафрикански усогласени политики и рамки за ИКТ.

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

Совет на Европа

Советот на Европа (CE) е составен од 47 земји членки. Неговата Конвенција за киберкриминал (позната и како Конвенцијата од Будимпешта)[8] се смета, засега, за најрелевантен меѓународен правен инструмент кој обезбедува правна рамка за справување со киберкриминалот. Конвенцијата од Будимпешта е отворена за да пристапат кон неа како земјите членки на Советот на Европа така и оние кои не се членки. До денес Конвенцијата од Будимпешта е ратификувана од 61 држава.[9] Таа е надополнета со нејзиниот Протокол за ксенофобија и расизам како дела сторени преку компјутерски системи.[10]

Важно е дека Конвенцијата од Будимпешта им овозможува на државите (i) квалификување како кривично дело на листа на напади извршени врз компјутери или со помош на компјутери, (ii) алатки за процедурално право со помош на кои

7 Канцеларија на ОН за борба против дрога и криминал (2012 г.): Користењето на Интернетот за терористички цели. Достапно на: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

8 Совет на Европа, Конвенција за киберкриминал, CETS бр. 185. Достапно на: https://www.coe.int/en/web/cybercrime/the-budapest-convention

9 Имено, Сенегал е потписник на Конвенцијата од Будимпешта. Тунис и Мароко се во процес на потпишување и ратификување на Конвенцијата од Будимпешта.

10 Совет на Европа, Дополнителен протокол на Конвенцијата за киберкриминал во однос на квалификувањето како кривично дело на акти од расистичка и ксенофобична природа извршени преку компјутерски системи, ETS бр. 189. Достапно на: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

истражувањето на киберкриминалот и обезбедувањето електронски докази во однос на кое било дело ќе бидат поефективни и ќе подлежат на заштитни механизми за владеење на правото, и (iii) меѓународна полициска и судска соработка во полето на киберкриминалот и е-доказите.

Освен тоа, Советот на Европа ја изработи Конвенцијата за заштита на поединецот во однос на автоматската обработка на лични податоци (Конвенција бр. CETS 108),[11] чија цел е да го „заштити секој поединец, без оглед на неговата националност или живеалиштето, во однос на обработката на неговите лични податоци, со што придонесува за почитување на неговите човекови права и фундаментални слободи, а особено правото на приватност“.[12]

Оваа Конвенција беше првиот законски обврзувачки меѓународен инструмент во областа на заштита на податоци. Согласно оваа Конвенција, страните се обврзани да ги преземат неопходните чекори во нивните соодветни национални законодавства за примена на начелата, со цел да се обезбеди почитување во рамки на нивната територија на основните човекови права на сите поединци во однос на обработката на лични податоци. Конвенцијата бр. 108 беше ажурирана во мај 2018 година, со цел да ги опфати најновите случувања во полето на новите технологии и заштитата на податоците. До денес, Конвенцијата е ратификувана од 53 земји, од кои дел се, а дел не се членки на Советот на Европа.[13]

Додека Конвенцијата од Будимпешта е единствената меѓународна правна рамка која го уредува киберкриминалот, борците за човекови права особено го истакнуваат фактот дека Конвенцијата од Будимпешта се базира врз претпоставката дека државите имаат воспоставено механизми за заштита на човековите права. Меѓутоа, земјите кои не се членки на Советот на Европа може ги немаат воспоставено истите механизми за заштита на човековите права.

Освен тоа, Советот на Европа нуди насоки за толкување на конвенциите и разни програми за градење капацитети, како што е програмата GLACY+ која им помага на државите во изработката на ефективно законодавство за киберпростор.[14] .

Африканска Унија

Во 2014 година Африканската Унија ја усвои Конвенцијата за кибербезбедност и заштита на лични податоци (позната и како Конвенцијата од Малабо).[15] Меѓутоа, конвенцијата сè уште не е влезена во сила, затоа што беше усвоена само од пет земји членки на Африканската Унија (Сенегал, Маврициус, Гвинеја, Намибија и Гана) и потпишана од девет земји членки. Во членот 25 (1) се вели дека „секоја земја потписничка ги усвојува законодавните и/или регулациски мерки што смета дека се ефективни за да може да ги квалификува како важни кривични дела оние кои ги засегаат доверливоста, целосноста, достапноста и опстојувањето на системите за информациски и комуникациски технологии, податоците што тие ги обработуваат и основната мрежна инфраструктура, како и ефективни процедурални мерки за следење и гонење на прекршителите. Земјите потписнички го земаат предвид изборот на јазици што се користат во најдобрите меѓународни практики“.

11 ССовет на Европа, Конвенција за заштита на поединецот во однос на обработката на личните податоци, CETS бр. 180. Достапно на: https://www.coe.int/en/web/data-protection/home

12 Совет на Европа, Модернизирана конвенција за заштита на поединецот во однос на обработката на личните податоци. Достапно на: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8

13 Конвенцијата бр. 108 беше ратификувана од Зелен ’Рт, Маврициус, Сенегал и Тунис.

14 Совет на Европа, Глобална акција против киберкриминал (GLACY). Достапно на: https://www.coe.int/en/web/cybercrime/glacy-plus

15 Конвенција на Африканската Унија за кибербезбедност и заштита на личните податоци, 27 јуни 2014 г. Достапно на: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

СЛУЧАЈ ЗА АНАЛИЗА: КОНВЕНЦИЈАТА ЗА КИБЕРБЕЗБЕДНОСТ НА АФРИКАНСКАТА УНИЈА И КОНВЕНЦИЈАТА ОД БУДИМПЕШТА

Конвенцијата од Будимпешта е моментално единствената правно обврзувачка меѓународна правна рамка на темите кибербезбедност, киберпростор, и улогата на државата во тоа поле. Иако само мал број африкански држави ја имаат директно потпишано или биле поканети да ѝ пристапат, таа служеше како рамка-водилка за создавањето на Конвенцијата за кибербезбедност на Африканската Унија. Ова е пример за тоа како пошироките меѓународни норми може да се приспособат и усвојат во регионално специфичен контекст.

Извор: '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.

Економска заедница на западноафриканските држави

Во 2010 година Економската заедница на западноафриканските држави (ЕКОВАС) го усвои Дополнителниот закон за заштита на личните податоци во рамки на ЕКОВАС,[16] којшто е под влијание на директивите на ЕУ за заштита на лични податоци. Со овој Дополнителен закон се прецизира задолжителната содржина на законите за приватност на податоци и земјите членки се обврзуваат да формираат орган за заштита на личните податоци.

ЕКОВАС, исто така, усвои Директива за борба со киберкриминалот (2011) и Дополнителен закон за електронски трансакции во рамки на ЕКОВАС[17] .

Организација за безбедност и соработка во Европа

Организацијата за безбедност и соработка во Европа (ОБСЕ) работи на прашања од областа на кибер/ИКТ безбедноста, особено од аспект на борбата против тероризмот и киберкриминалот. Во 2013 година ОБСЕ усвои мерки за градење доверба во киберпросторот преку Одлуката на Постојаниот совет број 1106 од 3 декември 2013 година.[18] Овие мерки за градење доверба имаат цел да го намалат конфликтот што произлегува од користењето информациски комуникациски технологии.

Мерките за градење доверба идентификувани од ОБСЕ вклучуваат: размена на информации за киберзакани, безбедноста и користењето ИКТ, национална организираност, стратегии и терминологија, одржување консултации со цел да се

16 ЕКОВАС, Дополнителен закон за заштита на личните податоци, види http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

17 ЕКОВАС, Економска заедница на западноафриканските држави (ЕКОВАС), Директива C/DIR.1/08/11 за борба против киберкриминалот во рамки на ЕКОВАС, 2011 година. Достапно на: http://www.osiris.sn/Directive-C-DIR-1-08-11-du-19-aout.html i Član A/SA.2/01/10 o elektronskim transakcijama u okviru ECOWAS-a, 2010, dostupno na http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Electronic-Transaction-Act.pdf

18 ООдлука на ОБСЕ бр. 1202, Мерки за градење доверба на ОБСЕ за намалување на ризиците од конфликт кој произлегува од користењето информациски и комуникациски технологии, PC.DEC/1202, 10 март 2016 г. Достапно на: https://www.osce.org/pc/227281?download=true

намалат ризиците од погрешна перцепција и од можна појава на тензии, споделување информации за мерки преземени со цел да обезбеди отворен и безбеден Интернет, размена на информации за контакт-центри, и користењето на ОБСЕ како платформа за дијалог.

Меѓутоа, мерките за градење доверба се засновани врз доброволен пристап и поради тоа не се правно обврзувачки инструменти.

Организација на американските држави

Организацијата на американските држави (ОАД) формираше Работна група за киберкриминал уште во 1999 година, како главен форум за „зајакнување на меѓународната соработка во превенција, истражување и судско гонење на киберкриминалот, олеснување на размената на информации и искуства меѓу членовите и за давање на неопходните препораки за подобрување и обезбедување напори за справување со овие кривични дела“.[19] Работната група се состанува двапати годишно и им дава препораки на земјите членки.

ОАД, исто така, се занимава со кибербезбедноста во поширок размери. Во 2004 година Генералното собрание на ОАД, во Резолуцијата AG/RES.2004 (XXXIV-O/04) насловена како „Интерамериканска интегрална стратегија за справување со закани за кибербезбедноста“, даде надлежност за Секретаријатот на Интерамериканскиот комитет на ОАД против тероризам. Главни задачи на овој Секретаријат се да помогне во формирањето национални тимови за одговор при безбедносни компјутерски инциденти (CSIRTs), да создаде мрежа составена од овие тимови и да ја поддржи изработката на национални стратегии за кибербезбедност. Од 2007 година, Секретаријатот се стремеше да создаде сеопфатна програма за градење капацитети базирана врз работилници, технички курсеви, тркалезни маси со политички дискусии, вежби за управување со кризи и размена на најдобри практики.

Шангајска организација за соработка

Шангајската организација за соработка (ШОС), меѓународна организација со шест земји членки (Кина, Казахстан, Киргистан, Русија, Таџикистан и Узбекистан), во 2009 година усвои Спогодба меѓу владите на земјите членки на ШОС за соработка во полето на обезбедување меѓународна информациска безбедност.[20] Во 2011 година четири земји членки на ШОС поднесоа Нацрт-меѓународен кодекс на однесување за информациска безбедност до Генералното собрание на ОН. Во 2015 година до Генералното собрание на ОН беше доставен нов Нацрт-меѓународен кодекс на однесување[21].

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

20 Спогодба меѓу владите на земјите членки на ШОС за соработка во полето на обезбедување меѓународна информациска безбедност, 2009 година. Достапно на: https://unidir.org/cpp/en/organization-pdf-export/eyJvcmdhbml6YXRpb25fZ3JvdXBfaWQiOiIxMiJ9

21 Шангајска организација за соработка, Нацрт-меѓународен кодекс на однесување, допис од 9 јануари 2015 година до Генералното собрание на ОН, A/69/723. Достапно на: https://digitallibrary.un.org/record/786846?ln=en

СЛУЧАЈ ЗА АНАЛИЗА: НАЦРТ-МЕЃУНАРОДЕН КОДЕКС НА ОДНЕСУВАЊЕ НА ШОС, 2015 ГОДИНА

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

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

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

Азиско-тихоокеанска економска соработка

ШОС се однесува на концептот „меѓународна информациска безбедност", што ја истакнува важноста на содржината како извор за потенцијална безбедносна закана.

Азиско-тихоокеанската економска соработка (АПЕК) во 2002 година ја издаде Стратегијата за кибербезбедност на АПЕК, којашто содржи препораки во полето на законодавството за киберкриминал, безбедносни и технички упатства, јавна свест и обука и едукација.[22] Декларацијата од Лима (2005) има цел да ги подобри информациските инфраструктури заради унапредување на информациското општество.[23] Декларацијата се осврнува и на мрежната безбедност и на важноста од формирање тимови за одговор при компјутерски инциденти (ЦЕРТ). Стратегијата на АПЕК за обезбедување сигурна, безбедна и одржлива онлајн средина има цел да обезбеди информациска и мрежна безбедност, да ги усогласи рамките за обезбедување на трансакциите и комуникациите и да се справува со киберкриминалот. Сè почесто, тоа вклучува тесна соработка со приватниот сектор и со други меѓународни организации. Стратегискиот акциски план на АПЕК ТЕЛ за 2010 – 2015 година има за цел да „промовира безбедна, отпорна и сигурна ИКТ средина", вклучително во следниве клучни области: зголемување на отпорноста на домашната критична инфраструктура, безбедност и управување со ризик, градење капацитети за кибербезбедност, подигнување на свеста за кибербезбедноста, иницијативи за кибербезбедност со индустријата, активности за промовирање сигурна и безбедна онлајн средина за ранливи групи и економија на Интернет[24].

22 Стратегија за кибербезбедност на АПЕК. Достапно на: https://www.ccdcoe.org/uploads/2018/10/APEC-020823-CyberSecurityStrategy.pdf

23 АПЕК, Декларација од Лима, 2005 година. Достапно на: https://www.apec.org/Meeting-Papers/Sectoral-Ministerial-Meetings/Telecommunications-and-Information/2005_tel

24 АПЕК, Декларација од Лима, 2005 година. Достапно на: https://ccdcoe.org/organisations/apec/

Асоцијација на земји на Југоисточна Азија

Асоцијацијата на земји на Југоисточна Азија (АСЕАН), којашто ја сочинуваат десет земји членки (Брунеј, Камбоџа, Индонезија, Лаос, Малезија, Мјанмар (Бурма), Филипините, Сингапур, Тајланд и Виетнам), издаде Изјава на министрите за надворешни работи за соработка во обезбедувањето кибербезбедност и дискутираше за кибербезбедноста во контекст на борбата против тероризам и транснационален криминал[25].

