Vijeće
Europske unije

Bruxelles, 16. prosinca 2020.
(OR. en)

14133/20

Međuinstitucijski predmet:
2020/0305(NLE)

CYBER 280	RECH 529
JAI 1118	COMPET 642
JAIEX 121	IND 273
EJUSTICE 107	COTER 115
COSI 254	ENFOPOL 350
DATAPROTECT 154	COPS 485
COPEN 387	MI 578
TELECOM 269	IXIM 139
PROCIV 99	POLMIL 201
CSC 367	HYBRID 48
CIS 65	CSCI 96
RELEX 1019	POLGEN 234

POPRATNA BILJEŠKA

Od:	Secretary-General of the European Commission, signed by Mrs Martine DEPREZ, Director
Datum primitka:	16. prosinca 2020.
Za:	Jeppe TRANHOLM-MIKKELSEN, glavni tajnik Vijeća Europske unije
Br. dok. Kom.:	JOIN(2020) 18 final
Predmet:	ZAJEDNIČKA KOMUNIKACIJA EUROPSKOM PARLAMENTU I VIJEĆU Strategija EU-a za kibersigurnost za digitalno desetljeće

Za delegacije se u prilogu nalazi dokument JOIN(2020) 18 final.

Priloženo: JOIN(2020) 18 final

EUROPSKA
KOMISIJA

VISOKI PREDSTAVNIK
UNIJE ZA VANJSKE
POSLOVE I
SIGURNOSNU POLITIKU

Bruxelles, 16.12.2020.
JOIN(2020) 18 final

ZAJEDNIČKA KOMUNIKACIJA EUROPSKOM PARLAMENTU I VIJEĆU

Strategija EU-a za kibersigurnost za digitalno desetljeće

ZAJEDNIČKA KOMUNIKACIJA EUROPSKOM PARLAMENTU I VIJEĆU

Strategija EU-a za kibersigurnost za digitalno desetljeće

I. UVOD: KIBERSIGURNA DIGITALNA TRANSFORMACIJA U OKRUŽENJU SLOŽENIH PRIJETNJI

Kibersigurnost je sastavni dio sigurnosti Europljana. Bez obzira na to je li riječ o povezanim uređajima, elektroenergetskim mrežama ili bankama, avionima, javnim upravama ili bolnicama kojima se koriste, ljudi zaslužuju da pritom budu zaštićeni od kiberprijetnji. Gospodarstvo, demokracija i društvo Unije više nego ikad prije ovise o sigurnim i pouzdanim digitalnim alatima i povezivosti. Kibersigurnost je stoga ključna za izgradnju otporne, zelene i digitalne Europe.

Promet, energetika i zdravstvo, telekomunikacije, financije, sigurnost, demokratski procesi, svemirski sektor i obrana uvelike ovise o sve povezanijim mrežnim i informacijskim sustavima. Uzajamna ovisnost sektora veoma je velika jer mreže i informacijski sustavi ovise o stalnoj opskrbi električnom energijom kako bi funkcionirali. Povezanih uređaja već je više od ljudi na planetu, a predviđa se da će ih do 2025. biti 25 milijardi[1], od toga četvrtina u Europi. Digitalizaciju obrazaca rada ubrzala je pandemija bolesti COVID-19, tijekom koje je 40 % radnika u Uniji prešlo na rad na daljinu, što će vjerojatno imati trajne posljedice za svakodnevni život[2]. To povećava osjetljivost na kibernapade[3]. Povezani predmeti često se dostavljaju potrošačima s poznatim slabim točkama, što dodatno povećava prostor za napad zlonamjernim kiberaktivnostima[4]. Industrijski sektor EU-a sve je više digitaliziran i povezan; to znači i da kibernapadi mogu imati daleko veći utjecaj na industriju i ekosustave nego ikad prije.

Prijetnje dodatno pogoršavaju geopolitičke napetosti zbog globalnog i otvorenog interneta te kontrole nad tehnologijama u cijelom lancu opskrbe[5]. Zbog tih napetosti sve više država podiže digitalne granice. Ograničenja interneta i na internetu ugrožavaju globalni i otvoreni kiberprostor, kao i vladavinu prava, temeljna prava, slobodu i demokraciju, što su temeljne vrijednosti EU-a. Kiberprostor se sve više iskorištava u političke i ideološke svrhe, a povećana polarizacija na međunarodnoj razini ometa učinkovit multilateralizam. Hibridne

[1] Procijenilo trgovinsko udruženje za telekomunikacije GSMA; https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf. Međunarodna korporacija za podatke predviđa 42,6 milijardi povezanih strojeva, senzora i kamera; https://www.idc.com/getdoc.jsp?containerId=prUS45213219

[2] U anketi provedenoj u lipnju 2020. 47 % voditelja poduzeća izjavilo je da namjerava dopustiti zaposlenicima rad na daljinu u punom radnom vremenu čak i kad se omogući povratak na radno mjesto; 82 % ih je namjeravalo omogućiti rad na daljinu barem dio vremena; https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time

[3] https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

[4] Zlonamjerni softver Mirai, jedan od dosad najštetnijih, stvorio je botnete s više od 600 000 uređaja koji su ometali više velikih internetskih stranica u Europi i Sjedinjenim Američkim Državama.

[5] Uključujući elektroničke komponente, analizu podataka, oblak, brže i pametnije mreže s 5G ili naprednijom tehnologijom, šifriranje, umjetnu inteligenciju te nove paradigme za računalstvo i pouzdanu obradu podataka kao što su lanac blokova, pomak s računalstva u oblaku na računalstvo na rubu te kvantno računalstvo.

prijetnje kombinacija su kampanja dezinformiranja i kibernapada na infrastrukturu, gospodarske procese i demokratske institucije, pri čemu postoji mogućnost nanošenja fizičke štete, nezakonitog pristupa osobnim podacima, krađe industrijskih ili državnih tajni, širenja nepovjerenja i slabljenja socijalne kohezije. Tim se aktivnostima narušavaju međunarodna sigurnost i stabilnost te prednosti koje kiberprostor osigurava za gospodarski, društveni i politički razvoj.

Usmjeravanje zlonamjernih aktivnosti na ključnu infrastrukturu velik je globalni rizik[6]. Internet ima decentraliziranu arhitekturu bez središnje strukture i njime upravlja mnogo dionika. Iako je stalna meta zlonamjernih pokušaja ometanja, uspijeva održati eksponencijalan porast prometa[7]. Istodobno se sve više povećava oslanjanje na osnovne funkcije globalnog i otvorenog interneta, kao što su sustav naziva domena (DNS) te ključne internetske usluge za komunikaciju i smještaj na poslužitelju, aplikacije i podatke. Te su usluge sve koncentriranije u rukama nekoliko privatnih poduzeća[8]. Zbog toga su europsko gospodarstvo i društvo osjetljivi na disruptivne geopolitičke ili tehničke događaje koji utječu na osnovu interneta ili na jedno ili više tih poduzeća. Povećana upotreba interneta i promjenjivi obrasci zbog pandemije dodatno su razotkrili krhkost opskrbnih lanaca koji ovise o toj digitalnoj infrastrukturi.

Zabrinutost u pogledu sigurnosti uvelike odvraća od korištenja internetskim uslugama[9]**.** Oko 40 % korisnika iz Unije suočilo se sa sigurnosnim problemima, a 60 % ih smatra da se ne mogu zaštititi od kiberkriminaliteta[10]. U posljednje je tri godine trećina ispitanika primila lažnu elektroničku poštu ili telefonske pozive u kojima se traže osobni podaci, ali njih 83 % nikada nije prijavilo kiberkriminalitet. Svako osmo poduzeće bilo je izloženo kibernapadima[11]. Više od polovine računala poduzeća i potrošača koja su se zarazila zlonamjernim softverom ponovno se zarazi tijekom iste godine[12]. Svake se godine zbog povreda podataka izgubi stotine milijuna podatkovnih zapisa; prosječni trošak povrede za jedno poduzeće povećao se 2018. na više od 3,5 milijuna EUR[13]. Posljedice kibernapada

[6] Svjetski gospodarski forum, *Global Risks Report 2020* (Izvješće o globalnim rizicima za 2020.).

[7] Prema podacima Organizacije za gospodarsku suradnju i razvoj, internetski je promet zbog pandemije porastao za 60 %; https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/. Tijelo europskih regulatora za elektroničke komunikacije i Komisija redovito objavljuju izvješća o stanju internetskih kapaciteta tijekom mjera izolacije zbog koronavirusa. Prema izvješću Agencije Europske unije za mrežnu i informacijsku sigurnost (ENISA), u trećem tromjesečju 2019. ukupno je bilo 241 % više distribuiranih napada uskraćivanjem usluga (DDoS) nego u trećem tromjesečju 2018. DDoS napadi sve su jači, a najveći se dogodio u veljači 2020. uz vršno opterećenje prometa od 2,3 terabita u sekundi. U slučaju „ispada CenturyLinka" u kolovozu 2020. problem usmjeravanja kod pružatelja internetskih usluga u SAD-u prouzročio je pad globalnog internetskog prometa za 3,5 %; https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service

[8] Internet Society, *The Global Internet Report: Consolidation in the Internet Economy* (Globalno izvješće o internetu: konsolidacija internetskog gospodarstva); https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/

[9] https://data.europa.eu/euodp/hr/data/dataset/S2249_92_2_499_ENG

[10] Indeks digitalnog gospodarstva i društva za 2020.; https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020; https://data.europa.eu/euodp/hr/data/dataset/S2249_92_2_499_ENG

[11] Eurostatovo priopćenje za medije, *ICT security measures taken by vast majority of enterprises in the EU* (Sigurnosne mjere u području informacijskih i komunikacijskih tehnologija koje je poduzela većina poduzeća u EU-u), 6/2020, 13. siječnja 2020. „Kibernapadi na ključnu infrastrukturu postali su nova normalna pojava u sektorima kao što su energetika, zdravstvo i promet"; Svjetski gospodarski forum, *The Global Risks Report 2020* (Izvješće o globalnim rizicima za 2020.).

[12] Izvor: Comparitech.

[13] *Annual Cost of a Data Breach Report* (Godišnje izvješće o troškovima povrede podataka), 2020., Institut Ponemon, i na temelju kvantitativne analize 524 nedavne povrede u 17 geografskih područja i 17 sektora;

često se ne mogu izolirati pa mogu izazvati lančane reakcije u cijelom gospodarstvu i društvu, što utječe na milijune pojedinaca[14].

Istrage gotovo svih vrsta kaznenih djela imaju digitalnu komponentu. U 2019. zabilježeno je da se broj incidenata u odnosu na prethodnu godinu utrostručio. Procjenjuje se da postoji 700 milijuna novih primjera zlonamjernog softvera, najčešćeg načina izvedbe kibernapada[15]. Procjenjuje se da će 2020. godišnji trošak kiberkriminaliteta za svjetsko gospodarstvo iznositi 5,5 bilijuna EUR, dvostruko više nego 2015.[16] To je najveći prijenos ekonomskog bogatstva u povijesti, veći i od svjetske trgovine drogom. U slučaju velikog napada ucjenjivačkim softverom WannaCry 2017. trošak za svjetsko gospodarstvo procijenjen je na više od 6,5 milijardi EUR[17].

Digitalne usluge i financijski sektor uz javni su sektor i proizvodnju među najčešćim metama kibernapada, no pripravnost i informiranost poduzeća i pojedinaca kad je riječ o kibersigurnosti i dalje je niska[18], a radnicima nedostaju vještine u tom području[19]. Tijekom 2019. zbilo se gotovo 450 kiberincidenata koji su uključivali europsku ključnu infrastrukturu kao što su financije i energetika[20]. Zdravstvene organizacije i zdravstveni djelatnici posebno su teško pogođeni tijekom pandemije. Budući da tehnologija postaje neraskidivo povezana s fizičkim svijetom, kibernapadi ugrožavaju živote i dobrobit najranjivijih skupina[21]. Više od dvije trećine poduzeća, posebno malih i srednjih (MSP), smatra se „početnicima" u području kibersigurnosti, a smatra se i da su europska poduzeća slabije pripremljena od onih u Aziji i Americi[22]. Procjenjuje se da je u Europi još nepopunjeno 291 000 radnih mjesta stručnjaka za kibersigurnost. Zapošljavanje i osposobljavanje stručnjaka za kibersigurnost spor je proces pa su organizacije izložene većim kibersigurnosnim rizicim[23].

Nedostatan kolektivni pregled situacije s kiberprijetnjama u EU-u. Razlog je tome što nacionalna tijela sustavno ne prikupljaju i ne dijele informacije, primjerice iz privatnog

---

https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

[14] Izvješće Zajedničkog istraživačkog centra (JRC), *Cybersecurity – our digital anchor* (Kibersigurnost, naše digitalno sidro); https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor

[15] Izvor: AV-TEST, https://www.av-test.org/en/statistics/malware/

[16] JRC, *Cybersecurity – Our Digital Anchor* (Kibersigurnost, naše digitalno sidro).

[17] Izvor: Cyence.

[18] Razina informiranosti poduzeća i dalje je niska i kad je riječ o kiberkrađi poslovnih tajni, osobito među MSP-ovima. (PwC, *Study on the scale and impact of industrial espionage and theft of trade secrets through cyber: Dissemination report on measures to tackle and prevent cyber-theft of trade secrets* (Istraživanje opsega i posljedica industrijske špijunaže i krađa poslovnih tajni kiberdjelovanjem: Izvješće o širenju informacija o mjerama za suzbijanje i sprečavanje kiberkrađe poslovnih tajni), 2018.)

