EUROPSKA
KOMISIJA

VISOKI PREDSTAVNIK
UNIJE ZA VANJSKE
POSLOVE I
SIGURNOSNU POLITIKU

Bruxelles, 13.9.2017.
JOIN(2017) 450 final

ZAJEDNIČKA KOMUNIKACIJA EUROPSKOM PARLAMENTU I VIJEĆU

Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a

1. UVOD

Kibersigurnost je ključan čimbenik našeg blagostanja i sigurnosti. Naš svakodnevni život i naša gospodarstva sve više ovise o digitalnim tehnologijama te smo stoga sve izloženiji. Kiberincidenti se razlikuju po tome tko je odgovaran za njih i što se njima želi postići. Zlonamjerne kiberaktivnosti ne ugrožavaju samo naša gospodarstva i napredak u uspostavi jedinstvenog digitalnog tržišta, već i samo funkcioniranje naših demokracija, naše slobode i naše vrijednosti. Naša sigurnost u budućnosti ovisi o preobrazbi naše sposobnosti za zaštitu EU-a od kiberprijetnji: i civilna i vojna infrastruktura ovise o sigurnim digitalnim sustavima. To je potvrđeno na sastanku Europskog vijeća u lipnju 2017.[1] te u Globalnoj strategiji Europske unije za vanjsku i sigurnosnu politiku[2].

Rizici se eksponencijalno povećavaju. Istraživanja pokazuju da se od 2013. do 2017. gospodarski učinak kiberkriminaliteta peterostruko povećao, a do 2019. mogao bi se i učetverostručiti[3]. Posebno se povećala uporaba ucjenjivačkih softvera (*ransomware*)[4] te nedavni napadi[5] upućuju na drastično povećanje aktivnosti kiberkriminaliteta. Međutim, ucjenjivački softveri nisu ni izdaleka jedina prijetnja.

Kiberprijetnje se povezuju i s državnim i s nedržavnim akterima. Često su kriminalne prirode, odnosno motivira ih dobit, ali mogu biti i političke i strateške prirode. Opasnost od kriminala povećava se jer je teško razgraničiti kiberkriminalitet i „tradicionalni" kriminal s obzirom na to da se zločinci internetom koriste za unaprjeđenje svojih aktivnosti, ali i kao sredstvom za pronalaženje novih načina i alata za počinjenje kaznenih djela[6]. U velikoj većini slučajeva mala je vjerojatnost da će počinitelj biti pronađen, a još manja da će biti kazneno progonjen.

Istovremeno državni akteri sve više ostvaruju svoje geopolitičke ciljeve uporabom tradicionalnih alata, primjerice vojne sile, ali i s pomoću manje transparentnih kiberalata, među ostalim i uplitanjem u nacionalne demokratske postupke. Uporaba kiberprostora za ratovanje, kao jedinog područja ili kao dijela hibridne taktike, sada je općenito poznata. Kampanje dezinformiranja, lažne vijesti i kiberoperacije usmjerene na ključnu infrastrukturu sve su učestalije i zahtijevaju odgovor. Zbog toga je Komisija u svojem Dokumentu za razmatranje o budućnosti europske obrane[7] istaknula važnost suradnje u području kiberobrane.

Ako znatno ne povećamo razinu svoje kibersigurnosti, rizik će se povećavati paralelno s digitalnom preobrazbom. Očekuje se da će se do 2020. deseci milijardi uređaja „interneta stvari" povezati na internet, ali kibersigurnost još nema prioritet u njihovu dizajnu[8]. Ako ne uspijemo zaštititi uređaje kojima će se kontrolirati elektroenergetske mreže, automobili i prometne mreže, tvornice, financije, bolnice i domovi, posljedice bi mogle biti katastrofalne i

---

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

2 http://europa.eu/globalstrategy/

3 Vidjeti na primjer, McAfee i Centar za strateške i međunarodne studije „Neto gubici: procjena troškova kiberkriminaliteta na svjetskoj razini" (*Net losses: Estimating the Global Cost of Cybercrime*), 2014.

4 Ucjenjivački softver vrsta je zlonamjernog programa kojim se korisnicima onemogućuje ili ograničava pristup vlastitom sustavu zaključavanjem zaslona ili korisničkih datoteka dok ne plate otkupninu.

5 U svibnju 2017. ucjenjivačkim softverom WannaCry napadnuto je više od 400 000 računala u više od 150 zemalja. Mjesec dana kasnije žrtva ucjenjivačkog softvera „Petya" bila je Ukrajina i više poduzeća diljem svijeta.

6 Procjena prijetnje od teškog i organiziranog kriminala u EU-u (*Serious and Organised Crime Threat Assessment*), Europol, 2017.

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

8 „IDC and TXT Solutions" (2014), SMART 2013/0037, „Kombinacija usluga u oblaku i interneta stvari" (*Cloud and IoT combination*), studija za Europsku komisiju.

znatno narušiti povjerenje potrošača u nove tehnologije. Rizik se dodatno povećava zbog opasnosti od politički motiviranih napada na civilne mete i nedostataka u vojnoj kiberobrani.

Zahvaljujući pristupu utvrđenom u ovoj Zajedničkoj komunikaciji EU će se moći bolje suočiti s tim prijetnjama. Njime bi se EU-u mogla osigurati veća otpornost, strateška neovisnost i sposobnost u pogledu tehnologije i vještina te bi se moglo pridonijeti izgradnji snažnog jedinstvenog tržišta. Za to su potrebne odgovarajuće strukture s pomoću kojih ćemo osigurati visoku razinu kibersigurnosti i omogućiti potrebne reakcije uz potpuno sudjelovanje svih ključnih aktera. Tim bi se pristupom pridonijelo i uspješnijem odvraćanju od kibernapada jer bi se pojačali napori usmjereni na otkrivanje, praćenje i kažnjavanje počinitelja napada. Njime bi se priznala i globalna dimenzija razvojem međunarodne suradnje kao platforme za vodeću ulogu EU-a u području kibersigurnosti. Ti se koraci temelje na pristupima jedinstvenog digitalnog tržišta, globalne strategije, Europskog programa sigurnosti[9], Zajedničkog okvira za suzbijanje hibridnih prijetnji[10] i Komunikacije o pokretanju Europskog fonda za obranu[11],[12].

EU se već bavi mnogim od tih pitanja i sada sve te različite smjerove rada treba objediniti. EU je 2013. donio Strategiju za kibernetičku sigurnost EU-a, kojom je pokrenut niz ključnih aktivnosti za poboljšanje kiberotpornosti[13]. Njezini glavni ciljevi i načela koji uključuju poticanje pouzdanog, sigurnog i otvorenog kiberekosustava i dalje su aktualni. Međutim, budući da se prijetnje stalno razvijaju i produbljuju, potrebno je uložiti veće napore kako bismo se u budućnosti oduprli napadima i kako bismo ih suzbili[14].

Uzimajući u obzir opseg politika EU-a te alate, strukture i sposobnosti koje ima na raspolaganju, EU može riješiti problem kibersigurnosti. Iako su države članice i dalje odgovorne za nacionalnu sigurnost, zbog opsega i prekogranične prirode prijetnje opravdano je djelovanje EU-a kojim će se državama članicama osigurati poticaji i potpora za razvoj i održavanje većeg broja boljih nacionalnih kapaciteta u području kibersigurnosti, uz istodobno jačanje kapaciteta na razini EU-a. Tim se pristupom sve dionike – EU, države članice, industriju i građane – želi potaknuti da osiguraju prioritetni tretman kibersigurnosti, što je neophodno za jačanje otpornosti i bolji odgovor EU-a na kiberprijetnje. Njime će se osigurati konkretni koraci za otkrivanje i istragu svih oblika kiberincidenata na štetu EU-a i njegovih država članica i za prikladan odgovor na te incidente, uključujući kaznenim progonom zločinaca. Takvim pristupom EU-u će se omogućiti da u okviru svojeg vanjskog djelovanja aktivno promiče kibersigurnost na globalnoj razini. EU će tako s reaktivnog prijeći na proaktivni pristup, u okviru kojeg će odgovarati na postojeće i buduće prijetnje i tako zaštititi europsko blagostanje, društvo i vrijednosti te temeljna prava i slobode.

2. JAČANJE OTPORNOSTI EU-A NA KIBERNAPADE

Za snažnu kiberotpornost potreban je zajednički i sveobuhvatan pristup. To podrazumijeva čvršće i učinkovitije strukture za promicanje kibersigurnosti i odgovaranje na kibernapade u državama članicama, ali i u institucijama, agencijama i tijelima EU-a. Potreban je i sveobuhvatniji međusektorski pristup usmjeren na jačanje kiberotpornosti i strateške

[9] COM(2015) 185 final.
[10] JOIN(2016) 18 final.
[11] COM (2017) 295.
[12] Pristup se temelji i na neovisnim znanstvenim savjetima Skupine znanstvenih savjetnika na visokoj razini mehanizma Europske komisije za znanstveno savjetovanje (vidi upućivanja u nastavku).
[13] JOIN(2013) 1 final. Procjena te strategije dostupna je u dokumentu SWD (2017) 295.
[14] Ako nije navedeno drugačije, prijedlozi iz ove Komunikaciji nemaju utjecaj na proračun. Svaka inicijativa koja utječe na proračun slijedit će godišnji proračunski postupak i ne može dovesti u pitanje sljedeći višegodišnji financijski okvir za razdoblje nakon 2020.

neovisnosti, kao i snažno jedinstveno tržište, znatno poboljšanje tehničkih sposobnosti EU-a i znatno veći broj stručnjaka. U središtu tog pristupa mora biti široko prihvaćanje ideje da je kibersigurnost zajednički društveni izazov te da bi trebalo uključiti različite razine uprave, gospodarstva i društva.