Комонвелтот на нации

Комонвелтот на нации опфаќа 53 земји членки и се фокусира на градење капацитети, споделување информации и обезбедување помош на своите земји членки во спроведувањето правни рамки за справување со киберкриминалот. Во рамки на Комонвелтот на нациите има две платформи: Форумот за кибербезбедност и Иницијативата за кибербезбедност, кои функционираат во рамки на Организацијата за телекомуникации на Комонвелтот. Второспоменатата организација го има усвоено Моделот за киберуправување на Комонвелтот,[26] којшто беше одобрен со Декларацијата од Абуџа во октомври 2013 година и беше промовиран за време на Форумот за кибербезбедност на Комонвелтот во Лондон, во 2014 година.[27]

Моделот за киберуправување[28] на Комонвелтот содржи Нацрт-збирка на начела што треба да се земат предвид за да се придонесе за безбеден и ефективен глобален киберпростор; да се поддржи поширок економски и социјален развој; да се дејствува индивидуално и колективно во справувањето со киберкриминалот; да се остваруваат права и должности во киберпросторот.

Европска Унија

Документите усвоени од Европската Унија (ЕУ), а коишто се најрелевантни за кибербезбедноста, може да бидат правно необврзувачки документи (како што се комуникациите) или пак различни видови правно обврзувачки акти кои им наметнуваат обврски на земјите членки или на одредени субјекти.

Во 2013 година ЕУ го објави својот прв сеопфатен документ – нејзината Стратегија за кибербезбедност – во која се опфатени широк спектар киберзакани. Во 2016 година ЕУ ја усвои Директивата за безбедност на мрежите и информациските системи (Директива НИС).[29] Стратегијата ги утврдува визијата, улогите, одговорностите и потребните активности на ЕУ во полето на кибербезбедноста. Значајно е дека документот во контекст на кибербезбедноста истакнува дека централизиран надзор од ЕУ не е решение, па затоа националните влади треба да останат главни субјекти што ќе ги организираат превенцијата и справувањето со киберинцидентите на национално ниво.

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

26 Модел за киберуправување на Комонвелтот. Достапно на: https://ccdcoe.org/uploads/2018/11/CommW-140304-CommonwealthCybergovernanceModel.pdf

27 Форум за кибербезбедност на Комонвелтот во Лондон во 2014 година. Достапно на: https://ccdcoe.org/uploads/2018/11/CommW-140304-CommonwealthCybergovernanceModel.pdf

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

29 Европска Унија, Директива за безбедност на мрежите и информациските системи, L 194/1, 2016. Достапно на: 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

Како една од своите цели, Стратегијата на ЕУ за кибербезбедност го идентификува развојот на политики и на способности за киберодбрана поврзани со рамката на Заедничката безбедносна и одбранбена политика, и истакнува листа на предвидени активности за соработка на Европската агенција за одбрана и земјите членки.

Активности поврзани со кибербезбедноста се вметнати и во Дигиталната агенда на ЕУ, којашто ги смета довербата и безбедноста на Интернет за витален елемент на едно живо дигитално општество. Имено, Европската агенда за безбедност става приоритет врз киберкриминалот како една од најрелевантните закани на повидок.

Стратегијата на ЕУ за кибербезбедност предвидува дека „особено сериозен киберинцидент или напад би можел да претставува доволна основа за дадена земја членка да се повика на Клаузулата за солидарност на ЕУ (член 222 од Договорот за функционирањето на Европската Унија).

На 25 мај 2015 година влезе во сила Општата регулатива на ЕУ за заштита на личните податоци (ОРЗЛП).[30] Оваа регулатива, во суштина, го преобликува начинот на кој се постапува со податоците во секој сектор, од здравство, па до банкарство итн. Важно е дека Регулативата важи не само за организации во рамките на ЕУ, туку и за организации надвор од неа, доколку тие им нудат стоки и услуги на субјекти на податоци од ЕУ или го следат однесувањето на субјекти на податоци од ЕУ.

ОРЗЛП важи за сите компании кои обработуваат и чуваат лични податоци на субјекти на податоци со седиште во ЕУ, без оглед на локацијата на компанијата.

Северноатлантска алијанса

Првата политика за киберодбрана на Организацијата на Северноатлантски договор (НАТО) беше изработена во 2008 година. На Лисабонскиот самит во 2010 година, киберодбраната беше вклучена во Стратегискиот концепт на НАТО, а декларацијата од самитот го забрза ажурирањето на Политиката за киберодбрана во 2011 година и создавањето на придружен Акциски план во 2012 година.

Нова подобрена Политика за киберодбрана беше одобрена на Самитот во Велс, според која „поголем дигитален напад на земја членка би можел да биде опфатен со членот 5“ [од Северноатлантскиот договор].[31]

Политиката се стреми дополнително да ги подобри споделувањето информации и заемната помош меѓу сојузниците, да ги унапреди обуката и вежбите и да ја продлабочи соработката со индустријата. На Варшавскиот самит во 2016 година, НАТО го препозна киберпросторот како поле на операции и се заложи да ја продлабочи соработката меѓу НАТО и ЕУ во однос на киберодбраната, како и да посвети повеќе ресурси на способностите за киберодбрана. Во 2018 година, министрите за одбрана на земјите членки на НАТО се договорија за создавање на нов Центар за кибероперации во седиштето на НАТО, којшто треба да помогне во интегрирање на кибераспектите во планирањето и операциите на НАТО на сите нивоа.

НАТО е домаќин на Комитетот за киберодбрана, претходно познат како Комитет за одбранбена политика и планирање (киберодбрана). Овој Комитет е високо советодавно тело, одржува консултации со земјите членки и го врши севкупното управување со интерната киберодбрана на НАТО. Освен тоа, има и Одбор за управување со киберодбрана, којшто работи под покровителство на Дивизијата за

30 Општа регулатива на ЕУ за заштита на личните податоци. Достапно на: https://eugdpr.org/the-regulation/gdpr-faqs/

31 Северноатлантски договор, 1949. Достапно на: https://www.nato.int/cps/ie/natohq/official_texts_17120.htm

нови безбедносни предизвици во седиштето на НАТО, а е составен од претставници на сите поголеми засегнати страни во полето на кибербезбедноста во рамките на НАТО. Имено, Одборот за управување со кибероодбраната го врши стратегиското планирање и ги дава извршните насоки во однос на мрежите на НАТО, а потпишува и меморандуми за разбирање со земјите членки со цел да се олесни размената на информации и да се координира помошта.

Освен тоа, Агенцијата на НАТО за консултации, контрола и команда (NC3) е главно тело за консултации во однос на техничките аспекти и аспектите поврзани со спроведувањето на кибероодбраната.

Групата седум (Г7)

Г7 е неформална група на седум земји (Канада, Франција, Германија, Италија, Јапонија, Обединетото Кралство и Соединетите Американски Држави, со ЕУ со статус на набљудувач) која редовно се состанува за да дискутира за важни политички и економски прашања. Од 2016 година, Г7 изработува повеќе документи поврзани со кибербезбедноста и ја поставува како важна тема во разни декларации од самити[32].

ИНФОРАМКА: УПАТСТВА ЗА ЗАШТИТА НА ЛИЧНИ ПОДАТОЦИ ЗА АФРИКА

Во мај 2018 година организацијата „Internet Society“ и Комисијата на Африканската Унија ги промовираа Упатствата за заштита на лични податоци за Африка за време на Африканскиот интернет-самит во Дакар, Сенегал.

Упатствата содржат 18 препораки фокусирани на три прашања:

1. Препораки за создавање доверба, приватност и одговорно користење на личните податоци;
2. Препораки за активности што треба да ги преземат владите и креаторите на политики, органите за заштита на податоци и контролорите и обработувачите на податоци;
3. Препораки за решенија со повеќе засегнати страни, добросостојба на дигиталниот граѓанин и мерки за овозможување и одржување.

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

2. 2. Иницијативи на недржавни чинители

Бидејќи државите не беа подготвени да го изразат своето opinio iuris и државната практика во киберпросторот, не постои заемен договор за тоа како меѓународното право се применува во киберпросторот, што од своја страна доведе до ситуација во која недржавни чинители започнуваат да ја исполнуваат таа празнина. Приватните компании за ИКТ и граѓанските организации беа особено проактивни во предлагањето норми за киберпросторот усогласени со човековите права, чија цел е да придонесат за побезбеден и посигурен Интернет.

Група научници и експерти по меѓународно хуманитарно право го изработија Прирачникот од Талин за примена на меѓународното хуманитарно право во кибероперации.[33] Иако овој документ е повеќе академски, тој ги реафирмира основните начела на меѓународното хуманитарно право, како што се начелото на дистинкција, пропорционалност и неопходност во киберпросторот. Освен тоа, оваа група експерти го објави Прирачникот од Талин 2.0, кој се осврнува на применливото право во мирнодопско време во киберпросторот[34].

32 Групата 7, Коминике од самитот на Г7 во Шарлевуа. Достапно на: https://www.consilium.europa.eu/en/press/press-releases/2018/06/09/the-charlevoix-g7-summit-communique/

33 ТПрирачникот од Талин. Достапно на: https://ccdcoe.org/research/tallinn-manual/

34 Проспект од Прирачникот од Талин 2.0. Достапно на: https://www.almendron.com/tribuna/wp-content/uploads/2018/03/ccd-coe-tallinn-manual-onepager-web.pdf

СЛУЧАЈ ЗА АНАЛИЗА: КОНЦЕПТИТЕ НА „ОРУЖЕН НАПАД“ И „ПРИМЕНА НА СИЛА“ ВО КИБЕРПРОСТОРОТ – ПРЕМОСТУВАЊЕ НА ЈАЗИЧНАТА ДИЛЕМА МЕЃУ ПРАВНАТА, ПОЛИТИЧКАТА И ТЕХНИЧКАТА ЗАЕДНИЦА

Важно е да се разграничат режимите во меѓународното право: (i) ius ad bellum (со кое се уредуваат ситуациите во кои државата може да употреби сила како инструмент на својата национална политика), и (ii) ius in bello (меѓународно хуманитарно право со кое се утврдуваат правилата за тоа кога можат да се спроведуваат операциите при оружен напад).

Во контекст на ius ad bellum, согласно член 51 од Повелбата на ОН, оруженият напад може да поттикне самоодбрана. Оттука, горливото прашање е кога дадена кибероперација претставува оружен напад на кој една држава правно оправдано може да одговори со кибер или кинетички дејства на ниво на користење сила. Овде акцент се става на поимот „оружен“ затоа што Меѓународниот суд на правдата во пресудата за Никарагва се произнесе дека постојат „мерки кои не претставуваат оружен напад, но во секој случај може да вклучуваат примена на сила“. Следствено на тоа, државите може да се соочат со кибероперација којашто претставува примена на сила, но при која државата не е во можност да се брани затоа што кибероперациите не се квалификувани како оружен напад. За да се разреши оваа дилема, повеќе стручњаци по меѓународно право се залагаат за тоа „оруженият напад“ во киберпросторот да ги опфаќа сите дејства кои резултираат со последици аналогни на оние предизвикани од кинетички дејства (физички последици).

Во контекст на ius in bello, пред да може да се примени меѓународното хуманитарно право, мора да има напад (дефиниран преку пристап базиран врз последици при толкување на поимот „напад“.

„Мајкрософт“, приватна транснационална корпорација, во февруари 2017 година предложи државите да ја усвојат „Дигиталната Женевска конвенција“ со која се идентификуваат норми за киберпросторот во мирнодопско време. „Мајкрософт“ редовно објавува документи со политики и блогерски објави чија цел е да придонесат за градење доверба меѓу различните засегнати страни во киберпросторот. Меѓутоа, иако државите генерално прифаќаат проактивни иницијативи од недржавни чинители, сè уште постои скептицизам кон можноста за успех.[35]

Истовремено, компаниите за ИКТ сè почесто бараат од државите да регулираат одредено злонамерно однесување во киберпросторот. На пример, „Мајкрософт“ бараше од Конгресот на Соединетите Американски Држави да усвои регулативи за ограничување на користењето технологии за препознавање на ликот[36].

35 Документ за политики на „Мајкрософт“, Дигитална Женевска конвенција за заштита на киберпросторот. Достапно на: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH ; види, исто така, во Упатства за кибербезбедност на „Мајкрософт“. Достапно на: https://www.microsoft.com/en-us/cybersecurity/default.aspx

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

Беа изработени и други инструменти од мекото право, како што се Принципите од Манила за посредничка одговорност,[37] и тие им даваат насоки на државите во однос на политиките за правна одговорност на посредниците за содржината поставена на нивните платформи. Недржавните чинители, особено компаниите за ИКТ и граѓанските организации, станаа попроактивни во предлагањето норми за примена во киберпросторот. Особен предводник во последниве години беше „Мајкрософт“[38].

И граѓанските организации станаа поактивни пополнувајќи го вакуумот во киберпросторот оставен од државите и предлагајќи норми насочени кон промовирање на човековите права во киберпросторот. На пример, „Член 19“ (лондонска невладина организација), заедно со неколку други НВО, ги поддржаа Начелата од Камден за слобода на изразување и еднаквост на Интернет.[39] Освен тоа, беа усвоени и инструментите на мекото право, како што се Принципите од Манила за посредничка одговорност.

