EVROPSKA
KOMISIJA

VISOKI PREDSTAVNIK
UNIJE ZA ZUNANJE
ZADEVE IN
VARNOSTNO POLITIKO

Bruselj, 13.9.2017
JOIN(2017) 450 final

SKUPNO SPOROČILO EVROPSKEMU PARLAMENTU IN SVETU

Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU

1. UVOD

Kibernetska varnost je življenjskega pomena za naše blagostanje in varnost. V vsakdanjem življenju in v gospodarstvu smo vse bolj odvisni od digitalnih tehnologij, zato smo čedalje bolj izpostavljeni. Kibernetski incidenti so vse bolj raznoliki tako glede tega, kdo je zanje odgovoren, kot tudi glede njihovega cilja. Zlonamerne kibernetske dejavnosti ne ogrožajo le našega gospodarstva in napredka na poti k enotnemu digitalnemu trgu, ampak tudi delovanje našega gospodarstva, naše svoboščine in vrednote. Naša prihodnja varnost je odvisna od tega, ali bomo lahko preobrazili svojo sposobnost za obrambo EU pred kibernetskimi grožnjami: tako civilna infrastruktura kot vojaška zmogljivost sta odvisni od varnih digitalnih sistemov. To je priznal Evropski svet junija 2017[1], enako pa je ugotovljeno tudi v globalni strategiji za zunanjo in varnostno politiko za Evropsko unijo[2].

Tveganja eksponentno naraščajo. Kot kažejo študije, se je gospodarski učinek kibernetske kriminalitete v obdobju 2013–2017 povečal za petkrat, do leta 2019 pa bi se lahko povečal še za štirikrat[3]. Narasla je zlasti uporaba izsiljevalskega programja[4], saj nedavni napadi[5] kažejo na močan porast dejavnosti na področju kibernetske kriminalitete. Toda izsiljevalsko programje še zdaleč ni edina grožnja.

Kibernetske grožnje izvirajo tako od državnih kot nedržavnih akterjev: pogosto so sicer kriminalne v želji po dobičku, a lahko so tudi politične in strateške. Nevarnost kriminalitete je še večja zaradi izginjanja ločnice med kibernetsko in „tradicionalno“ kriminaliteto, saj zločinci izkoriščajo internet tako za stopnjevanje svojih dejavnosti kot za vir novih metod in orodij za kazniva dejanja[6]. Toda v veliki večini primerov je zelo malo možnosti, da bi zločinca izsledili, še manj pa je možnosti za kazenski pregon.

Hkrati pa državni akterji svoje cilje vse bolj dosegajo ne le s tradicionalnimi sredstvi, kot je vojaška sila, ampak tudi z diskretnejšimi kibernetskimi orodji, med katerimi je vmešavanje v notranje demokratične procese. Uporaba kibernetskega prostora kot področja za vojskovanje, bodisi kot edinega sredstva bodisi kot dela hibridnega pristopa, je zdaj splošno priznana. Dezinformacijske kampanje, lažne novice in kibernetske operacije, katerih cilj je kritična infrastruktura, so vse pogostejše in nanje se je treba odzvati. Zato je Komisija v razmisleku o prihodnosti evropske obrambe[7] poudarila pomen sodelovanja na področju kibernetske obrambe.

Če ne bomo bistveno izboljšali svoje kibernetske varnosti, bo tveganje naraščalo skupaj z digitalno preobrazbo. Z internetom naj bi se bo do leta 2020 povezalo na desetine milijard naprav v „internetu stvari“, toda kibernetska varnost pri njihovi konstrukciji še ni prednostna naloga[8]. Če ne bomo zaščitili naprav, ki nadzorujejo naša elektroenergetska omrežja, avtomobile, prometna omrežja, tovarne, finance, bolnišnice in hiše, bi lahko bile posledice strahotne, zaupanje potrošnikov v tehnologije v vzponu pa hudo prizadeto. Tveganje je še

---

1 http://www.consilium.europa.eu/en/press/press-releases/2017/06/23-euco-conclusions/.

2 http://europa.eu/globalstrategy/.

3 Glej npr. študijo McAfee & Centre for Strategic and International Studies *Net losses*: *Estimating the Global Cost of Cybercrime* (Neto izgube: ocene stroškov kibernetske kriminalitete na svetovni ravni) iz leta 2014.

4 Izsiljevalsko programje je vrsta zlonamerne programske opreme, ki uporabniku prepreči ali omeji dostop do sistema tako, da zaklene zaslon sistema ali uporabnikove datoteke, dokler ne plača odkupnine.

5 Maja 2017 je izsiljevalski program WannaCry prizadel več kot 400 000 računalnikov v več kot 150 državah. Mesec dni pozneje je izsiljevalski program „Petja“ napadel Ukrajino in več podjetij po vsem svetu.

6 EUROPOL: Ocena ogroženosti zaradi hudih oblik kriminala in organiziranega kriminala, 2017.

7 https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_sl.pdf.

8 *IDC and TXT Solutions* (2014), SMART 2013/0037, Kombinacija storitev v oblaku in interneta stvari (*Cloud and IoT combination*), študija za Evropsko komisijo.

večje zaradi nevarnosti politično motiviranih napadov na civilne cilje in pomanjkljivosti vojaške kibernetske obrambe.

Pristop, predstavljen v tem skupnem sporočilu, bo Evropi omogočil, da bo bolje pripravljena na te grožnje. Z njim bi postali odpornejši in strateško bolj avtonomni, okrepili bi zmogljivosti na področju tehnologije ter znanj in spretnosti, hkrati pa pripomogli k nastanku močnega enotnega trga. V ta namen so potrebne ustrezne strukture, s katerimi bi vzpostavili močno kibernetsko varnost in se odzvali, kadar bi bilo treba, ob sodelovanju vseh ključnih akterjev. S takim pristopom bi tudi bolje odvračali kibernetske napade in naredili več za to, da bi zaznali in izsledili krivce ter zahtevali njihovo odgovornost. Ta pristop bi tudi upošteval svetovno razsežnost, saj bi razvijal mednarodno sodelovanje kot platformo za vodilno vlogo EU na področju kibernetske varnosti. Ti koraki izhajajo iz pristopov enotnega digitalnega trga, globalne strategije, evropske agende za varnost[9], skupnega okvira o preprečevanju hibridnih groženj[10] in sporočila o vzpostavitvi evropskega obrambnega sklada[11][12].

EU se že ukvarja z marsikaterim od teh problemov: čas je, da različne delovne tokove speljemo v isto smer. EU je leta 2013 oblikovala strategijo za kibernetsko varnost, s katero se je začela vrsta ključnih procesov za boljšo kibernetsko odpornost[13]. Še vedno veljajo njeni glavni cilji in načela, to je ustvarjanje podlage za zanesljiv, varen in odprt kibernetski ekosistem. Toda v razmerah, v katerih se grožnje nenehno spreminjajo in postajajo vse hujše, je potrebno več ukrepanja, da bi lahko v prihodnje vzdržali napade in jih odvrnili[14].

EU ima glede na obseg svojih politik ter orodij, struktur in zmogljivosti, ki jih ima na razpolago, dobre možnosti za reševanje problema kibernetske varnosti. Za nacionalno varnost so sicer še naprej odgovorne države članice, vendar obseg in čezmejna narava grožnje govorita v prid ukrepanju EU, ki bi državam članicam zagotovilo spodbude in podporo za razvoj in vzdrževanje več in boljših zmogljivosti na področju kibernetske varnosti, hkrati pa krepilo zmogljivost na ravni EU. Ta pristop je zastavljen tako, da bi vse akterje, torej EU, države članice, industrijo in posameznike, spodbudil k prednostni obravnavi kibernetske varnosti, ki je nujna, da bi okrepili odpornost in zagotovili boljši odgovor EU na kibernetske napade. Prispeval bo konkretne korake, ki bodo pripomogli k odkrivanju in preiskavi vseh oblik kibernetskih incidentov, naperjenih proti EU in njenim državam članicam, in ustreznemu odzivu nanje, tudi s pregonom storilcev kaznivih dejanj. To bo omogočilo zunanje ukrepe EU za učinkovito spodbujanje kibernetske varnosti na svetovni ravni. Tako bo EU od pristopa, za katerega je bilo značilno predvsem reagiranje, prešla na proaktiven pristop, pri katerem se bo odzivala na sedanje in prihodnje grožnje ter tako varovala evropsko blagostanje, družbo, vrednote ter temeljne pravice in svoboščine.

2. KREPITEV ODPORNOSTI EU NA KIBERNETSKE NAPADE

Za močno kibernetsko odpornost je potreben kolektiven in širok pristop. V ta namen so potrebne krepkejše in učinkovitejše strukture za spodbujanje kibernetske varnosti in odziv na

[9] COM(2015) 185 final.
[10] JOIN(2016) 18 final.
[11] COM(2017) 295.
[12] Ta pristop je utemeljen tudi z neodvisnimi znanstvenimi nasveti skupine znanstvenih svetovalcev na visoki ravni mehanizma Evropske komisije za znanstveno svetovanje (Scientific Advice Mechanism High Level Group of scientific advisors, gl. navedbe v nadaljevanju).
[13] JOIN(2013) 1 final. Ocena te strategije je na voljo v dokumentu SWD(2017) 295.
[14] Če ni navedeno drugače, predlogi Komisije ne vplivajo na proračun. Pri pobudah, ki bodo imele proračunske posledice, bodo upoštevani postopki sprejemanja letnega proračuna in te pobude ne morejo prejudicirati naslednjega večletnega finančnega okvira za obdobje po letu 2020.

kibernetske napade v državah članicah, pa tudi v samih institucijah, agencijah in organih EU. Pri njem je za krepitev kibernetske odpornosti in strateške avtonomnosti potreben tudi bolj celosten pristop, ki zajema več politik, skupaj z močnim enotnim trgom, velikim napredkom v tehnološki zmogljivosti EU in bistveno večjim številom usposobljenih strokovnjakov. V njegovem središču pa je širše zavedanje o tem, da je kibernetska varnost skupen družbeni izziv, za katerega je potrebno sodelovanje na več ravneh države, gospodarstva in družbe.

2.1 Krepitev Agencije Evropske unije za varnost omrežij in informacij

Agencija Evropske unije za varnost omrežij in informacij (ENISA) mora imeti ključno vlogo pri krepitvi kibernetske odpornosti EU in odziva na kibernetske grožnje, vendar jo sedanja pooblastila omejujejo. Komisija zato predstavlja velikopotezen predlog reforme, ki zajema tudi **trajno pooblastilo za agencijo**[15]. To bo agenciji ENISA omogočilo, da bo nudila pomoč državam članicam, institucijam EU in podjetjem na ključnih področjih, vključno z izvajanjem direktive o varnosti omrežij in informacijskih sistemov[16] in predlaganega certifikacijskega okvira za kibernetsko varnost.

