DCAF Geneva Centre for Security Sector Governance

HYRJE NË QEVERISJEN E SIGURISË KIBERNETIKE - MJET PUNE PËR DEPUTETË TË PARLAMENTIT

HYRJE NË QEVERISJEN E SIGURISË KIBERNETIKE - MJET PUNE PËR DEPUTETË TË PARLAMENTIT

Autorë

Franziska Klopfer

Franziska është koordinatore projekti në Divizionin e Evropës dhe Azisë Qendrore në DCAF.

Irina Rizmal

Irina është asistente projekti në Divizionin e Evropës dhe Azisë Qendrore në DCAF.

Milan Sekuloski

Milan është menaxher projekti në nivel kombëtar në Divizionin e Evropës dhe Azisë Qendrore në DCAF.

Teresa Hatzl

Teresa është ish-zyrtare projekti në Divizionin e Partneritetit Publik-Privat në DCAF.

Dragan Mladenovic, PhD

Dragan është ekspert i sigurisë dhe mbrojtjes kibernetike.

Tabela e përmbajtjes

Hyrje 4
Pjesa I - Konceptet kryesore 4
Nevojat, politikat dhe synimet strategjike të sigurisë kibernetike 4
Sfidat në qeverisjen e sigurisë kibernetike 5
Një nocion i ri i ofrimit, kontrollit dhe mbikëqyrjes së sigurisë 6
Shembuj të pyetjeve për mbikëqyrje 6
Pjesa II - Krimi kibernetik 7
Përkufizimi 7
Kompjuterët dhe rrjetet si shënjestër kryesore 7
Kompjuterët dhe rrjetet si mjete për të kryer vepër penale 8
Kompjuterët dhe rrjetet si vendndodhje e krimit 8
Trendet dhe përgjigjet ndaj krimit kibernetik 8
Shembuj të pyetjeve për mbikëqyrje 10
Pjesa III - Lufta kibernetike 10
Përkufizimi 10
Problemet në rregullimin e konfliktit kibernetik 11
Përpjekjet ndërkombëtare për rregullimin e luftimit kibernetik 12
Përgjigjet ligjore ndërkombëtare ndaj luftës kibernetike 12
Shembuj të pyetjeve për mbikëqyrje 13
Pjesa IV - Spiunazhi kibernetik 13
Përkufizimi 13
Sfidat specifike të spiunazhit kibernetik 14
Sjellje e pranueshme, krim kibernetik apo akt i agresionit? 14
Aktorët e deleguar, armatat private dhe konfliktet hibride 15
Adresimi, rregullimi dhe kundërvënia ndaj spiunazhit kibernetik 15
Shembuj të pyetjeve për mbikëqyrje 16
Pjesa IV - Terrorizmi kibernetik 16
Përkufizimi 16
Terrorizmi kibernetik kundrejt përdorimit të internetit për qëllime terroriste 16
Konsideratat e sundimit të ligjit 18
Shembuj të pyetjeve për mbikëqyrje 19
Pjesa V - Haktivizmi 19
Përkufizimi 19
Motivet e haktivistëve dhe dallimi mes krimin kibernetik dhe terrorizmin kibernetik 19
Hakerët kapuç-bardhë, kapuç-hirtë dhe kapuç-zi 20
Shembuj të pyetjeve për mbikëqyrje 20

Hyrje

Siguria kibernetike është një nga aspektet më të fundit të politikave të sigurisë kombëtare që po bëhet gjithnjë e më e rëndësishme në të gjithë sektorët e sigurisë të vendeve evropiane. Politikëbërësit janë ende duke zënë hapin me ritmin e zhvillimeve teknologjike që shfrytëzohen nga një vistër aktorësh, miqësorë dhe armiqësorë. Kjo kërkon që kornizat e reja ligjore dhe të politikave të zhvillohen shpejt dhe në mënyrë gjithëpërfshirëse. Përveç garantimit të sigurisë kombëtare, rrjetet e mbrojtura dhe të sigurta janë gjithashtu të rëndësishme për t'i dhënë hov ekonomisë kombëtare dhe për modernizimin e qeverisjes së sektorit publik në vendet e EJL (konsideroni, për shembull, rëndësinë vendimtare që ka rrjeti i sigurt për funksionimin e mirë të shërbimeve të e-qeverisjes që futen në përdorim). Një hapësirë e sigurt kibernetike është gjithashtu e nevojshme për të garantuar që qytetarët mund të ushtrojnë të drejtat e tyre, siç janë qasja në informata dhe liria e shprehjes. Të qenit të vetëdijshëm për mundësitë, rreziqet dhe kërcënimet që i sjell hapësira kibernetike është me rëndësi vendimtare.

Deputetët e parlamenteve luajnë rol jetik në zhvillimin e kornizave legjislative dhe institucionale të sigurisë kibernetike, si dhe në garantimin që parimet e qeverisjes së mirë aplikohen për sigurinë kibernetike. Meqë kjo ka të bëjë me përgjegjësinë e miratimit të legjislacionit të ri, ata gjithashtu kanë kompetencë që të thërrasin hisedarët e ndryshëm për diskutime të politikave, duke garantuar modele gjithëpërfshirëse të qeverisjes shumëpalëshe - diçka që është veçanërisht e rëndësishme në sigurinë kibernetike. Në fund, deputetët e parlamentit gjithashtu kryejnë rolin e rojës duke bërë mbikëqyrjen e zbatimit të ligjeve dhe politikave për (ose lidhur me) sigurinë kibernetike.

Duke pasur parasysh këto përgjegjësi, është me rëndësi të madhe që deputetët e parlamentit të jenë në hap me kohën sa i përket zhvillimeve më të fundit në sigurinë kibernetike, duke i pajisur ata me njohuri dhe mirëkuptim adekuat për të trajtuar çështjet e politikave dhe debatet nga pikëpamja e informuar. Ky botim synon që deputetëve të parlamenteve që janë të angazhuar në zhvillimin e legjislacionit dhe mbikëqyrjen e çështjeve të sigurisë kibernetike t'u ofrojë pasqyrë bazë të çështjeve kryesore, tendencave dhe sfidave të qeverisjes.

Kjo hyrje në çështjet e qeverisjes së sigurisë kibernetike, si mjet pune për deputetë të parlamentit, shpjegon elementet kryesore të sigurisë kibernetike dhe qeverisjen e saj: krimin kibernetik, luftën kibernetike, terrorizmin kibernetik, spiunazhin kibernetik dhe haktivizmin si dhe sfidat e mundësitë në qeverisjen e tyre. Çdo pjesë plotësohet me listën e pyetjeve të mundshme që deputetët e parlamentit mund t'i ngrenë në lidhje me çështjen. Pyetjet kanë për qëllim rritjen e llogaridhënies së qeverisë dhe atë të hisedarëve të tjerë të rëndësishëm të sigurisë kibernetike. Ato mund të përfshihen në pyetjet që i parashtrohen qeverisë, të diskutohen në dëgjime publike ose të inkurajojnë hetime parlamentare.

PJESA I - KONCEPTET KRYESORE

Nevojat, politikat dhe synimet strategjike të sigurisë kibernetike

Me ardhjen e World Wide Web dhe kalimin gjithnjë e më të madh në jetë online është bërë e nevojshme që të rivlerësohen rreziqet e sigurisë dhe përgjigjet ndaj tyre. Epoka aktuale e informacionit ka shtyrë informacionin dhe sigurinë kibernetike në ballë të zhvillimeve si aspekt i rëndësishëm i sigurisë individuale, organizative, kombëtare dhe ndërkombëtare. Sipas standardit ISO/IEC, siguria kibernetike paraqet "ruajtjen e konfidencialitetit, integritetit dhe disponueshmërisë së informacionit"[1], në mesin e veçorive tjera.[2]

Në konceptin e qeverisjes së mirë të sektorit të sigurisë, politika e sigurisë synon të garantojë jo vetëm sigurinë e shtetit, por edhe sigurinë e individit. Aplikimi i kësaj qasjeje në botën online nënkupton që siguria kibernetike duhet të përpiqet të krijojë hapësirë të sigurt në internet për të gjithë. Për të arritur këtë, politika e sigurisë kibernetike duhet të përfshijë një sërë çështjesh, duke filluar nga mbrojtja e integritetit të shtetit dhe garantimi i të drejtave të njeriut të qytetarëve, zbatimi i ligjit dhe parandalimi i krimeve të kryera në ose përmes hapësirës kibernetike. Prandaj, çështjet e qeverisjes së sigurisë kibernetike nuk duhet të adresojnë vetëm çështjet e ruajtjes së sigurisë dhe rimëkëmbshmërisë online, por edhe të forcimit të sigurisë dhe nxitjes së mundësive online.