Иницијативата „Глобална мрежа“ е инцијатива со повеќе засегнати страни којашто развива глобални стандарди за Интернетот. Нејзините начела за слобода на изразување и за приватност им даваат упатства и насоки на индустријата за ИКТ и на нејзините засегнати страни во заштитата и унапредувањето на човековите права низ светот[40].

Во однос на спречувањето насилен екстремизам на Интернет, група социјални медиуми, имено „Фејсбук“, „Твитер“, „Јутуб“ и „Мајкрософт“, се здружија во Глобален интернет-форум за справување со тероризмот,[41] каде што овие гиганти од интернет-сферата развиваат нормативни стандарди за регулирање на насилниот екстремизам на своите платформи.

Генерално, приватните компании за ИКТ треба да спроведат ефективна, проактивна и инклузивна длабинска анализа за човековите права, вклучително и суштинска соработка со поединци чии човекови права може да бидат засегнати од приватните компании за ИКТ.

ИНФОРАМКА: ПОСРЕДНИЧКА ОДГОВОРНОСТ

Сета комуникација што го вклучува Интернет е овозможена преку посредници. Со оглед на комплексноста на Интернет, има повеќе различни видови посредници:

- Даватели на услуги на Интернет (ISPs) се однесува на даватели на пристап до Интернет;
- Даватели на веб-хостинг услуги („домаќини“) обично се однесува на секое лице или компанија што контролира веб-локација или веб-страница и што овозможува кое било трето лице да објавува и поставува содржина;
- Платформи на социјални медиуми како што се „Фејсбук“, „Твитер“, „Јутуб“ итн., коишто ги поттикнуваат поединците да се поврзат и да водат интеракција со други корисници и да споделуваат содржина;
- Пребарувачи, како што е „Гугл“, се софтверски програми кои користат алгоритми за вчитување податоци, датотеки или документи како одговор на пребарување.

Тие се даватели на пристап до Интернет, социјални мрежи и пребарувачи. Посредничка одговорност значи политики со кои се уредени правните обврски на посредниците за содржината на овие комуникации.
Извор: 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 Принципите од Манила за посредничка одговорност. Достапно на: https://www.manilaprinciples.org/

38 Документ за политики на „Мајкрософт“, Дигитална Женевска конвенција за заштита на киберпросторот. Достапно на: https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace

39 „Член 19“, Начелата од Камден за слобода на изразување и еднаквост. Достапно на: https://www.article19.org/data/files/pdfs/standards/the-camden-principles-on-freedom-of-expression-and-equality.pdf

40 Повеќе информации за иницијативата „Глобална мрежа“ може да најдете овде https://globalnetworkinitiative.org/

41 Јавна политика на „Гугл“, Ажурирање на Глобалниот интернет-форум за справување со тероризмот, 4 декември 2017 година. Достапно на: https://www.blog.google/around-the-globe/google-europe/update-global-internet-forum-counter-terrorism/

Насочувачките принципи за бизнис и човекови права (GPBHR) предвидуваат постоење на корпоративна одговорност за почитувањето на човековите права. За компаниите за ИКТ тоа значи да се земат предвид прашања специфични за таа индустрија, како што се слободата на изразување, приватноста и безбедноста. Важно е дека некои од најгорливите прашања од длабинската анализа произлегуваат од користењето на производите, услугите, технологиите и апликациите на компаниите од страна на корисниците и од напорите на владите да ги ограничат правата на корисниците.

Главни наоди

- **Пропустите во квалификувањето на одредени дејства како кривично дело во одредена земја може да создадат рај за престапниците, со потенцијал да влијае врз други земји глобално.**
- **Разликите во квалификувањето на одредени дејства како кривични дела создаваат предизвици за меѓународната соработка во кривичната област, што вклучува киберкриминал, особено во однос на начелото за двојна инкриминација.**
- **Компаративната анализа на делата од областа на киберкриминалот може да ги истражи добрите практики кои државите може да ги користат во изработката на националните закони, во согласност со новите меѓународни стандарди во оваа област.**

Библиографија

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

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

ПОГЛАВЈЕ 4
СПРОВЕДУВАЊЕ НА МЕЃУНАРОДНИ И РЕГИОНАЛНИ НОРМИ И СТАНДАРДИ ВО НАЦИОНАЛЕН КОНТЕКСТ

ЦЕЛИ

Во ова поглавје ќе истражиме како меѓународните и регионалните правни рамки од претходното поглавје, како и други норми од областа на киберпросторот може да се спроведат на национално ниво, особено преку соодветно законодавство, политики и стратегии.

Целите за учење за ова поглавје се следните:

- Понатамошно разбирање на рамките и на другите норми во киберпросторот и нивна применливост во национален контекст.
- Зголемено разбирање за потребата од национално законодавство, политики и стратегии за киберпросторот.
- Зголемено знаење за тоа како да се создадат или изменат националното законодавство, политиките и стратегиите за киберпросторот врз основа на добри практики за УБС.

Вовед

Користењето на киберпросторот стана сè почеста појава помеѓу поединци, влади и компании, без разлика дали е за користење информации, обезбедување и користење јавни и приватни услуги, или пак за одржување на оперативните процеси. Таквата зачестеност значи дека сите овие чинители се потенцијално подложни на повеќе киберупади и напади, ранливост што претставува закана за човековите права, како и за националната и човековата безбедност.

Иако на меѓународно и регионално ниво има воспоставени одредени норми за безбедни практики во киберпросторот и општа рамка за правни очекувања во однос на правата во неговите рамки, сега поголемо внимание се обрнува на потребата од поврзани и сеопфатни национални пристапи кон предизвиците во киберпросторот. Сè поголемата зависност од киберпросторот значи сè поголема потреба од ефективно национално законодавство, политики и стратегии за заштита на податоците, информациите и знаењето што се пренесуваат и користат во киберпросторот, како и за зголемување на безбедноста на граѓаните во тој простор.

Меѓународните или регионалните рамки анализирани во последното поглавје – кои се состојат од резолуции, извештаи, конвенции и спогодби за човекови права и регулирање на киберпросторот – создадоа збир на норми кои земјите треба да ги почитуваат при правењето измени на нивното законодавство, политики и стратегии за киберпросторот и кибербезбедноста, и може да им помогнат во составувањето или ажурирањето на националните политики и стратегии за киберпростор и кибербезбедност. Освен тоа, приватните компании и невладините организации бараа понатаму да се работи на споменатите рамки и норми со цел детално да се утврдат доминантните пристапи во кибербезбедноста. Државите може да се послужат со разните вакви елементи со цел воспоставување на холистичко управување со киберпросторот и кибербезбедноста што се заснова врз начелата на добро управување со безбедносниот сектор.

Следниве добри практики истакнуваат клучни регулаторни аспекти кои државите треба да ги земат предвид и да ги зајакнат при создавањето или менувањето на национална стратегија за кибербезбедност.[1]

Освен тоа, националните политики и стратегии треба да вклучуваат меѓународна перспектива или да бидат надополнети со политики и стратегии конкретно насочени кон меѓународна соработка, со цел регулативата и безбедноста во киберпросторот да не се ограничат во рамки на националните граници.

1 Добрите практики се засноваат врз: Cybersecurity Policy Framework. A Practical guide to the development of national cybersecurity policy. Microsoft (2018).

Добра практика 1: Државите треба да изработат и усвојат национални закони, политики и стратегии за регулирање на киберпросторот.

Иако киберпросторот, во практика, е глобален медиум, правно гледано, обврската за негово регулирање и за обезбедување добро управување со него ја имаат државите, затоа што не постои некоја меѓународна раководна структура.[2] Исто така, важно е да се спомене дека „истите права што луѓето ги имаат офлајн мора да се заштитат и онлајн“.[3] Па така, ако на ИКТ компаниите им се дозволи да работат без задоволителна регулациска рамка, тоа може да доведе до практики кои отстапуваат од јавниот интерес и кои потенцијално ги повредуваат човековите права.[4] Оттука, државите – како примарни носители на обврските поврзани со човековите права и како заштитници на јавниот интерес – треба да ги опфатат најновите технолошки достигнувања во своите законодавни напори за ограничување на просторот за потенцијално несакани последици од дејствата на приватниот сектор. Затоа, националното законодавство, политиките и стратегиите, како и улогата на безбедносниот сектор во регулирање на киберпросторот и обезбедување кибербезбедност, имаат суштинско значење за обезбедување добри практики на управување.

Освен тоа, меѓународните и регионалните рамки и норми се од поопшта природа, додека националното законодавство, националните политики и стратегии овозможуваат да се опфатат националните потреби и специфичностите на киберпросторот и на кибербезбедноста.

И на крај, потпирањето исклучиво на рамки и на норми воспоставени на меѓународно и регионално ниво не е гаранција дека другите држави нема да извршат повреда на овие незадолжителни начела, ниту пак гарантира почитување на нормите од страна на приватните и јавните чинители во една држава.[5] Тоа значи дека воспоставувањето законодавство, политики и стратегии за управување со киберпросторот и кибербезбедноста или нивната измена може да послужат како посеопфатен и кохезивен начин за обезбедување на почитувањето на законите и човековите права во киберпросторот во рамките на една држава.

При изработката на законодавство за киберкриминал, треба да се имаат предвид следниве услови:

- Тоа мора да биде доволно (технолошки) неутрално за да го амортизира постојаниот напредок на технологијата и криминалот, затоа што инаку ризикува да биде застарено уште кога ќе влезе во сила.

- Овластувањата за спроведување на законот мора да имаат заштитни мерки со цел да се обезбеди почитување на владеењето на правото и на човековите права.

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

3 UСовет за човекови права на Обединетите нации, Резолуција за унапредување, заштита и уживање на човекови права на Интернет, A/HRC/20/L.13, 29 јуни 2012 г., став 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.

- Мора да биде доволно усогласено или барем компатибилно со законите на другите земји за да се овозможи меѓународна соработка, како, на пример, да се почитува условот за двојна инкриминација.

ПРИМЕР ЗА ДОБРА ПРАКТИКА

Киберкриминалот е клучна област во која националното законодавство и политиките имаат пресудно значење. На африканските држави кои подготвуваат законодавство за киберкриминал како водилка може да им послужи особено Конвенцијата за кибербезбедност и заштита на лични податоци на Африканската Унија, усвоена во Малабо, во јуни 2014 година.[6]

Уште од 1997 година, Алжир постепено се подготвува за борба против киберкриминалот. Резултат на тоа е законодавство коешто е во голема мера приспособено на борбата против криминалот во согласност со голем број фундаментални начела, иако постојат слабости и од двата аспекта. Алжирскиот закон ги опфаќа повеќето од одредбите од Конвенцијата од Будимпешта, во некои случаи со алтернативна формулација. Ги вклучува следниве прекршоци: измамнички пристап и задржување во системот; преземање комуникација и зборови искажани приватно или во доверливост; бришење или измена на податоци содржани во системот после измамнички пристап или задржување; менување на функционирањето на системот после измамнички пристап или задржување; злоупотреба на електронски уреди; детска порнографија; и прекршоци поврзани со повреда на интелектуалната сопственост и сродни права.

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

Добра практика 2: Државите треба да го ажурираат националното законодавство во однос на актуелните предизвици во киберпросторот.

При изработката и усвојувањето на национално законодавство за киберпростор и кибербезбедност (без разлика дали тоа е со ажурирање на постојното законодавство или со создавање ново), креаторите на закони и политики треба да имаат предвид неколку актуелни предизвици.

Како прво, напредокот на иновациите во киберпросторот е многу побрз од националните законодавни процеси. Оттука, дури и најсовремениот законодавен текст во оваа област може да заостанува – а најверојатно и ќе заостанува – зад најновата технологија. Како второ, за составување законодавство за киберпросторот неопходно е добро познавање и експертиза во областа на ИТ, што е реткост во јавниот сектор, затоа што овој профил лица се многу подобро платени во приватниот сектор. Како трето, дури и законодавецот да успее да донесе соодветни закони за регулирање на киберпросторот, транснационалниот карактер на прашањата

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

од киберсферата ја прават примената на националните закони комплицирана, а понекогаш и невозможна.

Брзиот напредок во технолошките иновации е во изразена спротивност со бавните и честопати пролонгирани национални законодавни процеси.[7] Од таа причина, се користат голем број технологии и кибералатки без неопходната регулација. Типичен пример за таков регулаторен вакуум е користењето вештачка интелигенција (AI). Додека најголем дел од земјите немаат донесено соодветно законодавство за регулирање на содржината од социјалните медиуми кои користат човечки модератори на содржина, веќе се воведуваат алатки кои работат на вештачка интелигенција за да ги заменат луѓето што ја вршат оваа работа[8].

Во секој случај, државите ќе избегнуваат да носат законодавни акти на брз и некоординиран начин. Иако загриженоста на јавноста поврзана со брзиот технолошки напредок може да претставува политички стимул за донесување закони со цел да се покажат компетентноста и реактивноста на државните институции, брзото усвојување на голем број норми може да биде полошо отколку да им се допушти на приватните компании да работат без целосна регулација додека се тестираат нови технологии. Поради тоа, државите треба да ги следат новите технологии и да идентификуваат нови трендови, но да носат законодавство само откако ќе спроведат внимателен процес на разгледување што ќе ги опфати сите засегнати страни, вклучувајќи ги и приватниот сектор и граѓанското општество.