Reformirana agencija ENISA bo imela močno svetovalno vlogo pri razvoju in izvajanju politike, med drugim tudi s spodbujanjem skladnosti med sektorskimi pobudami z direktivo o varnosti omrežij in informacijskih sistemov ter pomočjo pri vzpostavitvi centrov za izmenjavo in analizo informacij v kritičnih sektorjih. Agencija ENISA bo zvišala merila in okrepila pripravljenost Evrope, saj bo vsako leto organizirala vseevropske vaje kibernetske varnosti, na katerih bo kombiniran odziv na več ravneh. Podpirala bo tudi razvoj politik EU na področju certificiranja kibernetske varnosti v informacijski in komunikacijski tehnologiji (IKT) in imela pomembno vlogo pri stopnjevanju operativnega sodelovanja in kriznega upravljanja po vsej EU. Agencija bo tudi osrednja točka za informacije in znanje v skupnosti kibernetske varnosti.

Odločitev, ali so potrebni skupni ukrepi za ublažitev ali odziv s podporo EU, ni možna brez hitrega in skupnega razumevanja groženj in incidentov še v času, ko se odvijajo. Za tako izmenjavo informacij je potrebna udeležba vseh zadevnih akterjev, tako organov in agencij EU kot držav članic, na tehnični, operativni in strateški ravni. Agencija ENISA bo prispevala tudi k situacijskemu zavedanju na ravni EU v sodelovanju z ustreznimi organi na ravni držav članic in EU, predvsem mrežo skupin za odzivanje na incidente na področju računalniške varnosti [17], CERT-EU, Europolom ter Obveščevalnim in situacijskim centrom (INTCEN). To je mogoče upoštevati pri obveščevalnih podatkih o grožnjah in oblikovanju politik v zvezi z rednim spremljanjem razmer na področju groženj in učinkovitega operativnega sodelovanja, pa tudi pri odzivanju na čezmejne incidente velikega obsega.

2.2 Enotnemu trgu kibernetske varnosti naproti

Rast trga kibernetske varnosti v EU – v smislu proizvodov, storitev in procesov – je ovirana na več načinov. Ključni vidik je pomanjkanje shem certificiranja kibernetske varnosti, priznanih po vsej EU, s katerimi bi v proizvode vgradili višje standarde odpornosti in ustvarili

[15] COM(2017) 477.

[16] Direktiva 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji.

[17] Kot je določeno v členu 9 direktive o varnosti omrežij in informacijskih sistemov.

podlago za tržno zaupanje povsod v EU. Komisija zato predlaga vzpostavitev **certifikacijskega okvira EU za kibernetsko varnost**[18]. V okviru bi bil določen postopek vzpostavitve shem certificiranja kibernetske varnosti za vso EU, ki bi zajemal proizvode, storitve in/ali sisteme, pri katerih se stopnja zagotovila prilagaja uporabi (najsi gre za kritične infrastrukture ali naprave za potrošnike)[19]. Podjetjem bo prinesel jasne koristi, saj jim pri čezmejnem trgovanju ne bo treba prestajati različnih certifikacijskih postopkov, s tem pa se jim bodo znižali upravni in finančni stroški. Uporaba shem, oblikovanih v tem okviru, bo pripomogla tudi h krepitvi zaupanja potrošnikov, saj bo certifikat o skladnosti kupce in uporabnike informiral in jim dal zagotovila o varnostnih lastnostih proizvodov in storitev, ki jih kupujejo in uporabljajo. Tako bodo visoki standardi kibernetske varnosti omogočali tudi konkurenčno prednost. S tem bi se okrepila odpornost, saj bi se proizvodi in storitve IKT uradno ocenjevali z opredeljenim sklopom standardov kibernetske varnosti, ki bi jih bilo mogoče oblikovati v tesni povezavi s širšo stalno dejavnostjo na področju standardov IKT[20].

Sheme v tem okviru bi bile prostovoljne in za prodajalce ali ponudnike storitev ne bi pomenile nobenih novih regulativnih obveznosti Sheme ne bi bile v nasprotju s pravnimi zahtevami, ki se uporabljajo, kot je zakonodaja EU o varstvu podatkov.

Komisija bo po vzpostavitvi okvira pozvala zadevne zainteresirane strani, da se osredotočijo na tri prednostna področja, ki so:

- varnost na kritičnih področjih uporabe ali področjih uporabe z visokim tveganjem[21]: sistemi, od katerih smo odvisni pri svojih vsakdanjih dejavnostih, od avtomobilov do strojev v tovarnah, od največjih sistemov, kot so letala ali elektrarne, do najmanjših, kot so medicinski pripomočki, so vse bolj digitalno povezami med sabo. Pri glavnih sestavnih delih IKT v takih proizvodih in sistemih bi bile zato potrebne stroge varnostne ocene;

- kibernetska varnost v digitalnih proizvodih, omrežjih, sistemih in storitvah široke uporabe, ki se tako v zasebnem kot v javnem sektorju uporabljajo za obrambo pred napadi in izpolnjevanje regulativnih obveznosti[22], npr. šifriranje elektronske pošte, požarni zidovi in navidezna zasebna omrežja; izjemno pomembno je, da širitev uporabe takih orodij ne prinese novih virov tveganja ali novih ranljivih točk;

- uporaba metod „varnosti v zasnovi“ v nizkocenovnih medsebojno povezanih digitalnih napravah za uporabnike široke potrošnje, ki tvorijo „internet stvari“: s pomočjo shem tega okvira bi bilo mogoče sporočiti, da so proizvodi narejeni z uporabo najsodobnejših metod varnega razvoja, da so prestali ustrezen varnostni preskus in da so se prodajalci zavezali, da bodo v primeru na novo odkritih ranljivih točk ali groženj posodobili njihovo programsko opremo.

Pri teh prednostnih nalogah bi bilo treba upoštevati zlasti spreminjajoče se razmere na področju groženj za kibernetsko varnost ter pomembnost bistvenih storitev, kot so promet,

---

[18] COM(2017) 477.

[19] Stopnja zagotovila označuje raven varnostne ocene in je navadno sorazmerna s stopnjo tveganja, povezano s področji uporabe ali funkcijami (tj. višja stopnja zagotovila bi se zahtevala za proizvode ali storitve IKT, ki se uporabljajo na področjih uporabe ali v funkcijah z visokim tveganjem).

[20] COM(2016) 176.

[21] Izjeme bi bili primeri, v katerih obvezno ali prostovoljno certificiranje urejajo drugi akti Unije.

[22] Na primer Direktiva (EU) 2016/1148, Uredba (EU) 2016/679, Direktiva (EU) 2015/2366 in drugi predlogi zakonodajnih aktov, kot je Evropski zakonik o elektronskih komunikacijah, zahtevajo, da organizacije vzpostavijo ustrezne varnostne ukrepe za reševanje ustreznih tveganj na področju kibernetske varnosti.

energija, zdravstvo, bančništvo, infrastrukture finančnega trga, pitna voda ali digitalna infrastruktura[23].

Čeprav za noben proizvod, sistem ali storitev IKT ni mogoče zajamčiti „stoodstotne“ varnosti, obstaja več dobro znanih in dokumentiranih napak pri zasnovi proizvodov IKT, ki jih je mogoče izkoristiti za napade. Pristop „varnosti v zasnovi“, ki bi ga uporabljali proizvajalci povezanih naprav, bi zagotovil, da bi bilo vprašanje kibernetske varnosti rešeno, še preden bi se novi proizvodi dali na trg. To bi lahko spadalo pod načelo „skrbnega ravnanja“, ki bi ga oblikovali še naprej skupaj z industrijo in ki bi lahko zmanjšalo število ranljivih točk v proizvodih / programski opremi z uporabo vrste metod od zasnove do preskušanja in preverjanja, po potrebi tudi uradnega preverjanja, dolgoročnega vzdrževanja, uporabe procesov varnega razvojnega cikla, razvoja posodobitev in popravkov za odpravljanje dotlej še neodkritih ranljivih točk ter hitre posodobitve in popravila[24]. S tem bi se povečalo tudi zaupanje potrošnikov v digitalne proizvode.

Priznati je treba tudi pomembno vlogo, ki jo imajo pri odkrivanju šibkih točk v obstoječih proizvodih in storitvah raziskovalci varnosti pri tretjih osebah, in v vseh državah članicah bi morali ustvariti pogoje za omogočanje usklajenega razkrivanja šibkih točk[25], ki bi izhajali iz dobrih praks[26] in upoštevnih standardov[27].

Hkrati bi bilo treba **posamezne sektorje**, ki se soočajo s posebnimi vprašanji, spodbujati k oblikovanju lastnega pristopa. Tako bi splošne strategije kibernetske varnosti dopolnili s posebnimi strategijami kibernetske varnosti za posamezne sektorje, kot so finančne storitve[28], energetika, promet in zdravstvo[29].

Komisija je že poudarila posebna vprašanja v zvezi z **odškodninsko odgovornostjo**, ki izhajajo iz novih digitalnih tehnologij[30], trenutno poteka analiza posledic, naslednje stopnje pa bodo končane do junija 2018. Na področju kibernetske varnosti se zastavljajo vprašanja glede odgovornosti za škodo v podjetjih in dobavnih verigah. Če ta vprašanja ostanejo brez odgovora, bo oviran razvoj močnega enotnega trga proizvodov in storitev kibernetske varnosti.

Razvoj enotnega trga EU je naposled odvisen tudi od upoštevanja kibernetske varnosti v politiki trgovine in naložb. Učinek tujih nabav na kritične tehnologije, pri katerih je pomemben primer ravno kibernetska varnost, je ključen vidik v okviru **pregleda neposrednih tujih naložb v Evropski uniji**[31], katerega cilj je omogočiti pregled naložb iz tretjih držav na podlagi varnosti ter javnega reda in miru. V tem smislu je v gospodarstvih več tretjih držav

---

[23] Sektorji s področja uporabe Direktive 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji.

[24] Kibernetska varnost na evropskem enotnem digitalnem trgu (Cybersecurity in the European Digital Single Market), Skupina znanstvenih svetovalcev na visoki ravni, marec 2017

[25] Usklajeno razkrivanje ranljivih točk je oblika sodelovanja, ki raziskovalcem varnosti omogoča lažjo prijavo ranljivih točk lastniku ali prodajalcu informacijskega sistema, tako da lahko organizacija pravilno in pravočasno diagnosticira in popravi ranljivo točko, še preden se informacije o njej razkrijejo tretjim osebam ali javnosti.