[19] Vidjeti *ENISA Threat Landscape 2020* (ENISA-ino izvješće o okruženju prijetnji za 2020.). Također, *Verizon Data Breach Investigations Report 2020* (Verizonovo izvješće o istragama povrede podataka za 2020.); https://enterprise.verizon.com/resources/reports/dbir/

[20] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f

[21] Meta ucjenjivačkih softvera bile su bolnice i zdravstvene evidencije, npr. u Rumunjskoj (lipanj 2020.), Düsseldorfu (rujan 2020.) i u klinici Vastaamo (listopad 2020.).

[22] PwC, *The Global State of Information Security 2018* (Globalno stanje informacijske sigurnosti za 2018.); ESI Thoughtlab, *The Cybersecurity Imperative* (Imperativ kibersigurnosti), 2019.

[23] Agencija EU-a za kibersigurnost, *Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees and ENISA's Higher Education Database* (Razvoj vještina u području kibersigurnosti u EU-u: certifikacija kibersigurnosnih diploma i ENISA-ina baza podataka visokog obrazovanja), prosinac 2019.

sektora, koje bi mogle pomoći u procjeni stanja kibersigurnosti u EU-u. Države članice prijave samo mali dio incidenata, a razmjena informacija nije ni sustavna ni sveobuhvatna[24]; moguće je da su kibernapadi samo jedan od aspekata usklađenih zlonamjernih napada na europska društva. Trenutačno postoji samo ograničena uzajamna operativna pomoć među državama članicama i nije uspostavljen operativni mehanizam između država članica i institucija, agencija i tijela EU-a u slučaju velikih prekograničnih kiberincidenata ili kiberkrize[25].

Stoga je povećanje kibersigurnosti ključno kako bi ljudi imali povjerenja u inovacije, povezivost i automatizaciju i upotrebljavali ih u svoju korist te kako bi se zaštitila temeljna prava i slobode, među ostalim prava na privatnost i zaštitu osobnih podataka te sloboda izražavanja i informiranja. Kibersigurnost je nužna za mrežnu povezivost te globalni i otvoreni internet koji moraju biti temelj preobrazbe gospodarstva i društva tijekom 2020-ih. Pridonosi boljim i brojnijim poslovima, fleksibilnijim radnim mjestima, učinkovitijem i održivijem prometu i poljoprivredi te lakšem i pravednijem pristupu zdravstvenim uslugama. Ključna je i za prelazak na čišću energiju u okviru europskog zelenog plana[26] s pomoću prekograničnih mreža i pametnih brojila te izbjegavanjem nepotrebnog udvostručivanja pohrane podataka. Naposljetku, od ključne je važnosti za međunarodnu sigurnost i stabilnost te razvoj gospodarstava, demokracija i društava diljem svijeta. Države, poduzeća i pojedinci stoga moraju upotrebljavati digitalne alate odgovorno i vodeći računa o sigurnosti. Informiranost o kibersigurnosti i kiberhigijena moraju biti temelj digitalne transformacije svakodnevnih aktivnosti.

Nova strategija EU-a za kibersigurnost za digitalno desetljeće ključna je sastavnica Komunikacije Komisije „Izgradnja digitalne budućnosti Europe”[27], Komisijina europskog plana oporavka[28], Strategije za sigurnosnu uniju za razdoblje 2020.–2025.[29], Globalne strategije EU-a za vanjsku i sigurnosnu politiku[30] i Strateškog programa Europskog vijeća za razdoblje 2019.–2024.[31] Novom se strategijom utvrđuje kako će Unija zaštititi svoje građane, poduzeća i institucije od kiberprijetnji te unaprijediti međunarodnu suradnju i preuzeti vodstvo u osiguravanju otvorenog i globalnog interneta.

II. RAZMIŠLJANJE NA GLOBALNOJ, A DJELOVANJE NA EUROPSKOJ RAZINI

Cilj je ove strategije osigurati globalni i otvoreni internet sa snažnim zaštitnim mehanizmima kako bi se uklonili rizici koji prijete sigurnosti i temeljnim pravima i slobodama građana Europe. Na temelju napretka ostvarenog u okviru prethodnih strategija, ova strategija sadržava konkretne prijedloge za uvođenje **triju glavnih instrumenata, odnosno regulatornog i investicijskog instrumenta te instrumenta politike**, za **tri područja djelovanja EU-a**: **(1) otpornost, tehnološka suverenost i vodstvo, (2) izgradnja**

[24] Države članice dužne su skupini za suradnju dostaviti godišnje sažeto izvješće o obavijestima primljenima u skladu s člankom 10. stavkom 3. Direktive o sigurnosti mrežnih i informacijskih sustava (Direktiva (EU) 2016/1148).
[25] Uspostavljeni su standardni operativni postupci za uzajamnu pomoć među članovima mreže timova za odgovor na računalne sigurnosne incidente (CSIRT).
[26] Europski zeleni plan, COM(2019) 640 final.
[27] Izgradnja digitalne budućnosti Europe, COM(2020) 67 final.
[28] Europa na djelu: oporavak i priprema za sljedeću generaciju, COM(2020) 98 final.
[29] Strategija EU-a za sigurnosnu uniju za razdoblje 2020.–2025., COM(2020) 605 final.
[30] https://eeas.europa.eu/topics/eu-global-strategy_en
[31] https://www.consilium.europa.eu/en/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/#

operativnog kapaciteta za sprečavanje, odvraćanje i odgovor te (3) unapređenje globalnog i otvorenog kiberprostora. EU predano podupire tu strategiju **nezapamćenom razinom ulaganja u digitalnu tranziciju EU-a u sljedećih sedam godina**, koja bi mogla biti četverostruko veća od prethodnih razina, u okviru novih tehnoloških i industrijskih politika i programa oporavka[32].

Kibersigurnost se, primjenom poticaja, obveza i referentnih vrijednosti, mora uključiti u sva ta digitalna ulaganja, posebno ulaganja u ključne tehnologije kao što su umjetna inteligencija, šifriranje i kvantno računalstvo. To može potaknuti rast europskog kibersigurnosnog sektora i pružiti sigurnost potrebnu za postupno ukidanje naslijeđenih sustava. Europskim fondom za obranu (EDF) poduprijet će se europska rješenja u području kiberobrane kao dio europske obrambene tehnološke i industrijske baze. Kibersigurnost je uključena u vanjske financijske instrumente kojima se podupiru naši partneri, posebno u Instrument za susjedstvo, razvoj i međunarodnu suradnju. Sprečavanjem zlouporabe tehnologija, zaštitom ključne infrastrukture i osiguravanjem cjelovitosti opskrbnih lanaca omogućuje se i da Unija poštuje UN-ove standarde, pravila i načela odgovornog ponašanja država[33].

1. OTPORNOST, TEHNOLOŠKA SUVERENOST I VODSTVO

Ključna infrastruktura i ključne usluge EU-a sve su više međuovisne i digitalizirane. Sve stvari povezane s internetom u EU-u, bez obzira na to je li riječ o automatiziranim automobilima, industrijskim nadtornim sustavima ili kućanskim aparatima, te cijeli opskrbni lanci kojima ih se stavlja na raspolaganje moraju biti sigurni, otporni na kiberincidente i mora ih se moći brzo popraviti kad se otkriju slabe točke. To je ključno kako bi se privatnom i javnom sektoru Unije omogućio izbor među najsigurnijim infrastrukturama i uslugama. U nadolazećem desetljeću EU može postati predvodnik u razvoju sigurnih tehnologija u cijelom lancu opskrbe. Stvaranje otpornosti te podizanje industrijskih i tehnoloških kapaciteta u području kibersigurnosti trebalo bi mobilizirati sve potrebne regulatorne i investicijske instrumente te instrumente politike. Kibersigurnošću integriranom u industrijske procese, aktivnosti i uređaje mogu se ublažiti rizici te potencijalno smanjiti troškovi poduzećima i širem društvu, što će povećati otpornost.

1.1. Otporna infrastruktura i ključne usluge

Pravila EU-a o sigurnosti mrežnih i informacijskih sustava (NIS) ključna su za jedinstveno tržište kibersigurnosti. Komisija predlaže reformu tih pravila u okviru revidirane Direktive o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (Direktiva NIS) kako bi se povećala **kiberotpornost svih relevantnih javnih i privatnih sektora koji obavljaju funkcije bitne za gospodarstvo i društvu[34]**. Preispitivanje je potrebnao kako bi se smanjile nedosljednosti na unutarnjem tržištu

[32] Ulaganja u cijeli opskrbni lanac digitalne tehnologije, radi potpore digitalnoj tranziciji ili svladavanju s njom povezanih izazova, trebala bi iznositi najmanje 20 %, odnosno 134,5 milijardi EUR, od 672,5 milijardi EUR osiguranih Mehanizmom za oporavak i otpornost, u obliku bespovratnih sredstava i zajmova. U višegodišnjem financijskom okviru za razdoblje 2021.–2027. financiranje EU-a predviđeno za kibersigurnost u sklopu programa Digitalna Europa i za istraživanja u području kibersigurnosti u okviru programa Obzor Europa, s posebnim naglaskom na potporu malim i srednjim poduzećima, ukupno bi moglo iznositi 2 milijarde EUR, uz ulaganja država članica i industrije.

[33] https://undocs.org/A/70/174

[34] [*unijeti upućivanje na prijedlog NIS-a*]

usklađivanjem područja primjene, zahtjeva u pogledu sigurnosti i izvješćivanja o incidentima, nacionalnog nadzora i provedbe te sposobnosti nadležnih tijela.

Reformiranom Direktivom NIS dobit će se temelj za podrobnija pravila, koja su potrebna i za strateški važne sektore, uključujući energetiku, promet i zdravstvo. Kako bi se osigurao dosljedan pristup najavljen u okviru Strategije za sigurnosnu uniju za razdoblje 2020.–2025., uz reformu direktive predlaže se i preispitivanje propisa o otpornosti ključne infrastrukture[35]. Energetske tehnologije s digitalnim komponentama i sigurnost povezanih opskrbnih lanaca važni su za kontinuitet osnovnih usluga i za strateški nadzor ključne energetske infrastrukture. Komisija će stoga predložiti mjere, uključujući „mrežni kodeks" kojim se utvrđuju pravila za kibersigurnost u prekograničnim tokovima električne energije, koje bi trebalo donijeti do kraja 2022. Komisijin je prijedlog i da financijski sektor mora ojačati digitalnu operativnu otpornost te biti sposoban izdržati sve vrste poremećaja i prijetnji povezanih s informacijskim i komunikacijskim tehnologijama[36]. Kad je riječ o prometu, Komisija je dodala odredbe o kibersigurnosti[37] u propise EU-a o zaštiti zračnog prometa te će i dalje raditi na povećanju kiberotpornosti svih vrsta prometa. Jačanje kiberotpornosti **demokratskih procesa i institucija** ključna je sastavnica akcijskog plana za europsku demokraciju u cilju zaštite i promicanja slobodnih izbora te demokratske rasprave i pluralizma medija[38]. Naposljetku, kad je riječ o sigurnosti infrastrukture i usluga u okviru budućeg svemirskog programa, Komisija će nastaviti s razradom strategije za kibersigurnost programa Galileo za sljedeću generaciju usluga globalnog navigacijskog satelitskog sustava i drugih novih elemenata svemirskog programa[39].

1.2. Izgradnja europskog kiberštita

S obzirom na širenje povezivosti i sve sofisticiranije kibernapade, centri za razmjenu i analizu informacija (ISAC) imaju važnu funkciju, među ostalim na sektorskoj razini, u omogućavanju razmjene informacija o kiberprijetnjama među različitim dionicima[40]. Osim toga, mreže i računalni sustavi zahtijevaju stalno praćenje i analizu kako bi se u stvarnom vremenu otkrili prodori i nepravilnosti. Mnoga privatna poduzeća, javne organizacije i nacionalna tijela osnovali su stoga timove za odgovor na računalne sigurnosne incidente (CSIRT) i centre za sigurnosne operacije (SOC).

Centri za sigurnosne operacije ključni su za prikupljanje evidencija[41] i izoliranje sumnjivih događaja koji se pojavljuju na komunikacijskim mrežama koje nadziru. To čine utvrđivanjem signala i uzoraka te izvlačenjem informacija o prijetnjama iz velikih količina podataka koje je potrebno procijeniti. Doprinijeli su otkrivanju aktivnosti zlonamjernih programa te time pomogli obuzdati kibernapade. Rad u tim centrima vrlo je zahtjevan i brz, zbog čega umjetna

[35] [unijeti upućivanje na *prijedlog* direktive o otpornosti ključnih subjekata].
[36] Prijedlog uredbe o digitalnoj operativnoj otpornosti za financijski sektor i o izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014 i (EU) br. 909/2014, COM(2020) 595 final.
[37] Provedbena uredba Komisije 2019/1583.
[38] Komunikacija o akcijskom planu za europsku demokraciju, COM(2020) 790 final. Prema planu, u okviru europske mreže za suradnju u području izbora izborne mreže država članica podupirat će djelovanje zajedničkih stručnih timova za suzbijanje prijetnji izbornim procesima, uključujući kiberprijetnje; https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en
[39] To uključuje novu inicijativu za državne satelitske komunikacije (GOVSATCOM) i svemirski otpad (SST).
[40] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing
[41] Tako da ih tijela kaznenog progona i sudstvo mogu upotrijebiti kao dokaz.

inteligencija i posebno tehnike strojnog učenja mogu pružiti neprocjenjivu potporu stručnjacima[42].

Komisija predlaže izgradnju **mreže centara za sigurnosne operacije diljem EU-a**[43] te potporu poboljšanju postojećih i uspostavi novih centara. Podupirat će i osposobljavanje i razvoj vještina osoblja koje upravlja tim centrima. Na temelju analize potreba provedene s relevantnim dionicima i uz potporu Agencije EU-a za kibersigurnost (ENISA), Komisija bi mogla izdvojiti više od 300 milijuna EUR za potporu javno-privatnoj i prekograničnoj suradnji u stvaranju nacionalnih i sektorskih mreža, uključujući i MSP-ove, na temelju odgovarajućih odredbi o upravljanju, razmjeni podataka i sigurnosti.