2.1. Jačanje Agencije Europske unije za mrežnu i informacijsku sigurnost

Agencija Europske unije za mrežu i informacijsku sigurnost (ENISA) ima ključnu ulogu u jačanju kiberotpornosti i odgovora EU-a na kibernapade, ali ograničava je njezin postojeći mandat. Komisija stoga predstavlja ambiciozan prijedlog reforme koji uključuje **trajni mandat agencije**[15]. Time će se osigurati da ENISA može podupirati države članice, institucije EU-a i poduzeća u ključnim područjima, među ostalim i u provedbi Direktive o sigurnosti mrežnih i informacijskih sustava[16] („Direktiva NIS") i predloženog okvira za kibersigurnosnu certifikaciju.

Reformirana ENISA imat će snažnu savjetodavnu ulogu u području razvoja i provedbe politika, uključujući promicanje usklađenosti između sektorskih inicijativa i Direktive NIS i pomoć pri uspostavi centara za razmjenu i analizu informacija u ključnim sektorima. ENISA će postrožiti standarde i poboljšati pripravnost Europe organiziranjem paneuropskih vježbi u području kibersigurnosti u okviru kojih će se kombinirati odgovori na različitim razinama. Agencija će podupirati i razvoj politike EU-a za kibersigurnosnu certifikaciju u području informacijske i komunikacijske tehnologije (IKT) i imat će važnu ulogu u poboljšanju operativne suradnje i upravljanja krizama u cijelom EU-u. Agencija će biti i središnja točka za pružanje informacija i znanja u kibersigurnosnoj zajednici.

Brzo i zajedničko razumijevanje prijetnji i incidenata preduvjet je za donošenje odluke o tome jesu li potrebne zajedničke mjere za njihovo ublažavanje ili djelovanje uz potporu EU-a. U takvoj razmjeni informacija moraju sudjelovati svi relevantni akteri – tijela i agencije EU-a te države članice – na tehničkoj, operativnoj i strateškoj razini. U suradnji s nadležnim tijelima na razini država članica i EU-a, posebno s timovima za odgovor na računalne sigurnosne incidente[17], CERT-EU-om, Europolom i Centrom EU-a za analizu obavještajnih podataka (INTCEN), ENISA će pridonijeti i informiranosti o stanju na razini EU-a. Te se informacije mogu uzeti u obzir pri prikupljanju obavještajnih podataka o prijetnjama i izradi politika u kontekstu redovnog praćenja prijetnji i učinkovite operativne suradnje te u okviru odgovora na prekogranične incidente velikih razmjera.

2.2. Ususret jedinstvenom tržištu u području kibersigurnosti

Rast kibersigurnosnog tržišta u EU-u – u pogledu proizvoda, usluga i postupaka – ograničava se na više načina. Ključni aspekt je nepostojanje programa kibersigurnosne certifikacije priznatih u cijelom EU-u kojima je cilj ugraditi u proizvode više standarde otpornosti i povećati povjerenje u tržište u cijelom EU-u. Komisija stoga podnosi prijedlog za uspostavu **okvira EU-a za kibersigurnosnu certifikaciju**[18]. Time bi se propisao postupak za uspostavu

[15] COM (2017) 477.
[16] Direktiva 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije.
[17] Kako je opisano u članku 9. Direktive NIS.
[18] COM (2017) 477.

programa kibersigurnosne certifikacije na razini EU-a za proizvode, usluge i/ili sustave, kojima bi se razina jamstva prilagođavala predviđenoj uporabi (to mogu biti ključne infrastrukture ili uređaji za široku potrošnju)[19]. Od njega bi korist imala poduzeća jer u slučaju prekograničnog poslovanja ne bi morala prolaziti nekoliko postupaka certifikacije, čime bi se ograničili administrativni i financijski troškovi. Provedbom programa razvijenih na temelju tog Okvira pridonijelo bi se i jačanju povjerenja potrošača jer bi se potvrdom o sukladnosti informiralo kupce i korisnike o sigurnosnim obilježjima proizvoda i usluga koje kupuju i upotrebljavaju i jamčila njihova sigurnost. Na taj bi način visoke norme kibersigurnosti postale izvor konkurentne prednosti. Rezultat bi bio veća otpornost proizvoda i usluga IKT-a koji bi se formalno ocjenjivali na temelju definiranih normi kibersigurnosti, a koje bi se mogle razvijati u kombinaciji sa sveobuhvatnijim tekućim aktivnostima u području norma IKT-a[20].

Programi unutar okvira bili bi dobrovoljni i njima se ne bi uvele neposredne regulatorne obveze za prodavače ili pružatelje usluga. Sustavi ne bi bili u suprotnosti s primjenjivim pravnim zahtjevima, na primjer sa zakonodavstvom EU-a o zaštiti podataka.

Nakon uspostave Okvira Komisija će pozvati relevantne dionike da se usmjere na tri prioritetna područja:

- sigurnost u ključnim ili visokorizičnim primjenama[21]: sustavi o kojima ovisimo u svakodnevnom životu sve su više digitalizirani i međusobno povezani, od automobila i strojeva u tvornicama do najvećih sustava, primjerice zrakoplova ili elektrana, ili onih najmanjih, primjerice medicinskih proizvoda. Stoga bi bile potrebne stroge procjene sigurnosti ključnih komponenti IKT-a u takvim proizvodima i sustavima;

- kibersigurnost u digitalnim proizvodima, mrežama, sustavima i uslugama široke uporabe koji se upotrebljavaju u privatnom i javnom sektoru u cilju obrane protiv napada i primjene regulatornih obveza[22], na primjer, šifriranje e-pošte, vatrozidovi i virtualne privatne mreže. Od ključne je važnosti da se širenjem takvih alata ne stvore novi izvori rizika ili nove ranjivosti;

- uporaba metoda „integrirane sigurnosti" u cjenovno pristupačnim, digitalnim, međusobno povezanim uređajima za široku potrošnju koji čine internet stvari: programi obuhvaćeni tim okvirom mogli bi biti znak da su proizvodi proizvedeni primjenom najnaprednijih sigurnih razvojnih metoda, da su podvrgnuti prikladnom ispitivanju sigurnosti i da su se trgovci obvezali ažurirati svoj softver u slučaju novootkrivenih ranjivosti ili prijetnji.

U okviru tih prioriteta posebno treba uzeti u obzir stalni razvoj kiberprijetnji i važnost osnovnih usluga, kao što su prijevoz, energija, zdravstvena skrb, bankarstvo, infrastruktura financijskog tržišta, pitka voda ili digitalna infrastruktura[23].

---

[19] Razina jamstva označava stupanj strogoće procjene sigurnosti i obično je razmjerna razini rizika povezanog s područjima primjene ili funkcijama (tj. viša razina jamstva potrebna je za proizvode ili usluge IKT-a koji se upotrebljavaju u visoko rizičnim područjima primjene ili funkcijama).

[20] COM (2016) 176.

[21] Iznimka su slučajevi kada su obvezna ili dobrovoljna certifikacija uređene drugim aktima Unije.

[22] Na primjer, Direktivom (EU) 2016/1148, Uredbom (EU) 2016/679, Direktivom (EU) 2015/2366 i drugim zakonodavnim prijedlozima kao što je Europski zakonik o elektroničkim komunikacijama propisano je da organizacije moraju uspostaviti prikladne mjere sigurnosti za uklanjanje relevantnih rizika povezanih s kibersigurnošću.

[23] Sektori obuhvaćeni područjem primjene Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije.

Iako se ni za jedan proizvod, sustav ili uslugu IKT-a ne može jamčiti da je „100 % siguran”, postoji nekoliko poznatih i dokumentiranih nedostataka u dizajnu proizvoda IKT-a koji se mogu iskoristiti za napad. Pristupom „integrirane sigurnosti” koji su prihvatili proizvođači povezanih uređaja, softvera i opreme osiguralo bi se rješavanje pitanja kibersigurnosti prije stavljanja novih proizvoda na tržište. To bi moglo biti dio načela „dužne pažnje” koje će se dalje razvijati zajedno s industrijom, a kojim bi se mogla smanjiti ranjivost proizvoda/softvera primjenom različitih metoda od dizajna do ispitivanja i provjere, uključujući, prema potrebi, formalnu provjeru, dugoročno održavanje i primjenu postupaka sigurnog razvojnog ciklusa te razvoj ažuriranja i zakrpa za uklanjanje prethodno neotkrivenih ranjivosti te za brzo ažuriranje i popravak[24]. Time bi se povećalo i povjerenje potrošača u digitalne proizvode.

Nadalje, trebalo bi priznati važnu ulogu koju istraživači trećih strana koji se bave pitanjima sigurnosti imaju u otkrivanju ranjivosti postojećih proizvoda i usluga te bi u svim državama članicama trebalo stvoriti uvjete za koordinirano otkrivanje ranjivosti[25] na temelju najbolje prakse[26] i relevantnih normi[27].

Istodobno bi **različite sektore**, koji se suočavaju s različitim problemima, trebalo potaknuti da razviju vlastiti pristup. Na taj način opće strategije kibersigurnosti dopunile bi se sektorskim strategijama kibersigurnosti u područjima kao što su financijske usluge[28], energetika, promet i zdravstvo[29].

Komisija je već istaknula posebna pitanja **odgovornosti**[30] povezana s novim digitalnim tehnologijama i u tijeku su aktivnosti analize implikacija. Sljedeći koraci bit će provedeni do lipnja 2018. Kibersigurnost otvara pitanja povezana s pripisivanjem odgovornosti za štetu u poduzećima i opskrbnim lancima. Ako se ta pitanja ne riješe, ugrozit će se razvoj snažnog jedinstvenog tržišta kibersigurnosnih proizvoda i usluga.

Naposljetku, razvoj jedinstvenog tržišta EU-a ovisi i o uključivanju kibersigurnosti u trgovinsku politiku i politiku ulaganja. Učinak inozemnih stjecanja ključnih tehnologija, među kojima je važan primjer upravo kibersigurnost, ključni je aspekt okvira za **praćenje stranih izravnih ulaganja u Europsku uniju**[31], čiji je cilj omogućiti praćenje ulaganja iz trećih zemalja iz razloga sigurnosti i javnog reda. Isto tako, zbog kibersigurnosnih zahtjeva više trećih zemalja već je uvelo prepreke trgovini robom i uslugama iz EU-a u važnim sektorima. Okvirom EU-a za kibersigurnosnu certifikaciju dodatno će se ojačati međunarodni položaj Europe i trebalo bi ga dopuniti trajnim naporima usmjerenima na razvoj globalnih normi za visoku razinu sigurnosti i sporazumima o uzajamnom priznavanju.