Së këndejmi, hapi i parë në hartimin e politikës dhe strategjisë së suksesshme të sigurisë kibernetike është që të përkufizohen objektivat e sigurisë dhe të përcaktohet se çka nënkupton ruajtja e sigurisë dhe forcimi i mbrojtjes online për vendin dhe qytetarët e tij. Duhet të përkufizohen asetet e rendesishme që janë esenciale për mbrojtjen e funksionimit normal të shtetit dhe për integritetin e përgjithshëm të jetës online. Rrjetet e energjisë elektrike dhe shërbimet kyçe të internetit janë shembuj të qartë të aseteve të rëndësishme që kërkojnë vëmendje dhe mbrojtje të konsiderueshme. Në të njëjtën kohë, faktorët kryesorë të cenueshmërisë në sigurinë kibernetike vijnë nga gabimet njerëzore dhe dështimet teknike. Përdoruesit e painformuar të internetit që klikojnë në vegëzën e gabuar janë shkaqet më të shpeshta të incidenteve kibernetike. Edukimi dhe vetëdijesimi i ngritur i përdoruesve është po aq me rëndësi për parandalimin në sigurinë kibernetike sa është edhe teknologjia e shëndoshë dhe ekspertët e duhur për ta përdorur këtë teknologji.

Sfidat në qeverisjen e sigurisë kibernetike

Pas përkufizimit të objektivave të sigurisë kibernetike, duhet të vendoset korniza e qeverisjes, e cila përcakton rolet dhe përgjegjësitë e aktorëve të ndryshëm në arritjen e objektivave. Sfidë qenësore në qeverisjen e sigurisë kibernetike është fakti se rolet dhe përgjegjësitë e

1 Organizata Ndërkombëtare për Standardizim. (2016). ISO/IEC 27000:2016(en) Information technology — Security techniques — Information security management systems — Overview and vocabulary.

2 Disa nga përkufizimet e sigurisë kibernetike përfshijnë veçori të tjera të informacionit, siç janë autenticiteti, llogaridhënia, mosmohueshmëria, dhe besueshmëria, përveç atyre tri të lartpërmendura.

aktorëve të ndryshëm ende nuk janë përkufizuar qartë në të drejtën ose standardet ndërkombëtare. Shumë korniza kombëtare ligjore dhe të politikave gjithashtu ende nuk pasqyrojnë qartë ndikimin e aktorëve të ndryshëm. Për shembull, kush e kontrollon dhe kush është përgjegjës për infrastrukturë dhe përmbajtje të sigurt online? Cilat detyra apo privilegje rrjedhin nga kjo përgjegjësi?

Shumë shërbime themelore kibernetike janë në pronësi dhe drejtohen nga aktorët privatë, ndërkohë që shteti varet nga bashkëpunimi i tyre aktiv, për shembull në sigurimin e rrjeteve dhe shërbimeve të veta. Bashkëpunimi dhe angazhimi i aktorëve të ndryshëm është prandaj me rëndësi thelbësore për sigurinë kibernetike efektive dhe efikase dhe për të garantuar që politikëbërja në fushën e sigurisë kibernetike bëhet me pjesëmarrje dhe llogaridhënie. Për shembull, po bëhet gjithnjë e më e zakonshme që aktorët privatë dhe publikë të ndajnë informacione për të zbuluar dhe parandaluar më mirë incidentet kibernetike. Në të njëjtën kohë, shumë kompani private shpesh kanë teknologji dhe ekspertizë më të avancuar sesa sektori publik dhe mund t'i ndajnë këto mjete në përpjekje për të rritur sigurinë e përgjithshme kibernetike të vendit, duke i bërë kështu në fund të fundit më të sigurta edhe bizneset e tyre. Në fund, të gjithë hisedarët e sigurisë kibernetike - qeveria, ligjvënësi, sektori privat, shoqëria civile, komuniteti teknik dhe akademik - luajnë rol në procesin e politikës së sigurisë kibernetike, qoftë në formë të kontributit për planifikimin e politikës, bashkëpunimit në zbatimin e politikës ose mbikëqyrjes së tërë procesit të politikës.

Megjithatë, shtrirja e saktë e përgjegjësive dhe rolet që duhet t'i luajnë këta hisedarë duhet të përkufizohet në çdo kontekst të politikave. Në përgjithësi, kredibiliteti dhe zbatimi i tërë procesit mbështetet në gjithpërfshirjen dhe transparencën e tij.

Një nocion i ri i ofrimit, kontrollit dhe mbikëqyrjes së sigurisë

Siguria kibernetike duhet të jetë llogaridhënëse. Mekanizmat e kontrollit dhe mbikëqyrjes shpesh nuk kanë qartësi për shkak të kombinimit kompleks të aktorëve të përfshirë shtetërorë dhe jo-shtetërorë. Si rezultat, duhet të zhvillohen modele të reja jo vetëm të bashkëpunimit por edhe të kontrollit dhe mbikëqyrjes.

Deputetët e parlamentit duhet të luajnë rol të rëndësishëm në mbikëqyrjen e qeverisjes së sigurisë kibernetike. Për shkak se siguria kibernetike prek jo vetëm politikat e sigurisë, por edhe fushat e tjera të politikave, mbikëqyrja e sigurisë kibernetike duhet të bëjë bashkë anëtarët e komisioneve të sigurisë dhe të mbrojtjes me komisionet përgjegjëse për telekomunikim, arsim, shoqëri të informacionit dhe për të drejtat e njeriut, dhe jo vetëm.

Shembuj të pyetjeve për mbikëqyrje:

- A ka vendi strategji të sigurisë kibernetike me vizion të përcaktuar qartë? Cila ministri apo agjenci shtetërore është përgjegjëse për zbatimin e saj? A u zhvillua strategjia

përmes procesit gjithëpërfshirës, duke angazhuar të gjithë hisedarët relevantë (shtetërorë dhe jo-shtetërorë)?

- A ka listë të infrastrukturës kritike të identifikuar të informacionit dhe, nëse po, a është kjo listë shteruese? Cila agjenci shtetërore është përgjegjëse për ta mbajtur këtë listë të azhurnuar? Kush është përgjegjës për kontrollin e mbrojtjes së infrastrukturës kritike të informacionit?
- Cilët janë aktorët e ndryshëm të sigurisë kibernetike? Cilat janë rolet e tyre? Cilat duhet të jenë përgjegjësitë e tyre?
- A ka mekanizma të kontrollit dhe mbikëqyrjes për aktorët kryesorë shtetërorë dhe jo-shtetërorë të sigurisë kibernetike? A funksionon kontrolli dhe mbikëqyrja e aktorëve kryesorë shtetërorë dhe jo-shtetërorë të sigurisë kibernetike? A mbahen ata llogaridhënës për të garantuar që aktivitetet e tyre janë jo vetëm efektive, por edhe brenda kufijve ligjorë?

PJESA II - KRIMI KIBERNETIK

Përkufizimi

Krimi kibernetik në përgjithësi kuptohet si akt kriminalë ku kompjuterët dhe rrjetet janë shënjestër kryesore, përdoren si mjete për të kryer vepër penale ose janë vendndodhja e krimit.

Edhe pse nuk ka përkufizim të pranuar universalisht, mund të bëhet dallim midis dy llojeve kryesore të krimit kibernetik:

- Krimi i mundësuar nga kibernetika, duke iu referuar formave 'tradicionale' të krimit tani të transferuara në sferën kibernetike, siç janë aktet kriminale të fokusuara në financa, aktet që pengojnë sigurinë e fëmijëve dhe të rinjëve, dhe madje edhe terrorizmi;
- Krimi i avancuar kibernetik (i njohur edhe si krimi i teknologjisë së lartë), duke iu referuar sulmeve të sofistikuara ndaj pajisjeve kompjuterike dhe softuerit.[3]

Së pari, është e rëndësishme të mos ngatërrohet krimin kibernetik me sigurinë kibernetike. Të dy kërcënimet e lidhura me kibernetikën dallojnë për nga motivi, dashja, mjetet e përdorura, shënjestra, shtrirja, pasojat, si dhe aktorët e përfshirë në parandalim dhe zbutje. Në praktikë, krimi kibernetik është i shumëllojshëm nga spam-i dhe email-et phishing, dallaveret dhe mashtrimet në internet, si dhe përfaqësimi i rremë, deri te përmbajtja e ndaluar fyese dhe e kundërligjshme, vjedhja e identitetit, dhe materiali online i abuzimit seksual të fëmijëve. Motivi kryesor prapa akteve kriminale kibernetike, si në rastin e krimit 'tradicional',

3 Përkufizimi i krimit kibernetik sipas Interpolit.

përgjithësisht konsiderohet se është fitimi financiar. Kriminelët kibernetikë janë, në thelb, hakerë me dashje qëllimkeqe.

Kompjuterët dhe rrjetet si shënjestër kryesore

Kur bëhet fjalë për mjetet që përdoren më së shpeshti, këto përfshijnë softuerin qëllimkeq si viruset, kuajt trojanë, adware dhe spyware për të fituar qasje në sisteme, për monitorim të aktiviteteve dhe mbledhje të dhënash; botnet-ët, apo kompjuterët e rrëmbyer personalë që kryejnë detyra me telekomandim pa dijeninë e përdoruesve të tyre; dhe sulmet e tipit të refuzimit të shërbimit, Denial of Service (DoS), që kanë për synim shterjen e resurseve të disponueshme për një rrjet, aplikacion ose shërbim, me qëllim që të parandalohen përdoruesit nga qasja në to.