Države članice potiču se na zajedničko ulaganje u taj projekt. Centri bi tada mogli učinkovitije razmjenjivati i povezivati otkrivene signale te stvarati visokokvalitetne obavještajne podatke o prijetnjama i slati ih ISAC-ima i nacionalnim tijelima, što bi omogućilo potpuniji pregled situacije Cilj bi bio u fazama povezati što više centara diljem EU-a kako bi se prikupilo zajedničko znanje i razmjenjivali primjeri dobre prakse. Tim će se centrima pružiti potpora za poboljšanje otkrivanja i analize incidenata te za brži odgovor na njih s pomoću najsuvremenijih tehnologija umjetne inteligencije i strojnog učenja nadopunjenih superračunalnom infrastrukturom koju je u EU-u razvilo Zajedničko poduzeće za europsko računalstvo visokih performansi[44].

U okviru trajne suradnje ta će mreža tijela i svi zainteresirani dionici, uključujući zajedničku jedinicu za kibersigurnost (vidjeti odjeljak 2.1.), dobivati pravodobna upozorenja o kiberincidentima. **Služit će kao pravi kibersigurnosni štit EU-a**, s čvrstom mrežom kontrolnih točaka, koji će moći otkriti potencijalne prijetnje prije nego što uzrokuju veliku štetu.

1.3. Ultrasigurna komunikacijska infrastruktura

Državne satelitske komunikacije Europske unije[45], sastavnica svemirskog programa, pružat će sigurne i ekonomične komunikacijske kapacitete koji se temelje na svemirskoj tehnologiji radi zaštite sigurnosno kritičnih misija i operacija koje vode EU i njegove države članice, uključujući aktere nacionalne sigurnosti te institucije, tijela i agencije EU-a.

Države članice obvezale su se surađivati s Komisijom na uvođenju sigurne kvantne komunikacijske infrastrukture (QCI) za Europu[46]. QCI će javnim tijelima omogućiti potpuno nov način prijenosa povjerljivih informacija, u kojem se koristi ultrasiguran oblik šifriranja za zaštitu od kibernapada ostvaren europskom tehnologijom. Imat će dvije glavne sastavnice:

[42] Izvor: istraživanje Instituta Ponemon, *Improving the Effectiveness of the SOC* (Poboljšanje učinkovitosti SOC-a), 2019.; za studije o korištenju umjetne inteligencije u centrima za sigurnosne operacije vidjeti na primjer: Khraisat, A., Gondal, I., Vamplew, P. *et al., Survey of intrusion detection systems: techniques, datasets and challenges* (Studija o sustavima za otkrivanje neovlaštenog ulaska: tehnike, skupovi podataka i izazovi), *Cybersecur* 2, 20 (2019.).

[43] Razvit će se detaljniji mehanizmi za upravljanje, načela rada i financiranje tih centara te način na koji će dopuniti postojeće strukture kao što su digitalnoinovacijski centri.

[44] https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking

[45] GOVSATCOM je sastavnica svemirskog programa Unije.

[46] Deklaraciju o europskoj kvantnoj komunikacijskoj infrastrukturi (EuroQCI) dosad je potpisala većina država članica, a razvoj i uvođenje infrastrukture će se u razdoblju 2021.–2027. financirati sredstvima programa Obzor Europa i Digitalna Europa te Europske svemirske agencije, ovisno o odgovarajućim mehanizmima upravljanja; https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network

postojeće zemaljske svjetlovodne komunikacijske mreže koje povezuju strateške lokacije na nacionalnoj i prekograničnoj razini te povezane svemirske satelite koji pokrivaju cijelu Uniju, uključujući njezina prekomorska područja[47]. Ta inicijativa za razvoj i uvođenje novih i sigurnijih oblika šifriranja te razvijanje novih načina zaštite ključne komunikacije i podataka može pomoći u zaštiti osjetljivih informacija, a time i ključnih infrastruktura.

U tom kontekstu, a i šire, Komisija će istražiti mogućnost uvođenja višeorbitalnog sustava sigurne povezivosti. Temeljio bi se na GOVSATCOM-u i QCI-ju i objedinio bi najsuvremenije tehnologije (kvantna tehnologija, 5G, umjetna inteligencija, računalstvo na rubu) u skladu s najrestriktivnijim kibersigurnosnim okvirom, a omogućivao bi sigurne usluge kao što su pouzdana, sigurna i ekonomična povezivost te šifrirana komunikacija za ključne državne aktivnosti.

1.4. Sigurnost sljedeće generacije širokopojasnih pokretnih mreža

Građani i poduzeća Unije koji upotrebljavaju napredne i inovativne aplikacije omogućene **5G mrežom i mrežama budućih generacija** trebali bi imati koristi od najviših sigurnosnih standarda. Države članice i Komisija, uz potporu ENISA-e, zajedno su izradile paket mjera EU-a za 5G[48] iz siječnja 2020., sveobuhvatan i objektivan pristup kibersigurnosti 5G mreža koji se temelji na procjeni mogućih planova smanjenja rizika i utvrđivanju najdjelotvornijih mjera. Usto, Unija konsolidira kapacitete u području 5G mreža i šire kako bi izbjegla ovisnost i potaknula održiv i raznolik lanac opskrbe.

Komisija je u prosincu 2020. objavila izvješće o učincima Preporuke od 26. ožujka 2019. o kibersigurnosti 5G mreža[49]. U izvješću se navodi da je od dogovora o paketu mjera postignut znatan napredak te da je većina država članica na dobrom putu da provede mjere iz paketa u bliskoj budućnosti, iako postoje određene razlike i nedostaci koji su već utvrđeni u izvješću o napretku iz srpnja 2020.[50]

U listopadu 2020. Europsko vijeće pozvalo je EU i države članice da „u potpunosti iskoriste paket instrumenata za kibersigurnost mreža 5G" i da „primijene relevantna ograničenja na visokorizične dobavljače za ključna sredstva koja su u koordiniranim procjenama rizika EU-a definirana kao kritična i osjetljiva"[51].

EU i njegove države članice trebali bi u budućnosti osigurati primjereno i koordinirano smanjivanje utvrđenih rizika, posebno u pogledu cilja smanjenja izloženosti visokorizičnim dobavljačima i izbjegavanja ovisnosti o njima na nacionalnoj razini i razini Unije, te osigurati

[47] Razvoj svemirske komponente nužan je za uspostavljanje veza između dviju točaka na velikim udaljenostima (> 1 000 km), koje zemaljska infrastruktura ne može podržavati. Iskorištavanjem svojstava kvantne mehanike, QCI će u početku strankama omogućiti sigurnu razmjenu nasumičnih tajnih ključeva za šifriranje i dešifriranje poruka. Uključivat će i uvođenje infrastrukture za testiranje i sukladnost, koja će služiti za ocjenjivanje sukladnosti europskih uređaja i sustava za kvantnu komunikaciju s QCI-jem te certifikaciju i potvrđivanje tih uređaja i sustava prije njihove integracije u QCI. Bit će izveden tako da podržava dodatne aplikacije kad dosegnu potrebnu razinu tehnološke zrelosti. Trenutačni pokusni projekt OpenQKD (https://openqkd.eu/) prethodnik je te infrastrukture za testiranje i sukladnost.

[48] Komunikacija Komisije „Sigurno uvođenje 5G mreža u EU-u – Provedba paketa instrumenata EU-a", COM(2020) 50 final.

[49] Izvješće Komisije o učincima Preporuke Komisije od 26. ožujka 2019. o kibersigurnosti 5G mreža, 15. prosinca 2020.

[50] Izvješće Skupine za suradnju u području mrežne i informacijske sigurnosti o provedbi paketa mjera od 24. srpnja 2020.

[51] EUCO 13/20, izvanredni sastanak Europskog vijeća (1. i 2. listopada 2020.) – zaključci.

da se u obzir uzimaju sve nove znatne promjene ili rizici. Pozivaju se države članice da u potpunosti iskoriste te mjere za svoja ulaganja u digitalne kapacitete i povezivost.

Na temelju izvješća o učincima Preporuke iz 2019., Komisija potiče države članice da ubrzaju rad na dovršetku provedbe glavnih mjera iz paketa do drugog tromjesečja 2021. Poziva ih i da nastave zajednički pratiti ostvareni napredak i još više usklađivati pristupe. Na razini Unije nastojat će se ostvariti tri glavna cilja kako bi se podržao taj proces: daljnja konvergencija pristupâ smanjivanju rizika diljem EU-a, podupiranje stalne razmjene znanja i izgradnje kapaciteta te promicanje otpornosti opskrbnih lanca i drugih strateških sigurnosnih ciljeva EU-a. Konkretne mjere povezane s tim ključnim ciljevima navedene su u posebnom dodatku ovoj Komunikaciji.

Komisija će nastaviti blisko surađivati s državama članicama na ostvarivanju tih ciljeva i mjera uz potporu ENISA-e (vidjeti Prilog).

Unijine mjere za 5G pobudile su zanimanje u zemljama izvan EU-a koje trenutačno razvijaju svoje pristupe za zaštitu komunikacijskih mreža. Službe Komisije, u suradnji s Europskom službom za vanjsko djelovanje i mrežom delegacija EU-a, spremne su, na zahtjev, nadležnim tijelima diljem svijeta dati dodatne informacije o svojem sveobuhvatnom i objektivnom pristupu koji se temelji na riziku.

1.5. Internet sigurnih stvari

Svaka povezana stvar ima slabe točke koje se mogu iskoristiti uz potencijalno dalekosežne posljedice. Pravila unutarnjeg tržišta uključuju zaštitne mjere protiv nesigurnih proizvoda i usluga. Komisija već radi na osiguravanju **transparentnih sigurnosnih rješenja i certifikacije u okviru Akta o kibersigurnosti** te na poticanju sigurnih proizvoda i usluga bez ugrožavanja učinkovitosti[52]. Prvi kontinuirani program rada Unije donijet će u prvom tromjesečju 2021. (ažurirat će se najmanje jednom u tri godine) kako bi se industriji, nacionalnim tijelima i tijelima za normizaciju omogućilo da se unaprijed pripreme za buduće europske programe kibersigurnosne certifikacije[53]. S obzirom na to da se internet stvari širi, treba ojačati provediva pravila kako bi se osigurala opća otpornost i povećala kibersigurnost.

Komisija će razmotriti sveobuhvatan pristup, uključujući moguća **nova horizontalna pravila za povećanje kibersigurnosti svih povezanih proizvoda i odgovarajućih usluga na unutarnjem tržištu**[54]. Kad je riječ o softverskim slabim točkama, takva bi pravila mogla uključivati **novu obvezu održavanja za proizvođače povezanih uređaja**, koja podrazumijeva kontinuirano ažuriranje softvera i sigurnosti te, na kraju životnog vijeka, brisanje osobnih i drugih osjetljivih podataka. Tim bi se pravilima ojačala inicijativa „pravo na popravak zastarjelog softvera" predstavljena u akcijskom planu za kružno gospodarstvo i

[52] Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agenciji Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i o stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti). Aktom o kibersigurnosti promiče se IKT certifikacija na razini EU-a primjenom europskog okvira za kibersigurnosnu certifikaciju na temelju kojeg se uspostavljaju dobrovoljni europski programi kibersigurnosne certifikacije radi osiguravanja odgovarajuće kibersigurnosti IKT proizvoda, usluga i procesa u Uniji te smanjenja rascjepkanosti unutarnjeg tržišta u pogledu programa kibersigurnosne certifikacije u Uniji. Uz to, poduzeća za rejting u području kibersigurnosti obično imaju sjedište izvan EU-a pa su njihova transparentnost i nadzor ograničeni; https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings

[53] Propisano člankom 47. stavkom 5. Akta o kibersigurnosti.

[54] U zaključcima Vijeća poziva se na horizontalne mjere za kibersigurnost povezanih uređaja; 13629/20, 2. prosinca 2020.

dopunile mjere za određene vrste proizvoda, kao što su obvezni zahtjevi koji će biti predloženi za pristup tržištu određenih bežičnih proizvoda (donošenjem delegiranog akta na temelju Direktive o radijskoj opremi[55]) te cilj da se pravila o kibersigurnosti za motorna vozila primjenjuju za sve nove tipove vozila od srpnja 2022.[56] Pravila bi se usto temeljila na predloženoj reviziji općih pravila o sigurnosti proizvoda, koja se ne odnose izravno na aspekte kibersigurnosti[57].

1.6. Veća sigurnost globalnog interneta

Skup temeljnih protokola i potporne infrastrukture osigurava funkcionalnost i integritet interneta u cijelom svijetu[58]. Taj skup uključuje DNS i njegov hijerarhijski i delegirani sustav zona, kojem su na vrhu hijerarhije korijenska zona i trinaest korijenskih DNS poslužitelja[59] na koje se oslanja World Wide Web. Komisija namjerava razviti **krizni plan, financiran sredstvima EU-a, za rješavanje ekstremnih scenarija koji utječu na integritet i dostupnost globalnog korijenskog DNS sustava**. Surađivat će s ENISA-om, državama članicama, dvama operaterima korijenskih DNS poslužitelja[60] iz EU-a i širom zajednicom dionika kako bi se ocijenila uloga tih operatera u osiguravanju globalne dostupnosti interneta u svim okolnostima.