---

[24] Kibersigurnost na europskom jedinstvenom digitalnom tržištu, Skupina znanstvenih savjetnika na visokoj razini, ožujak 2017.

[25] Koordinirano otkrivanje ranjivosti vrsta je suradnje kojom se istraživačima u području sigurnosti olakšava i omogućuje prijavljivanje ranjivosti vlasniku ili prodavaču informacijskog sustava, čime se organizaciji omogućuje da pravilno i pravovremeno dijagnosticira i ukloni ranjivost prije otkrivanja detaljnih informacija o ranjivosti trećim osobama ili javnosti.

[26] Na primjer, Vodič o dobroj praksi u pogledu otkrivanja ranjivosti. Od izazova do preporuka (*Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*), ENISA, 2016.

[27] ISO/IEC 29147:2014 Informacijska tehnologija -- Sigurnosne tehnike -- Otkrivanje ranjivosti.

[28] Komisijinim budućim aktivnostima u području financijske tehnologije obuhvatit će se kibersigurnost financijskog sektora.

[29] Na primjer, u sektoru energetike kombiniranjem vrlo starih informacijskih tehnologija s najnovijima, posebno sa zahtjevima elektroenergetske mreže u stvarnom vremenu.

[30] COM (2017) 228.

[31] COM (2017) 478.

2.3. Potpuna provedba Direktive o sigurnosti mrežnih i informacijskih sustava

Glavni alati za suzbijanje rizika u području kibersigurnosti u nadležnosti su država članica, no EU je prepoznao potrebu za strožim normama. Kiberincidenti velikih razmjera rijetko utječu samo na jednu državu članicu zbog sve globaliziranije, digitalno ovisne i međusobno povezane prirode ključnih sektora, primjerice bankarstva, energetike ili prometa.

Direktiva o sigurnosti mrežnih i informacijskih sustava („Direktiva NIS") prvi je zakonodavni akt u području kibersigurnosti koji se primjenjuje u cijelom EU-u[32]. Cilj joj je povećati otpornost poboljšanjem nacionalnih sposobnosti za kibersigurnosti poticanjem bolje suradnje među državama članicama i zahtjevima da poduzeća u važnim gospodarskim sektorima uvedu učinkovite prakse upravljanja rizikom i ozbiljne incidente prijavljuju nacionalnim tijelima. Te se obveze primjenjuju i na tri vrste pružatelja ključnih internetskih usluga: računalstvo u oblaku, tražilice i internetska tržišta. Cilj joj je snažniji i sustavniji pristup i bolji protok informacija.

Potpuna provedba Direktive u svim državama članicama do svibnja 2018. od ključne je važnosti za kiberotpornost EU-a. Države članice podupiru taj postupak zajedničkim naporima te će se do jeseni 2017. donijeti smjernice za potporu usklađenijoj provedbi, posebno u pogledu operatora ključnih usluga. U okviru paketa za kibersigurnost Komisija donosi i Komunikaciju[33] kako bi poduprla napore država članica pružanjem nabolje prakse iz država članica koja je relevantna za provedbu Direktive te smjernice za primjenu Direktive u praksi.

Direktivu će trebati dopuniti u području protoka informacija. Na primjer, Direktivom su obuhvaćeni samo ključni strateški sektori, ali logično je da bi za sustavnu procjenu ranjivosti i ulaznih točaka za počinitelje kibernapada bio potreban sličan pristup svih dionika koji su žrtve kibernapada. Nadalje, postoji niz prepreka suradnji i razmjeni informacija između javnog i privatnog sektora. Vlade i javna tijela nevoljko razmjenjuju informacije važne za kibersigurnost iz straha da će time ugroziti nacionalnu sigurnost ili konkurentnost. Privatna poduzeća nevoljko razmjenjuju informacije o svojim ranjivostima na kibernapade i povezanim gubicima iz straha da će time ugroziti osjetljive poslovne informacije ili ugled ili prekršiti pravila o zaštiti podataka[34]. Treba povećati povjerenje kako bi javno-privatna partnerstva mogla osigurati temelje za širu suradnju i razmjenu informacija među većem broju sektora. Uloga centara za razmjenu informacija i analizu od posebne je važnosti za stvaranje nužnog povjerenja za razmjenu informacija između privatnog i javnog sektora. Prvi koraci poduzeti su u pogledu posebnih ključnih sektora, primjerice, u zrakoplovnom sektoru uspostavljen je Europski centar za kibersigurnost u zrakoplovstvu[35], dok su u energetskom sektoru razvijeni centri za razmjenu informacija i analizu[36]. Komisija će tom pristupu pridonijeti u punoj mjeri uz potporu agencije ENISA, pri čemu će trebati brže djelovanje u pogledu sektora koji pružaju ključne usluge kako su utvrđene u Direktivi NIS.

---

[32] Direktiva 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije.

[33] COM (2017) 476.

[34] Kibersigurnost na europskom jedinstvenom digitalnom tržištu, Skupina znanstvenih savjetnika na visokoj razini, ožujak 2017. Posebno pitanje odnosi se na poslovne tajne u pogledu kojih je u Komunikaciji iz srpnja 2016. „Jačanje europskog sustava kibernetičke sigurnosti" istaknuta suzdržanost u pogledu prijavljivanja kiberkrađe poslovnih tajni i važnost pouzdanih načina prijave kojima se osigurava povjerljivost.

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

[36] To su neprofitne, članske organizacije koje su osnovali privatni i javni subjekti radi razmjene informacija o kiberprijetnjama, rizicima, sprječavanju, ublažavanju i odgovoru. Vidi, na primjer, Europske centre za razmjenu i analizu informacija u području energetike (http://www.ee-isac.eu).

2.4. Otpornost koja se temelji na brzom odgovoru na hitne situacije

Učinak kibernapada može se ublažiti brzim i učinkovitim odgovorom. Takvim odgovorom može se i pokazati da javna tijela nisu bespomoćna kada se suočavaju s kibernapadima te se može pridonijeti izgradnji povjerenja. Kada je riječ o odgovoru institucija EU-a, u prvoj fazi kiberaspekte bi trebalo uključiti u postojeće mehanizme EU-a za upravljanje krizama: integrirani politički odgovor EU-a na krize, koji bi koordiniralo predsjedništvo Vijeća[37] i EU-ovi opći sustavi brzog uzbunjivanja[38]. Potreba za odgovorom na posebno ozbiljan kiberincident ili napad trebala bi biti dostatna osnova da se država članica pozove na klauzulu solidarnosti EU-a[39].

Brz i učinkovit odgovor ovisi i o mehanizmu brze razmjene informacija među svim ključnim dionicima na nacionalnoj razini i razini EU-a te je u tom pogledu potrebno pojasniti njihove uloge i odgovornosti. Komisija se s institucijama i državama članicama savjetovala o „planu" za osiguranje učinkovitog postupka za operativni odgovor na kiberincidente velikih razmjera na razini Unije i država članica. U **Planu** predstavljenom u Preporuci[40] iz ovog paketa objašnjava se kako se kibersigurnost uključuje u postojeće mehanizme za upravljanje krizama na razini EU-a i utvrđuju se ciljevi i načini suradnje među državama članicama te između država članica i nadležnih institucija, službi, agencija i tijela EU-a[41] pri odgovoru na kiberincidente i kiberkrize velikih razmjera. U Preporuci se od država članica i institucija EU-a traži i da radi provedbe Plana uspostave okvir EU-a za odgovor na kiberkrize. Plan će se redovito ispitivati u okviru vježbi za upravljanje kiberkrizama i drugim vrstama kriza[42] i ažurirat će se prema potrebi.

Budući da bi kiberincidenti mogli znatno utjecati na funkcioniranje gospodarstava i na svakodnevni život ljudi, mogla bi se istražiti mogućnost uspostave **Fonda za hitne kibersigurnosne incidente** po uzoru na slične krizne mehanizme u drugim područjima politika EU-a. Time bi se državama članicama omogućilo da zatraže pomoć na razini EU-a tijekom ili nakon velikog incidenta pod uvjetom da je država članica uspostavila razborit kibersigurnosni sustav prije incidenta, među ostalim i da je u potpunosti provela Direktivu NIS i razradila okvire za upravljanje krizama i nadzor na nacionalnoj razini. Takav fond, kojim bi se dopunili postojeći mehanizmi za upravljanje krizama na razini EU-a, mogao bi uključivati sposobnost za brz odgovor u interesu solidarnosti i financiranje određenih mjera za brzo djelovanje, primjerice zamjenu ugrožene opreme ili uporabu alata za ublažavanje, pri čemu bi se iskoristilo iskustvo stečeno u okviru mehanizma EU-a za civilnu zaštitu.

2.5. Mreža za stručnost u području kibersigurnosti s Europskim centrom za istraživanje i stručnost u području kibersigurnosti

Tehnološki alati za kibersigurnost strateška su imovina i ključne tehnologije za poticanje budućeg rasta. U strateškom je interesu EU-a osigurati da EU zadrži i razvije bitne sposobnosti za zaštitu svojeg digitalnoga gospodarstva, društva, demokracije, ključne računalne opreme i softvera te za pružanje ključnih kibersigurnosnih usluga.

---

37 Time se omogućuje koordinacija odgovora na velike međusektorske krize na najvišoj političkoj razini.

38 Ti odgovori omogućuju unutarnju razmjenu i koordinaciju informacija o novim višesektorskim krizama ili predvidljivim ili neizbježnim prijetnjama koje zahtijevaju djelovanje na razini EU-a.

39 U skladu s člankom 222. Ugovora o funkcioniranju Europske unije.

40 C(2017) 6100.

41 Uključujući Europol, ENISA-u, tim za hitne računalne intervencije u institucijama, tijelima i agencijama EU-a (CERT-EU) i Obavještajnog i situacijskog centra EU-a (INTCEN).

