



EVROPSKA
KOMISIJA

VISOKI PREDSTAVNIK
UNIJE ZA ZUNANJE
ZADEVE IN
VARNOSTNO POLITIKO

Bruselj, 16.12.2020
JOIN(2020) 18 final

SKUPNO SPOROČILO EVROPSKEMU PARLAMENTU IN SVETU

Strategija EU za kibernetško varnost v digitalnem desetletju

SKUPNO SPOROČILO EVROPSKEMU PARLAMENTU IN SVETU

Strategija EU za kibernetško varnost v digitalnem desetletju

I. UVOD: KIBERNETSKO VARNA DIGITALNA PREOBRAZBA V KOMPLEKSNEM OKOLJU GROŽENJ

Kibernetška varnost je neločljiv del varnosti Evropejcev. Evropejci si ne glede na to, ali uporabljajo povezane naprave ali električno omrežje ali obiščejo banke, letala, javne uprave ali bolnišnice, zaslužijo, da lahko to počnejo z vedenjem, da so zavarovani pred kibernetškimi grožnjami. Gospodarstvo, demokracija in družba EU so bolj kot kdaj koli odvisni od varnih in zanesljivih digitalnih orodij in povezljivosti. Kibernetška varnost je zato bistvena za izgradnjo odporne, zelene in digitalne Evrope.

Promet, energija in zdravje, telekomunikacije, finance, varnost, demokratični procesi, veselje in obramba so močno odvisni od omrežij in informacijskih sistemov, ki so vse bolj medsebojno povezani. Medsebojne odvisnosti med sektorji so zelo močne, ker je delovanje omrežij in informacijskih sistemov odvisno od stalne oskrbe z električno energijo. Število povezanih naprav je že zdaj večje od števila ljudi na planetu, njihovo število pa se bo po napovedih do leta 2025 povečalo na 25 milijard¹; četrtnina teh naprav bo v Evropi. Pandemija COVID-19, med katero je 40 % delavcev v EU prešlo na delo na daljavo, je pospešila digitalizacijo delovnih vzorcev, kar bo imelo verjetno trajne učinke na vsakdanje življenje². S tem se povečuje ranljivost za kibernetške napade³. Potrošnikom se pogosto pošiljajo povezani predmeti z znanimi ranljivostmi, kar še dodatno povečuje napadno površino za zlonamerne kibernetške dejavnosti⁴. Industrijsko okolje v EU postaja vse bolj digitalizirano in povezano; to tudi pomeni, da imajo lahko kibernetški napadi večji vpliv na panoge in ekosisteme kot kadar koli prej.

Okolje groženj dopolnjujejo geopolitične napetosti v zvezi z globalnim in odprtim internetom ter nadzorom nad tehnologijami v celotni dobavni verigi⁵. Te napetosti se odražajo v vse večjem številu nacionalnih držav, ki postavljajo digitalne meje. Omejitve

¹ Ocena združenja telekomunikacijskih operaterjev GSMA; <https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf>. Družba International Data Corporation napoveduje 42,6 milijarde povezanih strojev, senzorjev in kamer; <https://www.idc.com/getdoc.jsp?containerId=prUS45213219>.

² V raziskavi, izvedeni junija 2020, je 47 % vodij podjetij navedlo, da nameravajo zaposlenim omogočiti delo na daljavo s polnim delovnim časom tudi potem, ko se bo mogoče vrniti na delovno mesto; 82 % jih je nameravalo delo na daljavo dovoliti vsaj del časa; <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 Ena od najbolj uničujočih zlonamernih programskih oprem doslej, znana kot Mirai, je ustvarila botnete več kot 600 000 napravami, ki so povzročali motnje na več pomembnih spletnih mestih v Evropi in ZDA.

⁵ Vključno z elektronskimi sestavnimi deli, podatkovno analitiko, oblakom, hitrejšimi in pametnejšimi omrežji s tehnologijo 5G in naslednjimi, šifriranjem, umetno inteligenco ter novimi računalniškimi paradigmi in paradigmi obdelave zaupanja vrednih podatkov, kot so blokovna veriga, z oblaka na rob in kvantno računalništvo.

interneta in na internetu ogrožajo globalen in odprt kibernetski prostor ter pravno državo, temeljne pravice, svobodo in demokracijo – temeljne vrednote EU. Kibernetski prostor se vse bolj izkorišča v politične in ideološke namene, večja polarizacija na mednarodni ravni pa ovira učinkovit multilateralizem. Hibridne grožnje združujejo dezinformacijske kampanje s kibernetskimi napadi na infrastrukturo, ekonomske procese in demokratične institucije, s katerimi se lahko povzroči fizična škoda, pridobi nezakonit dostop do osebnih podatkov, ukradejo industrijske ali državne skrivnosti, zaseje nezaupanje in oslabi socialna kohezija. Te dejavnosti ogrožajo mednarodno varnost in stabilnost ter koristi, ki jih kibernetski prostor prinaša za gospodarski, družbeni in politični razvoj.