Kako bi klijent mogao pristupiti resursu pod određenim nazivom domene na internetu, njegov zahtjev (obično za jedinstveni lokator resursa ili URL) treba pretvoriti ili „prevesti" u IP adresu upućivanjem na DNS poslužitelje. Međutim, građani i organizacije u EU-u sve se više oslanjaju na nekoliko javnih DNS prevoditelja kojima upravljaju subjekti izvan EU-a. Takva konsolidacija DNS prevođenja u rukama nekoliko trgovačkih društava[61] sam postupak prijevoda čini ranjivim u slučaju značajnih događaja koji utječu na jednog velikog pružatelja usluga te tijelima EU-a otežava suzbijanje mogućih zlonamjernih kibernapada i velikih geopolitičkih i tehničkih incidenata[62].

Radi ublažavanja sigurnosnih problema povezanih s tržišnom koncentracijom, Komisija će poticati relevantne dionike, uključujući poduzeća, pružatelje internetskih usluga i proizvođače preglednika iz EU-a da donesu strategiju diversifikacije DNS prevođenja.

---

[55] Direktiva 2014/53/EU.

[56] U skladu s Pravilnikom UN-a donesenim u lipnju 2020.; http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf

[57] Revizija postojećih općih pravila o sigurnosti proizvoda (Direktiva 2001/95/EZ); u planu je i prijedlog prilagođenih pravila o odgovornosti proizvođača u digitalnom kontekstu unutar područja primjene regulatornog okvira EU-a o odgovornosti.

[58] „Javna jezgra otvorenog interneta, odnosno njegovi glavni protokoli i infrastruktura koji su globalno javno dobro, omogućuje temeljnu funkcionalnost interneta i osnova je njegova normalnog funkcioniranja. ENISA bi trebala podupirati sigurnost i stabilnost funkcioniranja javne jezgre otvorenog interneta, uključujući, ali ne ograničavajući se na ključne protokole (posebno DNS, BGP i IPv6), rad sustava naziva domena (kao što je funkcioniranje svih vršnih domena) te rad korijenske zone."; Uvodna izjava 23. Akta o kibersigurnosti.

[59] https://www.iana.org/domains/root/servers

[60] To su i.korijenski poslužitelji kojima upravlja Netnod iz Švedske i k.korijenski poslužitelji kojima upravlja RIPE NCC iz Nizozemske.

[61] *Consolidation in the DNS resolver market – how much, how fast how dangerous?* (Konsolidacija na tržištu DNS prevoditelja – koliko, kojom brzinom i koliko opasno?) (), *Evidence of decreasing Internet entropy – the lack of redundancy in DNS resolution by major websites and services* (Dokazi o smanjivanju entropije interneta – nedostatak redundancije u DNS prevođenju velikih internetskih stranica i servisa) ( ).

[62] Postoje i dokazi da se DNS podaci mogu upotrebljavati za izradu profila, što utječe na prava na privatnost i zaštitu podataka.

Komisija usto namjerava doprinijeti sigurnoj internetskoj povezivosti podupiranjem razvoja javne **europske usluge DNS prevoditelja**. Ta inicijativa, DNS4EU, nudit će alternativnu europsku uslugu za pristup globalnom internetu. DNS4EU bit će transparentan, usklađen s najnovijim tehničkim i integriranim standardima i pravilima u području sigurnosti, zaštite podataka i privatnosti te će biti dio Europskog industrijskog saveza za podatke i oblak[63].

Komisija će, u suradnji s državama članicama i industrijom, **ubrzati prihvaćanje ključnih internetskih standarda, uključujući IPv6[64], te dobro poznatih standarda i dobrih praksi internetske sigurnosti za DNS, usmjeravanje i sigurnost elektroničke pošte[65]**, ne isključujući pritom regulatorne mjere kao što je europska klauzula o vremenskom ograničenju valjanosti za IPv4 kako bi se usmjerilo tržište u slučaju nedovoljnog napretka prema njihovu donošenju. Unija bi trebala (primjerice, u okviru strategije EU-a i Afrike[66]) promicati provedbu tih standarda u partnerskim zemljama kao način podupiranja razvoja globalnog i otvorenog interneta te suzbijanja zatvorenih modela interneta koji se temelje na kontroli. Naposljetku, Komisija će razmotriti potrebu za mehanizmom za sustavnije praćenje i prikupljanje zbirnih podataka o internetskom prometu te za savjetovanjem o mogućim poremećajima[67].

1.7. Veća prisutnost u tehnološkom opskrbnom lancu

S obzirom na planiranu financijsku potporu kibersigurnoj digitalnoj transformaciji u višegodišnjem financijskom okviru za razdoblje 2021.–2027., Unija ima jedinstvenu priliku udružiti resurse kako bi industrijsku strategiju[68] i vodstvo u digitalnim tehnologijama i kibersigurnosti proširila na cijeli digitalni opskrbni lanac (uključujući podatke i računalstvo u oblaku, procesorske tehnologije sljedeće generacije, ultrasigurnu povezivost i 6G mreže), u skladu sa svojim vrijednostima i prioritetima. Intervencija javnog sektora trebala bi se oslanjati na alate predviđene regulatornim okvirom EU-a za javnu nabavu i važnim projektima u zajedničkom europskom interesu. Usto, njome se mogu potaknuti privatna ulaganja putem javno-privatnih partnerstava (među ostalim, na temelju iskustva u ugovornom javno-privatnom partnerstvu u području kibersigurnosti i njegove provedbe preko Europske organizacije za kibersigurnost), poduzetničkog kapitala za potporu MSP-ovima ili industrijskih saveza te strategija za tehnološke kapacitete.

Posebna pozornost posvetit će se i Instrumentu za tehničku potporu[69] te tome da MSP-ovi na najbolji način koriste najnovije kibersigurnosne alate – posebno one koji nisu obuhvaćeni područjem primjene revidirane Direktive NIS – među ostalim provedbom posebnih aktivnosti u okviru digitalnoinovacijskih centara na temelju programa Digitalna Europa. Cilj je

---

[63] Zajednička izjava: Izgradnja nove generacije oblaka za poslovni i javni sektor u EU-u; https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe

[64] Uvođenje protokola IPv6 je uznapredovalo zbog znatne iscrpljenosti ponude i povećanja troškova IPv4 adresa. No njegovo uvođenje u Uniji nije ujednačeno.

[65] Takvi standardi obuhvaćaju DNSSEC, HTTPS, DNS putem HTTPS-a (DoH), DNS putem TLS-a (DoT), SPF, DKIM, DMARC, STARTTLS, DANE te standarde i dobre prakse usmjeravanja, npr. Zajednički dogovorene norme za sigurnost pri usmjeravanju (MANRS).

[66] Zajednička komunikacija „Put prema sveobuhvatnoj strategiji s Afrikom”, 9. ožujka 2020. JOIN(2020) 4 final.

[67] Takav „centar za praćenje interneta” mogao bi biti među aktivnostima Europskog centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja; Prijedlog uredbe o osnivanju Europskog centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja i Mreže nacionalnih koordinacijskih centara, COM(2018) 630 final.

[68] Komunikacija o novoj industrijskoj strategiji za Europu, COM(2020) 102 final.

[69] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=COM:2020:0409:FIN

potaknuti sličan iznos ulaganja država članica, koji bi onda uložio i sektor u okviru partnerstva kojim se zajednički upravlja s državama članicama u predloženom **Centru za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja i Mreži koordinacijskih centara (CCCN)**. CCCN bi trebao imati ključnu ulogu, uz doprinos sektora i akademskih zajednica, u razvoju tehnološke suverenosti EU-a u području kibersigurnosti, izgradnji kapaciteta za osiguravanje osjetljivih infrastruktura kao što je 5G i smanjenju ovisnosti o drugim dijelovima svijeta za najvažnije tehnologije.

Komisija namjerava poduprijeti, možda s CCCN-om, stvaranje posebnog magistarskog studija u području kibersigurnosti i doprinijeti zajedničkom europskom planu za istraživanje i inovacije u području kibersigurnosti nakon 2020. Ulaganja u okviru CCCN-a temeljila bi se i na suradnji u istraživanju i razvoju unutar mreže centara izvrsnosti u području kibersigurnosti, pri čemu bi se najbolji europski istraživački timove povezali sa sektorom radi izrade i provedbe zajedničkih istraživačkih programa, u skladu s planom Europske organizacije za kibersigurnost[70]. Komisija će se i dalje oslanjati na istraživački rad ENISA-e i Europola te će u okviru programa Obzor Europa nastaviti podupirati pojedinačne internetske inovatore koji razvijaju sigurne komunikacijske tehnologije za veću privatnost koje se temelje na softveru i hardveru otvorenog koda, kao što to trenutačno radi u okviru inicijative Internet sljedeće generacije.

1.8. Kvalificirana radna snaga EU-a u području kibersigurnosti

Unijine mjere za usavršavanje radne snage, razvoj, privlačenje i zadržavanje najboljih talenata u području kibersigurnosti te ulaganje u istraživanja i inovacije svjetske klase općenito su važan element zaštite od kiberprijetnji. To područje ima velik potencijal. Stoga se osobita pozornost mora posvetiti razvoju, privlačenju i zadržavanju raznovrsnijih talenata. Revidiranim Akcijskim planom za digitalno obrazovanje poboljšat će se informiranost o kibersigurnosti među građanima, posebice djecom i mladima, te organizacijama, osobito MSP-ovima[71]. Potaknut će se i sudjelovanje žena u obrazovanju u području znanosti, tehnologije, inženjerstva i matematike („STEM") te u unapređivanju digitalnih vještina za IKT poslove. Usto, Komisija će zajedno s Uredom Europske unije za intelektualno vlasništvo pri Europolu, ENISA-om, državama članicama i privatnim sektorom razviti informativne alate i smjernice za povećanje otpornosti poduzeća iz Unije na **krađe intelektualnog vlasništva kiberdjelovanjem**[72].

Obrazovanjem – uključujući strukovno obrazovanje i osposobljavanje (SOO), informiranje i vježbe – trebale bi se i dodatno povećati vještine u području kibersigurnosti i kiberobrane na razini Unije. U tu bi svrhu relevantni akteri EU-a kao što su ENISA, Europska obrambena agencija (EDA) i Europska akademija za sigurnost i obranu (EASO)[73] trebali tražiti sinergije između svojih aktivnosti.

Strateške inicijative

Unija bi trebala osigurati:

- donošenje revidirane Direktive NIS,

[70] https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies
[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en
[72] https://ec.europa.eu/commission/presscorner/detail/hr/IP_20_2187
[73] Putem platforme za obrazovanje, osposobljavanje, evaluaciju i vježbe u području kibersigurnosti (ETEE).

- regulatorne mjere za internet sigurnih stvari,
- ostvariti do 4,5 milijardi EUR javnih i privatnih ulaganja u razdoblju 2021.–2027. putem ulaganja u kibersigurnost u okviru CCCN-a (posebno u okviru programa Digitalna Europa, Obzor Europa i Mehanizma za oporavak),
- EU-ovu mrežu centara za sigurnosne operacije koji se temelje na umjetnoj inteligenciji i infrastrukturu za ultrasigurnu komunikaciju koja koristi kvantne tehnologije,
- široku prihvaćenost kibersigurnosnih tehnologija putem namjenske potpore MSP-ovima u okviru digitalnoinovacijskih centara,
- razvoj usluge DNS prevoditelja EU-a kao sigurne i otvorene alternative za pristup internetu za građane, poduzeća i javnu upravu EU-a, i
- dovršetak provedbe paketa mjera za 5G do drugog tromjesečja 2021. (vidjeti Prilog).

2. IZGRADNJA OPERATIVNOG KAPACITETA ZA SPREČAVANJE, ODVRAĆANJE I ODGOVOR

Kiberincidenti, slučajni ili izazvani namjernim djelovanjem kriminalaca, državnih i ostalih nedržavnih aktera, mogu prouzročiti golemu štetu. Zbog njihova opsega i složenosti, primjerice čestog ugrožavanja krajnje mete korištenjem usluga, hardvera i softvera trećih strana, Unija se teško može suprotstaviti prijetnjama u cjelini bez sustavne i sveobuhvatne razmjene informacija i suradnje pri zajedničkom odgovoru. Unijin je cilj **potpunom provedbom regulatornih alata, mobilizacijom i suradnjom** pružati potporu državama članicama u obrani svojih građana i gospodarskih i nacionalnih sigurnosnih interesa, uz potpuno poštovanje temeljnih prava i sloboda te vladavine prava. Nekoliko zajednica koje se sastoje od mreža, institucija, tijela i agencija EU-a te nadležnih tijela država članica odgovorno je za sprečavanje kiberprijetnji, kao i obeshrabrivanje i odvraćanje od njih te odgovaranje na njih, koristeći se svojim instrumentima i inicijativama[74]. Te zajednice uključuju: i. tijela NIS-a, kao što su CSIRT-ovi, i tijela za odgovor na katastrofe, ii. tijela kaznenog progona i pravosudna tijela, iii. kiberdiplomaciju, i iv. kiberobranu.

2.1. Zajednička jedinica za kibersigurnost

Zajednička jedinica za kibersigurnost djelovala bi kao virtualna i fizička platforma za suradnju različitih zajednica za kibersigurnost u EU-u, s naglaskom na operativnoj i tehničkoj koordinaciji protiv velikih prekograničnih kiberincidenata i kiberprijetnji.