42 Na primjer, one kojima upravlja ENISA. https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme

Javno-privatno partnerstvo za kibersigurnost[43], uspostavljeno 2016., bilo je važan prvi korak kojim su potaknuta ulaganja do 1,8 milijardi EUR do 2020. Međutim, opseg ulaganja u drugim dijelovima svijeta[44] upućuje na to da EU mora učiniti više u pogledu ulaganja i riješiti problem fragmentacije kapaciteta unutar EU-a.

S obzirom na složenost kibersigurnosne tehnologije, potrebna ulaganja velikih razmjera i potrebu za rješenjima koja funkcioniraju u cijelom EU-u, djelovanjem EU-a može se osigurati dodana vrijednost. Nastavljajući se na rad država članica i javno-privatnog partnerstva dodatni korak bio bi jačanje kapaciteta EU-a u području kibersigurnosti posredstvom **mreže centara za stručnost u području kibersigurnosti**[45]**,** u čijem bi središtu djelovao **Europski centar za istraživanje i stručnost u području kibersigurnosti**. Ta mreža i njezin Centar poticali bi razvoj i primjenu tehnologije u području kibersigurnosti i dopunjavali bi napore usmjerene na jačanje kapaciteta u tom području na razini EU-a i nacionalnoj razini. Komisija će pokrenuti procjenu učinka kako bi razmotrila dostupne mogućnosti, uključujući mogućnost uspostave zajedničkog pothvata, u cilju uspostave navedene strukture 2018.

Komisija će kao prvi korak i osnovu za daljnje promišljanje predložiti pokretanje pilot-faze u okviru programa Obzor 2020. kako bi se olakšalo povezivanje nacionalnih centara u mrežu radi novog poticaja razvoju sposobnosti i tehnologije u području kibersigurnosti. U tu svrhu planira predložiti kratkoročnu financijsku injekciju od 50 milijuna EUR. Tom će se aktivnošću dopuniti tekuća provedba javno-privatnog partnerstva za kibersigurnost.

Glavni zadatak mreže i Centra bilo bi objedinjenje i oblikovanje istraživačkih napora. Kako bi podupirao razvoj industrijskih sposobnosti, Centar bi mogao djelovati kao voditelj projekata za razvoj sposobnosti koji može voditi multinacionalne projekte. Time bi se dodatno potaknule inovacije i konkurentnost industrije EU-a na globalnoj razini u području razvoja digitalnih tehnologija sljedeće generacije, među ostalim umjetne inteligencije, kvantnog računalstva, tehnologije ulančanih blokova (*blockchain*) i sigurnih digitalnih identiteta te u osiguravanju pristupa masovnim podacima za poduzeća sa sjedištem u EU-u, što je od ključne važnosti za kibersigurnost u budućnosti. Centar bi se pri poboljšanju infrastrukture za računalstvo visokih performansi oslanjao na aktivnosti EU-a: to je od ključne važnosti za analizu velike količine podataka, brzo šifriranje i dešifriranje podataka, provjeru identiteta, simulaciju kibernapada i analizu videozapisa[46].

Mreža centara za stručnost mogla bi imati i sposobnosti za podupiranje industrije ispitivanjem i simulacijom, na čemu bi se temeljila kibersigurnosna certifikacija opisana u odjeljku 2.2. Njezinim sudjelovanjem u svim aktivnostima EU-a u području kibersigurnosti osiguralo bi se stalno ažuriranje njezinih ciljeva u skladu s potrebama. Centar bi nastojao poboljšati norme kibersigurnosti ne samo u području tehnologije i kibersigurnosnih sustava, već i u području razvoja vrhunskih vještina kod stručnjaka pružanjem rješenja i predložaka za nacionalne mjere usmjerene na razvoj digitalnih vještina. Tako bi pojačao i kibersigurnosne sposobnosti na razini EU-a i nastavio sinergije, posebno s agencijom ENISA, CERT-EU-om, Europolom, mogućim budućim Fondom za hitne kibersigurnosne intervencije i nacionalnim CSIRT-ima.

Mreža za stručnost svoje aktivnosti mora posebno usmjeriti na nedostatak europskih sposobnosti za procjenu **šifriranja** proizvoda i usluga kojima se koriste građani, poduzeća i

[43] C(2016) 4400 final.

[44] SAD će u kibersigurnost samo 2017. uložiti 19 milijardi dolara, što je povećanje od 35 % u odnosu na 2016. Bijela kuća, Ured za odnose s javnošću „Informativni članak: Nacionalni akcijski plan za kibersigurnost”, 9. veljače 2016.

[45] Mreža bi uključivala postojeće i buduće centre za kibersigurnost uspostavljene u državama članicama, čiji bi članovi bili uglavnom javne istraživačke organizacije i laboratoriji.

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

javna tijela na jedinstvenom digitalnom tržištu. Snažno šifriranje osnova je za sigurne digitalne identifikacijske sustave koji imaju ključnu ulogu u osiguravanju učinkovite kibersigurnosti[47]. Njime se štiti i intelektualno vlasništvo osoba i omogućuje zaštita temeljnih prava, primjerice slobode izražavanja i zaštite osobnih podataka, te se osigurava sigurno internetsko trgovanje[48].

Budući da EU-ova civilna i obrambena tržišta kibersigurnosti dijele zajedničke izazove[49] i tehnologiju za dvojnu uporabu zbog kojih je potrebna bliska suradnja u ključnim područjima, mogla bi se razviti druga faza mreže i njezina Centra koja bi uključivala obrambenu dimenziju, pri čemu bi se u potpunosti poštovale odredbe Ugovora koje se odnose na zajedničku sigurnosnu i obrambenu politiku. Obrambena dimenzija i njezina tehnološka usmjerenost mogle bi pridonijeti suradnji država članica u području kiberobrane, među ostalim i razmjenom informacija, informiranosti o stanju, jačanjem stručnosti i koordiniranih reakcija i podupiranjem razvoja zajedničkih sposobnosti država članica. Mogla bi služiti i kao platforma s pomoću koje će države članice moći utvrditi prioritete za kiberobranu EU-a, pridonijeti razvoju zajedničkih strategija, olakšati zajedničko osposobljavanje, vježbe i ispitivanje za kiberobranu na europskoj razini i poduprijeti rad na taksonomijama i normama u području kiberobrane, pri čemu bi Centar imao potpornu i savjetodavnu ulogu. Kako bi mogao obavljati navedene aktivnosti, Centar bi trebao blisko surađivati s Europskom obrambenom agencijom u području kiberobrane te s agencijom ENISA u području kiberotpornosti te svoje djelovanje uskladiti s njihovim. U okviru te obrambene dimenzije uzeo bi se u obzir postupak pokrenut Dokumentom za razmatranje o budućnosti europske obrane.

Budući da je za kiberobranu potrebna visoka razina otpornosti, potrebno je posebno usmjeravanje istraživačkih i tehnoloških napora. Projekti ili tehnologije u području kiberobrane koje razvijaju poduzeća mogli bi se financirati sredstvima iz Europskog fonda za obranu i u fazi istraživanja i u fazi razvoja[50]. U tom kontekstu mogla bi biti osobito važna posebna područja, primjerice sustavi šifriranja utemeljeni na kvantnim tehnologijama, informiranost o stanju kibersigurnosti, biometrijski sustavi kontrole pristupa, napredni sustavi za otkrivanje stalnih prijetnji ili rudarenje podataka. Visoki predstavnik, Europska obrambena agencija i Komisija pomoći će državama članicama da utvrde u kojim bi se područjima zajednički kibersigurnosni projekti mogli financirati iz Europskog fonda za obranu.

2.6. Stvaranje snažne baze kibervještina u EU-u

Kibersigurnost ima snažnu obrazovnu dimenziju. Učinkovita kibersigurnost u velikoj mjeri ovisi o vještinama uključenih osoba. Međutim, predviđa se da će do 2022. u privatnom sektoru u Europi nedostajati 350 000 stručnjaka s potrebnom razinom vještina u području kibersigurnosti[51]. Obrazovanje u području kibersigurnosti trebalo bi razvijati na svim razinama, od redovitog osposobljavanja radne snage u području kibersigurnosti i dodatnog kibersigurnosnog osposobljavanja svih stručnjaka za IKT do novih kurikuluma za

[47] Komisija je u okviru programa Obzor 2020. već raspisala novi natječaj za nagradu Obzor u iznosu od 4 milijuna EUR za najbolje inovativno rješenje za metode neometane autentifikacije na internetu.

[48] Kibersigurnost na europskom jedinstvenom digitalnom tržištu, Skupina znanstvenih savjetnika na visokoj razini, ožujak 2017.

[49] Studija o sinergijama između civilnog i obrambenog tržišta kibersigurnosti (*Study on synergies between the civilian and the defence cybersecurity markets*, Optimity; SMART 2014-0059).

[50] U Programu razvoja europske obrambene industrije već sada će se dati prednost projektima kiberobrane i kiberobrana će biti jedna od tema poziva na podnošenje prijedloga koji će se objaviti 2018.

[51] Globalna studija o radnoj snazi u području informacijske sigurnosti (*Global Information Security Workforce Study*), 2017. Globalni manjak iznosi 1,8 milijuna.

kibersigurnost. Kako bi se mogla zadovoljiti potražnja za bržim obrazovanjem i osposobljavanjem, trebalo bi uspostaviti snažne akademske centre stručnosti, koji bi se mogli temeljiti na smjernicama Europskog centra za istraživanje i stručnost u području kibersigurnosti i ENISA-e. Cilj je postići da se podrazumijeva da se proizvodi i sustavi IKT-a oblikuju tako da od samog početka uključuju načela sigurnosti. Obrazovanje u području kibersigurnosti ne bi trebalo biti ograničeno na stručnjake za IT, već bi trebalo biti uključeno u kurikulume za druga područja, primjerice inženjering, poslovno upravljanje ili pravo, te u sektorske obrazovne programe. Naposljetku, trebalo bi razvijati svijest učitelja i učenika u osnovnim i srednjim školama o kiberkriminalu i kibersigurnosti u okviru stjecanja digitalnih kompetencija u školama.