[26] Na primer Vodnik po dobrih praksah za razkritje ranljivih točk. Od izzivov do priporočil (*Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*), ENISA, 2016.

[27] ISO/IEC 29147:2014 informacijska tehnologija – varnostne tehnike – razkritje ranljivih točk.

[28] Prihodnje delo Komisije o finančni tehnologiji bo zajemalo kibernetsko varnost za finančni sektor.

[29] Tako bi npr. v energetskem sektorju zelo stare informacijske tehnologije kombinirali z najnovejšimi, zlasti z zahtevami elektroenergetskega omrežja v realnem času.

[30] COM(2017) 228.

[31] COM(2017) 478.

zaradi zahtev glede kibernetske varnosti že prišlo do trgovinskih omejitev za blago in storitve iz EU v pomembnih sektorjih. Certifikacijski okvir EU za kibernetsko varnost bo še okrepil mednarodni položaj Evrope, dopolniti pa bi ga bilo treba s stalnimi prizadevanji za oblikovanje svetovnih standardov visoke varnosti in morebitnih sporazumov s tretjimi državami o vzajemnem priznavanju.

2.3 Izvajanje direktive o varnosti omrežij in informacijskih sistemov v polni meri

Glavna orodja za boj proti tveganjem na področju kibernetske varnosti so zdaj sicer v pristojnosti držav članic, toda EU se zaveda, da so potrebni višji standardi. Kibernetski incidenti velikega obsega le redko prizadenejo samo eno državo članico, saj so ključni sektorji, kot so bančništvo, energetika ali promet, vse bolj globalizirani, odvisni od digitalne tehnologije in medsebojno povezani.

Direktiva o varnosti omrežij in informacijskih sistemov je prvi zakonodajni akt o kibernetski varnosti na ravni celotne EU[32]. Zasnovana je za krepitev odpornosti z izboljšanjem nacionalnih zmogljivosti kibernetske varnosti; ustvarja pogoje za boljše sodelovanje med državami članicami in zahteva, da podjetja v pomembnih gospodarskih sektorjih sprejmejo učinkovite prakse obvladovanja tveganja in resne incidente prijavljajo nacionalnim organom. Te obveznosti veljajo tudi za tri vrste ponudnikov ključnih internetnih storitev: računalništva v oblaku, iskalnikov in spletnih tržnic. Njen cilj sta močnejši in bolj sistematičen pristop ter boljši pretok informacij.

Za kibernetsko odpornost EU je nujno potrebno, da začnejo vse države članice Direktivo v celoti izvajati do maja 2018. Proces podpira skupno delo držav članic, ki bo do jeseni 2017 omogočilo nastanek smernic za podporo bolj harmoniziranemu izvajanju, zlasti glede operaterjev bistvenih storitev. Komisija v tem svežnju o kibernetski varnosti izdaja tudi sporočilo[33], da bi prizadevanja držav članic podprla z navedbo dobrih praks iz držav članic, ki so pomembne za izvajanje Direktive, in z navodili za delovanje Direktive v praksi.

Direktivo bo treba dopolniti na področju pretoka informacij. Direktiva npr. pokriva samo ključne strateške sektorje, toda logično bi bil podoben pristop potreben pri vseh zainteresiranih straneh, ki so žrtev kibernetskih napadov, da bi lahko sistematično ocenjevale ranljive točke in vstopne točke za kibernetske napadalce. Poleg tega obstaja precej ovir za sodelovanje in izmenjavo informacij med javnim in zasebnim sektorjem. Vlade in javni organi neradi izmenjujejo informacije glede kibernetske varnosti, ker se bojijo, da bi tako ogrozili nacionalno varnost ali konkurenčnost. Zasebna podjetja nerada izmenjujejo informacije o svojih kibernetskih ranljivih točkah in izgubah, ki jih utrpijo zaradi njih, da ne bi ogrozila občutljivih poslovnih informacij, postavila na kocko svojega ugleda ali tvegala kršitev pravil o varstvu podatkov[34]. V javno-zasebnih partnerstvih je treba okrepiti zaupanje, da bi ustvarili podlago za širše sodelovanje in izmenjavo informacij med več sektorji. Centri za izmenjavo in analizo informacij imajo še posebej pomembno vlogo pri ustvarjanju zaupanja, potrebnega za izmenjavo informacij med zasebnim in javnim sektorjem. Prvi koraki v to smer so bili že narejeni za posebne kritične sektorje, kot je letalstvo, z ustanovitvijo

---

[32] Direktiva 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji.

[33] COM(2017) 476.

[34] Kibernetska varnost na evropskem enotnem digitalnem trgu (Cybersecurity in the European Digital Single Market), Skupina znanstvenih svetovalcev na visoki ravni, marec 2017. Posebno vprašanje zadeva poslovne skrivnosti, glede katerega je bilo v sporočilu z naslovom Krepitev odpornosti evropskega sistema kibernetske varnosti iz julija 2016 opozorjeno na zadržanost pri prijavljanju kibernetske tatvine poslovnih skrivnosti in pomembnost zaupanja vrednih kanalov poročanja, ki zagotavljajo zaupnost.

Evropskega centra za kibernetsko varnost v letalstvu[35] ter v energetiki z vzpostavitvijo centrov za izmenjavo in analizo informacij[36]. Komisija bo k temu pristopu prispevala v polni meri s podporo s strani agencije ENISA v pospešenem tempu, ki je potreben predvsem glede sektorjev, ki opravljajo bistvene storitve, določenih v direktivi o varnosti omrežij in informacijskih sistemov.

2.4 Odpornost prek hitrega odzivanja na krizne razmere

Ko pride do kibernetskega napada, je mogoče njegov učinek ublažiti s hitrim in učinkovitim odzivom. Tak odziv pokaže tudi, da javni organi pri kibernetski napadih niso nemočni, in prispeva k utrditvi zaupanja. Kar zadeva odziv institucij EU, bi bilo treba vidike kibernetske varnosti predvsem vključiti v obstoječe mehanizme EU za krizno upravljanje: integrirano politično odzivanje EU na krize, ki ga usklajuje predsedstvo Sveta[37], in splošni sistemi EU za zgodnje opozarjanje[38]. Potreba po odzivu na posebno hud kibernetski incident ali napad bi lahko bila zadosten razlog, da država članica uporabi solidarnostno klavzulo EU[39].

Hiter in učinkovit odziv je odvisen tudi od mehanizma za hitro izmenjavo informacij med vsemi ključnimi akterji na nacionalni ravni in ravni EU, za kar pa mora biti jasno, kakšne so njihove vloge in odgovornosti. Komisija se je posvetovala z institucijami in državami članicami o „načrtu“ za učinkovit proces operativnega odziva na kibernetski incident velikega obsega na ravni Unije in držav članic. V **načrtu**, predstavljenem v priporočilu[40], ki je del tega svežnja, je pojasnjeno, kako se kibernetska varnost vključuje v obstoječe mehanizme kriznega upravljanja na ravni EU, določeni pa so tudi cilji in načini sodelovanja med državami članicami ter med državami članicami in ustreznimi institucijami, službami, agencijami in organi EU[41] pri odzivu na kibernetske incidente in krize velikega obsega. Poleg tega se v priporočilu od držav članic in institucij EU zahteva, da za udejanjanje načrta vzpostavijo okvir EU za odzivanje na krize na področju kibernetske varnosti. Načrt se bo redno preizkušal na vajah kibernetskega in drugega kriznega upravljanja[42] ter po potrebi posodabljal.

Glede na to, da bi lahko kibernetski incidenti močno vplivali na delovanje gospodarstva in vsakodnevno življenje ljudi, bi lahko v naslednjem večletnem finančnem okviru preučili možnost vzpostavitve **sklada za nujno odzivanje na krize na področju kibernetske varnosti** po zgledu drugih tovrstnih kriznih mehanizmov na drugih področjih politike EU. Tako bi lahko države članice med hujšim incidentom ali po njem zaprosile za pomoč na ravni EU, če je zadevna država članica pred incidentom uvedla preudaren sistem kibernetske varnosti vključno z izvajanjem direktive o varnosti omrežij in informacijskih sistemov v polni meri, zrelim obvladovanjem tveganja in nadzornimi okviri na nacionalni ravni. Tak sklad, ki

---

35 https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa.

36 To so neprofitne organizacije, ki delujejo na pobudo članstva in ki so jih ustanovili zasebni in javni subjekti za izmenjavo informacij o kibernetskih grožnjah in tveganjih, njihovem preprečevanju in blažitvi ter odzivu nanje. Gl. npr. Evropski centri za izmenjavo in analizo in formacij (*European Energy Information Sharing and Analysis Centres*) (http://www.ee-isac.eu).

37 Na ta način je mogoče na najvišji politični ravni usklajevati odzive na hujše krize, ki prizadenejo več sektorjev.

38 Ti odzivi omogočajo notranjo izmenjavo informacij in usklajevanje glede nastajajočih večsektorskih kriz ali predvidljivih ali neposrednih groženj, pri katerih je potrebno ukrepanje na ravni EU.

39 V skladu s členom 222 Pogodbe o delovanju Evropske unije.

40 C(2017) 6100.

41 Vključno z Europolom, agencijo ENISA, skupino za odzivanje na računalniške grožnje za evropske institucije, organi in agencijami (CERT-EU) ter Obveščevalnim in situacijskim centrom EU (INTCEN).

42 Npr. vaje, ki jih izvaja agencija ENISA: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

bi dopolnjeval obstoječe mehanizme za krizno upravljanje na ravni EU, bi lahko uporabil zmogljivost za hitro odzivanje v interesu solidarnosti in posebne ukrepe za odziv na krizne razmere na področju financ, kot so nadomestitev prizadete opreme ali uporaba orodij za ublažitev ali odziv, pri čemer bi izkoristil izkušnje nacionalnih strokovnjakov v zvezi z mehanizmom Unije na področju civilne zaščite.

2.5 Strokovna mreža za kibernetsko varnost z evropskim raziskovalnim in strokovnim centrom za kibernetsko varnost

Tehnološka orodja kibernetske varnosti so strateška sredstva, a tudi ključne tehnologije za rast v prihodnosti. V strateškem interesu EU je zagotoviti, da bo EU obdržala in razvila bistvene zmogljivosti za zavarovanje svojega digitalnega gospodarstva, družbe in demokracije, zaščito kritične strojne in programske opreme ter zagotavljanje ključnih storitev kibernetske varnosti.

Pomemben prvi korak je bila vzpostavitev javno-zasebnega partnerstva za kibernetsko varnost[43] leta 2016, ki bo do leta 2020 sprožilo do 1,8 milijarde naložb. Toda obseg sedanjih naložb drugod po svetu[44] kaže, da bi morala EU narediti več na področju naložb in preseči razdrobljenost zmogljivosti, ki so razpršene po vsej EU.