Освен тоа, при усвојувањето законодавство во оваа материја, државите ќе избегнуваат да бидат прекумерно нормативни, зашто тоа може да го попречи процесот на иновација и истражување, како и да ги обесхрабри помалите ИКТ компании на пазарот, кои можеби не ќе можат да ги исполнат високите стандарди на прекумерно нормативното законодавство. Па така, кога ќе одлучуваат дали да донесат законодавство во однос на конкретна материја од киберсферата, државите ќе разгледаат други опции кои не се дел од законодавството: на пример, понекогаш со усвојување доброволни кодекси на однесување или збир на незадолжителни водечки начела, може да се исполни посакуваната регулаторна цел. Исто така, таквите инструменти на мекото право се полесни за изменување, а со тоа и попогодни да ги одразуваат најновите трендови во технологијата.

7 Европски суд на ревизори, „Предизвици за ефективна политика на ЕУ за кибербезбедност“ – Краток извештај (2019): 18, (https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf).

8 Генерално собрание на Обединетите нации, „Извештај на Специјалниот известувач за унапредувањето и заштитата на правото на слобода на мислење и изразување“, A/73/348, 29 август 2018 година, став 18.

ПРИМЕРИ ЗА ДОБРА ПРАКТИКА

Во Гана беа усвоени специфични прописи за банкарските и финансиски институции – кои го сочинуваат секторот што е најпогоден од киберкриминал – во склоп на Директивата за кибербезбедност за финансиските институции на Банката на Гана од 2018 година. Директивата наложува активна вклученост на извршните директори и на Одборот во зголемување на кибербезбедноста. Сите банки во земјата се обврзани да назначат Службеник за киберинформациска безбедност (CISO), кој би ги советувал високото раководство и Одборот за прашања поврзани со кибербезбедноста, а би дефинирал и соодветни мерки за справување со ризици за кибербезбедноста и за информацискатa безбедност.

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

Голем број африкански економии имаат зајакнати мерки за спроведување. Во Јужна Африка, со Законот за заштита на лични податоци (POPI) од 2013 година, се создаде Регулатор на информации за да се обезбеди приватноста на податоците. Во 2017 година, Регулаторот на информации започна со истрага на најголемиот упад во податоци во земјата што се случи истата година, при што беа украдени личните податоци на над 30 милиони луѓе. Агенцијата, исто така, поднесе официјални барања до засегнатите компании да дадат објаснувања.

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

Добра практика 3: Државите треба да ја зголемат киберекспертизата

Недостигот на експертиза и знаење во областа на ИТ во јавниот сектор е друга сериозна пречка за државите во усвојувањето законодавство за прашања поврзани со киберпросторот.[9] Единственото решение за овој проблем е државите да најдат начини за акумулирање на повеќе стручна експертиза. Има голем број начини на кои оваа цел може да се постигне, при што наједноставната би била државата да вработи неопходен број лица стручни во ИТ областа. Меѓутоа, државите обично имаат многу поограничени финансиски и други ресурси од приватните ИКТ компании и може да имаат проблеми во привлекувањето и задржувањето експерти за такви високопрофилни области какви што се кибербезбедноста, вештачката интелигенција или аналитиката на податоци.

Делумно решение би можело да биде преку алтернативни регулаторни шеми, кои би овозможиле пристап до експертизата на приватниот сектор на тој начин што би му се дозволило во одредена мера да учествува во регулаторниот процес, но целокупната одговорност и понатаму би останала кај државата. Со оглед на тоа дека приватните компании имаат високо ниво на експертиза и неопходно практично знаење за прашања поврзани со киберпросторот, правилата донесени во соработка со приватниот сектор може да го премостат традиционалниот јаз помеѓу напредувањето на технологијата и нивото на националното законодавство. Исто така, таквите корегулаторни шеми може да бидат многу помалку политизирани од самите национални законодавни процеси.

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

ПРИМЕРИ ЗА ДОБРА ПРАКТИКА

Националната кибер експертиза се зголемува во координација со приватниот сектор и странски мултинационални компании[10].

Во Кенија, иницијативите за кибербезбедност на приватниот сектор доведоа до формирање на Центар за навлегување во киберсферата во Најроби во март 2018 година од страна на „Serianu“, панафриканска консултантска фирма за кибербезбедност. Центарот обезбедува средина во која фирмите може да експериментираат и да ги тестираат своите способности во полето на кибербезбедноста. Исто така, обезбедува образовни капацитети за едукација на професионалци за кибербезбедност. Сличен центар беше отворен во Мавриций кон средината на 2017 година.

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

Во Нигерија, „Мајкрософт“ се здружи со Парадигма иницијативата Нигерија (PIN) со цел едукација на Нигеријците за сузбивање киберкриминал и за создавање економски можности. Во октомври 2009 година Комисијата за справување со економски и финансиски криминал (EFCC) на земјата објави дека затворила околу 800 веб-страници поврзани со киберкриминал и уапсила 18 киберкриминални банди. Комисијата навела дека „паметната технологија“ обезбедена од Мајкрософт им помогнала.

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

Добра практика 4: Државите треба да изработуваат и ажурираат закони кои ги штитат приватноста и личните податоци.

Заштитата на приватноста и на личните податоци има суштинско значење за кибербезбедноста и е област во која беше остварен конкретен напредок од аспект на спроведувањето на правото на приватност и заштита на личните податоци, особено во ЕУ. Општата регулатива на ЕУ за заштита на личните податоци (ОРЗЛП – види Поглавје 3), која влезе во сила во мај 2018 година, создаде регионален регулаторен режим со цел да им се даде контрола на поединците врз нивните лични податоци. Регулативата, исто така, послужи како расадник за закони за приватност и заштита на податоци на национално ниво.

Во 2014 година Африканската Унија ја усвои Конвенцијата за кибербезбедност и заштита на лични податоци од Малабо (види Поглавје 3). Конвенцијата сè уште не е влезена во сила. Според тоа, Конвенцијата од Будимпешта е моментално единствената законски обврзувачка меѓународна правна рамка на темата кибербезбедност, киберпростор и улогата на државата во таа област. Иако само мал број африкански држави директно ја потпишаа или беа поканети да пристапат, таа се користи како рамка-водилка за создавањето на Конвенцијата за кибербезбедност на Африканската Унија.

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

ПРИМЕРИ ЗА ДОБРА ПРАКТИКА

Во ноември 2018 година во парламентот на Кенија беше поднесен на разгледување нов Предлог-закон за заштита на податоци. Предлог-законот содржи голем број елементи од европската Општа регулатива за заштита на лични податоци (ОРЗЛП). На пример, наложува организациите да ги информираат корисниците за тоа зошто се собираат нивните податоци, за кои цели се користат и колку долго организацијата ќе ги чува податоците. Предлог-законот, исто така, вклучува одредба која им дава право на потрошувачите да бараат од организациите да ги избришат нивните податоци. Освен тоа, наложува организациите да имаат одредено ниво на безбедносни стандарди за складирање податоци.

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

Во јуни 2018 година Франција донесе Општа уредба за заштита на личните податоци (Loi relative à la protection des données personnelles) за да го усогласи францускиот национален закон со Општата директива на ЕУ за заштита на лични податоци (ОРЗЛП). Надоврзувајќи се на францускиот Закон за заштита на податоци од јануари 1978 година, Законот од 2018 година ги проширува овластувањата за заштита на податоци што ги има Националната комисија за информирање и слободи (Commission national de l'informatique et des libertés – CNIL), со што ја зајакнува нејзината функција на следниов начин:

• Зголемена регулаторна надлежност за спроведување безбедносни прописи, кодекси на однесување и за изработка на референтни документи и препораки. Освен тоа, CNIL ќе има надлежност да одобрува сертификациски тела, како и овластување да сертифицира усогласеност на производи, лица и процедури со ОРЗЛП и со францускиот национален закон.

• Се зголемуваат надзорните овластувања, со што службениците на CNIL имаат право да поднесуваат барања за сите документи што не се заштитени со обврска за професионална тајна. Освен тоа, службениците на CNIL може да користат нови видови санкции, а и административните такси беа значително зголемени. Во случај компанијата да не ги заштити личните податоци, надоместоците на штета може да се движат од 10 милиони евра, или 2 % од нејзиниот севкупен приход, до 20 милиони евра, или 4 % од севкупниот приход (повисокиот од двата) за најтешките повреди.

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

Добра практика 5: Државите треба да изработуваат и ажурираат закони кои ја штитат критичната инфраструктура.

Критичните инфраструктурни објекти, познати и како CIIs, имаат суштинско значење за добросостојбата на општото население. Критичните инфраструктурни објекти се средства, системи, мрежи (физички и виртуелни) кои се од суштинско значење за виталните општествени функции, вклучувајќи ги здравјето, безбедноста и економската и социјалната добросостојба, и чиј прекин или уништување би имал значително негативно влијание врз населението.

Примерите за критични инфраструктурни објекти вклучуваат:

- Електрични централи
- Снабдувањето со храна и вода
- Јавна безбедност: безбедносни сили, служби за итни случаи, цивилна заштита
- Јавно здравје: болници и медицинска нега, лаборатории
- Јавна администрација
- Транспорт (на пр., патен, железнички и воздушен)
- Депонирање отпад (отпад и отпадни води)
- Финансиски услуги (пр., банки, осигурителни компании)
- Мрежи на информациски и комуникациски технологии

Значителен дел од критичните инфраструктурни објекти (CII) имаат вградено нови технологии за поддршка на нивното работење. Иако ваквата модернизација помогна оваа инфраструктура да биде поефикасна во обезбедувањето јавни добра за населението, истовремено ги изложи и на слабости кои би можеле да имаат разорни ефекти врз локалното население.

Државите имаат обврска да ги штитат од кибернапад критичните инфраструктурни објекти што се наоѓаат во рамките на нивните граници. Заштитата на овие објекти од кибернапади треба да биде приоритет во стратегијата за кибербезбедност на државата. За таа цел, државите треба да изработат и воведат мерки за кибероодбрана кои ги штитат ранливите делови од информациските системи на критичните инфраструктурни објекти. Таквите мерки треба да можат да ги откријат кибернападите, да обезбедат одбрана од нив и да ги неутрализираат.

ПРИМЕРИ ЗА ДОБРА ПРАКТИКА

Во март 2019 година Парламентот на Јужна Африка усвои закон за критични инфраструктурни објекти чија цел е, меѓу другото, да се обезбеди идентификување и прогласување на дадена инфраструктура за критична; да се предвидат упатства и фактори што треба да се земат предвид за да се обезбеди транспарентно идентификување и прогласување критична инфраструктура; и да се предвидат мерки што треба да се воспостават заради заштита, обезбедување и отпорност на критичната инфраструктура. Со законот, исто така, се формира Советот за критична инфраструктура и му се дава дискреciско право на министерот за внатрешни работи одредени објекти да ги прогласи за критична инфраструктура и пропишува како тие се заштитуваат во интерес на националната безбедност.

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

ГЛАВНИ НАОДИ

- **Меѓународните или регионалните рамки обезбедуваат низа норми за изработка, донесување и изменување на законодавство, политики и стратегии во полето на кибербезбедноста.**
- **Државите имаат примарна улога во обезбедување добро управување со кибербезбедноста.**
- **Државите треба да изработат, усвојат и ажурираат национални закони, политики и стратегии за регулирање на киберпросторот и за справување со актуелните предизвици во киберпросторот, вклучително во областите на заштита на приватноста и личните податоци, како и заштита на критичната инфраструктура.**
- **Зголемувањето на експертизата за киберпросторот преку едукација и споделување знаење, особено преку јавно-приватни партнерства (ЈПП), има суштинско знаење за добро управување со кибербезбедноста.**

Библиографија

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

ПОГЛАВЈЕ 5
НАЦИОНАЛНИ СТРАТЕГИИ ЗА КИБЕРБЕЗБЕДНОСТ

ЦЕЛИ

Ова поглавје има цел да им даде на корисниците на овој водич вовед во националните стратегии за кибербезбедност (НСК). Поточно, насочено е кон зголемување на знаењето на корисниците во однос на главните елементи на НСК и дава примери за добри практики

Целите за учење на ова поглавје се следните:

- Зголемено знаење во однос на националните стратегии за кибербезбедност воопшто.
- Зголемено знаење во однос на главните елементи на националната стратегија за кибербезбедност.
- Зголемена свесност во однос на расположливите ресурси кои може да им послужат на творците на национални закони и политики во изработката на национални стратегии за кибербезбедност.

Вовед

Уште од неговото создавање, киберпросторот обезбеди најразлични можности за економски, технолошки и социјален развој. Меѓутоа, истовремено во подем беа транснационални закани – како што се државно спонзорирана кибершпионажа, воени киберактивности, киберкриминал, кибертероризам и користење на Интернет за терористички цели. Доколку овие безбедносни ризици, кои се поврзани со киберпросторот или се овозможени преку него, не се соодветно балансирани со сеопфатни стратегии и акциски планови, државите нема да можат да ги заштитат националната и човечката безбедност, ниту да го одржат економскиот раст.

Затоа, државите низ светот изработуваат и приспособуваат стратегии за да можат да се справат со променливата ситуација на безбедносните закани, вклучително и преку донесување нови или изменување на постојните национални безбедносни политики. Националните безбедносни политики кои се фокусираат на заканите присутни во киберпросторот се нарекуваат национални стратегии за кибербезбедност (НСК).