Efektet e sulmeve të tilla janë gjithashtu të shumëfishta. Individët privatë mund të pësojnë humbje financiare, si dhe të bien viktimë e vjedhjes së informacionit personal dhe të ndjeshëm dhe vjedhjes së identitetit. Kompanitë që bien viktimë e sulmeve kriminale kibernetike përballen me humbje potenciale financiare, me humbje të informacionit të ndjeshëm operativ, si dhe të dhënave të patentave ose të dhënave personale të klientëve dhe përdoruesve të tyre, ku të gjitha këto gjithashtu mund të sjellin në mënyrë indirekte pasoja të rënda për reputacion. Institucionet publike ose organizatat jo-komerciale mund të bëhen viktima të zhvatjes ose vjedhjes së të dhënave personale të përdoruesve të shërbimeve të tyre.

Kompjuterët dhe rrjetet si mjete për të kryer vepër penale

Akte të tjera kriminale që gjithashtu po përhapen në sferën kibernetike përfshijnë tregtinë e paligjshme të drogës, armëve dhe të dhënave dhe informacionit të ndjeshëm, trafikimin me njerëz dhe madje edhe vrasjet, rrahjet dhe format e tjera të dhunës me kontratë. Në përgjithësi, aranzhimet e tilla ndodhin në të ashtuquajturin 'darknet' (rrjeti i errët) ku përdoruesit mund të veprojnë në anonimitet të plotë. Duke përdorur darknet-in, individët dhe organizatat kriminale përdorin shërbime të enkriptuara të mesazheve për të komunikuar, dhe kriptovaluta për të kryer transaksione financiare, duke e bërë jashtëzakonisht të vështirë gjurmimin dhe identifikimin. Hakerët kapuçzi (kriminelë me shkathtësi, teknikë ose ekspertë teknikë të punësuar nga kriminelët, shih kapitullin për haktivizmin) gjithashtu shfrytëzojnë potencialin e darknet-it duke përfituar nga cenueshmërive e softuerit që ata i kanë zbuluar, duke ia shitur ato në mënyrë anonime kujtdo që kërkon mënyra për të shfrytëzuar sisteme specifike.

Kompjuterët dhe rrjetet si vendndodhje e krimit

Grupet kriminale kanë bërë kështu tranzicion jashtëzakonisht efikas në sferën dixhitale. Ata madje kanë zhvilluar edhe modele të reja biznesi që i ngjajnë disa prej bizneseve legjitime më të avancuara. Mu ashtu si disa kompani që ofrojnë "sigurinë si shërbim" dhe zhvillojnë

kapacitete të sigurisë kibernetike të blerësve të interesuar, grupet kriminale gjithashtu ofrojnë 'krimin si shërbim' në tregun kriminal kibernetik. Shqetësim tjetër është bashkëpunimi i mundshëm ndërmjet aktorëve të ndryshëm qëllimkëqij. Për shembull, kriminelët kibernetikë mund t'i ofrojnë shërbimet e tyre për grupet terroriste ose të kryejnë akte kriminale të sponsorizuara nga shtetet në hapësirën kibernetike vetëm për qëllime të fitimit financiar. Me fjalë të tjera, sfera dixhitale i ofron grupeve kriminale kanale dhe mundësi të reja për të kryer aktivitete të paligjshme që përndryshe mund të mos kenë qenë në dispozicion.

Trendet dhe përgjigjet ndaj krimit kibernetik

Në përgjithësi, krimi i mundësuar nga kibernetika është në rritje të madhe si në vendet e zhvilluara ashtu edhe në ato në zhvillim. Për nga vetë natyra, krimi kibernetik është ndërkombëtar, pra shkon përtej kufijve kombëtarë. Kryesit nuk ka nevojë të jenë në të njëjtin shtet si viktimat apo forcat policore që i ndjekin ata. Kjo përbën një nga sfidat kryesore në luftën kundër krimit kibernetik, meqë dallimet në sistemet ligjore dhe praktikat e vendeve të ndryshme të përfshira mund të ndikojnë në efikasitetin dhe realizueshmërinë e bashkëpunimit, si dhe në shkëmbimin e inteligjencës dhe provave.

Tutje, shumë pak forca policore në botë kanë kapacitetin për të trajtuar incidentet e krimit kibernetik në mënyrë të pavarur, edhe pse shumë prej tyre kanë njësi të dedikuara për krimet kibernetike ose njësi të 'krimit të teknologjisë së lartë'. Ashtu si me llojet e tjera të aktiviteteve qëllimkëqija në hapësirën kibernetike (shih kapitullin për spiunazhin kibernetik), ekziston asimetri e qartë e kostove të përfshira. Si rezultat, qasja tradicionale e veprimeve policore ndaj krimit disi ndryshohet në sferën kibernetike. Në vend që menjëherë të arrestojnë kryesit, njësitë policore të krimit kibernetik përqendrohen kryesisht në ndërprerjen e akteve kriminale në vazhdim dhe në adresimin e cenueshmërive të sigurisë që janë shfrytëzuar. Me sfidën e atribuimit që është e pranishme në mënyrë të barabartë në mbarë spektrin kibernetik dhe procesin e gjatë dhe kërkues të hetimeve, duke përfshirë përpunimin kriminalistik të të dhënave, realizimi i dënimeve zyrtare po ashtu vjen me ritëm më të ngadaltë sesa me krimet tradicionale.

Në nivel kombëtar, lufta kundër krimit kibernetik kërkon bashkëpunim mes të gjithë aktorëve. Sektori privat është shënjestra më e zakonshme e kriminelëve kibernetikë dhe përvojat dhe interesat e tij duhet të merren parasysh gjatë planifikimit të strategjive të krimit kibernetik. Ekspertët e krimit kibernetik nga sektori privat, akademia dhe shoqëria civile gjithashtu mund të kontribuojnë në planifikimin e politikës së krimit kibernetik me kapacitete dhe njohuri teknike. Për t'iu rrekur në mënyrë efikase krimit kibernetik, qeveritë duhet të nxisin bashkëpunimin publik-privat dhe të mbështesin krijimin e rrjeteve të besimit. Po aq me rëndësi është parandalimi i krimit kibernetik dhe mbështetja për përdoruesit individualë. Nëpërmjet ngritjes së vetëdijes dhe ndërtimit të kapaciteteve në nivel të përgjithshëm, përdoruesit duhet të mësojnë të njohin email-et potencialisht mashtruese, përmbajtjen qëllimkeqe, si dhe kontaktet potencialisht të rreme. Madje edhe përpjekjet relativisht të vogla si mësimi i përdoruesve për të mbajtur higjienën bazë kibernetike dhe për të përdorur fjalëka-

lime të forta, softuerë dhe enkriptim të licencuar të azhurnuar, mund të kenë ndikim të madh në parandalimin e krimit kibernetik.

Në nivel ndërkombëtar, është bërë përparim me adoptimin e Konventës së Këshillit të Evropës për Krimin Kibernetik[4], gjithashtu e referuar si Konventa e Budapestit. Konventa e Budapestit është i vetmi instrument i detyrueshëm ndërkombëtar për krimin kibernetik deri më sot, që u ofron udhëzime shteteve për zhvillimin e kornizave legjislative gjithpërfshirëse kombëtare për luftimin e krimit kibernetik dhe për krijimin e kornizës për bashkëpunim ndërkombëtar midis shteteve nënshkruese. Me gjashtëdhjetë e një palë dhe dhjetë të tjera që pritet të bashkohen, Konventa e Budapestit, megjithatë, ende nuk është dokument global universal. Sidoqoftë, në vitet e fundit mund të vërehen raste të bashkëpunimit ndërkombëtar. Për shembull, organizatat e bashkëpunimit ndërkombëtar policor, veçanërisht Europol dhe Interpol, janë angazhuar për rritjen e kapaciteteve ndërkombëtare dhe lehtësimin e kornizave të bashkëpunimit ndërkufitar midis shërbimeve policore. Me kërkesat e mëdha të lartpërmendura për të pasur njësi gjithpërfshirëse kombëtare për krimin kibernetik, kornizat e tilla mund të kompensojnë kapacitetet e kufizuara kombëtare, duke përfshirë zhvillimin e partneriteteve publike-private dhe rrjeteve të besimit ndërmjet ekspertëve nga sektorë të ndryshëm të shoqërisë.