EU bi, zajedno s državama članicama, trebao pridonijeti tim aktivnostima nastavljajući se na rad Koalicije za digitalne vještine i radna mjesta[52] i uspostavom, primjerice, programa naukovanja u području kibersigurnosti za MSP-ove.

2.7. Promicanje kiberhigijene i osviještenosti

Budući da je otprilike 95 % incidenata posljedica „neke vrste ljudske pogreške, neovisno o tome je li namjerna ili nije”,[53] ljudski čimbenik ima važnu ulogu. Za kibersigurnost smo stoga odgovorni svi. To znači da se mora promijeniti ponašanje građana, poduzeća i javne uprave kako bi se osiguralo da svi razumiju prijetnju te da imaju alate i vještine koji su im potrebni za brzo otkrivanje i aktivnu zaštitu od napada. Građani moraju razviti navike kiberhigijene, a poduzeća i organizacije moraju uvesti prikladne kibersigurnosne programe utemeljene na riziku i redovito ih ažurirati u skladu s dinamičnim razvojem rizika.

Direktivom NIS propisuju se ne samo odgovornosti država članica za razmjenu informacija o kibernapadima na razini EU-a već se uspostavljaju i razrađene nacionalne strategije za kibersigurnost te okviri za sigurnost mrežnih i informacijskih sustava. Javna uprava na razini EU-a i nacionalnoj razini trebala bi i dalje predvoditi te napore.

Prvo, države članice trebale bi poduzećima i građanima omogućiti veću dostupnost kibersigurnosnih alata. Posebno bi trebalo uložiti više napora u sprječavanje i ublažavanje učinka kiberkriminaliteta na krajnje korisnike. Primjer je kampanja Europola „NoMoreRansom”[54], osmišljena zahvaljujući bliskoj suradnji tijela za izvršavanje zakonodavstva i poduzeća koja se bave kibersigurnosti kako bi se korisnicima pomoglo da spriječe zaraze ucjenjivačkim softverom i dešifriraju podatke u slučaju napada. Takve programe trebalo bi uvesti i za druge vrste zlonamjernog softvera u drugim područjima i EU bi trebao pokrenuti **jedinstveni portal kojim bi se na jednom mjestu objedinili svi takvi alati** i na kojem bi se korisnike savjetovalo o sprječavanju i otkrivanju zlonamjernog softvera te na kojem bi bile dostupne poveznice na mehanizme za prijavu.

Drugo, države članice trebale bi ubrzati **uporabu sigurnijih kiberalata u razvoju e-uprave** i u potpunosti iskoristiti mrežu stručnosti. Trebalo bi promicati uvođenje sigurnih načina identifikacije na temelju okvira EU-a za elektroničku identifikaciju i usluge povjerenja za elektroničke transakcije na unutarnjem tržištu koji je na snazi od 2016. i kojim se osigurava predvidljivo regulatorno okruženje za sigurne i neometane elektroničke interakcije među

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

[53] IBM „Indeks kibersigurnosnih obavještajnih informacija”, 2014., naveden u publikaciji Securitymagazine.com, 19. lipnja 2014.

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

poduzećima, građanima i javnim tijelima[55]. Nadalje, javne institucije, posebno one koje pružaju klučne usluge, trebale bi osigurati osposobljavanje svojeg osoblja u područjima povezanima s kibersigurnošću.

Treće, države članice trebale bi u **kampanjama osvješćivanja** staviti naglasak na osvješćivanje u pogledu kibersigurnosti, među ostalim i u kampanjama usmjerenima na škole, sveučilišta, poslovnu zajednicu i istraživačka tijela. Aktivnosti u okviru Mjeseca kibersigurnosti, koji se održava u listopadu svake godine pod koordinacijom ENISA-e, proširit će se kako bi ostvarile veći doseg kao rezultat zajedničkih komunikacijskih napora na razini EU-a i na nacionalnoj razini. Jednako je važno podizanje razine svijesti u pogledu internetskih **kampanja dezinformiranja i širenja lažnih vijesti** na društvenim mrežama kojima se nastoje potkopati demokratski postupci i europske vrijednosti. Iako je primarna odgovornost na nacionalnoj razini, uključujući za izbore za Europski parlament, pokazalo se da objedinjavanje iskustva i njegova razmjena na europskoj razini imaju dodanu vrijednost kada je riječ o usmjeravanju djelovanja[56].

Snažnu ulogu ima i **industrija** općenito, a posebno pružatelji i proizvođači digitalnih usluga. Korisnike (građane, poduzeća i javne uprave) bi morala podupirati alatima koji će im omogućiti da preuzmu odgovornost za svoje djelovanje na internetu i jasno isticati da je održavanje kiberhigijene neophodan dio ponude potrošačima[57]. U cilju otkrivanja i uklanjanja ranjivosti industrija bi trebala nastojati uspostaviti unutarnje postupke za istrage, trijažu i uklanjanje ranjivosti, neovisno o tome je li izvor moguće ranjivosti izvan ili unutar predmetnog poduzeća.

Ključne mjere

- Potpuna provedba Direktive o sigurnosti mrežnih i informacijskih sustava;
- žurno donošenje Uredbe o novom mandatu agencije ENISA i europskom okviru za certifikaciju od strane Europskog parlamenta i Vijeća[58];
- zajednička inicijativa Komisije/industrije za definiranje načela „dužne pažnje” za smanjenje ranjivosti proizvoda/softvera i promicanje „integrirane sigurnosti”;
- brza provedba plana za prekogranične odgovore na velike incidente;
- pokretanje procjene učinka kako bi se istražila mogućnost da Komisija 2018. donese prijedlog o uspostavi mreže centara za stručnost u području kibersigurnosti i Europskog centra za istraživanje i stručnost u području kibersigurnosti na temelju neposredne pilot-faze;
- pomoć državama članicama pri utvrđivanju područja u kojima bi se za provedbu zajedničkih kibersigurnosnih projekata mogla osigurati sredstva iz Europskog fonda za obranu;
- jedinstvena točka na razini EU-a za pomoć žrtvama kibernapada, koja će pružati informacije o najnovijim prijetnjama i objedinjavati praktične savjete i alate za kibersigurnost;

[55] Uredba (EU) br. 910/2014 o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu (Uredba o eIDAS-u) donesena 23. srpnja 2014. Osim toga, Europska komisija u okviru Instrumenta za povezivanje Europe osigurava sastavne elemente i alate za interoperabilnost e-ID-a i e-potpisa (npr. preglednike pouzdanih popisa) .

[56] Primjer je radna skupina East StratCom koju su države članice i Visoki predstavnik uspostavili 2015. radi suzbijanja kampanji dezinformiranja koje je provodila Rusija. Ta skupina razvija komunikacijske proizvode i kampanje usmjerene na objašnjavanje politika EU-a u regiji Istočnog partnerstva.

[57] Neki proizvođači već su se naviknuli na taj pojam jer se u nekim europskim propisima o proizvodima (na primjer, u Direktivi o strojevima 2006/42/EZ) propisuju načela za „integriranu sigurnost”.

[58] COM (2017) 477.

- mjere država članica za uvođenje kibersigurnosti u programe za razvoj vještina, e-upravu i kampanje osvješćivanja;
- mjere industrije usmjerene na ubrzanje osposobljavanja svojih zaposlenika u području kibersigurnosti i uvođenje pristupa „integrirane sigurnosti" za svoje proizvode, usluge i postupke.

3. OSMIŠLJAVANJE UČINKOVITIH MJERA EU-A ZA ODVRAĆANJE OD KIBERNAPADA

Učinkovito odvraćanje znači uspostavu okvira mjera koje su vjerodostojne i imaju odvraćajući učinak na buduće kiberzločince i napadače. Dok god se počinitelji kibernapada (državni i nedržavni) nemaju čega bojati osim neuspjeha, neće imati razloga prestati pokušavati. Za uspostavu učinkovitih mjera odvraćanja potreban je djelotvorniji odgovor tijela kaznenog progona usmjeren na otkrivanje, sljedivost i kazneni progon kiberzločinaca. Osim toga EU treba podupirati svoje države članice pri razvoju dvojnih sposobnosti za kiberobranu. Kiberobrana će biti uspješnija tek kada se poveća vjerojatnost da će počinitelji biti uhvaćeni i kažnjeni. U slučaju kibernapada trebalo bi odmah provesti istragu i počinitelje privesti pravdi ili poduzeti mjere kojima će se omogućiti primjeren politički ili diplomatski odgovor. U slučaju velike krize koja ima važnu međunarodnu i obrambenu dimenziju, Visoki predstavnik trebao bi Vijeću predstaviti mogućnosti za primjereni odgovor.

Korak u smjeru boljeg kaznenopravnog odgovora na kibernapade već je napravljen donošenjem Direktive o napadima na informacijske sustave 2013.[59] Njome su uspostavljena minimalna pravila za definiranje kaznenih djela i sankcija u području napada na informacijske sustave i predviđene su operativne mjere za poboljšanje suradnje nadležnih tijela. Zahvaljujući Direktivi ostvaren je znatan napredak u pogledu usklađivanja kriminalizacije kibernapada u svim državama članicama, čime se olakšava prekogranična suradnja tijela za izvršavanje zakonodavstva koja istražuju tu vrstu kaznenih djela. Međutim, i dalje ima prostora za ostvarivanje punog potencijala Direktive potpunom provedbom svih njezinih odredaba u državama članicama[60]. Komisija će državama članicama i dalje pružati potporu u provedbi Direktive i za sada smatra da je nije potrebno izmijeniti.

3.1. Identifikacija počinitelja zlonamjernih djela

Kako bismo povećali vjerojatnost da se počinitelji kibernapada privedu pravdi, moramo žurno poboljšati svoje sposobnosti za njihovu identifikaciju. Pronalaženje korisnih informacija za istrage kiberkriminaliteta, većinom u obliku digitalnih tragova, glavni je izazov za tijela za izvršavanje zakonodavstva. Stoga moramo poboljšati svoje tehnološke sposobnosti za učinkovite istrage, među ostalim jačanjem jedinice Europola za kiberkriminalitet zapošljavanjem stručnjaka za kibersigurnost. Europol je postao glavni akter za potporu država članica pri istragama koje se provode u više jurisdikcija. Trebao bi postati centar za stručnost u području internetskih istraga i kiberforenzike za tijela država članica za izvršavanje zakonodavstva.