НСК можат да бидат во различни форми, а во зависност од киберподготвеноста на земјата, нивното ниво на деталност се разликува. Бидејќи НСК зависат од контекстот, невозможно е да се има готов модел на ефективна НСК. Сепак, може да се идентификуваат одредени стратегиски приоритети кои се содржани во најголемиот дел од нив. Тие се регулациските рамки, заштитата на критичната инфраструктура, меѓународната соработка и јавно-приватната соработка, како и истражувањето и развојот.

Иако нема општо утврдена дефиниција за НСК, Меѓународната унија за телекомуникации (ITU) ја дефинира националната стратегија за кибербезбедност како:

- Изразување визија, цели на високо ниво, начела и приоритети по кои земјата се води во справувањето со кибернапади.
- Приказ на засегнатите страни задолжени за подобрување на кибербезбедноста на нацијата и нивните соодветни улоги и одговорности.
- Опис на чекорите, програмите и иницијативите кои земјата ќе ги преземе за да ја заштити својата национална киберинфраструктура, и притоа ќе ги зголеми нејзината безбедност и отпорност[1].

Бидејќи киберзаканите се развиваат со брзо темпо, исто така се развиваше и опсегот на НСК: од исклучива заштита на поединци и организации како засебни чинители кон заштита на општеството како целина.

1 Меѓународна унија за телекомуникации, Водич за изработка на национална стратегија за кибербезбедност, 2018, стр. 13

Во суштина, НСК се стреми да оствари две меѓусебно поврзани цели:

- **1. Зголемување на кибербезбедноста за економијата на Интернет да изврши понатамошно придвижување на економскиот и социјалниот просперитет, и**
- **2. Заштита од киберзакани на општествата зависни од киберпросторот.**

Кибербезбедноста е комплексен предизвик којшто опфаќа повеќе различни аспекти на управување, аспекти на политика, оперативни, технички и правни аспекти. Националните политики генерално ја дефинираат методологијата и ги поставуваат целите за остварување на националните приоритети.

Добра практика 1: Националната стратегија за кибербезбедност е вградена во поширокаата национална безбедносна политика на државата.

НСК треба да се смета за дополнителна алатка за постигнување стратегиски национални приоритети. Оттука, важно е за една земја да го смета НСК како дел од својата општа безбедносна стратегија. Тоа дополнително придонесува за сеопфатен пристап кон националната безбедност.

Вклучувањето на кибербезбедноста како важен елемент во националната безбедносна стратегија, и обратно, покажува разбирање од страна на државата дека киберпросторот е клучен дел од скоро секој аспект на националната безбедност.

ПРИМЕРИ ЗА ДОБРА ПРАКТИКА

Во шведската национална стратегија за кибербезбедност се наведува дека нејзината стратегија се „базира врз целите за безбедност на Шведска: заштита на животите и здравјето на населението, функционирањето на општеството и на нашиот капацитет за поддршка на фундаменталните вредности какви што се демократијата, владеењето на правото и човековите права и слободи“.

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

Во спроведувањето на својата национална стратегија за кибербезбедност Финска ги следи начелата и процедурите утврдени во Безбедносната стратегија за општеството.

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

При изработката на сеопфатна НСК важно е визијата и целите на земјата да се преточат во конкретни дејства што би придонеле кон остварување на целите кои првично биле идентификувани.

Следниов животен циклус на НСК изработен од Меѓународната унија за телекомуникации е наменет како водич за стратегиско размислување на корисникот на национално ниво:

Слика 1: Животен циклус на НСК врз основа на Водичот на Меѓународната унија за телекомуникации за изработка на национална стратегија за кибербезбедност

Пред да се почне со изработка на НСК, од суштинско значење е државата да ги идентификува целите и намената на таквата стратегија и јасно да ја изрази својата визија во контекст на кибербезбедноста.

СЛУЧАЈ ЗА АНАЛИЗА: МИСИЈА НА ОАД ЗА ТЕХНИЧКА ПОМОШ НА МЕКСИКО

Во 2017 година Организацијата на американски држави (ОАД), преку нејзината Програма за кибербезбедност, а по барање на Владата на Мексико, свика комисија на меѓународни експерти за да споделат најдобри практики со мексиканските субјекти, да ја увидат моменталната состојба со кибербезбедноста во Мексико, да ја идентификуваат актуелната состојба на зрелост на кибербезбедноста, како и да ја унапредат националната рамка за кибербезбедност.

Експертите во комисијата доаѓаа од приватниот сектор, од други држави, од техничката заедница, од меѓународни организации и од граѓанското општество.

(Извор: 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)

Добра практика 2: Процесот на изработка на Национална стратегија за кибербезбедност треба да биде раководен од водечки орган и да вклучува широк дијапазон на засегнати страни interesnih strana i učesnika.

Со цел да се започне процесот на изработка на НСК, треба да се идентификува водечки орган. Тоа може да биде некој субјект кој веќе постои или новоформирана агенција. Една од клучните одговорности на овој водечки орган треба да биде координацијата на процесот на неутрален начин. Тој треба да биде одговорен за идентификување клучни засегнати страни кои треба да бидат вклучени во изработката на НСК и за обезбедување континуирана размена со засегнатите страни заради искористување на соодветното знаење и експертиза во процесот на изработката на НСК. Покрај тоа, водечкиот орган треба да биде одговорен за јасно утврдување на улогите и одговорностите на овие клучни засегнати страни.

СЛУЧАЈ ЗА АНАЛИЗА: ЧИЛЕАНСКИ МЕЃУМИНИСТЕРСКИ КОМИТЕТ

Процесот на изработка на национална стратегија за кибербезбедност во Чиле го водеше Меѓуминистерски комитет, којшто го сочинуваат претставници на Министерството за внатрешни работи и јавна безбедност и Министерството за национална одбрана.

Овој Меѓуминистерски комитет организираше и координираше сесии на работни групи за теми идентификувани како соодветни за националната стратегија за кибербезбедност. Различните теми на работните групи вклучуваа: информациска инфраструктура, превенција и санкции, едукација и подигнување на свеста, соработка и меѓународни односи, институционализација. Постојани членови на овие работни групи беа потсекретаријатите за внатрешни работи, одбрана, заедничко претседателство, правда, економија, телекомуникации, како и Националната агенција за разузнавање.

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

Иако е очигледен фактот дека приватниот сектор има посебна улога во обезбедувањето кибербезбедност, соработката меѓу јавниот и приватниот сектор сепак не е секогаш институционализирана.

Јавно-приватната соработка е дополнително важна за заштита на критичната инфраструктура, затоа што најголем дел од критичната инфраструктура е поседувана и стопанисувана од приватни субјекти. Оттука, тие треба да бидат активно вклучени во планирањето за заштита на националната критична инфраструктура од киберзакани.

Вклучувањето на што поголем број засегнати страни во процесот на изработка на НСК има суштинско значење за да може тие да ја прифатат стратегијата како своја. Клучно за фазата на спроведување е она што се спроведува да се чувствува како

свое. Освен тоа, со вклучување на сите релевантни засегнати страни дополнително се обезбедува дека тие чинители со своето експертско познавање ќе придонесат кон поголем успех.

ПРИМЕРИ ЗА ДОБРА ПРАКТИКА

Со цел да обезбеди оптимален исход од својата НСК, Обединетото Кралство на својата веб-страница спроведе процес на отворена консултација за да може секој да даде коментар за стратегијата.

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

Канадската влада иницираше процес на јавна онлајн консултација за да го слушне мислењето на Канаѓаните, на приватниот сектор, научната заедница и на други информирани засегнати страни во однос на состојбата со кибербезбедноста во Канада. Извештајот од овој процес на консултации беше објавен и ставен на располагање онлајн.

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

Во Стратегијата за кибербезбедност на Обединетото Кралство се наведува дека за постигнување на целта за сигурен и безбеден Интернет неопходни се здружени напори од страна на сите: приватниот сектор, поединците и државата. Како што сите имаме придобивки од користењето на киберпросторот, така сите имаме и одговорност да помогнеме во негова заштита.

Иако јавно-приватните партнерства се најчестата форма на институционализација на соработката меѓу јавниот и приватниот сектор, сепак и понатаму постојат одредени предизвици. Особено во однос на мандатот на јавно-приватното партнерство, недоволната јасност во однос на улогите и одговорностите, недовербата меѓу засегнатите страни, пречките во споделувањето информации, немањето поттик за соработка, како и недостигот на ефективен надзор, а со тоа и на отчетност.

СЛУЧАЈ ЗА АНАЛИЗА: ИДЕНТИФИКУВАЊЕ НА РЕЛЕВАНТНИТЕ ЗАСЕГНАТИ СТРАНИ

Сите засегнати страни не мора да бидат вклучени во секоја дискусија. Важно е да се идентификуваат релевантните засегнати страни кои имаат директен интерес и стручно знаење за да може да придонесат кон дискусијата.

Во продолжение е даден список на релевантни засегнати страни во изработката на НСК. Иако списокот не е исцрпен, сепак дава добар приказ на релевантните засегнати страни.

- **Држава:** релевантни министерства (ИКТ, економија, комуникации, итн.), регулаторни агенции, правосудство и служби за спроведување на законот, одбранбени и безбедносни служби
- **Приватен сектор:** компании за ИКТ, компании за информациска безбедност, деловни здруженија
- **Граѓанско општество:** групи кои имаат одредени интереси (како што се заштита на човековите права или на децата онлајн), идентитетски групи (вера, малцинство, права на жените), мрежи на организации од граѓанското општество.
- **Научна заедница:** универзитети, истражувачки субјекти, аналитички центри, самостојни истражувачи
- **Техничка заедница:** тимови за одговор при компјутерски инциденти, тимови за одговор при безбедносни компјутерски инциденти, организации за системска стандардизација на имиња на домени
- **Меѓународни орг.:** регионални и меѓународни организации (како што се Африканската Унија, ОБСЕ, ОАД, Советот на Европа), меѓународни институции (на пр., Светската банка, Меѓународната унија за телекомуникации)

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

Добра практика 3: Процесот на изработка на национална стратегија за кибербезбедност треба да вклучува обемна анализа на силните и на слабите страни на кибербезбедноста на земјата.

Како следна фаза во процесот на изработка на НСК важно е да се изврши процена и анализа на состојбата со кибербезбедноста во земјата за да се идентификуваат силните страни и слабостите во кибербезбедноста на таа земја. Во рамките на овие напори за процена и анализа, треба да се изврши мапирање и анализа на националната регулаторна рамка (вклучително закони, прописи, политики и програми поврзани со кибербезбедноста), на националната критична инфраструктура и на јавно-приватните партнерства, како и на техничките и институционалните капацитети за спречување ризици за кибербезбедноста (како што се тимови за одговор при компјутерски инциденти) и на заштита од закани за кибербезбедноста (како што се службениците за заштита на податоци).

Со процесот на анализа се врши процена на нивото на зрелост на кибербезбедноста на земјата за да се обезбеди дека НСК ќе биде по мера на актуелните потреби на самата таа земја.

СЛУЧАЈ ЗА АНАЛИЗА: МОДЕЛ НА ЗРЕЛОСТ НА КАПАЦИТЕТОТ ЗА КИБЕРБЕЗБЕДНОСТ, МИНИСТЕРСТВО ЗА КОМУНИКАЦИИ НА ГАНА

Капацитетот за кибербезбедност на Гана беше оценет преку Моделот за киберзрелост, изработен како алатка што треба да помогне во анализа на капацитетите за кибербезбедност на Гана од аспект на пет различни димензии:

- Политика и стратегија за кибербезбедност
- Киберкултура и киберопштество
- Едукација, обука и вештини за кибербезбедност
- Правни и регулаторни рамки
- Стандарди, организации и технологии.

Целта на оваа процена беше да ѝ се овозможи на владата на Гана подобро да ги разбере своите силни страни и слабости во однос на кибербезбедноста и следствено на тоа да го зголеми ефективното вложување во градење капацитети.

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

Врз основа на оваа процена, може да се изработи НСК под водство на посветен орган и со обемно вклучување на клучни засегнати страни. Идеално би било да се формираат работни групи за изработка на посебни делови од НСК во зависност од релевантната стручност на работната група. Добра практика е, пред да се донесе НСК, да се спроведе процес на анализа на НСК, во форма на онлајн консултации или работилници меѓу најразлични засегнати страни. На тој начин се овозможува НСК да биде заснована врз заедничка визија.

Во зависност од конкретната процедура на усвојување што се применува, овластување за донесување на НСК имаат собранието или владата. Усвоената НСК треба да биде објавена во службен весник или на веб-страницата на соодветното министерство, за да биде населението свесно за нејзиното постоење и за нејзината содржина, како и за приоритетите на државата во однос на кибербезбедноста, а таа може активно да придонесе кон остварувањето на стратегиските приоритети идентификувани во неа.

Не постои единствен пристап кога станува збор за структурирањето на процесот на изработка на НСК. Добрите практики ќе се разликуваат во зависност од опсегот на НСК, опсегот на вклучените засегнати страни и расположливите технички барања.
Во Чиле, Кенија и во Мексико нацрт-верзијата на НСК беше објавена и онлајн за да им се овозможи на различните засегнати страни да дадат свој коментар за неа и да ја прифатат како своја.

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

Најголем дел од НСК ја истакнуваат важноста на меѓународната соработка заради унапредување на кибербезбедноста и потребата од поефективни сојузи и партнерства со земји кои се истомисленички, вклучувајќи го и градењето капацитети. Освен тоа, повеќето НСК ги препознаваат почитувањето на основните права, особено правото на приватност и слободата на изразување и мислење, како и слободниот проток на информации, како незаменливи за постоење на безбеден киберпростор.