Shembuj të pyetjeve për mbikëqyrje:

- A ka vendi legjislacion për krim kibernetik, që identifikon llojet e ndryshme të krimit kibernetik dhe vendos sistem sanksionues të përkufizuar mirë? Deri në ç'masë përputhet ky legjislacion vendor me konventat ndërkombëtare në të cilat vendi është palë?
- A janë gjyqësori dhe policia të përgatitura mirë në aspektin e njohurive, ekspertizës dhe aftësive teknike?
- Cilat pjesë të shoqërisë janë më të ekspozuara ndaj krimit kibernetik? A ka iniciativa parandaluese që synojnë këta sektorë?
- A funksionon kontrolli dhe mbikëqyrja e aktorëve kryesorë shtetërorë dhe joshtetërorë? A po mbahen llogaridhënëse agjencitë e sigurisë për kapacitetet e tyre kibernetike për të garantuar se aktivitetet e tyre janë jo vetëm efektive, por edhe brenda kufijve ligjorë / nuk shkelin të drejtat e garantuara të qytetarëve për privatësi?
- A janë policia dhe gjyqësori duke përdorur të gjitha mjetet juridike në dispozicion për bashkëpunim efektiv ndërkombëtar? A duhet të ndryshojnë kornizat legjislative për të lehtësuar efikasitet më të mirë? Në të njëjtën kohë, cilat masa mbrojtëse ekzistojnë për mbrojtjen e të dhënave personale të qytetarëve që ndahen me vendet e treta? A është komunikimi me sektorin privat efikas dhe transparent (në formën e tij, nëse jo në përmbajtjen që duhet të klasifikohet)?

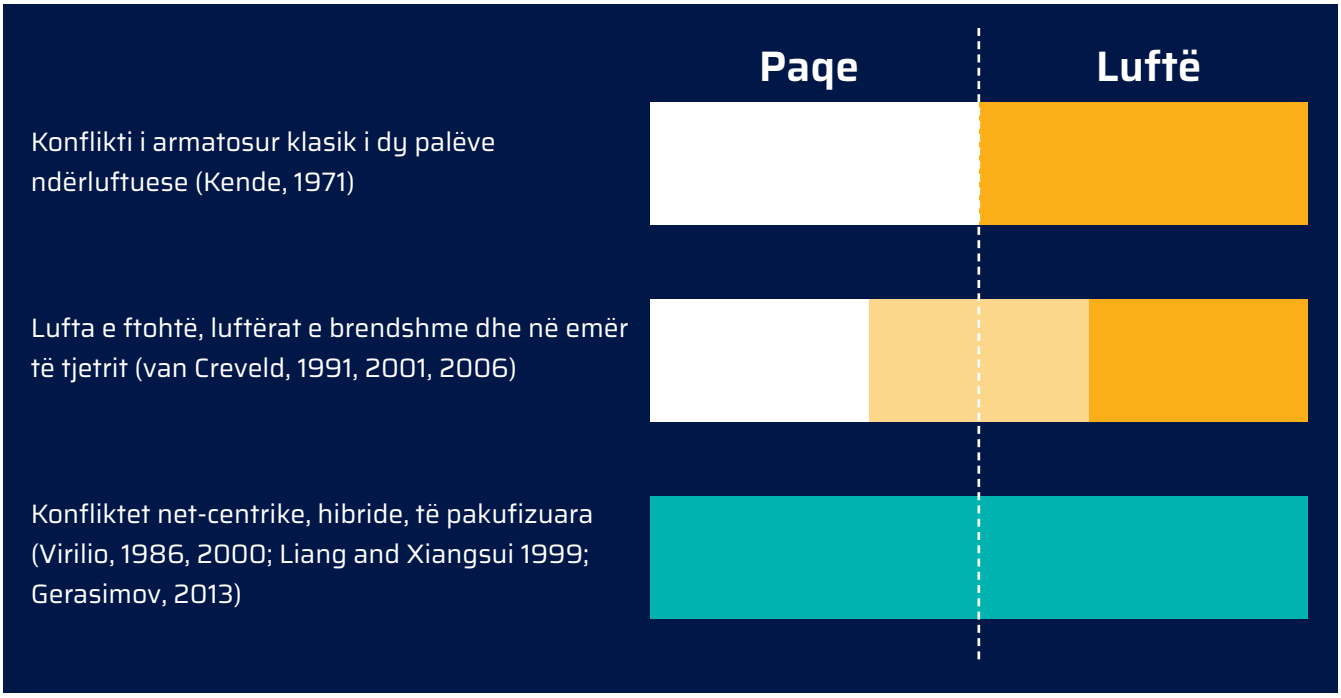
4 Konventa për Krimin Kibernetik. Këshilli i Evropës. Traktati nr.185.

PJESA III - LUFTA KIBERNETIKE

Përkufizimi

Luftimi kibernetik mund të përkufizohet si akt i "zhvillimit të luftës në hapësirën kibernetike ose nëpërmjet hapësirës kibernetike". Është lloj i ri i veçantë i luftimit[5] i cili përdor teknologjitë e informacionit dhe komunikimit (TIK) për të arritur objektiva dhe efekte ushtarake në fushat fizike, informatike dhe kibernetike. Efektet ushtarake mund të jenë identike me efektet e armëve kinetike, bërthamore, biologjike ose kimike.

Megjithatë, nuk ka marrëveshje ndërkombëtare se si duhet të përkufizohen përmbajtja, metodat, teknikat, mjetet dhe synimet e luftimit kibernetik. Edhe bashkësia ndërkombëtare ende nuk ka rënë dakord se si të zhvillohen masat kombëtare të ndërtimit të kapaciteteve dhe masat ndërkombëtare të ndërtimit të besimit, ose si të zbatohet e drejta ndërkombëtare ekzistuese ndaj luftimit kibernetik.



Problemet në rregullimin e konfliktit kibernetik

Teknologjitë e reja me aftësi sulmuese po dalin më shpejt sesa që vendet individuale janë në gjendje të zhvillojnë aftësitë mbrojtëse të nevojshme kundër tyre. Ato gjithashtu janë më të shpejta sesa aftësia e bashkësisë ndërkombëtare për të gjetur zgjidhje për rregullimin e konflikteve kibernetike.

5 Luftimi është proces i zhvillimit të konfliktit të armatosur ndërkombëtar. Lufta është konflikt i armatosur mes jo më pak se dy forcave të armatosura ndërluftuese që kanë të paktën organizim dhe komandë qendrore minimale, ndërsa të paktën njëra anë përfaqësohet nga njëfarë lloj qeverie (siç është forca e rregullt ushtarake ose policore, ose forca paramilitare e parregullt), që zhvillohet në vazhdimësi, sipas planit dhe strategjisë së unifikuar të forcave ndërluftuese. Luftimi tradicional zhvillohet në tokë, në det, në ajër dhe hapësirë kozmike.

Kryesit e sulmeve kibernetike shpesh veprojnë në mënyrë klandestine, ku efektet e sulmeve kibernetike të tyre në shumë raste janë të vonuara. Mund të kalojnë disa vite midis shfrytëzimit kibernetik dhe instalimit të armës qëllimkeqe dhe zbulimit të efekteve të saj. Sulmuesit mund të jenë njësi apo agjenci qeveritare, kompani private, organizata kriminale, terroristë, apo grupe joformale dhe individë.

Për dallim nga luftimi konvencional, efektet e konflikteve kibernetike shpesh nuk e arrijnë pragun e "aktit të agresionit"6, "përdorimit të forcës"7, "forcës së armatosur"8 ose "sulmit të armatosur"9 siç përkufizohet nga Karta e OKB-së, duke e bërë të vështirë aplikimin e rregullave ius ad bellum dhe ius in bello të Ligjit Ndërkombëtar të Konflikteve të Armatosura.

Në të vërtetë, shumica e shteteve nuk kanë kapacitete të mjaftueshme për:

- të zbuluar me saktësi sulmet kibernetike;
- të identifikuar dhe atribuuar sulmuesit; dhe
- përgjigje me kohë, me saktësi dhe të ligjshme ndaj sulmeve kibernetike.

Përpjekjet ndërkombëtare për rregullimin e luftimit kibernetik

Mungesa e rregullimit ligjor lë hapësirë për abuzim të mundshëm të sulmeve kibernetike, mbase edhe duke çuar në shpërthime të krizave ndërkombëtare dhe rajonale, veçanërisht në rajonet e ngarkuara me tensione kronike politike.

Komuniteti ndërkombëtar ende po përpiqet të krijojë marrëveshje mbi mënyrat për të rregulluar luftimin kibernetik. Ka propozime të ndryshme, një prej të cilëve është Doracaku i Talinit10, i zhvilluar nga grupi i studiuesve në Qendrën e Ekselencës së NATO-s për Bashkëpunim në Mbrojtje Kibernetike në Talin, Estoni.

Përgjigjet ligjore ndërkombëtare ndaj luftës kibernetike

Një përgjigje e mundshme praktike ndaj kërcënimeve kibernetike mund të jetë adoptimi dhe aplikimi i masave për ndërtim të kapaciteteve dhe besimit në nivel kombëtar, rajonal dhe ndërkombëtar.