Zbog raširene prakse povezivanja više korisnika, ponekad tisuća korisnika, s jednom IP adresom tehnički je vrlo teško provoditi istrage zlonamjernog ponašanja na internetu. Stoga je radi identifikacije jednog počinitelja ponekad nužno provoditi istrage protiv velikog broja korisnika, na primjer u slučaju teških zločina poput spolnog zlostavljanja djece . EU će stoga

[59] Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave.

[60] COM (2017) 474.

poticati uvođenje novog protokola (IPv6) jer se njime omogućuje dodjela jednog korisnika po IP adresi, čime će se nedvojbeno pomoći tijelima za izvršavanje zakonodavstva i pridonijeti istragama u području kibersigurnosti. Kao prvi korak za poticanje uvođenja Komisija će u svoje politike uključiti zahtjev za prelazak na IPv6 , među ostalim u zahtjevima u postupcima javne nabave, financiranju projekata i istraživanja te će poduprijeti uporabu potrebnih materijala za osposobljavanje. Nadalje, države članice trebale bi razmotriti uvođenje dobrovoljnih sporazuma s pružateljima internetskih usluga kako bi potaknule uvođenje protokola IPv6.

Belgija ima najveću stopu [61]uvođenja protokola IPv6 u svijetu, među ostalim i zbog suradnje javnog i privatnog sektora: relevantni dionici razmatrali su mogućnost ograničavanja uporabe jedne IP adrese na najviše 16 korisnika kao dio dobrovoljne samoregulatorne mjere, što je bio poticaj za prelazak na IPv6[62].

Općenito, trebalo bi i dalje poticati odgovornost na internetu. To znači promicanje mjera za sprječavanje zlouporabe naziva domena za slanje neželjenih poruka ili poruka čija je svrha krađa identiteta. Komisija će u tu svrhu raditi na poboljšanju funkcioniranja i dostupnosti naziva domene i sustava IP WHOIS[63] i točnosti njihovih podataka u skladu s naporima Internetske korporacije za dodijeljene nazive i brojeve[64].

3.2. Snažniji odgovor tijela za izvršavanje zakonodavstva

U odvraćanju od kibernapada glavnu ulogu imaju učinkovite **istrage** i **kazneni progon** kiberkriminaliteta. Međutim, postojeći postupovni okvir treba bolje prilagoditi internetskom dobu[65]. Kibernapadi mogu biti toliko brzi da naši postupci nisu učinkoviti i zbog toga može biti potrebna brza prekogranična suradnja. U tu svrhu, kako je najavljeno u okviru Europskog programa sigurnosti, Komisija će početkom 2018. iznijeti prijedloge za **olakšavanje prekograničnog pristupa elektroničkim dokazima**. Komisija istodobno provodi praktične mjere za poboljšanje prekograničnog pristupa elektroničkim dokazima za potrebe kaznenih istraga, uključujući financiranje namijenjeno osposobljavanju za prekograničnu suradnju, razvoj elektroničke platforme za razmjenu informacija u EU-u i standardizaciju obrazaca za pravosudnu suradnju koji se upotrebljavaju među državama članicama.

Prepreku učinkovitom kaznenom progonu čine i različiti forenzički postupci za prikupljanje e-dokaza u istragama kiberkriminaliteta u državama članicama. To bi se moglo poboljšati uspostavom zajedničkih forenzičkih standarda. Nadalje, potrebno je pojačati forenzičke sposobnosti za potporu sljedivosti i pripisivanju. Jedan korak bio bi daljnji razvoj forenzičkih sposobnosti Europola prilagodbom postojećih proračunskih i ljudskih resursa Europskog centra za kiberkriminalitet pri Europolu kako bi se mogla zadovoljiti rastuća potreba za operativnom potporom u prekograničnim istragama kiberkriminaliteta. Drugi korak bio bi

[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 upita i odgovora koji se upotrebljava za pretraživanje baza podataka u kojima su pohranjeni podaci o registriranim korisnicima ili korisnicima kojima je dodijeljeno pravo korištenja internetskog resursa.

[64] Internetska korporacija za dodijeljene nazive i brojeve (ICANN) neprofitna je organizacija odgovorna za koordinaciju održavanja i postupaka nekoliko baza podataka povezanih s identifikatorima na internetu.

[65] Na primjer, (virtualni) središnji poslužitelj za kontrolu i upravljanje botneta Avalanche premještao je fizičke poslužitelje i domene svakih pet minuta.

preslikavanje prethodno navedene tehnološke usmjerenosti na šifriranje promatranjem kako zločinci njegovom zlouporabom stvaraju velike probleme u suzbijanju teškog kriminala, među ostalim terorizma i kiberkriminaliteta. Komisija će objaviti rezultate trenutačnih razmatranja o **ulozi šifriranja u kaznenim istragama**[66] do listopada 2017[67].

Uzimajući u obzir da internet ne poznaje granice, okvirom za međunarodnu suradnju iz **Konvencije Vijeća Europe o kibernetičkom kriminalu iz Budimpešte**[68] heterogenoj skupini zemalja pruža se mogućnost primjene optimalnog pravnog standarda za različite nacionalne propise o kiberkiminalitetu. Sada se razmatra mogućnost dodavanja protokola Konvenciji[69], što bi također mogla biti korisna prilika za rješavanje problema prekograničnog pristupa elektroničkim dokazima u međunarodnom kontekstu. Umjesto stvaranja novih međunarodnih pravnih instrumenata za pitanja kiberkriminaliteta, EU poziva sve države da izrade prikladno nacionalno zakonodavstvo i uspostave suradnju unutar tog postojećeg međunarodnog okvira.

Opća dostupnost alata za anonimizaciju zločincima olakšava skrivanje. ***Darknet***[70] (mračni internet) omogućuje zločincima nove načine pristupa dječjoj pornografiji, drogama ili vatrenom oružju, često uz mali rizik da će biti uhvaćeni[71]. On je sada i glavni izvor alata koji se upotrebljavaju u svrhe kiberkriminaliteta, kao što su zlonamjerni softver i alati za hakiranje. Komisija će u suradnji s relevantnim dionicima analizirati nacionalne pristupe kako bi pronašla nova rješenja. Europol bi trebao olakšavati i podupirati istrage povezane s *darknetom*, procjenjivati prijetnje i pomagati pri utvrđivanju nadležnosti i davanju prioriteta visokorizičnim slučajevima, a EU može imati glavnu ulogu u koordinaciji međunarodnog djelovanja[72].

Jedno od rastućih područja aktivnosti kiberkriminaliteta jest zlouporaba podataka o kreditnim karticama ili drugih elektroničkih sredstava plaćanja. Podaci za plaćanje koji su pribavljeni kibernapadima na trgovce na internetu ili druga zakonita poduzeća potom se prodaju na internetu i zločinci ih mogu upotrijebiti za prijevaru[73]. Komisija predstavlja prijedlog o jačim mjerama odvraćanja u obliku **Direktive o borbi protiv prijevara i krivotvorenja bezgotovinskih sredstava plaćanja**[74]. Njome se nastoje ažurirati postojeća pravila u tom

---

66 Predsjedništvo Vijeća, Zaključak sastanka Vijeća za pravosuđe i unutarnje poslove od 8. i 9. prosinca 2016., br. 15391/16.

67 Osmo izvješće o napretku prema uspostavi učinkovite i istinske sigurnosne unije od 29. lipnja 2017., COM(2017) 354 final.

68 Konvencija je prvi međunarodni ugovor o zločinima počinjenima internetom i drugim računalnim mrežama koji je posebno usmjeren na povrede autorskih prava, računalnu prijevaru, dječju pornografiju i povrede mrežne sigurnosti. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 Do 2017. Konvenciju Vijeća Europe o kibernetičkom kriminalu ratificiralo je ili joj je pristupilo 55 vlada.

69 Nadležnost za izradu nacrta 2. dodatnog protokola uz Konvenciju iz Budimpešte o kibernetičkom kriminalu, T-CY (2017.)3.

70 *Darknet* se sastoji od sadržaja na sustavu prividnih mreža koje se koriste internetom, ali kojima se može pristupiti samo uz pomoć posebnog softvera, konfiguracija ili odobrenja. *Darknet* je mali dio dubokog interneta, odnosno dio do kojeg se ne može doći tražilicama.

71 Istaknuta iznimka nedavno su zatvorena najveća zločinačka tržišta mračnog interneta, AlphaBay i Hansa: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

72 Europol u tom području već ima važnu ulogu. Nedavni primjer dostupan je na: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

73 Prihod od prijevara važan je izvor prihoda za organizirani kriminal i stoga omogućuje počinjenje drugih kaznenih djela, primjerice terorizam, trgovanje drogom i trgovanje ljudima.

74 COM (2017) 489.

području i povećati sposobnost tijela za izvršavanje zakonodavstva za suzbijanje te vrste zločina.

Potrebno je poboljšati i sposobnosti tijela za izvršenje zakonodavstva u državama članicama za istrage kiberkriminaliteta te poboljšati razumijevanje takvih vrsta kaznenih dijela i istražne mogućnosti tužitelja i sudstva. Eurojust i Europol pridonose tom cilju i pojačanoj koordinaciji u bliskoj suradnji sa specijaliziranim savjetodavnim skupinama u okviru Europlova centra za kiberkriminalitet i s mrežama šefova jedinica za kiberkriminalitet i tužitelja specijaliziranih za kiberkriminalitet. Komisija će izdvojiti 10,5 milijuna EUR za borbu protiv kiberkriminaliteta, posebno u okviru svojeg **Fonda za unutarnju sigurnost - programa za policiju**. Osposobljavanje je važan element i Europska skupina za osposobljavanje i obrazovanje u području kiberkriminaliteta razvila je niz korisnih materijala. Te bi materijale sada trebalo uvesti u obrazovanje policijskih djelatnika uz potporu Agencije Europske unije za osposobljavanje u području izvršavanja zakonodavstva (CEPOL).