Покрај тоа, најголем дел од НСК како стратегиски приоритет ја вклучуваат превенцијата на киберкриминалот.

ПРИМЕРИ ЗА ДОБРА ПРАКТИКА

Канадската национална стратегија за кибербезбедност ги одразува канадските вредности, како што се владеењето на правото, отчетноста и приватноста.

(Извор: 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)

Националната стратегија за информациска и комуникациска технологија на Малави истакнува дека државата и понатаму ќе обезбедува погодна средина за еднакво учество и на јавниот и на приватниот сектор во изработката, воспоставувањето и користењето на ИКТ во урбаните и во руралните заедници.

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

Добра практика 5: Да се идентификува националната критична инфраструктура што ќе се вклучи во НСК.

Идентификувањето на националната критична инфраструктура има суштинско значење за развој на политики за нивна заштита од киберзакани. Без јасна дефиниција и список за тоа што претставува критична инфраструктура, тешко е овие критични елементи да бидат заштитени од киберризици.

Сè поголем дел од критичната инфраструктура е зависна од информациско-комуникациската технологија за своето работење и функционирање. Заштитата на националната критична инфраструктура од киберзакани има витално значење затоа што може да има последици во реалниот свет – и следствено на тоа, таа обично е вклучена како приоритет во националните стратегии за кибербезбедност на голем број држави.

Затоа, сè повеќе држави вршат идентификување на својата национална критична инфраструктура. Најголем дел од нив ги идентификуваат водата, електричната енергија и болниците како национална критична инфраструктура.

Директивата 2008/114/ЕЗ на Советот на ЕУ од 8 декември 2008 година за идентификувањето и означувањето на европската критична инфраструктура и проценатa на потребата од подобрување на нивната заштита, претставува важен документ во оваа насока. Поточно, оваа Директива на Европската Унија ја дефинира критичната инфраструктура како „елемент, систем или дел од него што се наоѓа во земјите членки, којшто е од суштинско значење за одржувањето на виталните општествени функции, здравјето, безбедноста, сигурноста, економската или социјалната добросостојба на луѓето, и чиј прекин или уништување би имале значително влијание во дадена земја членка како резултат на неодржувањето на тие функции“.

ПРИМЕРИ ЗА ДОБРА ПРАКТИКА

Член 17 од јужноафриканскиот Предлог-закон за заштита на критичната инфраструктура ги наведува факторите кои треба да бидат земени предвид при прогласување на нешто за критична инфраструктура. Такви фактори се, на пример: секторот во кој се одвиваат примарните функции на таквата инфраструктура; стратегиската важност, вклучително потенцијалното влијание од уништувањето, прекинот, откажувањето или деградацијата на таквата инфраструктура или прекинот на услуга кој може да влијае врз способноста на Јужноафриканската Република да функционира, да обезбедува основни јавни услуги или да ги одржува законот и редот; категоријата на ризик на таквата инфраструктура; ресурсите што му се на располагање на лицето кое ја контролира инфраструктурата; ефектите или ризикот од уништување, прекин, откажување или деградација на таквата инфраструктура; големината и локацијата на кое било население во ризик; претходни инциденти што резултирале со уништување; нивото на ризик или на закани на коишто е изложена таквата инфраструктура; посебните карактеристики или атрибути на таквата инфраструктура; обемот во кој прогласувањето на таа инфраструктура за критична би го унапредило интересот на јавноста; и кои било други фактори што може да ги пропише министерот.

Извор: https://pmg.org.za/bill/644/

Германската стратегија за национална критична инфраструктура (2009 г.) ја дефинира критичната инфраструктура како „организациски и физички структури и капацитети од такво витално значење за општеството и економијата на една земја што нивното откажување или деградација би резултирале со пролонгирани периоди на недостиг во снабдувањето, значителен прекин на јавната безбедност и сигурност, или други драматични последици“.

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

Франција ја дефинира критичната инфраструктура како „институции, структури или капацитети кои ги обезбедуваат суштинските стоки и услуги што го сочинуваат столбот на француското општество и неговиот начин на живот“. Самите оператори го составуваат списокот на критична инфраструктура, во кој може да бидат, на пример, производствени локации, контролни центри, мрежни јазли или податочни центри.

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

Швајцарија ги вклучува следниве сектори како дел од критичната инфраструктура: институции, енергија, депонирање отпад, финансии, здравство, вода и храна, информации и комуникација, транспорт, јавна безбедност.

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

Добра практика 6: Националната стратегија за кибербезбедност предвидува план за спроведување, вклучително и од аспект на истражувањето и развојот.

НСК е ефективна колку што е успешно нејзиното спроведување. Па така, ефективното спроведување на НСК зависи од донесувањето на план за спроведување (понекогаш се нарекува и акциски план), кој треба да ја преточи стратегијата во конкретни дејства и политики преку координирање на напорите и ресурсите.

Суштински дел од планот за спроведување е изработката на клучни показатели за следење и оценување на успешноста на НСК. При процесот на следење, државата треба да се погрижи НСК да биде спроведена согласно нејзиниот акциски план. Во фазата на оценување, пак, треба да процени дали НСК сè уште ги одразува своите цели и приоритети – и доколку не, да изврши нивно повторно оценување.[2]

Планот за спроведување треба да ги вклучува воспоставувањето механизам за пријавување инциденти и начинот за подигање на свеста на луѓето во однос на ризиците и заканите во киберпросторот. Пријавувањето компјутерски безбедносни инциденти игра суштинска улога во целокупното подобрување на националната кибербезбедност. Таквото пријавување придонесува за приспособување кон променливата ситуација со заканите според списокот мерки за кибербезбедност. Неопходен предуслов за пријавувањето е соработката меѓу јавниот и приватниот сектор. Оттука, довербата има витално значење во поддршка на отвореното споделување информации во однос на ризиците и заканите за киберпросторот. Воспоставувањето тим за одговор на компјутерски инциденти (CSIRT) се смета за основа на ефективното координирање на управувањето со инциденти.

2 Водич на Меѓународната унија за телекомуникации за изработка на стратегија за кибербезбедност, стр. 26.

За да биде планот за спроведување ефективен, треба да има иницијативи за подигнување на свеста во однос на индивидуалниот корисник и неговото/нејзиното знаење за заканите и ранливостите од полето на кибербезбедноста. Ова е многу важно за да се обезбеди дека индивидуалниот корисник знае како да се заштити себеси од ризици во киберпросторот кои потенцијално може да влијаат врз националната кибербезбедност на земјата.

Вложувањето во истражување и развој (R&D) и нивното негување е дополнителен предуслов за развој на нови алатки за одвраќање, заштита, откривање и приспособување во однос на сите видови киберзакани.

ПРИМЕРИ ЗА ДОБРА ПРАКТИКА

НСК на Кенија ја утврдува следнава цел: „Владата на Кенија е посветена на безбедноста, сигурноста и на просперитетот на нашата нација и на нејзините партнери. За нас кибербезбедноста е клучна компонента во таа заложба, затоа што им дава на организациите и на поединците зголемена доверба во онлајн и мобилните трансакции, поттикнува поголеми странски вложувања и отвора поширока палета трговски можности во рамки на глобалниот пазар. Успешното спроведување на стратегијата дополнително ќе ѝ овозможи на Кенија да ги постигне своите економски и општествени цели преку безбедна онлајн средина за граѓаните, индустријата и за странските партнери за водење бизнис“. (стр. 4)

Националната стратегија за кибербезбедност на Нигерија го идентификува индивидуалниот корисник како најслаба алка во синџирот на кибербезбедноста. Па така, стратегијата предвидува „иницијативи и мерки кои помагаат да се заштити општата јавност што користи Интернет, обезбедува материјали и алатки кои помагаат во заштита на граѓаните на Нигерија од киберзакани и штетни ранливости“.

(Извор: Нигерија, Национална стратегија за кибербезбедност, поглавје единаесет.)

Националната политика за ИКТ на Малави е придружена од детална Стратегија за спроведување, следење и оценување, додека спроведувањето на политиката за ИКТ се следи и оценува на годишно ниво во однос на неговата ефективност и одговорност или онака како што е пропишано. (Извор: Малави, Национална политика за ИКТ, 2013, стр. 11)

Националната стратегија за кибербезбедност на Мавританија во својата политика вклучува детален план за спроведување на самата политика. (Извор: Maurétanie, Stratégie Nationale de Modernisation de l’Administration et des TICs 2012-2016)

Националната стратегија за кибербезбедност на Полска како клучна компонента го идентификува зголемувањето на свесноста на корисниците за методите и безбедносните мерки во киберпросторот. (Полска, Национална стратегија за кибербезбедност, 2013 г.)

Тунис, Јужна Африка и Кенија имаат воспоставено функционални тимови за одговор при компјутерски инциденти (ЦЕРТ).

Добра практика 7: Да се обезбедат доволно ресурси за да се изработат кампањи за подигнување на свеста за кибербезбедноста наменети за општата јавност кои ќе го придружуваат спроведувањето на НСК.

Сите кои се поврзани на Интернет – од владини службеници, деловни сопственици, финансискиот и трговскиот сектор, па сè до општата јавност, како и децата – се ранливи на закани во однос на кибербезбедноста.

Генерално, постои општото разбирање дека кибербезбедноста не е одговорност само на една служба, субјект или поединец, туку е споделена одговорност на сите кои се поврзани на Интернет или користат апликации што се поврзани во онлајн просторот.

Според Организацијата на американските држави (ОАД), „киберкриминалот го сочинуваат најразлични поведенија и техники – вклучително кражба на идентитет, детска експлоатација, кибермалтретирање, внатрешни закани, фишинг, спеар фишинг и многу, многу други – кои треба да се третираат“.[3]

Бидејќи секој може да биде засегнат од различните видови киберкриминал, од пресудно значење е да се едуцира јавноста во однос на ризиците и заканите во киберпросторот.

СЛУЧАЈ ЗА АНАЛИЗА: ЗБИРКА АЛАТКИ ЗА КАМПАЊА ЗА ПОДИГНУВАЊЕ НА СВЕСТА ЗА КИБЕРБЕЗБЕДНОСТ – АНАЛИЗА НА СОСТОЈБАТА

Доброто разбирање на актуелниот контекст од аспект на заканите за кибербезбедноста е клучно за развој на успешни кампањи за подигнување на свеста.

Во таа насока, ОАД составија некои прашања-водилки кои помагаат во анализирањето на актуелната состојба:

- Колку е поврзана вашата земја?
- Каде и како луѓето се поврзани на Интернет?
- Кој е онлајн?
- Со помош на каков уред?
- Какви видови оперативни системи и канали за комуникација се користат?
- За какви производи и услуги?
- Како се користи Интернетот за деловно работење?

3 ОАД (2016 г.): Збирка алатки за подигнување на свеста за кибербезбедноста, стр. 8. Достапно на: https://thegfce.org/wp-content/uploads/2020/06/2015-oas-cyber-security-awareness-campaign-toolkit-english-1.pdf

- Каков е обемот на таквото деловно работење (на пр., трговец-поединец, земјоделска задруга, мали и средни претпријатија, лесно производство?)
- Со кои ризици за кибербезбедноста се соочува вашата земја?
- Со каков киберкриминал се соочуваат потрошувачите на мало?
- Со каков киберкриминал се соочуваат вашите компании?
- Дали овие видови киберкриминал се разликуваат според кохорта?
- Кои се ризиците за вашата критична инфраструктура?
- Дали во неодамнешното минато имало некои поголеми упади во владиниот или во трговскиот сектор?
- Дали има закани за поголеми упади во иднина?
- Кои се економските загуби или потенцијалот од киберзаканите?

Извор: ОАД, Збирка алатки за кампањи за подигнување на свеста од 2016 г. Достапно на: **https://thegfce.org/wp-content/uploads/2020/06/2015-oas-cyber-security-awareness-campaign-toolkit-english-1.pdf**

Успешните кампањи за подигнување на свеста пренесуваат пораки кои се лесни за разбирање, специфични за целта и планирани и развиени во рамки на процес со повеќе засегнати страни, во кој се вклучени владини служби, приватни компании (како што се даватели на услуги за Интернет, телекомуникациски компании), како и претставници на граѓанското општество, како што се невладините организации, медиумите и научната заедница.

ПРИМЕРИ ЗА ДОБРА ПРАКТИКА

Во 2015 година Јордан донесе Закон за сузбивање на киберкриминалот и беше формирана специјализирана единица, т. е. Одделение за киберкриминал. Ова Одделение, потпомогнато од Канцеларијата на ОН за борба против дроги и криминал, изработи видеозапис за подигнување на свеста за ризиците, видовите и правните последици од киберкриминалот.

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

StaySafeOnline, којашто е поддржана од Националниот сојуз за кибербезбедност од САД, се труди да поттикне култура на кибербезбедност. За таа цел, на својата веб-страница објави информативен графикон преку кој се објаснува како да се уверите дека сите во домот – вклучително и децата и постарите лица – го користат Интернет на безбеден и одговорен начин.