Zajednička jedinica za kibersigurnost bila bi važan korak prema dovršetku **europskog okvira za upravljanje kibersigurnosnim krizama**. Kao što je navedeno u političkim smjernicama

[74] Uključujući potporu ENISA-e operativnoj suradnji i upravljanju krizama, mrežu CSIRT-ova, mrežu organizacija za povezivanje u kiberkrizama (CyCLONe, postat će EU-CyCLONe, kako je predloženo u revidiranoj Direktivi NIS), Skupina za suradnju u području NIS-a, rescEU, Europski centar za kiberkriminalitet i Zajedničku radnu skupinu za borbu protiv kiberkriminaliteta pri Europolu te protokol za odgovor tijela kaznenog progona na krizne situacije, Obavještajni i situacijski centar EU-a (EU INTCEN) te alate za kiberdiplomaciju, Službu za jedinstvenu obavještajnu analizu (SIAC), kiberprojekte u okviru stalne strukturirane suradnje (PESCO), osobito timove za brz odgovor na kiberincidente i uzajamnu pomoć u području kibersigurnosti (CRRT).

predsjednice Komisije[75], jedinica bi trebala omogućiti državama članicama i institucijama, tijelima i agencijama EU-a da u potpunosti iskoriste postojeće strukture, resurse i sposobnosti te promiču načelo „**potrebe za razmjenom informacije**". Bila bi sredstvo za konsolidaciju dosadašnjeg napretka u provedbi Preporuke iz 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera („plan")[76]. Omogućila bi i daljnje jačanje suradnje u vezi sa strukturom plana i iskorištavanjem ostvarenog napretka, osobito u okviru Skupine za suradnju u području NIS-a i mreže CyCLONe.

Time bi se mogla riješiti **dva glavna nedostatka** koji trenutačno povećavaju slabosti i stvaraju neučinkovitost u odgovoru na prekogranične prijetnje i incidente koji utječu na Uniju. Prvo, civilne i diplomatske **zajednice** te **zajednice** tijela kaznenog progona i obrane u području kibersigurnosti još nemaju zajednički prostor za njegovanje strukturirane suradnje i olakšavanje operativne i tehničke suradnje. Drugo, relevantni dionici u području kibersigurnosti još ne koriste sav **potencijal** operativne suradnje i uzajamne pomoći unutar postojećih mreža i zajednica. Među ostalim, ne postoji platforma koja bi omogućila operativnu suradnju s privatnim sektorom. Jedinica bi trebala poboljšati i ubrzati koordinaciju te omogućiti Uniji da se suoči s kiberincidentima i kiberkrizama velikih razmjera i odgovori na njih.

Zajednička jedinica za kibersigurnost ne bi bila dodatno, samostalno tijelo niti bi utjecala na nadležnosti i ovlasti nacionalnih tijela za kibersigurnost ili sudionika iz EU-a. Djelovala bi kao zaštitni mehanizam u okviru kojeg bi se sudionici mogli osloniti na potporu i stručno znanje drugih članova, posebno u slučaju da različite kiberzajednice moraju blisko surađivati. Nedavni događaji ukazuju pak na potrebu da Unija poveća ambicije i spremnost za suočavanje sa stvarnim stanjem kad je riječ o kiberprijetnjama. U okviru svojeg doprinosa toj jedinici, akteri EU-a (Komisija i agencije i tijela EU-a) bit će stoga spremni znatno povećati resurse i sposobnosti kako bi podigli pripravnost i otpornost.

Zajednička jedinica za kibersigurnost ispunjavala bi tri glavna cilja. Prvo, osigurala bi **pripravnost** u zajednicama za kibersigurnost; drugo, razmjenom informacija osiguravala bi kontinuirani zajednički **pregled** situacije; treće, ojačala bi koordinirani **odgovor** i oporavak. Kako bi se postigli ti ciljevi, rad jedinice trebao bi se temeljiti na dobro definiranim **blokovima i ciljevima**, kao što su **sigurno i brzo dijeljenje informacija**, poboljšanje **suradnje** među sudionicima, uključujući interakciju između država članica i relevantnih subjekata iz EU-a, uspostavljanje strukturiranog **partnerstva s pouzdanom sektorskom** osnovom i olakšavanje koordiniranog pristupa **suradnji s vanjskim partnerima**. Kako bi se to postiglo, jedinica bi mogla olakšati razvoj okvira za suradnju na temelju pregleda raspoloživih kapaciteta na nacionalnoj razini i razini EU-a.

Da bi ta jedinica postala jezgra operativne suradnje EU-a u području kibersigurnosti, Komisija će surađivati s državama članicama i relevantnim institucijama, tijelima i agencijama EU-a, uključujući ENISA-u, CERT-EU i Europol, kako bi promovirala **postupni i uključivi pristup** uz potpuno poštivanje nadležnosti i ovlasti svih uključenih sudionika. U skladu s tim pristupom jedinica bi mogla unaprijediti suradnju među sastavnicama određene kiberzajednice ako one to smatraju potrebnim.

[75] „Ambicioznija Unija – moj plan za Europu", političke smjernice za sljedeću Europsku komisiju 2019.–2024. kandidatkinje za predsjednicu Europske komisije Ursule von der Leyen.
[76] Preporuka Komisije od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera, C(2017) 6100 final.

Predložena su četiri glavna koraka za uspostavu zajedničke jedinice za kibersigurnost:

- *definiranje*, pregledom dostupnih kapaciteta na nacionalnoj razini i razini EU-a,
- *priprema*, uspostavom okvira za strukturiranu suradnju i pomoć,
- *uvođenje*, provedbom okvira pomoću resursa koje su osigurali sudionici za početak rada jedinice,
- *proširenje*, jačanjem kapaciteta koordiniranog odgovora uz doprinos industrije i partnera.

Na temelju zaključaka savjetovanja s državama članicama, institucijama, tijelima i agencijama EU-a[77], Komisija će do veljače 2021., uz sudjelovanje Visokog predstavnika, u skladu s njegovim nadležnostima, predstaviti postupak, ključne etape i rokove za **definiranje, pripremu, uvođenje i proširenje zajedničke jedinice za kibersigurnost**.

2.2. Borba protiv kiberkriminaliteta

Naša ovisnost o internetskim alatima počiniteljima kiberkriminaliteta otvorila je golem prostor za napade i dovela do toga da istrage gotovo svih vrsta kaznenih djela imaju digitalnu komponentu. Nadalje, osnovne dijelove našeg društva ugrožavaju akterikiberprijetnji i oni koji upotrebljavaju kiberalate za planiranje i izvršavanje nezakonitih radnji. Stoga postoje bliske veze s ukupnom sigurnosnom politikom EU-a, što se odražava u elementima Strategije za sigurnosnu uniju iz 2020. i Agende EU-a za borbu protiv terorizma[78] koji se odnose na kibersigurnost.

Učinkovita borba protiv kiberkriminaliteta ključan je čimbenik kibersigurnosti: odvraćanje se ne može postići samo otpornošću, već zahtijeva i identifikaciju i kazneni progon počinitelja. Stoga je od ključne važnosti poticati suradnju i razmjenu između aktera u području kibersigurnosti i tijela kaznenog progona. Zato su na razini EU-a Europol i ENISA već uspostavili jaku suradnju u okviru koje su organizirali zajedničke konferencije i radionice te Komisiji, državama članicama i drugim dionicima dostavili zajednička izvješća o prijetnjama u području kibersigurnosti i tehnološkim izazovima. Komisija će nastaviti podupirati taj integrirani pristup kako bi osigurala usklađen i učinkovit odgovor na temelju sveobuhvatnih informacija.

Kao važan element tog odgovora, EU i nacionalna tijela moraju proširiti i poboljšati kapacitete tijela kaznenog progona za istragu kiberkriminaliteta, uz potpuno poštovanje temeljnih prava i postizanje potrebne ravnoteže između različitih prava i interesa. EU bi se trebao moći boriti protiv kiberkriminaliteta primjenom svrsishodnih i potpuno funkcionalnih propisa, s posebnim naglaskom na borbu protiv seksualnog zlostavljanja djece na internetu te na digitalne istrage, uključujući kriminalitet na „darknetu”. Tijela kaznenog progona moraju biti potpuno opremljena za digitalne istrage. Komisija će stoga predložiti akcijski plan za povećanje digitalnih kapaciteta agencija za kazneni progon osiguravanjem potrebnih vještina i alata. Osim toga, Europol će unaprijediti svoju ulogu stručnog centra za potporu

[77] Savjetovanje s državama članicama (među ostalim tijekom vježbe „Blue OLEx20”, koja je okupila voditelje nacionalnih tijela za kibersigurnost), institucijama, tijelima i agencijama EU-a koje je provedeno između srpnja i studenoga 2020.

[78] Komunikacija o Agendi EU-a za borbu protiv terorizma: predviđanje, sprečavanje, zaštita i odgovor., 9. prosinca 2020., COM(2020) 795 final.

nacionalnim tijelima kaznenog progona u borbi protiv kriminaliteta koji omogućuju kibertehnologije i koji o njima ovisi, čime će pridonijeti utvrđivanju zajedničkih forenzičkih standarda (preko Europolova laboratorija i centra za inovacije). Sve te aktivnosti zahtijevaju odgovarajuću prihvaćenost u državama članicama, koje se potiče da iskoriste nacionalne programe Fonda za unutarnju sigurnost i prijavljuju se s projektima na pozive na podnošenje prijedloga u okviru tematskog instrumenta.

Komisija će upotrijebiti sva odgovarajuća sredstva, uključujući postupke zbog povrede, kako bi osigurala potpuni prijenos i provedbu Direktive o napadima na informacijske sustave[79] iz 2013., uključujući statističke podatke koje će dostavljati države članice. Time će se bolje spriječiti zlouporaba naziva domena, među ostalim, prema potrebi, za distribuciju nezakonitog sadržaja, te nastojati postići dostupnost točnih registracijskih podataka nastavkom suradnje s Internetskom organizacijom za dodijeljene nazive i brojeve (ICANN) i drugim dionicima u sustavu upravljanja internetom, posebno putem radne skupine za javnu sigurnost Savjetodavnog odbora vlada ICANN-a. U skladu s time, prijedlogom u revidiranoj Direktivi NIS kao ključan element sigurnosti, stabilnosti i otpornosti DNS-a predviđeni su vođenje točnih i potpunih baza podataka naziva domena i registracijskih podataka ili „podataka WHOIS" te osiguravanje zakonitog pristupa tim podacima.

Komisija će nastaviti raditi i na osiguravanju odgovarajućih kanala i pojašnjavanju pravila za dobivanje prekograničnog pristupa elektroničkim dokazima za kaznene istrage (potrebno u 85 % istraga, pri čemu je 65 % ukupnih zahtjeva upućeno pružateljima iz druge jurisdikcije), olakšavanjem donošenja i provedbe „paketa o e-dokazima" te praktičnih mjera[80]. Ključno je da Europski parlament i Vijeće brzo donesu prijedloge za e-dokaze kako bi stručnjaci dobili djelotvoran alat. Elektronički dokazi moraju biti čitljivi pa će Komisija nastaviti raditi na potpori kapacitetima tijela kaznenog progona u području digitalnih istraga, među ostalim u pogledu šifriranja kad je to potrebno u kaznenim istragama, uz istodobno potpuno očuvanje svoje funkcije zaštite temeljnih prava i kibersigurnosti.

2.3. Alati EU-a za kiberdiplomaciju

EU se koristi svojim **alatima za kiberdiplomaciju**[81] za sprečavanje i suzbijanje zlonamjernih kiberaktivnosti, te odvraćanje od njih i odgovori na njih. Nakon uvođenja pravnog okvira za ciljane mjere ograničavanja protiv kibernapada u svibnju 2019.[82], EU je u skladu s režimom iz srpnja 2020.[83] uvrstio na popis šest pojedinaca i tri subjekta koji su

[79] Direktiva 2013/40/EU o napadima na informacijske sustave.
[80] COM(2018) 225 i 226; C(2020) 2779 final. Konkretno, projekt SIRIUS nedavno je dobio dodatna financijska sredstva u okviru Instrumenta za partnerstvo kako bi se poboljšali kanali za dobivanje zakonitog prekograničnog pristupa elektroničkim dokazima za kaznene istrage (potrebno u 85 % istraga teških kaznenih djela, pri čemu je 65 % ukupnih zahtjeva upućeno pružateljima iz druge jurisdikcije) i utvrdila usklađena pravila na međunarodnoj razini.
[81] https://www.consilium.europa.eu/hr/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/
[82] Odluka Vijeća (ZVSP) 2019/797 od 17. svibnja 2019. o mjerama ograničavanja protiv kibernapada koji predstavljaju prijetnju Uniji ili njezinim državama članicama (SL L 129I, 17.5.2019., str. 13.) i Uredba Vijeća (EU) 2019/796
od 17. svibnja 2019. o mjerama ograničavanja protiv kibernapada koji predstavljaju prijetnju Uniji ili njezinim državama članicama (SL L 129I, 17.5.2019., str. 1.).
[83] Odluka Vijeća (ZVSP) 2020/1127 od 30. srpnja 2020. o izmjeni Odluke (ZVSP) 2019/797 o mjerama ograničavanja protiv kibernapada koji predstavljaju prijetnju Uniji ili njezinim državama članicama (ST/9564/2020/INIT) (SL L 246, 30.7.2020., str. 12.–17.) i Provedbena uredba Vijeća (EU) 2020/1125 od 30. srpnja 2020. o provedbi Uredbe (EU) 2019/796 o mjerama ograničavanja protiv kibernapada koji

odgovorni za kibernapade koji štete Uniji i njezinim državama članicama ili su u njima sudjelovali. Još dvije osobe i jedno tijelo uvršteni su na popis u listopadu 2020.[84] Zlonamjerne kiberaktivnosti, uključujući one koje se razvijaju postupno, trebale bi se rješavati djelotvornim i sveobuhvatnim zajedničkim diplomatskim odgovorom EU-a, koristeći se svim mjerama dostupnima na razini EU-a.