Për këtë qëllim, Kombet e Bashkuara kanë krijuar Grupin e Ekspertëve Qeveritarë për Zhvillimet në Fushën e Informacionit dhe Telekomunikimeve në Kontekstin e Sigurisë Ndërkombëtare (UN GGE). Në periudhën midis 2004 dhe 2017, Grupi u mblodh pesë herë për të pleqëruar mbi kërcënimet ekzistuese dhe potenciale; normat, rregullat dhe

6 Karta e Kombeve të Bashkuara. 24 tetor 1945. Kombet e Bashkuara. 1 UNTS XVI, nen. 39.
7 Ibid., 1 UNTS XVI, nen. 2, para. 4.
8 Ibid., 1 UNTS XVI, Preambula.
9 Ibid., 1 UNTS XVI, nen. 51.
10 Schmitt, Michael N. (ed.) 2017. Tallinn Manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.

parimet e sjelljes së përgjegjshme shtetërore; dhe masat për ndërtim të besimit dhe kapaciteteve. Në Raportin e vitit 2013, GGE konkludoi se "E drejta ndërkombëtare, dhe në veçanti Karta e Kombeve të Bashkuara, është e zbatueshme dhe është thelbësore për ruajtjen e paqes dhe stabilitetit dhe promovimin e mjedisit të hapur, të sigurt, paqësor dhe të qasshëm të TIK-ut".11

Përpjekje të tjera janë bërë nga Organizata për Siguri dhe Bashkëpunim në Evropë (OSBE), nëpërmjet adoptimit të masave për ndërtim të besimit për ruajtjen e paqes dhe stabilitetit ndërkombëtar (MNB).12 MNB-të fokusohen në shkëmbimin e informacionit dhe në dialog; mbrojtjen e infrastrukturave kritike dhe sigurinë kombëtare; dhe promovimin dhe përmirësimin e bashkëpunimit publik-privat.

Megjithatë, të dyja këto nisma janë vullnetare (jo të detyrueshme për shtetet anëtare të OKB-së ose të OSBE-së) dhe ekzistenca e tyre nuk është garanci e plotë dhe e patundur për arritjen e paqes dhe sigurisë në hapësirën kibernetike në nivel ndërkombëtar.

Një zgjidhje e mundshme mund të jenë marrëveshjet dypalëshe dhe shumëpalëshe mid-is shteteve të ndryshme. Këto marrëveshje mund të përkufizojnë normat, standardet dhe parimet e sjelljes paqësore; të vendosin rregulla dhe procedura në rastet e incidenteve të rënda kibernetike; të lehtësojnë bashkëpunimin dhe krijimin e kapaciteteve të përbashkëta për zbulimin e sulmit kibernetik, identifikimin dhe atribuimin e sulmuesit.

Shembuj të pyetjeve për mbikëqyrje:

- A janë përkufizuar synimet strategjike për mbrojtje kibernetike?
- A ka vlerësim të njohjes së situatës? A i merr ky parasysh të gjitha elementet në vend që kanë nevojë për mbrojtje?
- Cilat janë cenueshmëritë dhe rreziqet kryesore? A identifikohen, rishikohen dhe adresohen ato rregullisht?
- Sa të zhvilluara janë kapacitetet ekzistuese kombëtare për mbrojtje kibernetike?
- Kush janë aktorët e ndryshëm, në nivel kombëtar dhe ndërkombëtar, që kontribuojnë në mbrojtjen kibernetike?
- Cilat korniza ekzistojnë për bashkëpunim ndërmjet aktorëve përgjegjës? Si janë të organizuara këto dhe sa janë llogaridhënëse, transparente dhe efektive?

11 Raporti i Grupit të Ekspertëve Qeveritarë për Zhvillimet në Fushën e Informacionit dhe Telekomuni-kimeve në Kontekstin e Sigurisë Ndërkombëtare. 24 qershor 2013. Asambleja e Përgjithshme e Kombeve të Bashkuara. Rezoluta A/68/98.

12 Vendim nr. 1106. Grupi fillestar i masave të OSBE-së për ndërtimin e besimit për të zvogëluar risqet e konfliktit që rrjedhin nga përdorimi i teknologjive të informacionit dhe komunikimit. 3.12.2013. Organizata për Siguri dhe Bashkëpunim në Evropë. PC.DEC/1106. Vendimi nr.1202. Grupi fillestar i masave të OSBE-së për ndërtimin e besimit për të zvogëluar risqet e konfliktit që rrjedhin nga përdorimi i teknologjive të informacionit dhe komunikimit. 10.3.2016. Organizata për Siguri dhe Bashkëpunim në Evropë. PC.DEC/1202.

- A është e mjaftueshme frekuenca dhe shtrirja e trajnimit për personelin përgjegjës?
- A merr pjesë vendi në trajnime dhe ushtrime rajonale dhe ndërkombëtare? Sa shpesh ndodhin këto?

PJESA IV - SPIUNAZHI KIBERNETIK

Përkufizimi

Spiunazhi kibernetik përkufizohet si akt i ndërmarrë fshehurazi ose nën pretendime të rreme që përdor kapacitetet kibernetike për të mbledhur (ose duke u përpjekur të mbledhë) informacion me qëllim që t'i komunikohet palës kundërshtare.13 Qasja fitohet qoftë nga individi që paraqitet si përdorues legjitim ose nëpërmjet përdorimit të sulmeve të sofistikuara me shënjestrim (të tilla si inxhinieria sociale) nëpërmjet të cilave përdoruesit e ligjshëm manipulohen në atë mënyrë që t'i hapet dera individëve që kërkojnë të realizojnë qasje të paligjshme.

Sfidat specifike të spiunazhit kibernetik

Një nga karakteristikat thelbësore të spiunazhit kibernetik është vetë asimetria e kostove që ajo nënkupton. Kostot e kundërvënies dhe mbrojtjes nga të gjitha cenueshmëritë janë të larta dhe në shpërpjesëtim në krahasim me kostot në anën e sulmuesit, i cili duhet të zbulojë dhe të shfrytëzojë një cenueshmëri të vetme. Përveç kësaj, duke marrë parasysh kohën e nevojshme për të zbuluar ndërhyrjen, spiunazhi kibernetik paraqet mjet efektiv sulmues për marrjen e informacionit mbi sistemet, proceset dhe individët. Vlerësimet e kohës së nevojshme për të zbuluar cenimin shkojnë nga një deri në tre muaj14, deri në të cilën kohë ndërhyrësi mund të realizojë qasje në larmi të madhe të informacionit të ndjeshëm. Me shtrirjen e depërtimit të internetit dhe shërbimit online në shoqëritë anekënd botës, spiunazhi kibernetik hap mundësi shumë më të gjera për të mbledhur informacione të ndjeshme për kundërshtarët.

Sjellje e pranueshme, krim kibernetik apo akt i agresionit?

Ka dakordim në rritje që spiunazhi kibernetik në përgjithësi është duke u bërë i pamposhtshëm. Megjithatë, definimi se çka përbën sjellje të pranueshme dhe çka duhet të sanksionohet ende mbetet sfidë e ndjeshme. Fakti që në të kaluarën spiunazhi tradicional nga ana e shteteve është trajtuar si sjellje e pranueshme shtetërore, e ka lënë të parregulluar

13 Sipas Manualit të Talinit të përmendur më lart.

14 Raporti Mandiant (2013) vlerëson se koha mesatare e mbajtjes së qasjes në rrjetin e viktimës është 356 ditë. Global Space (2013) vlerëson se cenimi mesatar mbetet i pazbuluar mesatarisht për 90 ditë. Foreign Policy (2015) vlerëson se mesatarisht viktimës i duhen 205 ditë për të zbuluar se është infektuar. Instituti Ponemon (2015) gjeti se cenimet mbeten të pazbuluara për 46 ditë mesatarisht. Kreps, Fletcher dhe Griffiths (2016) vlerësojnë se cenimi mbetet i pazbuluar mesatarisht për 3 muaj.

edhe spiunazhin e sotëm kibernetik. Rrjedhimisht, në praktikë, thjesht ndërhyrja në sistem kompjuterik, duke cenuar konfidencialitetin e tij, ende konsiderohet e pranueshme. Mirëpo, cenimet e integritetit ose disponueshmërisë së sistemit, të cilat mund të ndodhin si pasojë e kësaj ndërhyrjeje, konsiderohen si formë e sulmit kibernetik dhe të papranueshme. Nga aspekti normativ, spiunazhi kibernetik shihet si i pranueshëm dhe i papranueshëm, varësisht nga pasojat e tij.

Përveç kësaj, ekziston sfida e bërjes së dallimit midis aktiviteteve të mbledhjes së informacionit dhe atyre me dashje qëllimkeqe që mund të përbëjnë akte agresioni. Përsëri, kjo gjithashtu varet nga përdorimi i informacionit të marrë. Prandaj, ekziston vijë e hollë ndarëse ndërmjet akteve qëllimi kryesor i të cilave është spiunazhi kibernetik dhe atyre që duhet të konsiderohen kryekëput si sulme kibernetike. Kjo e bën jashtëzakonisht të vështirë vendosjen e parimeve dhe regjimeve ndërkombëtare që qeverisin nocionin e spiunazhit kibernetik, i cili për momentin mbetet i parregulluar.