EU lahko zagotovi dodano vrednost glede na zapletenost tehnologije kibernetske varnosti, velik obseg potrebnih naložb in nujnost rešitev, ki bi se obnesle povsod po EU. Izhajajoč iz dela, ki so ga opravile države članice in javno-zasebno partnerstvo, bi bil naslednji korak krepitev zmogljivosti EU za kibernetsko varnost prek **mreže strokovnih centrov za kibernetsko varnost**[45], v središču katere bi bil **Evropski raziskovalni in strokovni center za kibernetsko varnost**. Mreža in njen center bi spodbujala razvoj in uvajanje tehnologije na področju kibernetske varnosti in dopolnjevala prizadevanja za krepitev zmogljivosti na tem področju na ravni EU in nacionalni ravni. Komisija bo začela izvajati oceno učinka, da bi preučila razpoložljive možnosti, tudi možnost ustanovitve skupnega podjetja, da bi to strukturo vzpostavila leta 2018.

Da bi naredila prvi korak in pokazala pot za razmišljanje v prihodnje, bo Komisija predlagala začetek pilotne faze v okviru programa Obzorje 2020, v kateri bi pomagali povezati nacionalne centre v mrežo ter dali nov zagon razvoju kompetenc in tehnologije kibernetske varnosti. Zato namerava predlagati kratkoročno dodelitev financiranja v višini 50 milijonov EUR. Ta dejavnost bo dopolnila sedanje izvajanje javno-zasebnega partnerstva za kibernetsko varnost.

Osrednja naloga, ki se ji bo center posvetil najprej, bo združevanje in oblikovanje raziskovalnih dejavnosti. Da bi Center podprl razvoj industrijskih zmogljivosti, bi lahko prevzel vlogo projektnega vodje na področju zmogljivosti, ki bi lahko vodil večnacionalne projekte. To bi dalo dodaten zagon inovacijam in konkurenčnosti industrije EU na svetovni ravni v razvoju digitalnih tehnologij naslednje generacije, tudi z umetno inteligenco, kvantnim računalništvom, blokovno verigo in varnimi digitalnimi identitetami, ter v zagotavljanju dostopa do množičnih podatkov za podjetja s sedežem v EU, vse to pa je ključnega pomena za kibernetsko varnost v prihodnosti. Centru bi bilo v pomoč tudi prizadevanje EU za dvig infrastrukture visokozmogljivega računalništva na višjo raven: to je bistvenega pomena za

[43] C(2016) 4400 final.

[44] ZDA bodo v kibernetsko varnost samo v letu 2017 vložile 19 milijard dolarjev, kar je 35 % več kot v letu 2016. Bela hiša, urad tiskovnega predstavnika: 'Informativni pregled: Nacionalni akcijski načrt za kibernetsko varnost (Cybersecurity National Action Plan), 9. februar 2016.

[45] Mreža bi zajemala sedanje in prihodnje centre za kibernetsko varnost, ustanovljene v državah članicah, njihovo članstvo pa bi praviloma sestavljale javne raziskovalne organizacije in laboratoriji.

analizo velikih količin podatkov, hitro šifriranje in dešifriranje podatkov, preverjanje identitet, simulacijo kibernetskih napadov in analizo videogradiva[46].

Mreža strokovnih centrov bi lahko imela tudi zmogljivosti za podporo industriji s preskušanjem in simulacijami, ki bi bile podlaga za certificiranje kibernetske varnosti, opisane v oddelku 2.2. Ker bi sodelovala pri vseh dejavnostih EU na področju kibernetske varnosti, bi bilo mogoče njene cilje stalno posodabljati, kakor bi bilo potrebno. Center bi imel za cilj dvig standardov kibernetske varnosti, ne le pri tehnoloških sistemih in sistemih kibernetske varnosti, ampak tudi v razvoju znanj in spretnosti na najvišji ravni za strokovnjake, saj bi zagotavljal rešitve in vzorce za nacionalne dejavnosti na področju uvajanja digitalnih znanj in spretnosti. V tem pogledu bi tudi povečal zmogljivosti kibernetske varnosti na ravni EU in izhajal iz sinergij predvsem z agencijo ENISA, CERT-EU, Europolom, morebitnim prihodnjim skladom za nujno odzivanje na krize na področju kibernetske varnosti in nacionalnimi skupinami za odzivanje na incidente na področju računalniške varnosti.

Poseben poudarek v dejavnosti strokovne mreže mora biti na pomanjkanju evropske zmogljivosti za ocenjevanje **šifriranja** proizvodov in storitev, ki jih uporabljajo državljani, podjetja in vlade na enotnem digitalnem trgu. Močno šifriranje je podlaga za sisteme varne digitalne identifikacije, ki so ključnega pomena za učinkovito kibernetsko varnost[47]. Ohranja tudi varnost intelektualne lastnine ljudi in omogoča zaščito temeljnih pravic, kot sta svoboda izražanja in varstvo osebnih podatkov, ter zagotavlja varno spletno trgovanje[48].

Civilni in vojaški trg kibernetske varnosti EU se srečujeta s skupnimi izzivi[49] in tehnologijo z dvojno rabo, zaradi česar je potrebno tesno sodelovanje na kritičnih področjih, zato bi bilo mogoče drugo fazo mreže in njenega centra še razviti z obrambno razsežnostjo, pri čemer bi bile v polni meri upoštevane določbe Pogodbe o skupni varnostni in obrambni politiki. Obrambna razsežnost bi skupaj s tehnološkim jedrom lahko prispevala k sodelovanju držav članic na področju kibernetske obrambe, vključno s souporabo informacij, situacijskim zavedanjem, krepitvijo strokovnega znanja in usklajenih odzivov ter podporo razvoju skupnih zmogljivosti držav članic. Postala bi lahko tudi platforma, ki bi državam članicam pomagala pri ugotavljanju prednostnih nalog za kibernetsko obrambo EU in ki bi preučevala skupne rešitve, prispevala k razvoju skupnih strategij, omogočala skupno usposabljanje, vaje in preskuse na področju kibernetske obrambe na evropski ravni ter nudila podporo delu na področju taksonomij in standardov kibernetske obrambe, Center pa bi zagotavljal podporo in svetovanje. Da bi center lahko opravljal te dejavnosti, bi moral na področju kibernetske obrambe tesno in ob doslednem dopolnjevanju sodelovati z evropsko obrambno agencijo, na področju kibernetske odpornosti pa z agencijo ENISA. Ta obrambna razsežnost bi upoštevala tudi proces, ki se je začel z razmislekom o prihodnosti evropske obrambe.

Zaradi visoke stopnje odpornosti, ki je potrebna pri kibernetski obrambi, je za raziskovalne in tehnološke dejavnosti potrebna posebna usmeritev. Projekti ali tehnologije kibernetske obrambe, ki jih bodo razvila podjetja, bi lahko bili upravičeni do financiranja iz evropskega obrambnega sklada tako v fazi raziskav kot v fazi razvoja[50]. V tej zvezi bi lahko bila posebej

[46] COM(2012) 45 final in COM(2016) 178 final.

[47] Komisija bo že v okviru programa Obzorje 2020 razpisala nov natečaj za nagrado Obzorja v višini 4 milijone EUR za najboljšo inovativno rešitev za metode nemotene elektronske avtentikacije.

[48] Kibernetska varnost na evropskem enotnem digitalnem trgu (Cybersecurity in the European Digital Single Market), Skupina znanstvenih svetovalcev na visoki ravni, marec 2017.

[49] Študija o sinergijah med civilnim in vojaškim trgom kibernetske varnosti (*Study on synergies between the civilian and the defence cybersecurity markets*, Optimity; SMART 2014-0059).

[50] V evropskem programu za razvoj obrambne industrije bodo imeli že zdaj prednost projekti kibernetske obrambe, kibernetska obramba pa bo tudi ena od tem razpisa za zbiranje predlogov, ki bo objavljen leta 2018.

pomembna nekatera področja, kot so sistemi šifriranja na podlagi kvantnih tehnologij, kibernetsko situacijsko zavedanje, biometrični sistemi za nadzor dostopa, napredno odkrivanje stalnih groženj ali podatkovno rudarjenje. Visoki predstavnik, evropska obrambna agencija in Komisija bodo pomagali državam članicam pri ugotavljanju področij, na katerih bi bili skupni projekti kibernetske varnosti lahko upravičeni do financiranja iz evropskega obrambnega sklada.

2.6 Ustvarjanje močne podlage za kibernetska znanja in spretnosti v EU

Kibernetska varnost ima močno izobraževalno razsežnost. Učinkovita kibernetska varnost je v veliki meri odvisna od znanja in spretnosti ljudi, ki jih zadeva. Toda vrzel v znanjih in spretnostih na področju kibernetske varnosti pri strokovnjakih, ki delajo v zasebnem sektorju, naj bi do leta 2022 po napovedih znašala 350 000[51]. Vzgojo za kibernetsko varnost bi bilo treba oblikovati na vseh ravneh od rednega usposabljanja delovne sile na področju kibernetske varnosti prek dodatnega usposabljanja za kibernetsko varnost za vse strokovnjake za IKT do novih posebnih učnih načrtov za kibernetsko varnost. Ustanoviti bi bilo treba močne akademske strokovne centre, ki bi zadostili potrebam po pospešenem izobraževanju in usposabljanju in ki bi si lahko pomagali z navodili evropskega raziskovalnega in strokovnega centra za kibernetsko varnost in agencije ENISA. Cilj bi moral biti, da postane konstruiranje proizvodov in sistemov, v katerih so varnostna načela neločljiv sestavni del že od vsega začetka, nekaj samoumevnega. Izobraževanje za kibernetsko varnost ne bi smelo biti omejeno na strokovnjake za IKT, temveč bi moralo biti vključeno v učne načrte tudi na drugih področjih, kot so inženirstvo, poslovni menedžment ali pravo, pa tudi v posebnih sektorskih izobraževalnih usmeritvah. Tudi pri učiteljih, učencih in dijakih v osnovnošolskem in srednješolskem izobraževanju bi bilo treba ob pridobivanju digitalnih kompetenc v šolah razviti zavest o kibernetski kriminaliteti in kibernetski varnosti.

K temu bi morala skupaj z državami članicami prispevati tudi EU, in sicer tako, da bi izhajala iz dosežkov koalicije za digitalno pismenost in delovna mesta[52] ter uvedla npr. sheme vajeništva na področju kibernetske varnosti za mala in srednja podjetja.