Za brz i učinkovit zajednički diplomatski odgovor EU-a potreban je dobar zajednički pregled situacije i sposobnost brze pripreme zajedničkog stajališta EU-a. Visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku potaknut će i olakšati osnivanje **radne skupine država članica za kiberobavještajne podatke** u Obavještajnom i situacijskom centru EU-a (INTCEN) kako bi se unaprijedila strateška obavještajna suradnja u vezi s kiberprijetnjama i kiberaktivnostima. To će biti dodatna potpora za pregled situacije u EU-u i donošenje odluka o zajedničkom diplomatskom odgovoru. Radna skupina trebala bi surađivati s postojećim strukturama[85], uključujući, prema potrebi, one koje pokrivaju širu prijetnju hibridnog i stranog uplitanja, kako bi prikupila podatke i procijenila pregled situacije.

Visoki predstavnik će, kako bi ojačao svoju sposobnost sprečavanja i suzbijanja zlonamjernog ponašanja u kiberprostoru, te odvraćanja od njega i odgovaranja na njega, uz sudjelovanje Komisije u skladu s njezinim nadležnostima, iznijet će prijedlog da EU podrobnije definira stajalište o **odvraćanju od kibernapada**. Oslanjajući se na dosadašnju primjenu alata za kiberdiplomaciju, stajalište bi trebalo pridonijeti odgovornom ponašanju država i suradnji u kiberprostoru i sadržavati posebne smjernice za suzbijanje najtežih kibernapada, osobito onih koji utječu na našu ključnu infrastrukturu, demokratske institucije i procese[86], kao i napade u lancu opskrbe i krađu intelektualnog vlasništva kiberdjelovanjem. U okviru stajališta trebalo bi opisati kako bi Unija i države članice mogli iskoristiti svoje političke, gospodarske, diplomatske, pravne i strateške komunikacijske alate protiv zlonamjernih kiberaktivnosti te razmotriti kako bi Unija i države članice mogli unaprijediti sposobnost pripisivanja odgovornosti za zlonamjerne kiberaktivnosti. Usto, Visoki predstavnik, zajedno s Vijećem i Komisijom, nastoji razmotriti **dodatne mjere u okviru alata za kiberdiplomaciju**, uključujući mogućnost daljnjih opcija za mjere ograničavanja, i odlučivanje **kvalificiranom većinom za uvrštenje na popis u okviru horizontalnog režima sankcija protiv kibernapada**. Povrh toga, EU bi trebao poduzeti još intenzivnije raditi na jačanju suradnje s međunarodnim partnerima, uključujući NATO, kako bi se unaprijedilo zajedničko razumijevanje prijetnji, razvili mehanizmi suradnje i utvrdili zajednički diplomatski odgovori.

Visoki predstavnik, uz sudjelovanje Komisije, predložit će i ažuriranje **provedbenih smjernica za alat za kiberdiplomaciju[87]**, među ostalim radi učinkovitijeg donošenja odluka, te će nastaviti redovito organizirati vježbe i procjene alata za kiberdiplomaciju. Unija bi

---

predstavljaju prijetnju Uniji ili njezinim državama članicama (ST/9568/2020/INIT) (SL L 246, 30.7.2020., str. 4.–9.).

[84] Odluka Vijeća (ZVSP) 2020/1537 od 22. listopada 2020. o izmjeni Odluke (ZVSP) 2019/797 o mjerama ograničavanja protiv kibernapada koji predstavljaju prijetnju Uniji ili njezinim državama članicama (SL L 351I, 22.10.2020., str. 5–7.) i Provedbena uredba Vijeća (EU) 2020/1536 od 22. listopada 2020. o provedbi Uredbe (EU) 2019/796 o mjerama ograničavanja protiv kibernapada koji predstavljaju prijetnju Uniji ili njezinim državama članicama (SL L 351I, 22.10.2020., str. 1–4.).

[85] Kao što su Služba za jedinstvenu obavještajnu analizu EU-a (SIAC) i, prema potrebi, relevantni projekti uspostavljeni u okviru stalne strukturirane suradnje (PESCO) te sustav brzog uzbunjivanja (RAS) uspostavljen 2018. radi potpore EU-ovu općem pristupu suzbijanju dezinformiranja.

[86] Ponajprije traženjem sinergija s inicijativama na temelju Akcijskog plana za europsku demokraciju.

[87] 13007/17

trebala i dodatno **integrirati alate za kiberdiplomaciju u krizne mehanizme EU-a**, nastojati ostvariti sinergije s mjerama za suzbijanje hibridnih prijetnji, dezinformacija i vanjskog uplitanja na temelju Zajedničkog okvira za suzbijanje hibridnih prijetnji[88] i Akcijskog plana za europsku demokraciju. U tom bi kontekstu EU trebao razmotriti interakciju između alata za kiberdiplomaciju i moguće primjene članka 42. stavka 7. UEU-a i članka 222. UFEU-a[89].

2.4. Jačanje kapaciteta kiberobrane

EU i države članice moraju povećati sposobnost sprečavanja kiberprijetnji i odgovora na njih u skladu s razinom ambicije EU-a koja proizlazi iz Globalne strategije EU-a iz 2016.[90] U tu će svrhu Visoki predstavnik, u suradnji s Komisijom, predstaviti **preispitivanje okvira za politiku kiberobrane** kako bi se poboljšala daljnja koordinacija i suradnja među akterima EU-a[91], kao i s državama članicama i među njima, među ostalim u pogledu misija i operacija u okviru zajedničke sigurnosne i obrambene politike (ZSOP). Okvir bi trebao utjecati na predstojeći „strateški kompas"[92], čime bi se postigla dodatna integracija kibersigurnosti i kiberobrane u širi program sigurnosti i obrane.

EU je 2018. utvrdio kiberprostor kao područje djelovanja[93]. Predstojećom **Vojnom vizijom i strategijom o kiberprostoru kao području djelovanja** Vojnog odbora Europske unije trebalo bi se dodatno definirati kako kiberprostor kao područje djelovanja omogućuje vojne misije i operacije u okviru ZSOP-a EU-a. **Mreža vojnih timova za hitne računalne intervencije (vojni CERT-ovi)**[94], koju uspostavlja Europska obrambena agencija, dodatno će pridonijeti znatnom povećanju suradnje među državama članicama. Osim toga, radi kibersigurnosti ključnih svemirskih infrastruktura u nadležnosti svemirskog programa, ojačat će se Agencija Europske unije za svemirski program, posebno Centar za praćenje sigurnosti Galileo, a njegov mandat proširiti na druge ključne resurse svemirskog programa.

EU i države članice trebali bi pružiti dodatni poticaj **razvoju najsuvremenijih kapaciteta kiberobrane** s pomoću različitih politika i instrumenata EU-a, posebno ZSOP-a, i, prema potrebi, na temelju rada EDA-e. To zahtijeva velik naglasak na razvoju i upotrebi ključnih tehnologija kao što su umjetna inteligencija, šifriranje i kvantno računalstvo. U skladu s prioritetima razvoja kapaciteta EU-a iz 2018.[95] i na temelju zaključaka prvog potpunog izvješća o koordiniranom godišnjem preispitivanju u području obrane (CARD)[96], EU bi trebao dodatno poticati suradnju država članica u **istraživanju, inovacijama i razvoju**

---

[88] https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

[89] Odnosno klauzula o uzajamnoj obrani, klauzula solidarnosti.

[90] Zaključci Vijeća (14149/16) o provedbi globalne strategije EU-a u području sigurnosti i obrane.

[91] Osobito Europska služba za vanjsko djelovanje (ESVD), uključujući Vojni stožer Europske unije (EUMS), Europska akademija za sigurnost i obranu (EASO), Komisija i agencije EU-a, posebno Europska obrambena agencija (EDA).

[92] Zaključci Vijeća o sigurnosti i obrani od 17. lipnja 2020. (8910/20).

[93] https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/hr/pdf

[94] Uspostava mreže vojnih CERT-ova na razini EU-a odgovara cilju utvrđenom u okviru za politiku kiberobrane iz 2018. i usmjerena je na promicanje aktivne interakcije i razmjene informacija među vojnim CERT-ovima država članica EU-a.

[95] U lipnju 2018. države članice dogovorile su se u okviru Upravljačkog odbora EDA-e o usmjeravanju obrambene suradnje na razini EU-a.

[96] Odobrili ministri obrane u Upravljačkom odboru EDA-e u studenome 2020. https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card)

kapaciteta u području kiberobrane, potičući ih da koriste sav potencijal **stalne strukturirane suradnje (PESCO)**[97] i **Europskog fonda za obranu (EDF)**[98].

Predstojeći **akcijski plan Komisije za postizanje sinergije između civilne, obrambene i svemirske industrije**, koji će biti predstavljen u prvom tromjesečju 2021., uključivat će mjere za daljnju potporu sinergijama na razini programa, tehnologija, inovacija i novoosnovanih poduzeća, u skladu s upravljanjem odgovarajućim programima[99].

Povrh toga, radi podrške razmjeni informacija i uzajamnoj potpori, trebalo bi razviti relevantne sinergije i veze među inicijativama u području kiberobrane koje su poduzete u drugim okvirima, uključujući zajedničke projekte država članica povezane s kiberprostorom[100] u okviru PESCO-a, kao i sa strukturama EU-a za kibersigurnost.

Strateške inicijative

EU bi trebao:

- dovršiti europski okvir za upravljanje kibersigurnosnim krizama i utvrditi postupak, ključne etape i rokove za uspostavu zajedničke jedinice za kibersigurnost,
- nastaviti provedbu programa za kiberkriminalitet u okviru strategije za sigurnosnu uniju,
- poticati i olakšavati uspostavu radne skupine država članica za kiberobavještajne podatke u sastavu EU INTCEN-a,
- iznijeti stajalište Unije o odvraćanju od kibernapada radi sprečavanja i suzbijanja zlonamjernih kiberaktivnosti, odvraćanja od njih te odgovaranja na njih,
- preispitati okvir za politiku kiberobrane,
- olakšati razvoj vojne vizije i strategije o kiberprostoru kao području operativnog djelovanja za vojne misije i operacije ZSOP-a,
- poduprijeti sinergije između civilne, obrambene i svemirske industrije, i
- ojačati kibersigurnost ključnih svemirskih infrastruktura u okviru svemirskog programa.

3. UNAPREĐENJE GLOBALNOG I OTVORENOG KIBERPROSTORA

EU bi trebao nastaviti surađivati s međunarodnim partnerima na promicanju političkog modela i vizije kiberprostora koji se temelje na vladavini prava, ljudskim pravima, temeljnim slobodama i demokratskim vrijednostima kojima se postiže društveni, gospodarski i politički

[97] U okviru PESCO-a trenutačno se provodi nekoliko projekata povezanih s kibersigurnošću, ponajprije Platforma za razmjenu informacija o odgovoru na kiberprijetnje i kiberincidente, Timovi za brz odgovor na kiberincidente i uzajamna pomoć u području kibersigurnosti, Kiberakademija i inovacijski centar EU-a te Koordinacijski centar za kibernetičko i informacijsko područje (CIDCC).

[98] U okviru EDF-a Komisija je već utvrdila mogućnosti za potencijalne zajedničke aktivnosti istraživanja i razvoja u području kiberobrane usmjerene na jačanje suradnje, inovacijskih kapaciteta i konkurentnosti obrambene industrije.

[99] Kao što su Obzor Europa, Digitalna Europa i EDF.

[100] https://pesco.europa.eu/

razvoj na globalnoj razini te koji pridonose sigurnosnoj uniji. Međunarodna suradnja od ključne je važnosti kako bi kiberprostor ostao globalan, otvoren, stabilan i siguran. EU bi zato trebao nastaviti surađivati s trećim zemljama, međunarodnim organizacijama i širom zajednicom dionika radi razvoja i provedbe usklađene i cjelovite međunarodne kiberpolitike, imajući na umu sve veću povezanost gospodarskih aspekata novih tehnologija, unutarnje sigurnosti te vanjske, sigurnosne i obrambene politike. EU, kao snažan gospodarski i trgovinski blok utemeljen na osnovnim demokratskim vrijednostima, poštovanju vladavine prava i temeljnih prava, ima i jedinstvenu ulogu predvodnika u utvrđivanju i promicanju međunarodnih normi i standarda.

3.1. Vodeća uloga EU-a u pogledu standarda, normi i okvira u kiberprostoru

Jačanje međunarodne normizacije

Kako bi promicala i zaštitila svoju viziju kiberprostora na međunarodnoj razini, Unija se mora **snažnije angažirati i biti na čelu u međunarodnim procesima normizacije te povećati zastupljenost u međunarodnim i europskim tijelima za normizaciju, kao i u drugim organizacijama za izradu normi**[101]**.** Budući da se digitalne tehnologije brzo razvijaju, međunarodne norme sve su važnije za dopunjavanje uobičajenih regulatornih mjera u područjima kao što su umjetna inteligencija, računalstvo u oblaku, kvantno računalstvo i kvantna komunikacija. Treće zemlje sve više primjenjuju međunarodnu normizaciju kako bi unaprijedile svoj politički i ideološki program, koji često nije u skladu s vrijednostima EU-a. Osim toga, sve je veći rizik od konkurentnih okvira za međunarodnu normizaciju, što dovodi do fragmentacije.

Razvoj međunarodnih normi u području perspektivnih tehnologija i osnovne internetske arhitekture u skladu s vrijednostima EU-a ključan je kako bi se osiguralo da internet ostane globalan i otvoren te da tehnologije budu usmjerene na čovjeka i privatnost, a njihova upotreba zakonita, sigurna i etična. U okviru predstojeće strategije za normizaciju EU bi trebao definirati **ciljeve za međunarodnu normizaciju** te ih poduzetnom i koordiniranom komunikacijom promicati na međunarodnoj razini. Trebalo bi težiti većoj suradnji i raspodjeli tereta s partnerima sličnih stajališta i europskim dionicima.