Zlonamerni napadi na kritično infrastrukturo pomenijo veliko tveganje na svetovni ravni⁶. Internet ima decentralizirano arhitekturo brez centralne strukture in večdeležniško upravljanje. Uspeva mu ohranjati eksponentno povečevanje obsega prometa, medtem ko je stalno tarča zlonamernih poskusov povzročanja motenj⁷. Hkrati se povečuje zanašanje na glavne funkcije globalnega in odprtega interneta, kot je sistem domenskih imen (DNS), ter bistvene internetne storitve za komunikacije in gostovanje, aplikacije in podatke. Te storitve se vse bolj koncentrirajo v rokah nekaj zasebnih podjetij⁸. Zato sta evropsko gospodarstvo in družba občutljiva za moteče geopolitične ali tehnične dogodke, ki vplivajo na jedro interneta ali eno ali več od teh podjetij. Večja uporaba interneta in spreminjajoči se vzorci zaradi pandemije dodatno razkrivajo občutljivost dobavnih verig, ki so odvisne od te digitalne infrastrukture.

Od uporabe spletnih storitev najbolj odvrčajo pomisleki glede varnosti⁹. Približno dve petini uporabnikov v EU sta že izkusili težave, povezane z varnostjo, tri petine pa se jih čuti nesposobne zaščititi se pred kibernetsko kriminaliteto¹⁰. Tretjina uporabnikov je v zadnjih treh letih prejela goljufivo e-sporočilo ali telefonske klice z zahtevo po osebnih podatkih, vendar pa jih ni 83 % nikoli prijavilo kibernetskega kaznivega dejanja. Ena od osmih podjetij je bilo žrtev kibernetskih napadov¹¹. Več kot polovica osebnih računalnikov podjetij in potrošnikov, ki so bili enkrat okuženi z zlonamerno programsko opremo, je bila v istem letu

⁶ Svetovni gospodarski forum, The Global Risks Report 2020 (Poročilo o svetovnih tveganjih za leto 2020).

⁷ Po podatkih Organizacije za gospodarsko sodelovanje in razvoj se je zaradi pandemije internetni promet povečal za 60 %; <https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/>. Organ evropskih regulatorjev za elektronske komunikacije in Komisija redno objavljata [poročila](#) o stanju zmogljivosti interneta med ukrepi omejitve gibanja zaradi koronavirusa. Glede na poročilo agencije ENISA se je v tretjem četrtletju leta 2019 skupno število porazdeljenih napadov za zavrnitev storitve (DDoS) povečalo za 241 % v primerjavi s tretjim četrtletjem leta 2018. Povečuje se intenzivnost navedenih napadov, pri čemer se je doslej največji napad zgodil februarja 2020, ko je bil dosežen največji promet, in sicer 2,3 terabita na sekundo. Med t. i. izpadom CenturyLink avgusta 2020 je težava z usmerjanjem ponudnika internetnih storitev iz ZDA povzročila 3,5-odstotno zmanjšanje globalnega spletnega prometa; <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 (Poročilo o globalnem internetu: konsolidacija internetnega 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/sl/data/dataset/S2249_92_2_499_ENG.

¹⁰ Indeks digitalnega gospodarstva in družbe za leto 2020; <https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020>; https://data.europa.eu/euodp/sl/data/dataset/S2249_92_2_499_ENG.