2.7 Spodbujanje kibernetske higiene in ozaveščenosti

Glede na to, da naj bi 95 % incidentov omogočila „neka vrsta namerne ali nenamerne človeške napake“[53], gre tukaj v znatni meri za človeški dejavnik. Za kibernetsko varnost smo torej odgovorni vsi. To pomeni, da se mora vedenje oseb, združenj in javne uprave spremeniti tako, da se bomo vsi zavedali grožnje in da bodo na voljo potrebna orodja, znanja in spretnosti, s katerimi bo mogoče hitro odkriti napade in se dejavno zaščititi pred njimi. Kibernetska higiena mora ljudem priti v navado, podjetja in organizacije pa morajo uvesti primerne programe kibernetske varnosti, ki izhajajo iz tveganj, in jih redno posodabljati, da bodo ustrezala spreminjajočim se razmeram glede tveganj.

Direktiva o varnosti omrežij in informacijskih sistemov ne določa samo odgovornosti držav članic za izmenjavo informacij o kibernetskih napadih na ravni EU, ampak tudi vzpostavlja zrele nacionalne strategije in okvire kibernetske varnosti na področju varnosti omrežij in

[51] Študija o globalni delovni sili na področju varovanja tajnosti podatkov (*Global Information Security Workforce Study*), 2017. Primanjkljaj na svetovni ravni znaša 1,8 milijona.

[52] https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.

[53] IBM „Indeks inteligence za kibernetsko varnost“ (*The Cybersecurity Intelligence Index*) 2014, naveden v publikaciji Securitymagazine.com, 19. junija 2014.

informacijskih sistemov. Pri pospeševanju teh dejavnosti bi morale imeti vodilno vlogo javne uprave na ravni EU in nacionalni ravni.

Države članice bi morale omogočiti, da bi bila orodja kibernetske varnosti v največji možni meri na razpolago podjetjem in posameznikom. Predvsem bi bilo treba narediti več za preprečevanje in ublažitev učinkov kibernetske kriminalitete na končne uporabnike. Primer za to je sodelovanje Europola s kampanjo „Nič več izsiljevanja“ (*NoMoreRansom*)[54], ki je nastala v tesnem sodelovanju med organi odkrivanja in pregona ter podjetji za kibernetsko varnost, da bi uporabnikom pomagali preprečiti okužbe z izsiljevalskim programjem in dešifrirali podatke, če so bili žrtve napada. Take programe bi bilo treba uvesti za druge vrste zlonamerne programske opreme na drugih področjih, EU pa bi morala oblikovati **enotni portal, na katerem bi bila vsa taka orodja združena po načelu „vse na enem mestu“** in ki bi uporabnikom nudil nasvete za preprečevanje in odkrivanje zlonamerne programske opreme in povezave na mehanizme za prijavo.

Države članice bi morale tudi pospešiti **uporabo kibernetsko varnejših orodij pri razvoju e-uprave** in pri tem v celoti izkoristiti izkušnje strokovne mreže. Spodbujati bi bilo treba uvajanje varnih sredstev za identifikacijo, pri čemer bi izhajali iz okvira EU za elektronsko identifikacijo in storitve zaupanja za elektronske transakcije na notranjem trgu, ki je v veljavi od leta 2016 in zagotavlja predvidljivo regulativno okolje za omogočanje varnih in nemotenih elektronskih interakcij med podjetji, posamezniki in javnimi organi[55]. Poleg tega bi morale javne institucije, zlasti tiste, ki opravljajo bistvene storitve, zagotoviti, da so njihovi uslužbenci usposobljeni na področjih, povezanih s kibernetsko varnostjo.

Poleg tega bi države članice morale kibernetsko ozaveščenost obravnavati kot prednostno nalogo **v kampanjah ozaveščanja**, tudi v tistih, ki so namenjene šolam, univerzam, poslovni skupnosti in raziskovalnim organizacijam. Dejavnosti v okviru meseca kibernetske varnosti, ki poteka oktobra vsako leto, usklajuje pa ga agencija ENISA, se bodo stopnjevale, tako da bo njihov doseg širši, saj bodo pomenile skupno prizadevanje za komunikacijo na ravni EU in nacionalni ravni. Nič manj pomembno ni ozaveščanje glede spletnih **dezinformacijskih kampanj in lažnih novic** v družbenih medijih, ki so posebej namenjene spodkopavanju demokratičnih procesov in evropskih vrednot. Glavna odgovornost je sicer še vedno na nacionalni ravni, tudi za volitve v Evropski parlament, vendar sta se združevanje in skupna uporaba strokovnega znanja na evropski ravni izkazala za dodano vrednost, s katero je ukrepanje bolj osredotočeno[56].

Pomembno vlogo ima tudi **industrija** na splošno, še posebej pa ponudniki in proizvajalci digitalnih storitev. Uporabnike (posameznike, podjetja in javne uprave) mora podpirati z orodji, ki jim omogočajo prevzemanje odgovornosti za njihova dejanja na spletu, in jasno povedati, da je vzdrževanje kibernetske higiene nepogrešljiva sestavina ponudbe potrošnikom[57]. Da bi lahko odkrivala in odpravljala ranljive točke, bi si morala industrija

---

54 https://www.nomoreransom.org/.

55 Uredba (EU) št. 910/2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu (uredba eIDAS), sprejeta 23. julija 2014. Evropska komisija prek programa instrumenta za povezovanje Evrope zagotavlja tudi gradnike in orodja za interoperabilnost elektronske identifikacije in elektronskega podpisa (npr. brskalniki za zanesljive sezname).

56 Primer za to je projektna skupina East StratCom Task Force, ki so jo leta 2015 ustanovile države članice in visoki predstavnik za boj proti stalnim dezinformacijskim kampanjam Rusije. Skupina se ukvarja z razvojem komunikacijskih produktov in kampanj, namenjenih predvsem pojasnjevanju politik EU v regiji vzhodnega partnerstva.

57 Nekateri proizvajalci so tega koncepta že vajeni, saj del evropske zakonodaje o proizvodih (kot je Direktiva 2006/42/ES o strojih) določa načela „varnosti v zasnovi“.

prizadevati za vzpostavitev notranjih procesov za iskanje, razvrščanje in reševanje ranljivih točk ne glede na to, ali je morebitni izvor ranljivosti zunaj ali znotraj zadevnega podjetja.

Ključni ukrepi:

- izvajanje direktive o varnosti omrežij in informacijskih sistemov v polni meri;
- hitro sprejetje uredbe o določitvi novega pooblastila za agencijo ENISA in evropskem certifikacijskem okviru[58] s strani Evropskega parlamenta in Sveta;
- skupna pobuda Komisije/industrije za opredelitev načela „dolžnosti skrbnega ravnanja“, da bi se zmanjšalo število ranljivih točk in spodbujala „varnost v zasnovi“;
- hitra izvedba načrta čezmejnega odzivanja na hujše incidente;
- začetek ocene učinka za preučitev možnosti, da bi Komisija leta 2018 predlagala ustanovitev mreže strokovnih centrov za kibernetsko varnost in evropskega raziskovalnega in strokovnega centra za kibernetsko varnost, ki bi sledila takojšnji pilotni fazi;
- podpora državam članicam pri ugotovitvi področij, na katerih bi prišli v poštev skupni projekti na področju kibernetske varnosti za podporo evropskega obrambnega sklada;
- točka „vse na enem mestu“ za vso EU, ki bi nudila pomoč žrtvam kibernetskih napadov, dajala informacije o najnovejših grožnjah ter združevala praktične nasvete in orodja za kibernetsko varnost;
- ukrepanje držav članic za vključitev kibernetske varnosti v programe znanj in spretnosti, e-upravo in kampanje ozaveščanja;
- ukrepanje industrije za okrepitev usposabljanja v zvezi s kibernetsko varnostjo za svoje osebje in za uvedbo pristopa „varnost v zasnovi“ za svoje proizvode, storitve in procese.

3. DOSEGANJE UČINKOVITEGA KIBERNETSKEGA ODVRAČANJA V EU

Učinkovito odvračanje pomeni vzpostavitev okvira ukrepov, ki so verodostojni in odvračilni za morebitne kibernetske kriminalce in napadalce. Dokler se storilcem kibernetskih napadov, tako državnim kot nedržavnim, ni treba bati ničesar drugega kot tega, da jim ne bi uspelo, imajo kaj malo spodbude, da bi nehali poskušati. Osrednjega pomena za dosego učinkovitega odvračanja je učinkovitejši odziv organov odkrivanja in pregona s poudarkom na odkrivanju, sledljivosti in pregonu kibernetskih kriminalcev. Poleg tega mora EU podpirati države članice pri razvoju zmogljivosti kibernetske varnosti z dvojno rabo. Preobratu pri kibernetskih napadih se bomo približali šele, ko bomo povečali verjetnost, da bodo storilci ujeti in kaznovani. Kibernetske napade bi bilo treba nemudoma preiskati, storilce pa privesti pred sodišče oziroma sprejeti ukrepe za ustrezen politični ali diplomatski odziv. Visoki predstavnik bi lahko v primeru hujše krize pomembnih mednarodnih in obrambnih razsežnosti Svetu predstavil možnosti za ustrezen odziv.

Korak v smeri boljšega kazenskopravnega odziva na kibernetske napade je bil narejen že s sprejetjem direktive o napadih na informacijske sisteme leta 2013[59]. Z njo so bila vzpostavljena minimalna pravila za opredelitev kaznivih dejanj in sankcij na področju napada na informacijske sisteme in določeni operativni ukrepi za boljše sodelovanje med organi. Z Direktivo je v vseh državah članicah prišlo do primerljivega znatnega napredka pri kriminalizaciji kibernetskih napadov, kar olajšuje čezmejno sodelovanje med organi odkrivanja in pregona, ki preiskujejo te vrste kaznivih dejanj. Vendar so še vedno možnosti za

[58] COM(2017) 477.

[59] Direktiva 2013/40/EU Evropskega parlamenta in Sveta z dne 12. avgusta 2013 o napadih na informacijske sisteme.

to, da države članice s popolnim izvajanjem vseh določb Direktive v celoti izkoristijo njen potencial[60]. Komisija bo še naprej podpirala države članice pri izvajanju Direktive in zaenkrat meni, da predlogi sprememb niso potrebni.

3.1 Odkrivanje zlonamernih akterjev

Če naj bi imeli več možnosti, da storilce privedemo pred sodišče, moramo nujno izboljšati svojo zmogljivost odkrivanja odgovornih za kibernetske napade. Velik izziv za organe odkrivanja in pregona je, kako najti podatke, zlasti v obliki digitalnih sledi, ki bi koristili pri preiskavah kibernetske kriminalitete. Zato moramo okrepiti svojo tehnološko zmogljivost za učinkovito preiskavo, tudi tako, da bomo Europolovo enoto za kibernetsko kriminaliteto okrepili s kibernetskimi strokovnjaki. Europol je postal ključni akter za pomoč državam članicam pri preiskavah, ki potekajo na območjih, ki spadajo v več jurisdikcij. Postati bi moral središče strokovnega znanja o spletnih preiskavah in kibernetični forenziki za organe odkrivanja in pregona držav članic.