Unapređenje odgovornog ponašanja država u kiberprostoru

EU i dalje surađuje s međunarodnim partnerima na unapređivanju i promicanju globalnog, otvorenog, stabilnog i sigurnog kiberprostora u kojem se poštuje **međunarodno pravo, osobito Povelja Ujedinjenih naroda (UN)**[102], i **slijede dobrovoljne neobvezujuće norme, pravila i načela odgovornog ponašanja država**[103]. Zbog lošije učinkovite multilateralne rasprave o međunarodnoj sigurnosti u kiberprostoru javlja se jasna potreba da EU i države članice budu poduzetnije u raspravama u UN-u i drugim relevantnim međunarodnim forumima. EU je u najboljem položaju za **iznošenje, koordinaciju i konsolidaciju stajališta**

[101] Npr. Međunarodna organizacija za normizaciju (ISO), Međunarodna elektrotehnička komisija (IEC), Međunarodna unija za telekomunikacije (ITU), Europski odbor za normizaciju (CEN), Europski odbor za elektrotehničku normizaciju (CENELEC), Europski institut za telekomunikacijske norme (ETSI), Radna skupina za razvoj interneta (IETF), Partnerski projekt za treću generaciju (3GPP) i Institut inženjera elektrotehnike i elektronike (IEEE).

[102] https://www.un.org/en/sections/un-charter/un-charter-full-text/

[103] Kako je navedeno u relevantnim izvješćima skupina vladinih stručnjaka o napretku u području informatike i telekomunikacija u kontekstu međunarodne sigurnosti (UNGGE), koja je potvrdila Opća skupština UN-a, a posebno izvješćima iz 2015., 2013. i 2010.

država članica u međunarodnim **forumima** te bi trebao **razviti stajalište EU-a o primjeni međunarodnog prava u kiberprostoru**. Visoki predstavnik i države članice namjeravaju iznijeti svoj uključiv i usuglašen prijedlog o političkoj obvezi u vezi s **Akcijskim programom za unapređenje odgovornog ponašanja država u kiberprostoru**[104] u UN-u. Na temelju postojeće pravne stečevine koju je potvrdila Opća skupština UN-a[105], tim se akcijskim programom osigurava platforma za suradnju i razmjenu primjera dobre prakse unutar UN-a i predlaže uspostava mehanizma za praktičnu primjenu normi odgovornog ponašanja država i promicanje izgradnje kapaciteta. Nadalje, Visoki predstavnik namjera ojačati i potaknuti provedbu **mjera za izgradnju povjerenja** među državama, među ostalim razmjenom primjera dobre prakse na regionalnoj i multilateralnoj razini te doprinosom međuregionalnoj suradnji.

Veća globalna povezanost ne bi trebala uzrokovati cenzuru, masovni nadzor, povredu privatnosti podataka i represiju civilnog društva, akademske zajednice i građana. Unija bi trebala i dalje biti predvodnica u zaštiti i promicanju **ljudskih prava i temeljnih sloboda** na internetu. Zato bi trebala promicati daljnje poštovanje međunarodnog prava i standarda u području ljudskih prava[106], operacionalizirati Akcijski plan za ljudska prava i demokraciju za razdoblje 2020.–2024.[107] te unaprijediti smjernice o ljudskim pravima koje se odnose na slobodu izražavanja na internetu i izvan njega[108], čime bi **dala** nov poticaj **praktičnoj** primjeni instrumenata EU-a. Trebala bi kontinuirano **štititi branitelje ljudskih prava, civilno društvo i akademske zajednice koji se bave pitanjima kao što su kibersigurnost, privatnost podataka, nadzor i cenzura na internetu**. U tu bi svrhu trebala dati dodatne praktične smjernice, promicati dobru praksu i pojačati aktivnosti sprečavanja zlouporabe perspektivnih tehnologija, osobito diplomatskim mjerama ako je potrebno te kontrolom izvoza takvih tehnologija. Trebala bi se nastaviti boriti i za zaštitu najranjivijih članova društva na internetu predlaganjem propisa za bolju zaštitu djece od seksualnog zlostavljanja i iskorištavanja te donošenjem strategije o pravima djeteta.

Budimpeštanska konvencija o kiberkriminalitetu

EU i dalje podupire treće zemlje koje žele pristupiti **Budimpeštanskoj konvenciji Vijeća Europe o kiber**kriminalitetu i radi na dovršetku **Drugog dodatnog protokola uz Budimpeštansku konvenciju**, koji uključuje mjere i zaštitne mehanizme za poboljšanje međunarodne suradnje između izvršnih i pravosudnih tijela, kao i između vlasti i pružatelja usluga u drugim zemljama, te za koje Komisija sudjeluje u pregovorima u ime EU-a[109]. Postojeća inicijativa za novi pravni instrument o kiberkriminalitetu na razini UN-a mogla bi pojačati podjele i usporiti prijeko potrebne nacionalne reforme i povezane aktivnosti izgradnje kapaciteta, što bi moglo ometati učinkovitu međunarodnu suradnju u borbi protiv kiberkriminaliteta. EU ne vidi potrebu za novim pravnim instrumentom za kiberkriminalitet na razini UN-a. EU nastavlja sudjelovati u **multilateralnim razmjenama u području kiberkriminaliteta** kako bi se uključivošću, transparentnošću i uzimajući u obzir dostupno

[104] https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf

[105] Kako je navedeno u relevantnim izvješćima skupina vladinih stručnjaka o napretku u području informatike i telekomunikacija u kontekstu međunarodne sigurnosti (UNGGE), koja je potvrdila Opća skupština UN-a, a posebno izvješćima iz 2015., 2013. i 2010.

[106] Posebno Povelja UN-a i Opća deklaracija o ljudskim pravima.

[107] https://www.consilium.europa.eu/hr/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/

[108] https://www.consilium.europa.eu/media/28348/142549.pdf

[109] Odluka Vijeća od lipnja 2019. (9116/19).

stručno znanje osiguralo poštivanje ljudskih prava i temeljnih sloboda u cilju stvaranja dodane vrijednosti za sve.

3.2. Suradnja s partnerima i širom zajednicom dionika

EU bi trebao **intenzivirati i proširiti dijaloge o kibersigurnosti s trećim zemljama** kako bi promicao svoje vrijednosti i viziju kiberprostora, razmjenjivao primjere dobre prakse i ostvario uspješnu suradnju. Trebao bi uspostaviti strukturirane razmjene s regionalnim organizacijama kao što su Afrička unija, Regionalni forum ASEAN-a, Organizacija američkih država i Organizacija za europsku sigurnost i suradnju. Ako je to moguće i prikladno, isotodobno bi trebao nastojati naći zajedničko stajalište s drugim partnerima u pitanjima od zajedničkog interesa. U suradnji s delegacijama EU-a i, prema potrebi, veleposlanstvima država članica diljem svijeta, trebao bi osnovati neformalnu **mrežu EU-a za kiberdiplomaciju** radi promicanja svoje vizije o kiberprostoru, razmjene informacija i redovite koordinacije s obzirom na razvoj događaja u kiberprostoru[110].

Oslanjajući se na zajedničke izjave od 8. srpnja 2016.[111] i 10. srpnja 2018.[112], EU bi trebao nastaviti unapređivati **suradnju EU-a i NATO-a**, posebno u pogledu zahtjeva u pogledu interoperabilnosti kiberobrane. U tom bi kontekstu trebao nastaviti raditi na povezivanju relevantnih struktura ZSOP-a s NATO-ovom inicijativom *Federated Mission Networking* i tako omogućiti mrežnu interoperabilnost s NATO-om i partnerima kad je to potrebno. Usto, valjalo bi dodatno istražiti mogućnosti suradnje EU-a i NATO-a u području obrazovanja, osposobljavanja i vježbi, među ostalim ostvarivanjem sinergija između Europske akademije za sigurnost i obranu i NATO-ova Centra izvrsnosti za suradnju u području kiberobrane.

Unija, u skladu sa svojim vrijednostima, snažno podupire i promiče **višedionički model upravljanja internetom**. Nijedan subjekt, država ili međunarodna organizacija ne bi smio pokušavati kontrolirati internet. Unija bi trebala i dalje sudjelovati u forumima[113] u cilju poboljšanja suradnje i zaštite temeljnih prava i sloboda, posebno prava na dostojanstvo, privatnost te slobodu izražavanja i informiranja. Kako bi se unaprijedila suradnja više dionika u pitanjima kibersigurnosti, Komisija i Visoki predstavnik u skladu sa svojim nadležnostima nastoje unaprijediti **redovite i strukturirane razmjene s dionicima**, među ostalim s privatnim sektorom, akademskom zajednicom i civilnim društvom, naglašavajući da međupovezanost kiberprostora zahtijeva da svi dionici preuzmu specifične odgovornosti i komuniciraju u svrhu održavanja globalnog, otvorenog, stabilnog i sigurnog kiberprostora. Te će aktivnosti biti vrijedan doprinos potencijalnim ključnim mjerama na razini EU-a.

3.3. Jačanje globalnih kapaciteta za povećanje globalne otpornosti

Kako bi sve zemlje imale društvene, gospodarske i političke koristi od interneta i upotrebe tehnologija, Unija i dalje podupire svoje partnere u povećanju njihove kiberotpornosti i kapaciteta za istragu i kazneni progon kiberkriminaliteta te suzbijanje kiberprijetnji. Radi postizanja opće usklađenosti trebala bi razviti **program EU-a za izgradnju vanjskih kiberkapaciteta** kako bi usmjerio te aktivnosti u skladu sa svojim smjernicama za izgradnju

[110] Mogle bi se, prema potrebi, iskoristiti i aktivnosti neformalne mreže EU-a za digitalnu diplomaciju, koja uključuje ministarstva vanjskih poslova država članica.
[111] https://www.consilium.europa.eu/hr/press/press-releases/2016/07/08/eu-nato-joint-declaration/
[112] https://www.consilium.europa.eu/hr/press/press-releases/2018/07/10/eu-nato-joint-declaration/
[113] Kao što su Internetska organizacija za dodijeljene nazive i brojeve (ICANN) i Forum za upravljanje internetom (IGF).

vanjskih kiberkapaciteta[114] i Programom održivog razvoja do 2030.[115] Tim bi se programom trebala iskoristiti stručna znanja država članica te relevantnih institucija, tijela, agencija i inicijativa EU-a, uključujući mrežu EU-a za izgradnju kiberkapaciteta[116], u skladu s njihovim mandatima. Trebala bi osnovati **odbor za izgradnju kiberkapaciteta EU-a** u kojem bi se okupili relevantni institucionalni dionici EU-a i pratio napredak te utvrdile daljnje sinergije i potencijalni nedostaci. Nadalje, može poduprijeti intenzivniju suradnju s državama članicama te s partnerima iz javnog i privatnog sektora i drugim relevantnim međunarodnim tijelima radi koordinacije aktivnosti i izbjegavanja udvostručavanja.

Pri izgradnji kiberkapaciteta EU-a naglasak bi i dalje trebao biti na zapadnom Balkanu i susjedstvu EU-a, kao i na partnerskim zemljama koje doživljavaju brzi digitalni razvoj. Djelovanje EU-a trebalo bi biti potpora razvoju zakonodavstva i politika partnerskih zemalja u skladu s relevantnim politikama i standardima EU-a u području kiberdiplomacije. U tom bi kontekstu djelovanje EU-a na izgradnji kapaciteta u području digitalizacije trebalo uključivati kibersigurnost kao standardni element. EU bi u tu svrhu trebao razviti poseban program osposobljavanja za osoblje EU-a zaduženo za provedbu aktivnosti EU-a za izgradnju vanjskih digitalnih i kiberkapaciteta. Trebao bi i pomoći tim zemljama u rješavanju sve većeg problema zlonamjernih kiberaktivnosti koje štete razvoju njihovih društava te **integritetu i sigurnosti demokratskih sustava**, u skladu s djelovanjem u okviru Akcijskog plana za europsku demokraciju. Tu bi od velike koristi mogla biti razmjena znanja među kolegama iz država članica EU-a, kao i iz relevantnih agencija EU-a i trećih zemalja.

Naposljetku, u kontekstu pakta za civilni ZSOP iz 2018.[117], civilne misije ZSOP-a mogu isto tako pridonijeti širem odgovoru EU-a na izazove u području kibersigurnosti, osobito jačanjem vladavine prava te kapaciteta tijela za izvršavanje zakonodavstva i civilnih uprava u partnerskim zemljama.

Strateške inicijative

EU bi trebao:

- definirati ciljeve u postupcima međunarodne normizacije i promicati ih na međunarodnoj razini,
- unaprijediti međunarodnu sigurnost i stabilnost u kiberprostoru, posebno prijedlogom EU-a i država članica za Akcijski program za unapređenje odgovornog ponašanja država u kiberprostoru u Ujedinjenim narodima,
- ponuditi praktične smjernice za ostvarivanje ljudskih prava i temeljnih sloboda u kiberprostoru,
- bolje zaštititi djecu od seksualnog zlostavljanja i iskorištavanja te donijeti strategiju o pravima djeteta,
- ojačati i promicati Budimpeštansku konvenciju o kiberkriminalitetu, među ostalim radom na njezinu Drugom dodatnom protokolu,

[114] https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf
[115] https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm
[116] https://www.eucybernet.eu/
[117] https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/hr/pdf

- proširiti dijalog o kibersigurnosti EU-a s trećim zemljama te regionalnim i međunarodnim organizacijama, među ostalim putem neformalne mreže EU-a za kiberdiplomaciju,
- jačati suradnju sa širom zajednicom dionika, ponajprije redovitom i strukturiranom komunikacijom s privatnim sektorom, akademskom zajednicom i civilnim društvom, i
- predložiti program EU-a za izgradnju vanjskih kiberkapaciteta i odbor za izgradnju kiberkapaciteta EU-a.