Nga aspekti i sigurisë, spiunazhi kibernetik shihet si potencialisht i mbivendosur me nocionet e krimit kibernetik. Në këtë kuptim, kriminelët kibernetikë mund të kontraktohen nga aktorët e tretë për të kryer dhe/ose mundësuar aktet e spiunazhit kibernetik, të ngarkuar me detyrën për të depërtuar në sistemet e qeverisë dhe/ose korporatave dhe për të nxjerrë informacion të ndjeshëm.

Aktorët e deleguar, armatat private dhe konfliktet hibride

Sfidë tjetër është çështja e fushatave të spiunazhit kibernetik të sponsorizuar nga shtetet, ku shtetet mund të sponsorizojnë në mënyrë indirekte aktorët që kanë aftësinë për të depërtuar në sistemet e kundërshtarëve të tyre. Në këtë kuptim, hakerët janë bërë armata potenciale private të spiunëve në epokën dixhitale, në dispozicion të ofertuesit më të lartë. Ngritja e spiunazhit kibernetik ka shtuar gjithashtu një element tjetër në nocionin e zhvillimit të konflikteve hibride dhe luftimit asimetrik, ku konfliktet më nuk janë bardhë e zi por vijnë në forma dhe intensitet të ndryshëm. Duke u angazhuar në spiunazh kibernetik, shtetet tani janë në gjendje të zhvillojnë marrëdhënie hibride me kundërshtarët e tyre. Kjo do të thotë se, në fakt, marrëdhëniet në botën fizike vazhdojnë normalisht, ndërsa armiqësitë dhe konfliktet zhvillohen në fushën dixhitale, nëpërmjet praktikës së spiunazhit kibernetik, krahas hakimit dhe haktivizmit, krimit kibernetik dhe aktiviteteve sulmuese kibernetike.

Ashtu si me format e tjera të kundërvënies dhe mbrojtjes nga aktivitetet qëllimkëqija në hapësirën kibernetike, spiunazhi kibernetik bart sfidën e zbulimit dhe atribuimit. Përveç kësaj, spiunazhi kibernetik nuk kryhet medoemos nga shtetet ose aktorët e sponsorizuar nga shtetet. Ai gjithashtu mund të përdoret si mjet nga kriminelë kibernetikë, haktivistë si dhe aktorë privatë thjesht për të fituar avantazh ekonomik.

Adresimi, rregullimi dhe kundërvënia ndaj spiunazhit kibernetik

Strategjia më e mirë e mbrojtjes nga spiunazhi kibernetik pra është - të paktën për momentin - ajo e frenimit. Kjo nënkupton rritjen e kostove të vërteta ose të parashikuara të sulmit të mundshëm për kundërshtarin. Krahas ndërtimit të mbrojtjes më të fortë, kjo gjithashtu do të thotë nxitjen e bashkëpunimit dypalësh dhe shumëpalësh në arritjen e marrëveshjeve dhe/ose kodeve të sjelljes që rregullojnë nocionin e spiunazhit kibernetik, krahas llojeve të tjera të sjelljes në hapësirën kibernetike. Një shembull me sa duket i suksesshëm i kësaj është marrëveshja SHBA-Kinë e vitit 2015 në lidhje me spiunazhin ekonomik, e cila përcakton se asnjëri vend nuk do të kryejë ose nuk do të mbështetë me vetëdije vjedhjen kibernetike të pronës intelektuale me dashje të ofrimit të përparësive konkurruese për kompanitë apo sektorët komercialë.

Megjithatë, spiunazhi kibernetik për të marrë informata për qëllime të sigurisë kombëtare, mu ashtu si format tradicionale të spiunazhit, mbetet i parregulluar. Për këtë arsye, iniciativat e udhëhequra nga shtetet shënojnë rritje në debatet në lidhje me të drejtën për 'backfire', ose për t'ia kthyer me hakim (hack-back), kur zbulohet ndërhyrja në sistem, si formë më bindëse e frenimit. Ndër vendet e fundit që i janë bashkuar këtyre debateve është Gjermania, ku komuniteti kombëtar i inteligjencës po kërkon t'i jepet e drejta për të futur në përdorim mbrojtjen aktive. Kjo do të nënkuptonte juridiksionin për të shkatërruar të dhënat e vjedhura dhe të zhvendosura nga serverët gjermanë, si dhe për të kompromet uar serverët e huaj në mënyrë që të forcohen aftësitë vëzhguese kombëtare. Ideja prapa këtyre iniciativave është që të frenohen sulmuesit potencialë duke u kërcënuar me hakmarrje.

Shembuj të pyetjeve për mbikëqyrje:

- Çka po bëhet për të mbrojtur qytetarët dhe të dhënat e tyre nga spiunazhi kibernetik? Cilat janë ministritë apo agjencitë shtetërore përgjegjëse për luftimin e spiunazhit kibernetik?
- A ka vlerësim të cenueshmërive dhe nevojave të vendit lidhur me spiunazhin kibernetik dhe çfarë kundërmasash janë ndërmarrë?
- Si mund të përkufizohet dhe rregullohet më mirë spiunazhi kibernetik nga legjislacioni kombëtar dhe ai ndërkombëtar?

PJESA IV - TERRORIZMI KIBERNETIK

Përkufizimi

Terrorizmi kibernetik kombinon dy nga zhvillimet më të spikatura në botë: mbështetja në rritje e shoqërisë nga interneti dhe kërcënimi i terrorizmit ndërkombëtar.15 Natyra anonime e internetit, lehtësisht e qasshme dhe shpesh e parregulluar, e bën atë veçanërisht të prirë për shfrytëzim dhe keqpërdorim nga organizatat terroriste dhe aktorët e tjerë jo-shtetërorë. Mirëpo, ndërsa përdorimi i internetit për qëllime terroriste përbën sfidë për bashkësinë ndërkombëtare, ai gjithashtu siguron mjete të reja për kundër-terrorizmin.

Terrorizmi kibernetik kundrejt përdorimit të internetit për qëllime terroriste

Ndërkohë që nuk ka përkufizim të pranuar universalisht për terrorizmin kibernetik, shumica e përkufizimeve kombëtare i referohen sulmit që përdor mjete elektronike për të depërtuar dhe/ose për të ndërhyrë seriozisht në infrastrukturën kritike kombëtare.16 OSBE për shembull e përkufizon terrorizmin kibernetik si "terrorizëm në lidhje me internetin dhe më konkretisht, [...], si sulme terroriste në infrastrukturën kibernetike, veçanërisht në sistemet e kontrollit për infrastrukturën kritike energjetike jo-bërthamore".17

Skenarët e kërcënimit të terrorizmit kibernetik përfshijnë paralizimin e zonave të mëdha urbane, sektorit të shëndetit publik ose çrregullimin e sektorit financiar duke "ndryshuar disa njësha dhe disa zero".18 Ngritja e internetit të gjërave (Internet of Things)19 përbën një tjetër pasiguri të madhe që mund të shfrytëzohet lehtësisht nga organizatat terroriste për të kryer akte të terrorizmit kibernetik. Akte të terrorizmit kibernetik që do të kishin ndikim fizikisht shkatërrues konsiderohet se ka pak të ngjarë të ndodhin dhe kështu paraqesin më pak sfidë për shtete, për shkak të sasisë tejet të madhe të resurseve që kërkohen për të kryer aktin e tillë.20

Përveç kësaj, shumë organizata terroriste përdorin internetin për të kryer vepra penale tradicionale, si mashtrim, qasje të kundërligjshme dhe ndërhyrje të paligjshme në sistemet

15 Lentz, Christopher E. Lentz. 2010. A State's Duty to Prevent and Respond to Cyberterrorist Acts. Chicago Journal of International Law 10. No. 2.

16 Infrastruktura kombëtare kritike është aseti ose sistemi thelbësor për ruajtjen e funksioneve thelbësore shoqërore dhe që, nëse nxirret jashtë funksionit për periudhë të gjatë, do të krijonte rrezik serioz për shëndetin publik, ekonominë, mjedisin, qytetarët dhe sigurinë kombëtare.

17 Udhëzues i praktikave të mira për Mbrojtjen e Infrastrukturës Kritike Energjetike Jo-Bërthamore (NNCEIP) nga sulmet terroriste me fokus te kërcënimet që burojnë nga hapësira kibernetike. 2013. Organizata për Siguri dhe Bashkëpunim në Evropë. Nr.16.

18 Gen. Votel, Joseph L.. July 2015. Understanding Terrorism Today and Tomorrow. CTC Sentinel 8. Issue 7, pp.2–6.

19 Cambridge Dictionary e përkufizon "Internet of Things" si objekte që brenda vetes kanë pajisje llogaritëse që mund të lidhen me njëri-tjetrin dhe të shkëmbejnë të dhëna duke përdorur internetin. Interneti i Gjërave po bëhet gjithnjë e më i përfshirë në infrastrukturën kritike kombëtare.