Zaradi močno razširjene prakse postavljanja več – včasih več tisoč – uporabnikov na en naslov IP je preiskovanje zlonamernega spletnega ravnanja tehnično zelo zahtevno. Zaradi njega je treba včasih, npr. pri hudih zločinih, kot je spolna zloraba otrok, preiskati veliko uporabnikov, da bi odkrili enega zlonamernega akterja. EU bo zato spodbujala uvedbo novega protokola (IPv6), saj je z njim mogoče dodeliti po enega uporabnika na naslov IP, kar bi bilo zelo koristno pri odkrivanju in pregonu ter preiskavah na področju kibernetske varnosti. Komisija bo prvi korak pri spodbujanju uvedbe naredila s tem, da bo vključila zahtevo za premik v smeri protokola IPv6 v svoje politike, vključno z zahtevami glede javnega naročanja, financiranja projektov in raziskav ter s podporo potrebnemu gradivu za usposabljanje. Poleg tega bi morale države članice razmisliti o prostovoljnih sporazumih s ponudniki internetnih storitev o pospešeni uvedbi protokola IPv6.

Belgija je na prvem mestu na svetu[61] po stopnji uvedbe protokola IPv6, tudi po zaslugi javno-zasebnega partnerstva: pomembne zainteresirane strani so razmislile o omejitvi uporabe enega naslova IP na največ 16 uporabnikov v okviru prostovoljnega samoregulativnega ukrepa, kar je pomenilo spodbudo za prehod na protokol IPv6[62].

Nasploh bi bilo treba še naprej spodbujati spletno odgovornost. To pomeni spodbujanje ukrepov za preprečevanje zlorabe domenskih imen za razširjanje nenaročenih sporočil ali napade z ribarjenjem. Komisija si bo v ta namen v skladu z dejavnostmi Organizacije za dodeljevanje spletnih imen in številk prizadevala izboljšati delovanje sistemov WHOIS za domenska imena in naslove IP[63] ter razpoložljivost in točnost informacij v njih [64].

3.2 Stopnjevanje odziva organov odkrivanja in pregona

[60] COM(2017) 474.

[61] https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption.

[62] http://bipt.be/public/files/nl/22027/Raadpleging_ipv6.pdf.

[63] Protokol poizvedbe in odziva, ki se pogosto uporablja za poizvedbe v podatkovnih zbirkah, v katerih so shranjeni registrirani uporabniki internetnega vira ali tisti, ki jim je bil tak vir dodeljen.

[64] Organizacija za dodeljevanje spletnih imen in številk (ICANN) je neprofitna organizacija, odgovorna za usklajevanje vzdrževanja in postopkov več podatkovnih zbirk, povezanih z imenskimi prostori na internetu.

Za odvračanje kibernetskih napadov sta ključnega pomena učinkovito **preiskovanje** in **pregon** kriminalitete, ki jo omogoča kibernetski prostor. Toda današnji postopkovni okvir je treba bolje prilagoditi internetni dobi[65]. Kibernetski napadi so lahko tako hitri, da jim naši postopki ne morejo slediti, in zaradi njih lahko nastanejo posebne potrebe po hitrem čezmejnem sodelovanju. Kot je bilo napovedano že v evropski agendi za varnost, bo Komisija v začetku leta 2018 podala predloge za **lažji čezmejni dostop do elektronskih dokazov**. Komisija hkrati s tem izvaja praktične ukrepe za boljši čezmejni dostop do elektronskih dokazov za kazenske preiskave, vključno s financiranjem usposabljanja za čezmejno sodelovanje, razvojem elektronske platforme za izmenjavo informacij znotraj EU in standardizacijo oblik pravosodnega sodelovanja med državami članicami.

Učinkovit pregon ovirajo tudi razlike v forenzičnih postopkih za zbiranje elektronskih dokazov v preiskavah kibernetske kriminalitete po državah članicah. To bi lahko izboljšali s prizadevanjem za vzpostavitev skupnih forenzičnih standardov. Poleg tega bi bilo treba okrepiti forenzične zmogljivosti za podporo sledljivosti in pripisovanju. Korak v to smer bi bil nadaljnji razvoj forenzične zmogljivosti v Europolu, tako da bi obstoječe proračunske in človeške vire na Europolovem Evropskem centru za boj proti kibernetski kriminaliteti prilagodili rastočim potrebam po operativni podpori v čezmejnih preiskavah kibernetske kriminalitete. Drugi korak bi bil, da bi ob upoštevanju tehnološkega poudarka na šifriranju, predstavljenega zgoraj, preučili, kako zaradi njegove zlorabe s strani zločincev nastajajo veliki izzivi v boju proti hudim kaznivim dejanjem, vključno s terorizmom in kibernetsko kriminaliteto. Komisija bo rezultate sedanjih razmislekov o **vlogi šifriranja v kazenskih preiskavah**[66] objavila do oktobra 2017[67].

Internet ne pozna meja, zato je okvir za mednarodno sodelovanje, vzpostavljen v **Konvenciji Sveta Evrope o kibernetski kriminaliteti, sprejeti v Budimpešti**[68], priložnost, da raznolika skupina držav uporabi najboljši možni pravni standard za različne nacionalne zakonodaje na področju preprečevanja kibernetske kriminalitete. Trenutno se preučuje možnost, da bi Konvenciji dodali protokol[69], kar bi lahko bila priložnost za rešitev vprašanja čezmejnega dostopa do elektronskih dokazov v mednarodnem okviru. Komisija poziva vse države, da namesto priprave novih mednarodnih instrumentov za vprašanja kibernetske kriminalitete oblikujejo primerno nacionalno zakonodajo in nadaljujejo s sodelovanjem v tem obstoječem mednarodnem okviru.

Zaradi vseprisotnih orodij za anonimizacijo se zločinci še lažje skrijejo. „**Temno omrežje**“[70] je zločincem odprlo nove poti za dostop do posnetkov spolnih zlorab otrok, mamil ali

---

[65] Če navedemo le en primer, (navidezni) centralni strežnik za nadzor in vodenje botneta *Avalanche* je spreminjal fizične strežnike in domenska imena vsakih pet minut.

[66] Predsedstvo Sveta, „Zaključki zasedanja Sveta za pravosodje in notranje zadeve z dne 8–9 decembra 2016“, št. 15391/16.

[67] Osmo poročilo o napredku pri vzpostavljanju učinkovite in prave varnostne unije z dne 29. junija 2017, COM(2017) 354 final.

[68] Konvencija je prva mednarodna pogodba o hudodelstvih, zagrešenih prek interneta in drugih računalniških omrežij, ukvarja pa se predvsem s kršitvami avtorskih pravic, računalniškimi prevarami, otroško pornografijo in kršitvami varnosti omrežij. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. Leta 2017 je 55 vlad ratificiralo Konvencijo Sveta Evrope o kibernetski kriminaliteti ali pristopilo k njej.

[69] Pristojnosti za pripravo osnutka 2. dodatnega protokola h Konvenciji o kibernetski kriminaliteti, T-CY (2017)3.

[70] Temno omrežje je sestavljeno iz vsebine v prekrivnih omrežjih, ki uporabljajo internet, vendar je zanje potrebna posebna programska oprema, konfiguracija in avtorizacija za dostop. Temno omrežje je majhen del globokega spleta, tj. dela svetovnega spleta, ki ga brskalniki ne indeksirajo.

strelnega orožja, pri čemer je pogosto zelo malo verjetno, da bi jih zasačili[71]. Zdaj je to ključni vir orodij za kibernetsko kriminaliteto, kot so zlonamerna programska oprema in orodja za vdore v računalniški sistem. Komisija bo skupaj z ustreznimi zainteresiranimi stranmi analizirala nacionalne pristope, da bi našla nove rešitve. Europol bi moral omogočati in podpirati preiskave v temnem omrežju, ocenjevati grožnje, pomagati pri določitvi jurisdikcije in dajati prednost zadevam visokega tveganja, EU pa lahko ima vodilno vlogo pri usklajevanju mednarodnih ukrepov[72].

Eno izmed področij rastoče kibernetske kriminalitete je zloraba podatkov o kreditnih karticah ali drugih elektronskih plačilnih sredstvih. S podatki o plačilih, ki so bili pridobljeni s kibernetskimi napadi na spletne prodajalce na drobno ali druga zakonita podjetja, se nato trguje na spletu in jih zločinci lahko uporabijo za prevare[73]. Komisija predstavlja predlog za boljše odvračanje z **direktivo o boju proti spletnim prevaram in ponarejanju negotovinskih plačilnih sredstev**[74]. Njen cilj je posodobiti obstoječa pravila na tem področju ter okrepiti sposobnost organov odkrivanja in pregona za boj proti tej obliki kriminala.

Izboljšati je treba tudi zmogljivosti organov odkrivanja in pregona držav članic za preiskovanje kibernetske kriminalitete, kot tudi razumevanje kriminalitete, ki jo omogoča kibernetski prostor, in možnosti za preiskavo, ki jih imajo tožilci in pravosodje. Eurojust in Europol prispevata k temu cilju in razširjenemu usklajevanju, pri čemer tesno sodelujeta s specializiranimi svetovalnimi skupinami v Europolovem Centru za kibernetsko kriminaliteto, mrežami vodij enot za kibernetsko kriminaliteto in tožilcev, specializiranih za kibernetsko kriminaliteto. Komisija bo za bolj proti kibernetski kriminaliteti namenila 10,5 milijonov EUR, predvsem v okviru svojega **Sklada za notranjo varnost – programa za policijo**. Usposabljanje je pomemben element in Evropska skupina za usposabljanje in izobraževanje na področju kibernetske kriminalitete je pripravila več koristnih gradiv. Ta gradiva bi bilo treba zdaj s pomočjo Agencije Evropske unije za usposabljanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj razširiti med strokovnjaki organov odkrivanja in pregona.

3.3 Javno-zasebno partnerstvo proti kibernetski kriminaliteti

V digitalnem svetu, ki je sestavljen predvsem iz infrastrukture v zasebni lasti in številnih različnih akterjev v različnih jurisdikcijah, tradicionalni mehanizmi odkrivanja in pregona niso vedno učinkoviti. Zato se lahko javni organi učinkovito borijo proti kriminalu samo v sodelovanju z zasebnim sektorjem, tudi industrijo in civilno družbo. V tej zvezi je ključnega pomena tudi finančni sektor, zato je potrebnega več sodelovanja. Okrepiti je treba npr. vlogo finančnoobveščevalnih enot[75] v zvezi s kibernetsko kriminaliteto.