III. KIBERSIGURNOST U INSTITUCIJAMA, TIJELIMA I AGENCIJAMA EU-a

S obzirom na njihovu istaknutu političku ulogu, kritične zadaće koordiniranja jako osjetljivih pitanja i ulogu u upravljanju velikim javnim novčanim sredstvima, **institucije, tijela i agencije EU-a stalne su mete kibernapada**, osobito kiberšpijunaže. Međutim, stupanj kiberotpornosti i sposobnosti otkrivanja zlonamjernih kiberaktivnosti i odgovora na njih znatno se razlikuje među tim subjektima. Stoga je potrebno poboljšati ukupnu razinu kibersigurnosti dosljednim i homogenim pravilima.

U području informacijske sigurnosti ostvaren je napredak prema dosljednijim **pravilima za zaštitu klasificiranih i osjetljivih neklasificiranih podataka EU-a**. Međutim, interoperabilnost sustavâ klasificiranih podataka i dalje je ograničena, što sprečava neometan prijenos podataka između različitih subjekata. Potreban je daljnji napredak kako bi se primijenio međuinstitucijski pristup postupanju s klasificiranim i osjetljivim neklasificiranim podacima EU-a, koji bi mogao poslužiti i kao model interoperabilnosti u svim državama članicama. Trebalo bi utvrditi i početno stanje kako bi se pojednostavnili postupci s državama članicama. EU bi trebao unaprijediti sposobnost sigurne komunikacije s relevantnim partnerima, oslanjajući se u mjeri u kojoj je to moguće na postojeće aranžmane i postupke.

Kako je najavljeno u strategiji za sigurnosnu uniju, Komisija će stoga **2021. donijeti prijedloge zajedničkih obvezujućih pravila o informacijskoj sigurnosti i zajedničkih obvezujućih pravila o kibersigurnosti za sve institucije, tijela i agencije EU-a** na temelju trenutačnih međuinstitucijskih rasprava EU-a o kibersigurnosti[118].

Trenutačni i budući trendovi rada na daljinu zahtijevat će daljnja ulaganja u sigurnu opremu, infrastrukturu i alate koji omogućuju daljinski rad na osjetljivim i klasificiranim datotekama.

Usto, zbog sve agresivnijih kiberprijetnji i sve više sofisticiranijih kibernapada na institucije, tijela i agencije EU-a potrebna su veća ulaganja kako bi se postigla visoka razina kiberzrelosti. Za sve institucije, tijela i agencije EU-a uspostavlja se program informiranja o kibersigurnosti kako bi se osoblje upoznalo s kiberhigijenom i pružila potpora zajedničkoj kulturi kibersigurnosti.

CERT-EU je nužno ojačati boljim mehanizmom financiranja kako bi bio sposobniji institucijama, tijelima i agencijama EU-a pomagati u primjeni novih pravila o kibersigurnosti i poboljšanju kiberotpornosti. Potrebne su mu i šire ovlasti kako bi imao stabilne načine za postizanje navedenih ciljeva.

[118] Redovite međuinstitucijske rasprave EU-a o kibersigurnosti dio su šire razmjene informacija o mogućnostima i izazovima digitalne transformacije za institucije EU-a.

Strateške inicijative:

1. uredba o informacijskoj sigurnosti u institucijama, tijelima i agencijama EU-a;
2. uredba o zajedničkim pravilima o kibersigurnosti za institucije, tijela i agencije EU-a;
3. nova pravna osnova za CERT-EU radi jačanja njegova mandata i financiranja.

IV. ZAKLJUČCI

Usklađena provedba ove strategije pridonijet će kibersigurnom digitalnom desetljeću EU-a, ostvarenju sigurnosne unije i jačanju položaja EU-a na globalnoj razini.

EU bi trebao poticati standarde i norme za vrhunska rješenja i standarde kibersigurnosti za osnovne usluge i ključne infrastrukture, kao i za razvoj i primjenu novih tehnologija. Svaka organizacija i pojedinac koji se služi internetom dio je rješenja za ostvarenje kibersigurne digitalne transformacije.

Komisija i Visoki predstavnik u skladu sa svojim nadležnostima pratit će napredak na temelju ove strategije i izraditi kriterije za evaluaciju. Doprinosi tom praćenju trebali bi uključivati izvješća ENISA-e i redovita izvješća Komisije o sigurnosnoj uniji. Rezultati će utjecati na ciljeve predstojećeg digitalnog desetljeća[119]. Komisija i Visoki predstavnik će, u skladu sa svojim nadležnostima, nastaviti surađivati s državama članicama kako bi se utvrdile praktične mjere za povezivanje, prema potrebi, četiriju područja kibersigurnosti u Uniji: otpornost ključne infrastrukture i unutarnjeg tržišta, pravosuđe i izvršavanje zakonodavstva, kiberdiplomaciju i kiberobranu. Usto, Komisija i Visoki predstavnik nastavit će surađivati sa širom zajednicom dionika, ističući pritom potrebu da svi koji se služe internetom daju svoj doprinos održavanju globalnog, otvorenog, stabilnog i sigurnog kiberprostora u kojem svatko može sigurno živjeti svoj digitalni život.

[119] Kako je najavljeno u Programu rada Komisije za 2021.

Dodatak: Sljedeći koraci u području kibersigurnosti 5G mreža

Na temelju rezultata preispitivanja Preporuke Komisije o kibersigurnosti 5G mreža[120], sljedeći koraci u koordiniranom radu na razini EU-a trebali bi biti usmjereni na tri ključna cilja te na kratkoročne i srednjoročne glavne mjere utvrđene u tablici u nastavku, koje će provesti tijela država članica, Komisija i ENISA.

Prvi prioritet sljedeće faze jest **dovršetak provedbe paketa mjera na nacionalnoj razini i rješavanje pitanja utvrđenih u izvješću o napretku iz srpnja 2020**. U tom bi kontekstu **intenzivniji rad na koordinaciji ili razmjeni informacija** unutar radne skupine za NIS, kako je već utvrđeno u izvješću o napretku, mogao pozitivno utjecati na neke od strateških mjera iz paketa, a to bi moglo rezultirati **primjerima dobre prakse ili smjernicama**. Kad je riječ o tehničkim mjerama, ENISA bi na temelju prethodnog rada mogla pružiti dodatnu potporu detaljnijim razmatranjem određenih tema i **izradom sveobuhvatnog pregleda svih relevantnih smjernica o zahtjevima u pogledu kibersigurnosti 5G mreža za operatore pokretnih mreža**.

Drugo, države članice istaknule su važnost održavanja koraka s napretkom **neprekidnim praćenjem razvoja tehnologije, 5G arhitekture, prijetnji, primjene 5G tehnologije i 5G aplikacija te vanjskih čimbenika** kako bi se mogli **utvrditi i ukloniti novi rizici ili rizici u nastajanju**. Nadalje, trebalo bi dodatno razmotriti niz aspekata iz početne analize rizika, posebno kako bi se osiguralo da se odnosi na cijeli 5G ekosustav, uključujući sve relevantne dijelove mrežne infrastrukture i lanca opskrbe 5G tehnologijom. Iako je paket mjera osmišljen kao fleksibilan i prilagodljiv alat, u srednjem bi se roku, prema potrebi, mogli poduzeti koraci za njegovo proširenje ili izmjenu kako bi se osigurala njegova daljnja sveobuhvatnost i ažuriranost.

Treće, trebalo bi nastaviti poduzimati **mjere na razini EU-a** kako bi se poduprli i dopunili ciljevi paketa te kako bi ih se u potpunosti integriralo u relevantne politike Unije i Komisije, posebno u skladu s mjerama koje je Komisija najavila u Komunikaciji o paketu instrumenata od 29. siječnja 2020.[121] u raznim područjima (npr. financiranje EU-a za sigurne 5G mreže, ulaganja u 5G i buduće tehnologije, instrumenti trgovinske zaštite i tržišno natjecanje kako bi se izbjeglo narušavanje tržišta za 5G tehnologiju itd.).

Glavni akteri trebali bi, prema potrebi, početkom 2021. postići dogovor o detaljnim aranžmanima i najvažnijim etapama za glavne mjere navedene u nastavku.

Ključni cilj br. 1: osiguravanje usklađenih nacionalnih pristupa za djelotovorno smanjivanje rizika u cijeloj Uniji		
Područja	**Glavne kratkoročne i srednjoročne mjere**	**Glavni akteri**
Provedba paketa mjera u državama članicama	dovršiti provedbu mjera preporučenih u zaključcima o paketu do drugog tromjesečja 2021., uz povremene preglede stanja u okviru radne skupine za NIS	tijela država članica
Razmjena informacija	intenzivirati razmjenu informacija i razmotriti moguće	tijela država

[120] Izvješće Komisije o učincima Preporuke Komisije 2019/534 od 26. ožujka 2019. o kibersigurnosti 5G mreža.
[121] Komunikacija Komisije, Sigurno uvođenje 5G mreža u EU-u – Provedba paketa instrumenata EU-a, 29. siječnja 2020., COM(2020) 50 final

i primjera dobre prakse u pogledu strateških mjera koje se odnose na dobavljače	primjere dobre prakse, posebno u pogledu: - ograničenja za visokorizične dobavljače (SM03) i mjera povezanih s pružanjem upravljanih usluga (SM04) - sigurnosti i otpornosti lanca opskrbe, posebno na temelju ankete koju je BEREC proveo o SM05/SM06	članica, Komisija
Izgradnja kapaciteta i smjernice o tehničkim mjerama	provesti detaljne tehničke analize te izraditi zajedničke smjernice i alate, uključujući: - sveobuhvatnu i dinamičnu matricu sigurnosnih kontrola i primjera dobre prakse za sigurnost 5G mreža smjernice za provedbu odabranih tehničkih mjera iz paketa	ENISA, tijela država članica
Ključni cilj br. 2: potpora stalnoj razmjeni znanja i izgradnji kapaciteta		
Područja	**Glavne kratkoročne i srednjoročne mjere**	**Glavni akteri**
Kontinuirano stjecanje znanja	organizirati aktivnosti stjecanja znanja o tehnologiji i povezanim izazovima (otvorene arhitekture, karakteristike 5G mreža – npr. virtualizacija, kontejnerizacija, segmentiranje itd.), stanju prijetnji, stvarnim incidentima itd.	ENISA, tijela država članica, drugi dionici
Procjene rizika	ažurirati i razmjenjivati informacije o ažuriranim nacionalnim procjenama rizika	tijela država članica, Komisija, ENISA
Zajednički projekti koje financira EU za potporu provedbi mjera iz paketa	osigurati financijsku potporu iz sredstava EU-a projektima kojima se podupire provedba paketa, posebno u okviru programa Digitalna Europa (npr. projekti izgradnje kapaciteta za nacionalna tijela, testna okruženja ili drugi napredni kapaciteti itd.)	tijela država članica, Komisija
Suradnja dionika	poticati suradnju nacionalnih tijela koja se bave kibersigurnošću 5G mreža (npr. Skupina za suradnju u području NIS-a, tijela za kibersigurnost, regulatorna tijela za telekomunikacije) i s privatnim dionicima	tijela država članica, Komisija, ENISA
Ključni cilj br. 3: promicanje otpornosti opskrbnog lanca i drugi strateški sigurnosni ciljevi EU-a		
Područja	**Glavne kratkoročne i srednjoročne mjere**	**Glavni akteri**
Normizacija	definirati i provesti konkretan akcijski plan za povećanje zastupljenosti EU-a u tijelima za normizaciju u okviru idućih koraka u radu podskupine za normizaciju u području NIS-a kako bi se ostvarili specifični sigurnosni ciljevi, uključujući promicanje interoperabilnih sučelja radi lakše diversifikacije dobavljača	tijela država članica
Otpornost opskrbnog lanca	– provesti dubinsku analizu 5G ekosustava i opskrbnog lanca radi boljeg utvrđivanja i praćenja ključne infrastrukture te potencijalnih kritičnih ovisnosti – osigurati usklađenost funkcioniranja tržišta i opskrbnog lanca za 5G tehnologiju s pravilima i ciljevima EU-a u području trgovine i tržišnog natjecanja, kako su definirani u Komunikaciji Komisije od 29. siječnja, te primjenu provjere izravnih stranih ulaganja na ulaganja koja mogu utjecati na	tijela država članica, Komisija

	vrijednosni lanac 5G tehnologije, uzimajući u obzir ciljeve paketa – pratiti postojeće i očekivane tržišne trendove te procjenjivati rizike i mogućnosti u području otvorene radijske pristupne mreže (Open RAN), posebno provedbom neovisne studije	
Certifikacija	početi pripremu relevantnih prijedloga programa certifikacije za ključne komponente 5G mreže i procese dobavljača kako bi pridonijelo uklanjanju određenih rizika povezanih s tehničkim slabim točkama, kako je utvrđeno u planovima smanjenja rizika u paketu	Komisija, ENISA, nacionalna tijela i drugi dionici
Kapaciteti EU-a i sigurno uvođenje mreža	– ulagati u istraživanje i razvoj te kapacitete, među ostalim uspostavom partnerstva za pametne mreže i usluge – uvesti relevantne sigurnosne uvjete za programe financiranja i financijske instrumente EU-a (unutarnje i vanjske), kako je najavljeno u Komunikaciji Komisije od 29. siječnja	države članice, Komisija, dionici iz sektora 5G mreža
Vanjski aspekti	pozitivno odgovoriti na zahtjeve trećih zemalja koje žele razumjeti i potencijalno upotrebljavati pristup koji se temelji na paketu mjera razvijenih u EU-u	države članice, Komisija, ESVD, delegacije EU-a