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

ГЛАВНИ НАОДИ

- **Со цел да се справат со актуелните и со новите закани за кибербезбедноста, државите треба постојано да ги следат и да ги приспособуваат своите национални стратегии за кибербезбедност согласно променливите закани.**
- **Од суштинско значење е да се постават конкретна цел и стратегиски приоритети за да може националната стратегија за кибербезбедност да биде успешна.**
- **Стратегиите за кибербезбедност треба да ги препознаат почитувањето на основните права, како што се приватноста и слободата на изразување и верување, како и слободниот проток на информации, со цел да промовираат слободен и отворен киберпростор.**
- **Кибербезбедноста е прашање што опфаќа различни сектори и одговорности на различни јавни служби. Оттука, тесната соработка меѓу сите државни служби, како и со приватниот сектор, претставува важен столб за успешно спроведување на националната стратегија за кибербезбедност.**
- **За да се развијат нови алатки за одвраќање, заштита, откривање и приспособување во однос на новите видови киберзакани, државите треба да вложат повеќе средства во истражување и развој.**
- **За да се заштити националната критична инфраструктура од киберзакани, важно е прво да се дефинира што се смета за „национална критична инфраструктура“ во даден контекст.**

БИБЛИОГРАФИЈА

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

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

ПОГЛАВЈЕ 6
ЕФЕКТИВНА СОРАБОТКА МЕЃУ ЈАВНИОТ И ПРИВАТНИОТ СЕКТОР ВО КИБЕРПРОСТОРОТ

ЦЕЛИ

Ова поглавје има цел да им обезбеди на корисниците преглед на силните страни и на предизвиците поврзани со јавно-приватните партнерства во киберпросторот, особено меѓу службите за спроведување на законот и приватните компании при истраги за кривични дела и незаконска содржина на Интернет.

Целите за учење за ова поглавје се следните:

- Зголемено знаење за концептите на иницијативи со повеќе засегнати страни и јавно-приватни партнерства.
- Зголемена свесност за соработка меѓу службите за спроведување на законот и приватните компании.
- Зголемено разбирање на елементите за создавање ефективни пристапи кон кибербезбедноста со повеќе засегнати страни.

Вовед

Кибербезбедноста е трансверзално поле, па оттука, заедничка цел на сите национални стратегии за кибербезбедност (НСК) е соработката помеѓу јавните и приватните чинители во насока на подобрување за кибербезбедноста. Пристапите со повеќе засегнати страни кон киберпросторот и кибербезбедноста, кои се нарекуваат и јавно-приватни партнерства (ЈПП), стануваат сè посуштински во управувањето со кибербезбедноста, делумно поради огромната улога што ја имаат приватните компании и поради транснационалната карактеристика на киберпросторот. Ефективната соработка помеѓу сите засегнати страни – особено државата, ИКТ секторот, научната заедница и граѓанското општество – стана суштински елемент во спроведувањето меѓународни стандарди и норми и за ефективна НСК.

Растечките напори во однос на кибербезбедноста кои комбинираат јавни, јавно-приватни и приватни механизми се показател за посуштинска промена во начинот на кој се води бизнис во глобални рамки. Од аспект на овој тренд, соработката меѓу различни засегнати страни – државата, бизнис-заедницата и граѓанското општество – може да се смета за прагматичен одговор за надополнување на некои од пропустите во управувањето што ги има кај традиционалните регулаторни пристапи. Впрочем, таквите иницијативи имаат цел да го поддржат ефективното управување на тој начин што ќе се погрижат комерцијалните чинители да работат во рамки на владеењето на правото и почитувањето на човековите права. Групи составени од различни засегнати страни заедно може да изработат подобри пристапи и решенија отколку што би биле изработени само од една група засегнати страни.

1. Разбирање на концептот на јавно-приватни партнерства

Преглед

Јавно-приватните партнерства вклучуваат споделување на ресурсите (средства, вештини, експертиза и финансирање), ризиците и наградите меѓу засегнатите страни. Во полето на кибербезбедноста, ЈПП означува соработка меѓу владата и јавните институции од една страна, и индустријата за ИКТ, научната заедница и граѓанското општество од друга страна, во насока на зголемување на свесноста за кибербезбедноста, ублажување на ризиците за кибербезбедноста и обезбедување силни национални капацитети за кибербезбедност. Оваа соработка е повеќестрана и може да вклучува подобрување на капацитетите за киберодбрана и споделување информации. Економските интереси, регулаторните барања и односите со

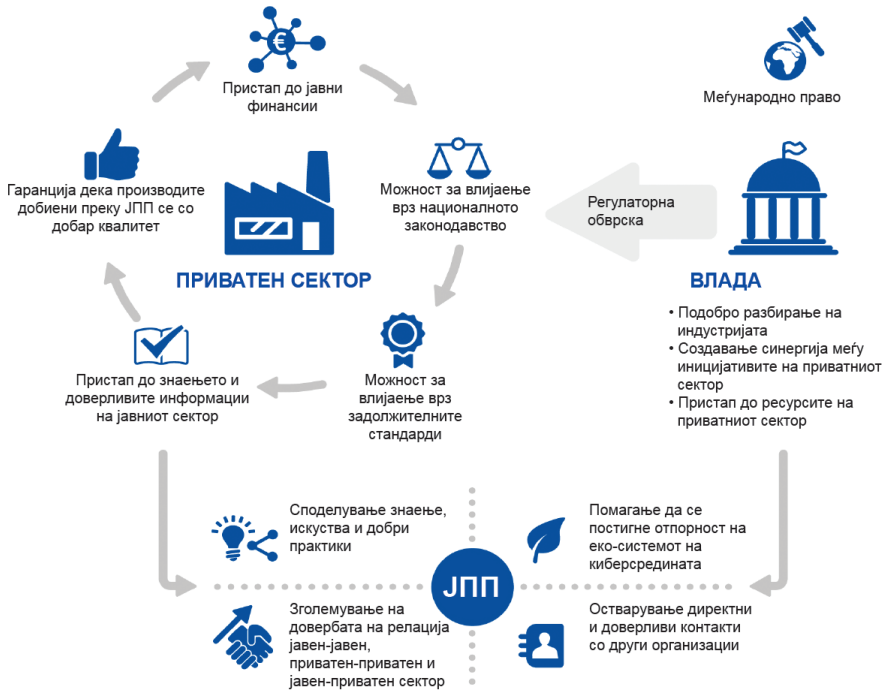
јавноста, исто така, може да бидат двигатели за ЈПП. Во земјите во развој, ЈПП во полето на кибербезбедноста главно се однесуваат на зголемување на свесноста за кибербезбедноста или на обезбедување силни национални капацитети за кибербезбедност.

ЈПП може да бидат од корист во полето на кибербезбедноста од неколку причини:

- Да поттикнат зголемување на свесноста за кибербезбедноста и разбирање во рамки на организациите во целото општество;
- Да ја збогатат националната база на кибервештини преку создавање иницијативи со цел да се идентификуваат и инспирираат повеќе луѓе и да им се овозможи да станат професионалци во полето на кибербезбедноста;
- На професионалците во полето на кибербезбедноста да им се обезбедат неопходните финансиски и технички ресурси преку посветени иницијативи;
- Заради истражување и развој во сферата на кибербезбедноста;
- Заради превенција на криминал и постапување во случај на измами;
- Заради сертификација и акредитација за кибербезбедност;
- За поврзување и поттикнување соработка меѓу јавни и приватни субјекти кои работат во полето на кибербезбедноста.

Јавно-приватните партнерства во полето на кибербезбедноста може да се категоризираат според следниве четири типа:

- Институционални ЈПП: воспоставени со правен акт поврзан со заштита на критична инфраструктура. Најчести начини на соработка се работни групи, групи за брзо реагирање и долгорочни заедници.
- Целноориентирани ЈПП: воспоставени со цел градење култура на кибербезбедност преку платформа или совет кој ги обединува јавниот и приватниот сектор заради размена на знаење и добри практики. Се фокусира на една тема или конкретна цел.
- Екстернализирани услуги за кибербезбедност: се воспоставуваат кога државите не можат ефективно да ги задоволат потребите на приватниот сектор што ги имаат идентификувано. ЈПП дејствуваат како автономно трето лице, но активно се занимаваат со потребите на индустријата и ѝ даваат поддршка на државата во создавањето политики или во нивното спроведување.
- Хибридни ЈПП: тимови за одговор при компјутерски инциденти (ЦЕРТ) кои работат во склоп на ЈПП. Владите им ја доверуваат на овие ЈПП задачата за обезбедување ЦЕРТ услуги на јавната администрација или на целата земја.



Причини и поттик за основање јавно-приватни партнерства
Извор: Јавно-приватни партнерства во киберпросторот, ENISA, ноември 2017 г., стр. 14

2. Улога на државите и на другите засегнати страни

Клучна улога на јавните институции во соработката со повеќе засегнати страни

Државите имаат примарна одговорност да развиваат ефективни НСК. Според тоа, творците на закони и политики се одговорни за создавање соодветни рамки согласно обврските на државата кои произлегуваат од меѓународното право, како и согласно нејзиното национално законодавство. Државите соработуваат со приватните чинители, како што се компаниите за ИКТ, во обезбедување доследност на корегулацијата и на саморегулацијата со меѓународното право за човекови права и со националните закони.

Покрај овој чисто законодавен пристап, државите може да играат важна улога во координирање и соработка со секторот на ИКТ и граѓанското општество преку создавање и поддржување колаборативни платформи. Тие се од особена важност за националните единици за упатување, кои пребаруваат и сигнализираат сомнителни онлајн контакти и бараат отстранување на содржина преку процеси на упатување со компаниите за ИКТ. Колаборативните платформи може да им обезбедат драгоцени информации на владите и да придонесат кон негување на поинклузивен процес на одлучување. Каналите за отворена комуникација помеѓу релевантните засегнати страни, исто така, помагаат да се идентификуваат и

затворат клучните пропусти во кибербезбедноста и да се отстранат потенцијалните судири на интерес. Институционализираните и координираните напори може да промовираат и комплементарни активности на различни засегнати страни, како и канализирање на човечки и финансиски ресурси помеѓу нив

СЛУЧАЈ ЗА АНАЛИЗА: ТИМОВИ ЗА ОДГОВОР ПРИ КОМПЈУТЕРСКИ ИНЦИДЕНТИ

Тимовите за одговор при компјутерски инциденти (ЦЕРТ) се единици на стручни лица чија задача е да им помогнат на поединците или институциите кои биле жртви на кибернапад. Нивна главна задача е да идентификуваат непријателски злонамерен софтвер и да спречат негово понатамошно ширење во мрежата, а притоа да ги ублажат последиците од нападот. Таквите единици се честопати составен дел од приватни компании или јавни институции, но може да постојат и на национално ниво како одделни владини агенции кои ги нудат своите услуги на најразлични приватни и јавни субјекти.

Иако националните ЦЕРТ се јавни служби, тие претставуваат добар пример за јавно-приватна соработка. Основната функција на секој ЦЕРТ е да обезбеди информации за неодамна откриени киберранливости, вклучително и релевантни софтверски ажурирања и крпеници. Најголем дел од националните ЦЕРТ може да примаат известувања за киберризици или киберинциденти преку јавен онлајн формулар. Освен тоа, некои национални ЦЕРТ располагаат со мобилни тимови кои може да се пратат во институцијата на која ѝ треба помош во случај на кибернапад.

Соработката меѓу јавниот и приватниот сектор има суштинско значење заради одржување стабилна и безбедна киберсредина. Јавните институции не можат сами да го обезбедат киберпросторот од две главни причини. Како прво, приватниот сектор е двигател на иновации во полето и го контролира најголем дел од киберпросторот. Како второ, дури и државата да ја поседува или контролира критичната киберинфраструктура, во однос на нејзината заштита таа во голема мера зависи од производите и услугите на приватните компании.

Освен тоа, државите се обврзани да ги почитуваат и штитат човековите права на своите граѓани онлајн, па затоа мора да се погрижат ниту една од постапките на приватните компании и националните ЦЕРТ да не врши повреда на човековите права, особено на правото на приватност и слободно изразување. За да ја исполнат оваа цел, ЦЕРТ треба да бидат независни од политичко влијание и да не служат како владини инструменти за повреда на приватноста на компјутерските системи и мрежи или приватноста и тајноста на комуникацијата.

При формирањето национални ЦЕРТ, владите треба да ја имаат предвид човечката димензија на кибербезбедноста во сите три нејзини аспекти: доверливост, пристапност и интегритет. Оттука, мора да се разбере дека кибербезбедноста во основа не се сведува на обезбедување мрежи, туку на подобрување на човековата безбедност. Што се однесува на заштитата

на доверливоста на информациите, правото на приватност треба да биде водечки стандард во сите операции за заштита и подобрување на доверливоста на податоците. Што се однесува на достапноста на податоците, од суштинско значење е да се почитуваат и штитат слободата на изразување и информации.

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

СЛУЧАЈ ЗА АНАЛИЗА: ЕДИНИЦИ ЗА УПАТУВАЊЕ НА ИНТЕРНЕТ НА НИВО НА ЕУ И НА НАЦИОНАЛНО НИВО

Единицата за упатување на Интернет (IRU) на Европската Унија е дел од Европскиот центар за борба против тероризам на Европол и е составена од тим на експерти за религиски мотивиран тероризам, јазици, изработувачи на информациски и комуникациски технологии и служби за спроведување на законот специјализирани за борба со тероризам[1] Започна со работа во 2015 година и ги има следниве надлежности:

- Да им обезбедува поддршка на надлежните органи на ЕУ преку обезбедување стратегиска и оперативна анализа;
- Да алармира за терористичка и насилна екстремистичка онлајн содржина и да ги споделува тие информации со релевантни партнери;
- Да открива и да бара отстранување на интернет-содржината користена од мрежи за криумчарење за привлекување мигранти и бегалци;
- Брзо да го спроведе и помогне процесот на упатување, во тесна соработка со индустријата[2].