Nekatere države članice so že sprejele ključne ukrepe. Na Nizozemskem finančne institucije sodelujejo z organi odkrivanja in pregona v projektni skupini za elektronsko kriminaliteto, ki

[71] Omembe vredna izjema je nedavna odstranitev dveh od največjih kriminalnih trgov v temnem spletu, in sicer *AlphaBay* in *Hansa*. https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

[72] Europol že ima pomembno vlogo na tem področju. Za nedavni primer gl. https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

[73] Izkupički od prevar so pomemben vir dohodka za organizirani kriminal, zato omogočajo druge kriminalne dejavnosti, kot so terorizem, nedovoljen promet s prepovedanimi drogami in trgovina z ljudmi.

[74] COM(2017) 489.

[75] Finančnoobveščevalne enote so nacionalni centri za sprejem in analizo poročil o sumljivih transakcijah in drugih informacij, pomembnih za pranje denarja, povezana predhodna kazniva dejanja in financiranje terorizma, ter za razširjanje informacij o rezultatih te analize.

se ukvarja s preprečevanjem spletnih prevar in kibernetske kriminalitete. Nemški strokovni center proti kibernetski kriminaliteti deluje kot operativno vozlišče, prek katerega si njegovi člani izmenjujejo informacije v tesnem sodelovanju z uradom nemške zvezne policije in oblikujejo ukrepe za zaščito pred kibernetsko kriminaliteto. V 16 državah članicah[76] so bili ustanovljeni centri odličnosti za kibernetsko kriminaliteto, ki omogočajo lažje sodelovanje med organi odkrivanja in pregona, akademskimi ustanovami in zasebnimi partnerji pri oblikovanju in izmenjavi dobrih praks, usposabljanju in krepitvi zmogljivosti.
Komisija podpira ustanovitev javno-zasebnih partnerstev in mehanizmov sodelovanja prek posebnih projektov, kot je mreža kibernetskih centrov in strokovnjakov za preprečevanje spletnih prevar[77], ki uporablja model izmenjave informacij in standardov za analizo in ublažitev tveganj elektronske kriminalitete in spletnih prevar.

V zvezi s kibernetsko kriminaliteto bi moralo biti zasebnim podjetjem omogočeno, da si z organi odkrivanja in pregona izmenjujejo informacije o konkretnih incidentih, tudi osebne podatke, ob polnem spoštovanju pravil o zaščiti podatkov. V reformi varstva podatkov EU, ki se bo začela uporabljati maja 2018, je določen skupen sklop pravil o pogojih, v katerih lahko sodelujejo organi odkrivanja in pregona ter zasebni subjekti. Evropska komisija si bo v sodelovanju z Evropskim odborom za varstvo podatkov in ustreznimi zainteresiranimi stranmi prizadevala ugotoviti dobre prakse na tem področju in po potrebi dala navodila.

3.4 Močnejši politični odziv

V nedavno sprejetem **okviru za skupni odziv EU na zlonamerne kibernetske dejavnosti**[78] („zbirka orodij za kibernetsko diplomacijo“) so določeni ukrepi skupne zunanje in varnostne politike, vključno z omejevalnimi ukrepi, s katerimi je mogoče doseči močnejši odziv EU na dejavnosti, ki škodujejo njenim političnim, varnostnim in gospodarskim interesom. Okvir je pomemben korak v smeri razvoja zmogljivosti opozarjanja in odziva na ravni EU in na ravni držav članic. Z njim bomo bolje usposobljeni za pripisovanje zlonamernih kibernetskih dejavnosti, kar bo vplivalo na vedenje morebitnih napadalcev, hkrati pa bo upoštevana tudi potreba po zagotavljanju ustreznih odzivov. Pripisovanje državnemu ali nedržavnemu akterju je še vedno suverena politična odločitev, ki temelji na podatkih iz vseh obveščevalnih virov. Trenutno potekajo dejavnosti v zvezi z izvajanjem okvira skupaj z državami članicami, nadaljevale pa bi se tudi ob doslednem usklajevanju z načrtom, da bi se lahko odzvali na kibernetske incidente velikega obsega[79]. Situacijsko zavedanje, potrebno za uporabo ukrepov znotraj okvira, bi bilo treba združiti, analizirati in uporabljati skupaj z INTCEN[80] v tesnem sodelovanju z državami članicami in institucijami EU.

3.5 Krepitev odvračanja v kibernetski varnosti prek obrambne zmogljivosti držav članic

Države članice že razvijajo zmogljivosti kibernetske obrambe. Poleg tega lahko EU glede na izginjanje ločnic med kibernetsko obrambo in kibernetsko varnostjo, glede na pretežno dvojno rabo kibernetskih orodij in tehnologij, pa tudi glede na precejšnjo raznolikost

[76] Avstrija, Belgija, Bolgarija, Ciper, Češka, Estonija, Francija, Grčija, Irska, Litva, Nemčija, Poljska, Romunija, Slovenija, Španija in Združeno kraljestvo.
[77] Pobuda EU-OF2CEN, katere cilj je omogočiti sistematično izmenjavo informacij v zvezi s spletnimi prevarami med bankami in organi odkrivanja in pregona po vsej EU za preprečevanje izplačil prevarantom in denarnim mulam ter preiskovanje in pregon storilcev. Sofinancira jo EU (Sklad za notranjo varnost – program za policijo).
[78] http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.
[79] C(2017) 6100.
[80] JOIN(2016) 018 final.

pristopov držav članic veliko pripomore k sinergijam med dejavnostmi na vojaškem in civilnem področju[81].

Države članice, ki razpolagajo z naprednejšimi zmogljivostmi za kibernetsko varnost in so jih pripravljene združiti, bi lahko ob podpori visokega predstavnika, Komisije in evropske obrambne agencije razmislile o tem, da bi kibernetsko obrambo vključile v okvir „stalnega strukturnega sodelovanja“. Podlaga za to bi bilo lahko navedeno prizadevanje za spodbujanje industrijskih zmogljivosti EU in strateške avtonomije. EU lahko spodbuja tudi interoperabilnost, tudi z omogočanjem razvoja zmogljivosti, usklajevanja usposabljanja in izobraževanja ter dejavnosti na področju standardizacije dvojne rabe.

V polni meri bi bilo treba izkoristiti tudi skupni okvir za odzivanje na hibridne grožnje, ki pogosto vključujejo kibernetske napade, zlasti prek hibridne fuzijske celice EU in nedavno ustanovljenega Evropskega centra za preprečevanje hibridnih groženj v Helsinkih, katerega naloga je spodbujanje strateškega dialoga ter izvajanje raziskav in analiz.

EU bo ponovno postavila v ospredje okvir politike EU za kibernetsko obrambo[82] iz leta 2014 kot orodje za nadaljnjo vključitev kibernetske varnosti v skupno varnostno in obrambno politiko. Bistvena je tudi kibernetska odpornost misij in operacij skupne varnostne in obrambne politike: oblikovani bodo standardizirani postopki in tehnične zmogljivosti, s katerimi bi bilo mogoče podpirati civilne in vojaške misije in operacije, pa tudi njihove vsakokratne strukture zmogljivosti za načrtovanje in izvajanje operacij ter izvajalce storitev informacijske tehnologije Evropske službe za zunanje delovanje. Evropska obrambna agencija in Evropska služba za zunanje delovanje bosta za boljše sodelovanje med državami članicami in uspešnejše usmerjanje dejavnosti EU na tem področju v sodelovanju s službami Komisije omogočali lažje sodelovanje na strateški ravni med oblikovalci politik kibernetske obrambe v državah članicah. EU bo v okviru svojih prizadevanj za tehnološko in industrijsko bazo evropske obrambe podpirala tudi razvoj evropskih rešitev na področju kibernetske varnosti. Sem spada tudi spodbujanje regionalnih grozdov odličnosti na področju kibernetske varnosti in obrambe.

Službe Komisije bodo v tesnem sodelovanju z Evropsko službo za zunanje delovanje, državami članicami in drugimi zadevnimi organi EU do leta 2018 vzpostavile **platformo za usposabljanje in izobraževanje za kibernetsko varnost**, s katero bi reševali sedanjo vrzel v znanju in spretnostih na področju kibernetske obrambe. To bo dopolnilo delo evropske obrambne agencije na tem področju ter pripomoglo k reševanju vrzeli v znanju in spretnostih na področju kibernetske varnosti in kibernetske obrambe.

Ključni ukrepi:

- pobuda Komisije za čezmejni dostop do elektronskih dokazov (v začetku leta 2018);
- hitro sprejetje direktive o boju proti spletnim prevaram in ponarejanju negotovinskih plačilnih sredstev s strani Evropskega parlamenta in Sveta;
- uvedba zahtev glede protokola IPv6 pri financiranju javnih naročil, raziskav in projektov EU; prostovoljni dogovori med državami članicami in ponudniki internetnih storitev o pospešenem uvajanju protokola IPv6;
- ponovno/okrepljeno osredotočenje Europola na kibernetsko forenziko in spremljanje temnega omrežja;

[81] EU razume kibernetski prostor kot področje za operacije, podobno kot kopno, zrak in morje. Dejavnosti za kibernetsko obrambo zajemajo tudi zaščito in odpornost sredstev v vesolju in kopenskih infrastruktur, ki so povezane z njimi.

[82] www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515.

- sprejetje okvira za skupni diplomatski odziv EU na zlonamerne kibernetske dejavnosti;
- okrepljena finančna podpora nacionalnim in nadnacionalnim projektom za izboljšanje kazenskega pravosodja v kibernetskem prostoru;
- vzpostavitev izobraževalne platforme za kibernetsko varnost za reševanje sedanje vrzeli v znanju in spretnostih na področju kibernetske obrambe v letu 2018.

4. KREPITEV MEDNARODNEGA SODELOVANJA NA PODROČJU KIBERNETSKE VARNOSTI

Mednarodno politiko EU na področju kibernetske varnosti vodijo temeljne vrednote in temeljne pravice, kot so svoboda izražanja, pravica do zasebnosti in varstvo osebnih podatkov, ter spodbujanje odprtega, svobodnega in varnega kibernetskega prostora, zasnovana pa je za reševanje nenehno spreminjajočega se izziva spodbujanja kibernetske stabilnosti v svetovnem merilu ob hkratnem prispevanju k strateški avtonomiji Evrope v kibernetskem prostoru.