¹¹ Eurostatovo sporočilo za javnost, „ICT security measures taken by vast majority of enterprises in the EU“ (Varnostni ukrepi na področju IKT, sprejeti v večini podjetij v EU), 6/2020 – 13. januar 2020. „Kibernetski napadi na kritično infrastrukturo so postali nova normalnost v sektorjih, kot so energetika, zdravstveno varstvo in promet“; WEF, The Global Risks Report 2020 (Poročilo o globalnih tveganjih za leto 2020).

spet okužena¹². Vsako leto se zaradi kršitev varstva podatkov izgubi več sto milijonov zapisov; povprečni stroški kršitve za posamezno podjetje so se leta 2018 zvišali na več kot 3,5 milijona EUR¹³. Vpliva kibernetkega napada pogosto ni mogoče obravnavati ločeno, saj lahko sproži verižno reakcijo v celotnem gospodarstvu in družbi ter prizadene več milijonov posameznikov¹⁴.

Preiskave skoraj vseh vrst kaznivih dejanj vključujejo digitalno komponento. Leta 2019 se je število incidentov na medletni ravni glede na poročila potrojilo. Po ocenah obstaja 700 milijonov novih vzorcev zlonamerne programske opreme – najpogostejšega sredstva za širjenje kibernetkih napadov¹⁵. Letni stroški kibernetke kriminalitete za svetovno gospodarstvo v letu 2020 so ocenjeni na 5,5 bilijona EUR, kar je dvakrat toliko kot leta 2015¹⁶. To predstavlja največji prenos gospodarskega premoženja v zgodovini, večji od trgovine s prepovedanimi drogami na svetovni ravni. Pri enem od večjih incidentov, napadu z izsiljevalskim programjem WannaCry leta 2017, so bili stroški za svetovno gospodarstvo ocenjeni na več kot 6,5 milijarde EUR¹⁷.

Digitalne storitve in finančni sektor so poleg javnega sektorja in proizvodnje med najpogostejšimi tarčami kibernetkih napadov, vendar kibernetka pripravljenost in ozaveščenost med podjetji in posamezniki ostajata na nizki ravni¹⁸, delovni sili pa zelo primanjkuje znanj in spretnosti na področju kibernetke varnosti¹⁹. Leta 2019 je bilo skoraj 450 kibernetkih incidentov, ki so vključevali evropsko kritično infrastrukturo, kot so finance in energija²⁰. Zdravstvene organizacije in zdravstvene delavce je pandemija še posebno močno prizadela. Ker postaja tehnologija neločljivo povezana s fizičnim svetom, kibernetki napadi ogrožajo življenja in dobro počutje najbolj ranljivih²¹. Več kot dve tretjini podjetij, zlasti MSP, se štejeta za „novince“ na področju kibernetke varnosti, evropska podjetja pa veljajo za slabše pripravljena kot podjetja v Aziji in Ameriki²². Po ocenah ostaja v Evropi prostih 291 000 delovnih mest za strokovnjake na področju kibernetke varnosti.

¹² Vir: Comparitech.

¹³ Letno poročilo inštituta Ponemon Institute o stroških kršitev varstva podatkov za leto 2020 in na podlagi kvantitativne analize 524 nedavnih kršitev na 17 geografskih območjih in v 17 panogah; <https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf>.

¹⁴ Poročilo Skupnega raziskovalnega središča z naslovom „Cybersecurity, our digital anchor“ (Kibernetka varnost, naše digitalno sidro); <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor>.

¹⁵ Vir: AV-TEST, <https://www.av-test.org/en/statistics/malware/>.

¹⁶ Skupno raziskovalno središče, Cybersecurity – Our Digital Anchor (Kibernetka varnost – naše digitalno sidro).

¹⁷ Vir: Cyence.

¹⁸ Ozaveščenost podjetij ostaja na nizki ravni tudi v zvezi s kibernetko krajo poslovnih skrivnosti, zlasti med MSP; PwC, študija o obsegu in učinku industrijskega vohunjenja in kraje poslovnih skrivnosti v kibernetkem prostoru: poročilo o razširjanju ukrepov za obravnavanje in preprečevanje kibernetke kraje poslovnih skrivnosti, 2018.

¹⁹ Glej poročilo agencije ENISA o grožnjah v letu 2020 (ENISA Threat Landscape 2020). Tudi poročilo družbe Verizon o preiskavah kršitev varstva podatkov za leto 2020 (Data Breach Investigations Report 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 Izsiljevalsko programje je bilo uporabljeno za napade na bolnišnice in zdravstveno dokumentacijo na primer v Romuniji (junija 2020), Düsseldorfu (septembra 2020) in Vastaamu (oktobra 2020).

²² PwC, The Global State of Information Security 2018 (Globalno stanje informacijske varnosti v letu 2018); ESI Thoughtlab, The Cybersecurity Imperative (Nujnost kibernetke varnosti), 2019.