NCпоред извештајот за транспарентност на Единицата за упатување на Интернет на ЕУ (EU IRU) од 2017 година, „соработката со приватниот сектор е од фундаментално значење за превенцијата“.[3] Од нејзиното основање во јули 2015 до декември 2017 година, Единицата (EU IRU) оцени 46.392 материјали со терористичка содржина за кои беа донесени 44.807 одлуки за упатување, при што стапката на отстранување содржина беше 92 проценти.[4]

Како што е наведено во извештајот за транспарентност и во надлежностите на Единицата, таа е одговорна за оценување онлајн содржина и нејзино упатување до соодветната компанија за ИКТ којашто е домаќин на содржината што треба да се отстрани. Како таква, Единицата се фокусира на содржина објавена од Ал каеда и Даеш и сродни групи и ја оценува таа содржина од аспект на мандатот на Европол, во согласност со начелата утврдени во Директивата на ЕУ за борба против тероризмот. Директивата на ЕУ за борба против тероризмот предвидува заштитни мерки во однос на отстранувањето содржина наведено во член 21 (3):

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

Мерките за отстранување и блокирање мора да се воспостават во рамки на транспарентни процедури и да обезбедат адекватна заштита, поточно да се обезбеди дека таквите мерки се ограничени на она што е неопходно и сразмерно и дека корисниците се информирани за причината за таквите мерки. Заштитните мерки што се однесуваат на отстранување или блокирање ја вклучуваат и можноста за судски правен лек.[5]

Доколку оценетата содржина врши повреда согласно надлежностите на Европол, таквата содржина се упатува до компанијата за ИКТ на чија платформа била откриена содржината. Во секој случај, на крајот одлуката дали пријавената содржина ќе биде отстранета или не ѝ се препушта на компанијата, откако таа ќе изврши процена во однос на нејзините услови за користење на услугите. Единицата за упатување на Интернет нема никакви законски овластувања за отстранување содржина.

Слични единици за упатување постојат во Обединетото Кралство, во Франција и во Холандија, додека во изјавите на Европол се наведува дека паралелни механизми се воспоставени во Белгија, Германија и во Италија.[6]

Освен тоа, Единицата за упатување на Интернет на ЕУ организира таканаречени заеднички Акциски денови на упатување со компаниите за ИКТ, како што се „Гугл“, „Твитер“ и „Телеграм“. Таквите Акциски денови на упатување ги собираат на едно место специјализираните единици за спроведување на законот од повеќе национални единици за упатување, потоа Единицата за упатување на Интернет на ЕУ и компаниите за ИКТ. Специјалистите за спроведување на законот оценуваат неколку стотици материјали со потенцијална терористичка содржина на посебна платформа и се стремат да идентификуваат шеми на користење на платформата од терористи и насилни екстремистички групи. Наодите потоа се споделуваат со соодветната компанија за ИКТ која учествува на настанот, којшто ја оценува пријавената содржина во однос на нејзините услови и одредби за користење. Крајната одлука за отстранување на пријавената содржина ја има компанијата. Заедничките Акциски денови на упатување промовираат координиран пристап меѓу владите и компаниите за ИКТ во справувањето со насилна екстремистичка и терористичка содржина на Интернет.[7]

Иницијативи предводени од индустријата за ИКТ и од граѓанското општество

Компаниите за ИКТ честопати се соочени со предизвици за корегулација и саморегулација во однос на нивните платформи, особено кога станува збор за заштита на човековите права, како што се слободата на говор и правото на приватност. Овие предизвици беа интензивирани со фактот дека платформите на социјалните медиуми станаа основни алатки преку кои општеството дискутира, споделува

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

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

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

и пристапува до информации. Како одговор на тоа, иницијативи предводени од индустријата за ИКТ – како што се споделувањето знаење и технологија меѓу компании; создавањето платформи за интерактивни алатки и ресурси за модерација на содржина; и обуки организирани од поголемите компании за помалите во однос на пристапи кон отстранувањето содржина – може да бидат делотворни алатки за зајакнување на кибербезбедноста.

СЛУЧАЈ ЗА АНАЛИЗА: INHOPE

Меѓународната асоцијација за дежурни линии на Интернет има глобално присуство во 43 земји и се труди да придонесе за Интернет во кој ќе „нема сексуална злоупотреба и експлоатација на деца“[8] Нејзината мисија е да ги „зајакне меѓународните напори за сузбивање материјали со сексуална злоупотреба на деца“.[9] INHOPE работи здружено со разни засегнати страни, меѓу кои Интерпол, Европол, „Твитер“, „CRISP“, „Мајкрософт“, „Гугл“, „Фејсбук“ и „Тренд МИКРО“.

INHOPE се состои од 48 дежурни линии кои ѝ обезбедуваат механизам на јавноста да пријавува онлајн содржина или активност за која се сомнева дека е незаконска. INHOPE ги дели незаконските активности во две различни категории: кривични нелегални активности кои се истражуваат и гонат од службите за спроведување на законот, на коишто INHOPE се фокусира, и граѓански нелегални активности кои може да се гонат од граѓански тела.

Примарен интерес на INHOPE се материјалите со сексуална злоупотреба на деца, вклучително и онлајн подведување, но вклучува и говор на омраза и ксенофобична онлајн содржина. Иако INHOPE дава дефиниција за говор на омраза, исто така, потврдува дека говорот на омраза е „екстремно комплексна“ материја која честопати не е незаконска согласно кривичното право. Па затоа, секоја пријава на дежурната линија за говор на омраза се оценува во однос на националното законодавство, т. е. онаму каде што е домаќинот (хост) на таа содржина.[10]

Секоја содржина анонимно пријавена на дежурна линија ја проверува аналитичар на содржина, кој оценува дали материјалот е незаконски. Ако аналитичарот смета дека пријавената содржина е незаконска, ќе се бара локацијата на таа содржина. Ако домаќинот кај кој е поставена содржината се наоѓа во истата земја, материјалот ќе биде пријавен кај националните служби за спроведување на законот и/или кај компанијата за ИКТ заради негово отстранување. Доколку домаќинот кај кој е поставен материјалот е во странска земја, тогаш тој се препраќа до дежурната линија во таа земја.

INHOPE изработи и Кодекс на практики за дежурни линии на Интернет, во кој се нагласува дека членките на INHOPE треба редовно да се консултираат со главните засегнати страни, вклучително владите, службите

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

за спроведување на законот, индустријата за ИКТ, како и со институциите за детска заштита, и дека членките треба да ги применуваат начелата на транспарентност, отчетност, одговорност и доверливост.

INHOPE, исто така, ја истакнува важноста на добросостојбата на персоналот кој ја проверува пријавената содржина и се свесни за психолошките ефекти што проверката на содржина со злоупотреба на деца и на насилна екстремистичка или терористичка содржина може да ги има врз лицата што ја вршат проверката. Еден официјален извештај изработен и објавен од француската дежурна линија „Point de Contact“, има цел да развие заеднички збир на најдобри практики за оперативно постапување и обработка на штетна и потенцијално нелегална содржина која може да ги загрози физичката безбедност и психолошката добросостојба на професионалците што вршат проверка на содржина[11].

3. Воспоставување ЈПП за кибербезбедност

Добра практика 1: Треба да се воспостави поволна средина како неопходен предуслов за воспоставување ефективни ЈПП.

Клучно за воспоставувањето ефективни ЈПП е создавањето на поволна средина. За тоа се неопходни четири клучни димензии: дефинирање политики, правна и регулаторна рамка, институционални аранжмани и финансиска поддршка/инвестиции. Освен тоа, Упатствата на ЕУ ја истакнуваат важноста на флексибилноста и транспарентноста од страна на сите вклучени партнери, како и заемно признавање на потребите и целите на разните засегнати страни кои се вклучени.[12]

Создавањето поволна средина треба да вклучува договор на засегнатите страни во однос на правната основа на ЈПП. Јавните институции треба да ја преземат водечката улога во создавање ЈПП или национални акциски планови. За да се направи тоа, треба да се обезбедат адекватни ресурси за внатрешна координација и соработка во рамки на ЈПП, како и да се заземе прагматичен пристап во справувањето со предизвиците во координацијата и соработката. Поттикнувањето учество на приватниот сектор, особено кај малите и средни претпријатија, е исто така важно за да се обезбеди создавање поволна средина, што дополнително ја унапредува соработката меѓу релевантните засегнати страни. И на крај, засегнатите страни во ЈПП треба да се залагаат за отворена комуникација со поширокота јавност.

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

12 Упатства на ЕУ https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru

Добра практика: Треба да се создадат јасни линии на одговорност и отчетност заради заштита на човековите права.

Утврдувањето јасни линии на одговорност и отчетност на сите засегнати страни има суштинско значење за да се обезбеди дека нема повеќе да се случуваат проблеми од типот на повреди на човековите права. Во контекст на НСК, ЈПП би можеле да бидат исклучително проблематични од неколку причини, вклучително и поради неподготвеноста на политичарите да преземат одговорност за строго законодавство за кибербезбедност, комбинирано со аверзијата на приватниот сектор кон прифаќањето одговорност или обврска за националната безбедност, што прави партнерството да нема јасни линии на одговорност и отчетност. Оттука, во договорите за ЈПП неопходно е вклучување јасни спецификации за механизми за одговорност и отчетност, за да се ублажат ризиците и да се обезбеди дека сите засегнати страни соодветно ги разбираат своите улоги и одговорности.

Добра практика 3: Мора да се гради и одржува доверба меѓу засегнатите страни.

Градењето и одржувањето доверба меѓу јавните и приватните субјекти е еден од најголемите предизвици за ЈПП. Развивањето и одржувањето на довербата е постојан процес којшто е културолошки специфичен и вклучува лични односи. Доверба не може да се постигне ако нема поволна средина. Други предизвици се недостигот на човечки ресурси во јавниот и во приватниот сектор; недоволниот буџет на јавниот сектор и ресурсите кои не ги исполнуваат очекувањата на приватниот сектор; како и недоволното разбирање и дијалог меѓу јавниот и приватниот сектор во однос на самиот концепт на ЈПП.

Јавните агенции и приватните субјекти треба да градат доверба врз база на отвореност, правичност и заемно почитување. Во случајот на ЈПП, важен тест за довербата е споделувањето информации. Учесниците треба да почувствуваат дека добиле дополнителни корисни информации со тоа што се дел од партнерствата, и дека истовремено нивните податоци се заштитени и безбедни.

СЛУЧАЈ ЗА АНАЛИЗА: ГЛОБАЛЕН ФОРУМ ЗА КИБЕРЕКСПЕРТИЗА

Глобалниот форум за киберекспертиза (GFCE) е платформа на која државите, меѓународните организации и приватните компании може да разменуваат најдобри практики и експертиза за градење киберкапацитети.

Активиран во април 2015 година, примарната цел на Глобалниот форум е да обезбеди наменска неформална платформа на која твроците на политики, практичарите и експертите од различни земји и региони ќе може да споделуваат искуства, експертиза и процена на клучни регионални и тематски киберпрашања. Уште од неговото активирање, фокусот на Глобалниот форум се промени кон тоа тој да биде координирачка платформа. Првичните интересни области за градење капацитети и експертиза без кибербезбедноста, киберкриминалот, заштитата на податоци и е-владеење. Во 2019 година Глобалниот форум се позиционираше на тој

начин да може да го олесни и координира споделувањето на знаење или експертиза за спроведувањето активности за градење киберкапацитети. Освен тоа, различните работни групи на Глобалниот форум се насочуваат кон развивање механизам за примање и препраќање информации.

Извор: 'History', the GFCE

ГЛАВНИ НАОДИ

- **Во киберпросторот и во кибербезбедноста, групите сочинети од различни засегнати страни се обично поефективни отколку кога работата ја врши само една засегната страна. Пристапите со повеќе засегнати страни, кои се нарекуваат и јавно-приватни партнерства (ЈПП), можат заедно да дадат подобри пристапи и решенија, и стануваат сè поклучни во управувањето со киберпросторот и решавањето проблеми со кибербезбедноста.**
- **ЈПП се структурирани во рамки на договори за соработка меѓу јавни и приватни институции.**
- **Државите може да играат важна улога во координацијата и соработката со секторот за ИКТ и со граѓанското општество преку создавањето и поддржувањето колаборативни платформи.**
- **Приватните чинители, како што е индустријата за ИКТ, можат, исто така, да водат ефективни иницијативи со повеќе засегнати страни во полето на кибербезбедноста.**
- **Државите треба да вложуваат во прагматични пристапи кон градењето ЈПП, кои вклучуваат отворена комуникација и инклузивно учество и кои мотивираат зголемено учеството на приватниот сектор.**

IZVORI

Јавно-приватни партнерства во киберпросторот, ENISA, ноември 2017 година, достапно на https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models/at_download/fullReport

Јавно-приватни партнерства во националните стратегии за кибербезбедност. Достапно на: https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf

Национален совет на САД за јавно-приватни партнерства. Дефиниција за ЈПП (2016)

Јавно-приватни партнерства во ЕУ: Широко распространети недостатоци и ограничени придобивки http://publications.europa.eu/webpub/eca/special-reports/ppp-9-2018/en/

Африкански ЦЕРТ https://www.africacert.org/african-csirts/

EU IRU. Достапно на: https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru

www.dcaf.ch