4.1 Kibernetska varnost v zunanjih odnosih

Kot kažejo dokazi, ljudje povsod po svetu menijo, da so kibernetski napadi iz drugih držav ena največjih groženj za nacionalno varnost[83]. Ker je grožnja globalna, je ustvarjanje in vzdrževanje trdnih zavezništev in partnerstev s tretjimi državami bistvenega pomena za preprečevanje in odvračanje kibernetskih napadov, ki so vse bolj pomembni za mednarodno stabilnost in varnost. EU bo v dvostranskih in regionalnih stikih, stikih z več zainteresiranimi stranmi in večstranskih stikih dajala prednost vzpostavitvi strateškega okvira za preprečevanje konfliktov in stabilnost v kibernetskem prostoru.

EU odločno zastopa stališče, da se v kibernetskem prostoru uporablja mednarodno pravo, še zlasti pa Ustanovna listina Združenih narodov. Kot dopolnilo zavezujočemu mednarodnemu pravu se EU zavzema za prostovoljne nezavezujoče norme, pravila in načela odgovornega ravnanja države, ki jih je oblikovala skupina vladnih strokovnjakov OZN[84]. Spodbuja tudi razvoj in izvajanje regionalnih ukrepov za krepitev zaupanja, tako v Organizaciji za varnost in sodelovanje v Evropi kot tudi v drugih regijah.

Na dvostranski ravni se bodo še razvili dialogi o kibernetskih vprašanjih[85], dopolnjevala pa jih bodo prizadevanja za lažje sodelovanje s tretjimi državami pri krepitvi načel potrebne skrbnosti in državne odgovornosti v kibernetskem prostoru. EU bo v mednarodnih stikih dajala prednost mednarodnim varnostnim vprašanjem v kibernetskem prostoru, a tudi pazila, da kibernetska varnost ne postane pretveza za tržno zaščito in omejevanje temeljnih pravic, vključno s svobodo izražanja in dostopa do informacij. Za celosten pristop h kibernetski varnosti je potrebno spoštovanje človekovih pravic in EU bo svoje temeljne vrednote še naprej spoštovala na svetovni ravni, izhajajoč iz Smernic EU o človekovih pravicah na spletu[86]. EU v tem pogledu poudarja pomen sodelovanja vseh zainteresiranih strani v upravljanju interneta.

Komisija je podala tudi predlog[87] za posodobitev izvoznih kontrol EU, vključno s kontrolami izvoza kritičnih tehnologij za kibernetski nadzor, ki bi lahko povzročile kršitev človekovih

[83] Pomlad 2017, Svetovna anketa o stališčih (*Global Attitudes Survey*), Pew Research Centre.
[84] A/68/98 in A/70/174.
[85] EU je imela septembra 2017 dialoge o kibernetskih vprašanjih z ZDA, Kitajsko, Japonsko, Republiko Korejo in Indijo.
[86] Smernice EU o človekovih pravicah glede svobode izražanja na spletu in drugje.
[87] COM(2016) 616.

pravic ali bi jih bilo mogoče zlorabiti proti varnosti EU, in bo okrepila dialoge s tretjimi državami za spodbujanje svetovnega zbliževanja in odgovornega ravnanja na tem področju.

4.2 Krepitev zmogljivosti kibernetske varnosti

Svetovna kibernetska stabilnost je odvisna od lokalne in nacionalne sposobnosti vseh držav za preprečevanje kibernetskih incidentov in odziv nanje ter preiskovanje in pregon primerov kibernetske kriminalitete. S podporo prizadevanjem za krepitev nacionalne odpornosti v tretjih državah se bo dvignila svetovna raven kibernetske varnosti, kar bo imelo za EU pozitivne posledice. Če se želimo zoperstaviti kibernetskim grožnjam, ki se hitro spreminjajo, si je treba prizadevati za napredek pri usposabljanju, v politiki in zakonodaji, potrebne pa so tudi učinkovito delujoče skupine za odzivanje na računalniške grožnje in kibernetsko kriminaliteto v vseh državah po svetu.

EU ima od leta 2013 vodilno vlogo pri mednarodni krepitvi zmogljivosti kibernetske varnosti in na te dejavnosti sistematično veže svoje razvojno sodelovanje. Še naprej bo spodbujala model krepitve zmogljivosti, ki bo izhajal iz pravic, v skladu s pristopom Digital4Development[88]. Prednostne naloge pri krepitvi zmogljivosti bodo v soseščini EU in državah v razvoju, v katerih povezljivost hitro narašča in se grožnje hitro razvijajo. Prizadevanja EU bodo dopolnjevala razvojno agendo EU ob upoštevanju agende za trajnostni razvoj do leta 2030 in splošnih prizadevanj za krepitev institucionalne zmogljivosti.

Da bi lahko EU bolje izkoristila svoje kolektivne izkušnje za podporo krepitvi zmogljivosti, bi bilo treba vzpostaviti posebno mrežo EU za krepitev kibernetske zmogljivosti, ki bi povezovala Evropsko službo za zunanje delovanje, organe držav članic za kibernetske zadeve, agencije EU, službe Komisije, akademske ustanove in civilno družbo. Oblikovane bodo smernice EU za krepitev kibernetske zmogljivosti, ki bodo pripomogle k boljšim političnim smernicam in dajanju prednosti dejavnostim EU za pomoč tretjim državam.

EU bo sodelovala tudi z drugimi donatorji na tem področju, da bi preprečila podvajanje dejavnosti in omogočila bolj ciljno usmerjeno krepitev zmogljivosti v različnih regijah.

4.3 Sodelovanje med EU in zvezo NATO

EU bo, izhajajoč iz precejšnjega napredka, ki je bil že dosežen, poglobila sodelovanje EU in zveze NATO na področju kibernetske varnosti, hibridnih groženj in obrambe, kot je predvideno v skupni izjavi z dne 8. julija 2016[89]. Med prednostnimi nalogami je ustvarjanje podlage za interoperabilnost z doslednimi zahtevami in standardi za kibernetsko obrambo, krepitvijo sodelovanja pri usposabljanju in vajah ter usklajevanjem zahtev za usposabljanje.

EU in zveza NATO bosta spodbujali tudi sodelovanje pri raziskavah in inovacijah na področju kibernetske obrambe in nadgradili sedanji tehnični dogovor o izmenjavi informacij v zvezi s kibernetsko varnostjo med svojima organoma za kibernetsko varnost[90]. Nedavne skupne dejavnosti pri boju proti hibridnim grožnjam, predvsem sodelovanje med hibridno fuzijsko celico EU in celico zveze NATO za hibridno analizo, bi bilo treba še nadgraditi, da bi okrepili odpornost in odgovor na kibernetske krize. Nadaljnje sodelovanje med EU in zvezo NATO bodo spodbujale vaje kibernetske obrambe, na katerih bodo sodelovali Evropska služba za zunanje delovanje in drugi subjekti ter ustrezni organi zveze NATO, vključno s centrom odličnosti za kibernetsko obrambo zveze NATO v Talinu. Zveza NATO in EU bosta

[88] SWD(2017) 157.
[89] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/.
[90] CERT-EU in zmogljivost zveze NATO za odzivanje na računalniške incidente (NCIRC).

prvič izvedli vzporedne, usklajene vaje odziva na hibridni scenarij, ki jih bo leta 2017 vodila zveza NATO, leta 2018 pa bo enako vlogo prevzela EU. Naslednje poročilo o sodelovanju med EU in zvezo NATO, ki bo Svetu EU in Svetu zveze NATO predloženo decembra 2017, bo priložnost za preučitev možnosti za nadaljnjo širitev sodelovanja, zlasti z zagotovitvijo skupnih, varnih in čvrstih komunikacijskih sredstev med vsemi udeleženimi institucijami in organi, tudi agencijo ENISA.

Ključni ukrepi:

- izpopolnitev strateškega okvira za preprečevanje konfliktov in stabilnost v kibernetskem prostoru;
- oblikovanje nove mreže za krepitev zmogljivosti za podporo sposobnostim tretjih držav za boj proti kibernetskim grožnjam ter smernic EU za krepitev kibernetske zmogljivosti s ciljem boljšega prednostnega razvrščanja dejavnosti EU;
- nadaljevanje sodelovanja med EU in zvezo NATO, vključno s sodelovanjem na vzporednih in usklajenih vajah ter večjo interoperabilnostjo standardov kibernetske varnosti.

5. SKLEPNA UGOTOVITEV

Kibernetska pripravljenost EU je ključnega pomena za enotni digitalni trg ter našo varnostno in obrambno unijo. Nujno je treba okrepiti evropsko kibernetsko varnost in odpravljati grožnje civilnim in vojaškim ciljem.

Prihodnji digitalni vrh, ki ga bo 29. septembra 2017 organiziralo estonsko predsedstvo, bo priložnost, da pokažemo, da smo skupaj trdno odločeni dati kibernetski varnosti osrednjo vlogo v EU kot digitalni družbi. Komisija v okviru te skupne zaveze poziva države članice, da izjavijo, kako nameravajo ukrepati na področjih, na katerih imajo glavno odgovornost. Tukaj bi morala biti zajeta krepitev kibernetske varnosti z:

- zagotovitvijo učinkovitega izvajanja direktive o varnosti omrežij in informacijskih sistemov z dne 9. maja 2018 v polni meri ter virov, ki jih javni organi, odgovorni za kibernetsko varnost, potrebujejo za uspešno opravljanje svojih nalog;
- uporabo enakih pravil tudi za javne uprave glede na njihovo vlogo v družbi in gospodarstvu kot celoti;
- zagotavljanje usposabljanja na področju kibernetske varnosti za javno upravo;
- dajanjem prednosti kibernetski ozaveščenosti v informacijskih kampanjah in vključitev kibernetske varnosti v akademske in poklicne učne načrte;
- podporo razvoju projektov kibernetske obrambe s pomočjo pobud za stalno strukturno sodelovanje in evropskega obrambnega sklada.

V tem skupnem sporočilu je predstavljeno, kolikšen je izziv in kakšen je obseg ukrepov, ki jih lahko sprejme EU. Potrebujemo odporno Evropo, ki lahko svoje ljudi učinkovito zaščiti tako, da predvidi možne kibernetske incidente, da v svoje strukture in ravnanje vgradi trdno zaščito, da si po kibernetskih napadih hitro opomore in odvrne tiste, ki so odgovorni za napade. V tem sporočilu so predlagani ciljno usmerjeni ukrepi, ki bodo še okrepili strukture in zmogljivosti EU za kibernetsko varnost, in sicer usklajeno, ob polnem sodelovanju držav članic in različnih zadevnih struktur EU ter ob spoštovanju njihovih pristojnosti in odgovornosti. Njegovo izvajanje bo jasno pokazalo, da so EU in države članice pripravljene sodelovati pri vzpostavitvi standarda kibernetske varnosti, ki bo kos rastočim izzivom, s katerimi se sooča Evropa.