20 Weimann, Gabriel. Mars 2004. https://www.usip.org/publications/2004/03/wwwterror-net-how-modern-terrorism-uses-internetwww.terror.net:%20How%20Modern%20Terrorism%20Uses%20the%20Internet. Raport Special Nr.116. Instituti Amerikan i Paqes.

kompjuterike. Kjo rezulton me mbivendosje midis krimit kibernetik (shih kapitullin për krimin kibernetik), sulmet kibernetike (shih kapitullin për luftën kibernetike) dhe terrorizmin kibernetik; në fund, duke e bërë të vështirë të bëhet dallimi midis tyre. Rezoluta 1566 e Këshillit të Sigurimit të Kombeve të Bashkuara mund të ofrojë udhëzim lidhur me këtë, meqë thekson elementin e motivuar politikisht, duke identifikuar "aktet terroriste" si:

> "[...] akte kriminale, duke përfshirë edhe ato kundër civilëve, të kryera me dashjen e shkaktimit të vdekjes ose lëndimit të rëndë trupor ose marrjes së pengjeve, me qëllim të provokimit të gjendjes së terrorit [...], që të frikësohet popullata ose të detyrohet qeveria ose organizata ndërkombëtare për të vepruar ose për të mos vepruar, të cilat përbëjnë vepra penale brenda fushëveprimit dhe siç përcaktohen në konventat dhe protokollet ndërkombëtare që kanë të bëjnë me terrorizmin [...]."21

Përveç kësaj, organizatat terroriste përdorin internetin në baza ditore për një sërë aktivitetesh, siç janë propaganda (duke përfshirë radikalizimin, nxitjen për terrorizëm, rekrutimin), financimi, trajnimi dhe planifikimi (duke përfshirë komunikimin sekret dhe informacionin nga burimet e hapura), si dhe për të kryer sulme kibernetike.22 Ndërsa përdorimi i internetit për qëllime propagandistike ka fituar rëndësi të madhe brenda bashkësisë ndërkombëtare, duke bërë thirrje për partneritete më të forta, duke përfshirë edhe industrinë e teknologjisë,23 sfida e përdorimit të internetit për qëllime financimi shumë shpesh është shpërfillur. Ndërkohë, zhvendosja e përgjithshme drejt përdorimit të teknologjisë në tregtinë ndërkombëtare e ka shndërruar internetin në aset për organizatat terroriste për të pastruar paratë, për të ngritur dhe për të transferuar fonde.24

Rrjedhimisht, agjencitë e zbatimit të ligjit dhe shërbimet e inteligjencës po monitorojnë gjithnjë e më shumë transferet e dyshimta financiare online dhe po zhvillojnë mjete dhe shkathtësi për të parandaluar, zbuluar dhe reaguar në mënyrë aktive ndaj aktivitetit terrorist që përfshin internetin. Qeveritë gjithashtu kanë filluar t'i kundërpërgjigjen përdorimit të internetit për qëllime propagandistike nëpërmjet komunikimeve strategjike, siç janë narrativet alternative dhe kundër-mesazhet, dhe rregullimi i përmbajtjes.25 Megjithatë, çdo aktivitet kundër terrorizmit në internet kërkon si parakusht përpjekje të bashkërenduara midis shteteve, sektorit privat dhe shoqërisë civile për t'iu përgjigjur në mënyrë efektive këtyre sfidave të reja.

21 Rezoluta e Këshillit të Sigurimit 1566 (2004) për Kërcënimet ndaj paqes dhe sigurisë ndërkombëtare të shkaktuara nga aktet terroriste. 8 tetor 2004. Këshilli i Sigurimit të Kombeve të Bashkuara. Rezoluta S/RES/1566. Op. para. 3.

22 Shih: Përdorimi i internetit për qëllime terroriste. 2012. Zyra e Kombeve të Bashkuara për Drogat dhe Krimin.

23 Shih: Komiteti Kundër Terrorizmit i KS; Teknologjia Kundër Terrorizmit; Forumi Global i Internetit Kundër Terrorizmit.

24 Jacobson, Michael. June 2009. Terrorist Financing on the internet. CTC Sentinel 2. Issue 6, pp.17–20.

25 Shih: Rekomandimet Cyrih-Londër për parandalimin dhe kundërvënien ndaj ekstremizmit të dhunshëm dhe terrorizmit online. 2017. Forumi Global kundër Terrorizmit.

Konsideratat e sundimit të ligjit

Në përgjithësi, aktivitetet kundër terrorizmit që përfshijnë internetin mund të kenë ndikim në një numër të të drejtave të njeriut (duke përfshirë privatësinë dhe liritë e shprehjes, shoqërimit, tubimit paqësor, fesë ose besimit). Në lidhje me përdorimin e internetit për qëllime propagandistike, qeveritë kanë adoptuar masa të reja, duke filluar nga mohimi i përpjekjeve për justifikimin ose thurjen e lavdeve (apologie) për aktet terroriste deri te ndalimi me ligj i nxitjes për t'i kryer këto.26 Sidoqoftë, duhet të theksohet se fjala që është moralisht e pështirë, trondit, shqetëson ose fyen nuk përshkallëzohet vetiu në nivelin kriminal; por "[t] ë tilla janë kërkesat e atij pluralizmi, tolerance dhe mirëkuptimi pa të cilat nuk ka 'shoqëri demokratike'."27 Mirëpo, sfida është identifikimi i pikës kthyese në të cilën kontestimi ose kritika shndërrohet në gjuhë urrejtjeje, thurje lavdesh (apologie) ose nxitje për të kryer akte terroriste. Identifikimi i kësaj pike kthyese nuk është gjithmonë i thjeshtë.

Në thelb, është e rëndësishme që qeveritë të përcaktojnë qartë veprat penale relevante në kodet e tyre kombëtare penale, në mënyrë që qytetarët të mund të parashikojnë pasojat e lidhura me veprime të caktuara dhe të shmangin tej-rregullimin, dhe kështu "efektin e shtangies" (chilling-effect) në fushën e të drejtave të njeriut. Garancitë e procesit të rregullt gjyqësor, të tilla si prezumimi i pafajësisë dhe e drejta për proces të drejtë gjyqësor, janë thelbësore për të garantuar që masat kundër terrorizmit janë efektive dhe respektojnë sundimin e ligjit. Përveç kësaj, mbikëqyrja efektive e aktorëve të sigurisë publike të përfshirë në luftën kundër terrorizmit (online dhe offline) është vendimtare për promovimin e proceseve të reformave në luftën kundër terrorizmit që janë në përputhje me të drejtat e njeriut.

Shembuj të pyetjeve për mbikëqyrje:

- A ka kornizë të qartë ligjore që identifikon veprimet e ndaluara në internet?
- A garantohet me Kushtetutë e drejta e lirisë së shprehjes dhe e drejta për të mos iu nënshtruar ndërhyrjes arbitrare ose të paligjshme në privatësi?
- A ka ndonjë komision parlamentar mandat ligjor për të mbikëqyrur punën e agjencive shtetërore përgjegjëse për luftën kundër terrorizmit?
- A i respekton standardet e të drejtave të njeriut legjislacioni që rregullon aktivitetet kundër terrorizmit në internet? A është adoptuar legjislacioni pas procesit të konsultimit publik dhe gjithpërfshirës?
- Çfarë mundësish ekzistojnë për parlamentin për të shoshitur kompanitë private në lidhje me praktikat e tyre për mbledhjen e informacionit personal të përdoruesve të tyre?

26 Shih Kundërvënia ndaj narrativeve terroriste. 2017. Këshilli i Sigurimit të Kombeve të Bashkuara. S / RES/2354 (2017). Preambular para. 12. Dhe Ndalimi i nxitjes për të kryer akte terroriste. 2005. Këshilli i Sigurimit të Kombeve të Bashkuara. S/RES/1624 (2005). Preambular para. 4 dhe Operative para. 1(a).

27 Handyside kundër Mbretërisë së Bashkuar. 4 nëntor 1976. Këshilli i Evropës: Gjykata Evropiane për të Drejtat e Njeriut: 5493/72, op. cit., para 49

PJESA V - HAKTIVIZMI

Përkufizimi

Sipas përkufizimit, haktivizmi është përzierje e hakimit dhe aktivizmit tradicional. Kjo shprehje nuk është përqafuar nga vetë "haktivistët", por më tepër u është atribuuar atyre nga hulumtuesit, gazetarët dhe profesionistët e sigurisë kibernetike në përpjekje për t'i dalluar aktorët e ndryshëm në hapësirën kibernetike. Haktivizmi mundëson forma të reja mobilizimi për aktivistët online në luftën e tyre për një kauzë të veçantë (p.sh. të drejtat e njeriut, liria e fjalës etj.). Kështu ai mundëson veprim nga distanca dhe mobilizim në shkallë të gjerë me një klik të miut. Për sa i përket pasojave, thjesht haktivizmi në përgjithësi shkakton dëme të vogla, prandaj shumë pak çështje arrijnë në pikën e ndjekjes penale, veçanërisht duke pasur parasysh sfidën plotësuese të atribuimit që ekziston këtu si edhe në kuadër të çdo lloj tjetër aktiviteti në hapësirën kibernetike.