3.3. Javno-privatna suradnja u borbi protiv kiberkriminaliteta

Obilježja digitalnog svijeta, koji čine uglavnom infrastruktura u privatnom vlasništvu i velik broj različitih dionika u različitim jurisdikcijama, umanjuju učinkovitost tradicionalnih mehanizama za izvršavanje zakonodavstva. Zbog toga je suradnja s privatnim sektorom, uključujući industriju i civilno društvo, od ključne važnosti za učinkovitu borbu javnih tijela protiv zločina. U tom kontekstu važan je i financijski sektor, s kojim bi trebalo pojačati suradnju. Na primjer, trebalo bi pojačati ulogu financijsko-obavještajnih jedinica[75] u kontekstu kiberkriminaliteta.

Neke države članice već su poduzele ključne korake. U Nizozemskoj financijske institucije i tijela za izvršavanje zakonodavstva surađuju u borbi protiv prijevara na internetu i kiberkriminaliteta u okviru Radne skupine za elektronički kriminal. Njemački centar za stručnost u borbi protiv kiberkriminaliteta operativno je čvorište u kojem njegovi članovi mogu razmjenjivati informacije u suradnji s njemačkom saveznom policijom i razvijati mjere kojima se osigurava zaštita od kiberkriminaliteta. Centre izvrsnosti za kiberkriminalitet osnovalo je 16 država članica[76] kako bi olakšale suradnju između tijela za izvršavanje zakonodavstva, akademske zajednice i privatnih partnera u cilju razvoja i razmjene najbolje prakse, osposobljavanja i jačanja kapaciteta.
Komisija podupire uspostavu javno-privatnih partnerstava i mehanizama suradnje u okviru posebnih projekata kao što je mreža kibercentara i stručnjaka za sprječavanje računalnih prijevara[77], koja primjenjuje model razmjene informacija i standarda radi analize i ublažavanja rizika od elektroničkog kriminala i prijevara.

U kontekstu kiberkriminaliteta, privatnim poduzećima mora se omogućiti da s tijelima za izvršavanje zakonodavstva razmjenjuju informacije o konkretnim incidentima, među ostalim i osobne podatke, u skladu s pravilima o zaštiti podataka. Reformom propisa EU-a o zaštiti podataka, koja će biti na snazi od svibnja 2018., osiguravaju se zajednička pravila kojima se

[75] Financijsko-obavještajne jedinice služe kao nacionalni centri za primanje i analizu izvješća o sumnjivim transakcijama i ostalih informacija koje su važne za pranje novca, povezana predikatna kaznena djela i financiranje terorizma te za širenje rezultata tih analiza.

[76] Austrija, Belgija, Bugarska, Cipar, Češka, Estonija, Francuska, Njemačka, Grčka, Irska, Litva, Poljska, Rumunjska, Slovenija, Španjolska i Ujedinjena Kraljevina.

[77] Inicijativom EU-OF2CEN nastoji se omogućiti sustavno širenje informacija o internetskim prijevarama u cijelom EU-u među bankama i tijelima za izvršavanje zakonodavstva radi sprječavanja isplata počiniteljima prijevara i posrednicima te provedbe istraga i kaznenog progona počinitelja. Inicijativu sufinancira EU (Fond za unutarnju sigurnost – program za policiju).

utvrđuju uvjeti za suradnju tijela za izvršavanje zakonodavstva i privatnih subjekata. Europska komisija surađivat će s Europskim odborom za zaštitu podataka i relevantnim dionicima kako bi utvrdila najbolju praksu u tom području i, prema potrebi, dala smjernice.

3.4. Jačanje političkog odgovora

U nedavno donesenom okviru za **zajednički diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti**[78] („alat za kiberdiplomaciju") utvrđuju se mjere u okviru zajedničke vanjske i sigurnosne politike, uključujući mjere ograničavanja koje se mogu iskoristiti za jačanje odgovora EU-a na aktivnosti koje nanose štetnu njegovim političkim, sigurnosnim i gospodarskim interesima. Okvir je važan korak u razvoju sposobnosti za upozoravanje i reagiranje na razini EU-a i država članica. Njime će se pojačati naša sposobnost za otkrivanje počinitelja zlonamjernih kiberaktivnosti u cilju utjecanja na ponašanje mogućih napadača te uzimajući u obzir potrebu za osiguravanjem razmjernih odgovora. Pripisivanje odgovornosti državnom ili nedržavnom akteru suverena je politička odluka utemeljena na informacijama iz svih izvora. Trenutačno se s državama članicama radi na provedbi Okvira i ti će se napori nastaviti u skladu s Planom kako bi se osigurao odgovor na kiberincidente velikih razmjera[79]. INTCEN bi u bliskoj suradnji s državama članicama i institucijama EU-a trebao povezati, analizirati i podijeliti uvid u stanje koji je nužan za primjenu mjera iz tog okvira[80].

3.5. Jače odvraćanje zahvaljujući obrambenim sposobnostima država članica

Države članice već razvijaju sposobnosti za kiberobranu. Nadalje, budući da ne postoji jasna razlika između kiberobrane i kibersigurnosti te zbog dvojne uporabe kiberalata i tehnologija, kao i zbog velikih razlika u pristupima država članica, EU može pridonijeti promicanju sinergija između vojnih i civilnih napora[81].

Države članice koje imaju naprednije sposobnosti za kibersigurnost i koje su ih voljne objediniti mogle bi razmotriti uključivanje kiberobrane u okvir „stalne strukturirane suradnje" (PESCO) uz potporu Visokog predstavnika, Komisije i Europske obrambene agencije. To bi se moglo poduprijeti prethodno navedenim aktivnostima za poticanje industrijskih sposobnosti i strateške neovisnosti EU-a. EU može promicati i interoperabilnost, među ostalim i olakšavanjem razvoja sposobnosti, koordiniranjem osposobljavanja i obrazovanja i naporima usmjerenima na normizaciju dvojne uporabe.

Trebalo bi u potpunosti iskoristiti i zajednički okvir za suzbijanje hibridnih prijetnji, koje često uključuju kibernapade, posebno uz pomoć Jedinice EU-a za otkrivanje hibridnih prijetnji i nedavno osnovanog Europskog centra za suzbijanje hibridnih prijetnji u Helsinkiju, čija je misija poticati strateški dijalog i provoditi istraživanje i analizu.

EU će ponovno u prvi plan dovesti okvir za politiku kiberobrane EU-a iz 2014.[82], kao alat za daljnju integraciju kibersigurnosti i obrane u zajedničku vanjsku i obrambenu politiku (ZVDP). Od ključne je važnosti kiberotpornost samih misija i operacija ZVDP-a: razvijat će se standardizirani postupci i tehničke sposobnosti kojima bi se mogle podupirati civilne i vojne misije i operacije te njihove strukture za planiranje i provedbu te pružatelji usluga informacijske tehnologije ESVD-a. Kako bi se pojačala suradnja država članica i bolje usmjerili napori EU-a u tome području, Europska obrambena agencija i ESVD, u suradnji sa

[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.
[81] EU shvaća kiberprostor kao prostor za djelovanje, baš kao i kopno, zrak i more. Napori u okviru kiberobrane uključuju i zaštitu i otpornost svemirskih objekata i povezanih zemaljskih infrastruktura.
[82] www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515

službama Komisije, olakšat će stratešku suradnju kreatora politika u području kiberobrane u državama članicama. EU će podupirati razvoj europskih kibersigurnosnih rješenja i u okviru svojih napora usmjerenih na stvaranje tehnološke i industrijske baze europskog obrambenog sektora. To uključuje i poticanje regionalnih klastera izvrsnosti u području kibersigurnosti i obrane.

Službe Komisije uspostavit će do 2018., u bliskoj suradnji s ESVD-om, državama članicama i ostalim relevantnim tijelima EU-a**, platformu za obrazovanje i osposobljavanje u području kiberobrane** radi uklanjanja postojećeg manjka vještina u području kiberobrane. Time će se dopuniti rad Europske obrambene agencije u tom području te će se pridonijeti rješavanju problema postojećeg manjka vještina u području kibersigurnosti i kiberobrane.

Ključne mjere

- inicijativa Komisije za prekogranični pristup elektroničkim dokazima (početak 2018.);
- žurno donošenje predložene Direktive o borbi protiv prijevara i krivotvorenja bezgotovinskih sredstava plaćanja u Europskom parlamentu i Vijeću;
- uvođenje zahtjeva povezanih s protokolom IPv6 u javnu nabavu, istraživanje i financiranje projekata; dobrovoljni sporazumi između država članica i pružatelja internetskih usluga o poticanju uvođenja protokola IPv6;
- obnovljena/proširena usmjerenost Europola na kiberforenziku i praćenje *darkneta*;
- provedba okvira za zajednički diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti;
- pojačana financijska potpora nacionalnim i transnacionalnim projektima za poboljšanje kaznenog pravosuđa u kiberprostoru;
- obrazovna platforma za kibersigurnost kako bi se uklonio postojeći manjak vještina u području kibersigurnosti i kiberobrane tijekom 2018.

4. JAČANJE MEĐUNARODNE SURADNJE U PODRUČJU KIBERSIGURNOSTI

U skladu s ključnim vrijednostima i temeljnim pravima EU-a, kao što su sloboda izražavanja i pravo na privatnost i zaštitu osobnih podataka te promicanje otvorenog, slobodnog i sigurnog kiberprostora, međunarodna politika kibersigurnosti EU-a usmjerena je na sve teži zadatak promicanja globalne kiberstabilnosti te na jačanje strateške neovisnosti Europe u kiberprostoru.

4.1. Kibersigurnost u vanjskim odnosima

Dokazi upućuju na to da ljudi u cijelom svijetu smatraju da su kibernapadi iz drugih zemalja jedna od najvećih prijetnji nacionalnoj sigurnosti[83]. S obzirom na globalnu prirodu prijetnje izgradnja i održavanje čvrstih saveza i partnerstava s trećim zemljama od ključne su važnosti za sprječavanje i odvraćanje od kibernapada, koji imaju sve veći utjecaj na međunarodnu stabilnost i sigurnost. EU će u svojim bilateralnim, regionalnim, višedioničkim i multilateralnim sporazumima dati prednost uspostavi okvira za sprječavanje sukoba i stabilnost u kiberprostoru.

EU snažno promiče stajalište da se u kiberprostoru mora primjenjivati međunarodno pravo, posebno Povelja UN-a. Kao dopunu obvezujućem međunarodnom pravu EU promiče dobrovoljne neobvezujuće norme, pravila i načela o odgovornom ponašanju država koje je

[83] Proljeće 2017., Ispitivanje javnog mnijenja, Istraživački centar Pew

istaknula UN-ova Skupina vladinih stručnjaka [84]. Potiče i razvoj i provedbu regionalnih mjera za izgradnju povjerenja u Organizaciji za sigurnost i suradnju u Europi i u drugim regijama.

Na bilateralnoj razini kiberdijalozi[85] će se i dalje razvijati i dopunjavati naporima usmjerenima na olakšavanje suradnje s trećim zemljama kako bi se poduprla načela dužne pažnje i državne odgovornosti u kiberprostoru. EU će u svojim međunarodnim angažmanima dati prednost pitanjima međunarodne sigurnosti u kiberprostoru te će istodobno osigurati da kibersigurnost ne postane izgovor za zaštitu tržišta i ograničavanje temeljnih prava i sloboda, među ostalim slobode izražavanja i pristupa informacijama. Sveobuhvatni pristup kibersigurnosti zahtijeva poštovanje ljudskih prava i EU će nastaviti štititi svoje temeljne vrijednosti na globalnoj razini u skladu s EU-ovim Smjernicama o ljudskim pravima u odnosu na slobodu izražavanja na internetu i izvan njega[86]. U tom pogledu EU ističe važnost uključenosti svih dionika u upravljanje internetom.

Komisija je iznijela i prijedlog[87] o modernizaciji izvoznih kontrola EU-a, uključujući uvođenje kontrola izvoza ključnih tehnologija za kibernadzor kojima bi se mogla povrijediti ljudska prava ili koje bi se mogle zlouporabiti na štetu sigurnosti EU-a te će pojačati dijaloge s trećim zemljama u cilju promicanja globalne konvergencije i odgovornog ponašanja u tom području.

4.2. Jačanje kapaciteta u području kibersigurnosti

Globalna kiberstabilnost ovisi o sposobnosti svih zemalja da na lokalnoj i nacionalnoj razini spriječe kiberincidente i na njih reagiraju te da provode istrage i kazneni progon slučajeva kiberkriminaliteta. Podupiranjem napora usmjerenih na jačanje nacionalne otpornosti u trećim zemljama povećat će se globalna razina kibersigurnosti, a to će imati pozitivne posljedice za EU. Za suočavanje sa sve dinamičnijim razvojem kiberprijetnji trebalo bi uložiti napore u osposobljavanje i razvoj politika i zakonodavstva te uspostaviti učinkovite timove za hitne računalne intervencije i jedinice za kiberkriminalitet u svim zemljama svijeta.

EU od 2013. ima vodeću ulogu u izgradnji međunarodnog kapaciteta za kibersigurnost i sustavno povezuje te napore sa svojom razvojnom suradnjom. EU će i dalje promicati model jačanja kapaciteta utemeljen na pravima u skladu s pristupom Digital4Development[88]. Prednost u jačanju kapaciteta imat će zemlje u susjedstvu EU-a i zemlje u razvoju u kojima se brzo povećava povezivost, ali se brzo razvijaju i prijetnje. Naporima EU-a dopunit će se EU-ov program razvoja u svijetlu Programa održivog razvoja do 2030. i općih napora usmjerenih na jačanje kapaciteta.

Kako bi se poboljšala sposobnost EU-a da za jačanje kapaciteta iskoristi stručnjake iz svih zemalja, trebalo bi uspostaviti posebnu mrežu EU-a za jačanje kapaciteta u području kibersigurnosti, u okviru koje će se okupiti ESVD, tijela država članica za kibersigurnost, agencije EU-a, službe Komisije, akademska zajednica i civilno društvo. Izradit će se smjernice EU-a za jačanje kapaciteta u području kibersigurnosti kako bi se osiguralo bolje političko usmjeravanje i lakše odredili prioriteti EU-a za pomoć trećim zemljama.

EU će surađivati i s drugim donatorima u tom području kako bi se izbjeglo preklapanje napora i olakšalo ciljano jačanje kapaciteta u različitim regijama.

---

84 A/68/98 i A/70/174.
85 EU je u rujnu 2017. održao kiberdijaloge sa SAD-om, Kinom, Japanom, Republikom Korejom i Indijom.
86 Smjernice EU-a o temeljnim pravima u odnosu na slobodu izražavanja na internetu i izvan njega.
87 COM (2016) 616.
88 SWD (2017) 157.

4.3. Suradnja EU-a i NATO-a

Nastavljajući se na već ostvaren znatan napredak, EU će produbiti svoju suradnju s NATO-om u području kibersigurnosti, hibridnih prijetnji i obrane, kako je predviđeno u Zajedničkoj izjavi od 8. srpnja 2016.[89]. Prioriteti uključuju poticanje interoperabilnosti s pomoću usklađenih zahtjeva i standarda za kiberobranu, jačanje suradnje u području osposobljavanja i vježbi te usklađivanje zahtjeva za osposobljavanje.

EU i NATO poticat će i suradnju u istraživanjima i inovacijama u području kiberobrane te će nadograđivati postojeće tehničke mehanizme za razmjenu informacija o kibersigurnosti između svojih tijela za kibersigurnost[90]. Nedavne zajedničke napore usmjerene na suzbijanje hibridnih prijetnji, posebno suradnju između jedinice EU-a za otkrivanje hibridnih prijetnji i jedinice NATO-a za analizu hibridnih prijetnji, trebalo bi dodatno iskoristiti za jačanje otpornosti i odgovora na kiberkrize. Daljnja suradnja između EU-a i NATO-a poticat će se s pomoću vježbi kiberobrane u kojima će sudjelovati ESVD i drugi subjekti EU-a i njihovi partneri u NATO-u, uključujući NATO-ov Centar izvrsnosti za suradnju u području kiberobrane u Tallinnu. NATO i EU prvi će put istodobno provoditi usporedne i koordinirane vježbe kao odgovor na hibridni scenarij. NATO će početi prvi 2017., a EU 2018. Sljedeće izvješće o suradnji između EU-a i NATO-a, koje se u prosincu 2017. podnosi odgovarajućim vijećima, bit će prilika da se razmotriti mogućnost daljnjeg širenja suradnje, posebno osiguravanjem zajedničkih, sigurnih i pouzdanih načina komunikacije među svim relevantnim institucijama i tijelima, uključujući ENISA-u.

Ključne mjere

- provedba strateškog okvira za sprječavanje sukoba i stabilnost u kiberprostoru;
- razvoj nove mreže za jačanje sposobnosti u cilju podupiranja sposobnosti trećih zemalja za suočavanje s kiberprijetnjama i Smjernice EU-a o jačanju sposobnosti u području kibersigurnosti kako bi se bolje odredili prioriteti za aktivnosti EU-a;
- daljnja suradnja između EU-a i NATO-a, uključujući sudjelovanje u usporednim i koordiniranim vježbama i pojačanu interoperabilnost kibersigurnosnih normi.

5. ZAKLJUČAK

Pripravnost EU-a za kibernapade od ključne je važnosti za jedinstveno digitalno tržište i našu obrambenu i sigurnosnu uniju. Nužno moramo poboljšati europsku kibersigurnost i suzbiti prijetnje protiv civilnih i vojnih ciljeva.

Idući digitalni sastanak na vrhu koji estonsko predsjedništvo organizira 29. rujna 2017. prilika je da se pokaže zajednička odlučnost u stavljanju kibersigurnosti u središte EU-a kao digitalnog društva. Kao dio te zajedničke obveze Komisija poziva države članice da se izjasne oko toga kako planiraju djelovati u područjima koja su prvenstveno u njihovoj nadležnosti. To bi trebalo uključivati jačanje kibersigurnosti:

- osiguravanjem potpune i učinkovite provedbe Direktive NIS do 9. svibnja 2018.i resursa koji su nadležnim tijelima za kibersigurnost potrebni za učinkovito izvršavanje njihovih zadaća;
- primjenom istih pravila na javne uprave s obzirom na ulogu koju imaju u društvu i gospodarstvu u cjelini;

[89] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/

[90] CERT-EU i NATO-ova jedinica za odgovor na računalne incidente (NCIRC).

- pružanjem osposobljavanja povezanog s kibersigurnošću u javnoj upravi;
- davanjem prednosti osvješćivanju o kibersigurnosti u informativnim kampanjama i uključivanjem kibersigurnosti u kurikulume za akademsko obrazovanje i strukovno osposobljavanje;
- iskorištavanjem inicijativa o „stalnoj strukturiranoj suradnji" (PESCO) i Europskog fonda za obranu za potporu razvoju projekata kiberobrane.

U ovoj Zajedničkoj komunikaciji utvrđen je opseg izazova i raspon mjera koje EU može poduzeti. Treba nam Europa koja je otporna i koja može učinkovito zaštiti građane predviđanjem mogućih kiberincidenata, uvođenjem snažne zaštite u svoje strukture i ponašanje, brzim oporavkom od kibernapada i odvraćanjem počinitelja. U ovoj Komunikaciji predlažu se ciljane mjere kojima će se na koordinirani način dodatno osnažiti kibersigurnosne strukture i sposobnosti EU-a, uz potpunu suradnju država članica i raznih uključenih struktura EU-a i poštovanje njihovih nadležnosti i odgovornosti. Njezinom provedbom jasno će se pokazati da će EU i države članice zajedno raditi na uspostavi standarda kibersigurnosti koji je primjeren sve većim izazovima s kojima se Europa danas suočava.