Motivet e haktivistëve dhe dallimi me krimin kibernetik dhe terrorizmin kibernetik

Ç'është më e rëndësishmja, haktivizmi shihet si çrregullues, jo shkatërrues. Kjo është ajo që e dallon atë nga format e tjera të aktiviteteve qëllimkëqija në hapësirën kibernetike, siç janë krimi kibernetik apo terrorizmi kibernetik. Haktivistët mbështeten kryesisht në taktika të tilla si përhapja e krimbave (worms) dhe viruseve, sulmet e shpërndara të mohimit të shërbimit (DDoS), shpërfytyrimi i uebsajteve dhe të ngjashme. Shkalla gjer në të cilën haktivistët përgjithësisht shihen si kërcënim i vogël portretizohet nga karakterizimi i zakonshëm se sulmet e tyre të llojit DDoS janë të barabarta me formën e protestave ulur në vitet '60.

Megjithatë, haktivistët gjithashtu angazhohen në aktivitete të tilla si zaptimi i llogarive në Twitter dhe faqeve në Facebook, si dhe vjedhja dhe/ose zbulimi i informacionit të ndjeshëm nga sistemet në të cilat depërtojnë.

Hakerët kapuç-bardhë, kapuç-hirtë dhe kapuç-zi

Duke qenë se haktivistët janë, në thelb, hakerë me kauzë, veprimet e veçanta që ata marrin me të depërtuar në sistem dallojnë midis llojeve të ndryshme të hakerëve. Këto janë:

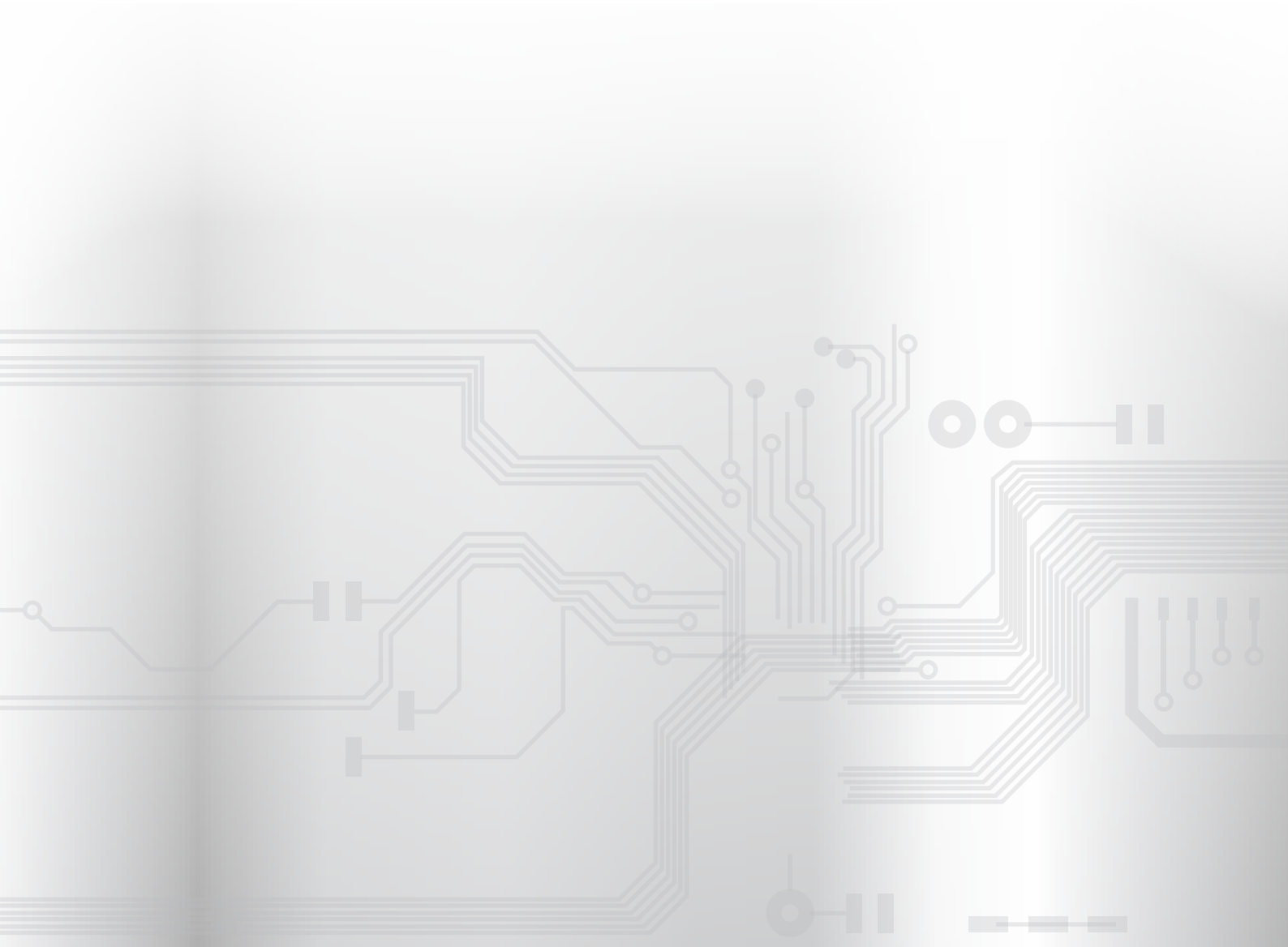
- Hakerë kapuç-bardhë janë ata që, pas zbulimit të cenueshmërive në sistem, ia raportojnë këto zhvilluesve të sistemit në mënyrë që të zhvillohen arna enkas dhe të përmirësohet siguria e përgjithshme e sistemit. Hakerët kapuç-bardhë gjithashtu përshkruhen si 'hakerë etikë'.

- Hakerët kapuç-hirtë gjithashtu ia raportojnë cenueshmëritë e zbuluara zhvilluesve të sistemit, por mund të kërkojnë kompensim financiar ose ndonjë formë tjetër shpërblimi për informacionin që kanë ofruar.
- Hakerët kapuç-zi nuk ia raportojnë cenueshmëritë e zbuluara zhvilluesve të sistemit dhe në vend të kësaj kërkojnë të përfitojnë nga ata qoftë nëpërmjet shfrytëzimit të drejtpërdrejtë ose nëpërmjet shitjes së këtij informacioni në tregun e zi për aktorët e tjerë, siç janë kriminelët kibernetikë.

Ekziston vijë shumë e hollë ndarëse midis haktivizmit dhe aktivitetit të kundërligjshëm në hapësirën kibernetike. Haktivistët, në disa raste, mund të bashkëpunojnë me kriminelë kibernetikë. Përveç kësaj, kërcënimet e drejtpërdrejta publike të bëra nga grupe të caktuara të haktivistëve drejtuar qeverive, ndërmarrjeve dhe individëve të ndryshëm, potencialisht mund të shkaktojnë panik dhe frikë në radhët e popullatës civile, që është një nga elementet thelbësore të përkufizimit të terrorizmit. Në fund, në debatet e kohëve të fundit është parë rritje e referimeve që i bëhen nocionit të haktivizmit të sponsorizuar nga shtetet, dhe megjithëse mund të bëhen supozime të arsyeshme për ekzistencën e tij, në praktikë është pothuajse e pamundur të provohet.

Shembuj të pyetjeve për mbikëqyrje:

- Cilat janë kapacitetet e zbatimit të ligjit për të identifikuar haktivizmin dhe për ta dalluar atë nga format e tjera të kërcënimeve kibernetike? A janë të mjaftueshme?
- A përcakton qartë legjislacioni përkatës cilat aktivitete të përfshira në termin "haktivizëm" janë të kundërligjshme (d.m.th. kur kalojnë pragun e fjalës së lirë)?
- Çka mund të bëhet nga qeveria për të mbështetur "hakerët kapuç-bardhë" ose për të shmangur ngatërrimin e tyre me "hakerët kapuç-hirtë" apo "hakerët kapuç-zi"? A ka ndonjë mekanizëm mbrojtës për sinjalizuesit që vlen për "hakerët kapuç-bardhë"?
- Çka po bëhet për të identifikuar haktivistët e mundshëm dhe për të parandaluar sjelljen kriminale? A ka masa mbrojtëse ligjore dhe operative për parandalimin e shërbimeve të sigurisë nga keqpërdorimi i autoritetit dhe minimi/paaftësimi i aktivizmit legjitim?
- Çka po bëhet për të rritur bashkëpunimin ndërkombëtar në kundërvënien ndaj haktivizmit qëllimkeq?



DCAF Geneva Centre for Security Sector Governance

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

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

DCAF Ljubljana
Gospodinjska ulica 8
1000 Ljubljana
Slovenia

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

DCAF Beirut
Gefinor Bloc C
Office 604, Ras Beirut
Lebanon

DCAF Tunis
Rue Ibn Zohr 14
1082 Tunis
Tunisia