Zaposlovanje in usposabljanje strokovnjakov za kibernetiko varnost je počasen proces, zaradi česar so tveganja za kibernetiko varnost za organizacije večja²³.

V EU primanjkuje kolektivnega situacijskega zavedanja kibernetičnih groženj. Nacionalni organi namreč sistematično ne zbirajo in si izmenjujejo informacij, kot so informacije, ki so na voljo iz zasebnega sektorja, kar bi lahko pomagalo oceniti stanje na področju kibernetične varnosti v EU. Države članice poročajo samo o majhnem delu incidentov, izmenjava informacij ni niti sistematična niti celovita²⁴, kibernetični napadi pa so lahko le en vidik usklajenih zlonamernih napadov na evropske družbe. Trenutno med državami članicami obstaja le omejena vzajemna operativna pomoč, med državami članicami ter institucijami, agencijami in organi EU pa ni vzpostavljen operativni mehanizem za primer obsežnih čezmejnih kibernetičnih incidentov ali kibernetične krize²⁵.

Izboljšanje kibernetične varnosti je zato bistveno, da bi lahko ljudje zaupali inovacijam, poveztivosti in avtomatizaciji ter jih uporabljali in izkoriščali, ter za zaščito temeljnih pravic in svoboščin, vključno s pravico do zasebnosti in varstva osebnih podatkov, ter svobode izražanja in obveščanja. Kibernetična varnost je nepogrešljiva za omrežno poveztivost ter globalen in odprt internet, ki morata podpirati preobrazbo gospodarstva in družbe v dvajsetih letih 21. stoletja. Prispeva k ustvarjanju boljših in številčnejših delovnih mest, prožnejšim delovnim mestom, učinkovitejšima in bolj trajnostnima prometu in kmetijstvu ter enostavnejšemu in pravičnejšemu dostopu do zdravstvenih storitev. Bistvena je tudi za prehod na čistejšo energijo v skladu z evropskim zelenim dogovorom²⁶, in sicer s čezmejnimi omrežji in pametnimi števci ter preprečevanjem nepotrebnega podvajanja shranjevanja podatkov. Bistvena je tudi za mednarodno varnost in stabilnost ter razvoj gospodarstev, demokracij in družb po vsem svetu. Vlade, podjetja in posamezniki morajo zato digitalna orodja uporabljati odgovorno in ob poudarjanju varnosti. Ozaveščenost o kibernetični varnosti in kibernetična higiena morata podpirati digitalno preobrazbo vsakdanjih dejavnosti.

Nova strategija EU za kibernetiko varnost v digitalnem desetletju je ključni element sporočila Oblikovanje digitalne prihodnosti²⁷, načrta Komisije za okrevanje Evrope²⁸, strategije za varnostno unijo za obdobje 2020–2025²⁹, globalne strategije za zunanjo in varnostno politiko EU³⁰ ter strateške agende Evropskega sveta za obdobje 2019–2024³¹. V njej je opredeljeno, kako bo EU ščitila svoje državljane, podjetja in institucije pred kibernetičnimi grožnjami, kako bo spodbujala mednarodno sodelovanje ter imela vodilno vlogo pri zagotavljanju zaščite globalnega in odprtega interneta.

²³ Agencija Evropske unije za kibernetiko varnost, Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees and ENISA's Higher Education Database (Razvoj znanj in spretnosti na področju kibernetične varnosti v EU: potrjevanje diplom s področja kibernetične varnosti in podatkovna zbirka agencije ENISA o visokošolskem izobraževanju), december 2019.

²⁴ Države članice morajo skupini za sodelovanje predložiti letno zbirno poročilo o priglasitvah, prejetih v skladu s členom 10(3) direktive o varnosti omrežij in informacijskih sistemov (Direktiva (EU) 2016/1148).

²⁵ Vzpostavljeni so standardni postopki delovanja za vzajemno pomoč med člani mreže skupin CSIRT.

²⁶ Evropski zeleni dogovor, COM(2019) 640 final.

²⁷ Oblikovanje digitalne prihodnosti Evrope, COM(2020) 67 final.

²⁸ Čas za Evropo: obnova in priprava za naslednjo generacijo, COM(2020) 98 final.

²⁹ Strategija EU za varnostno unijo za obdobje 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/#>.

II. RAZMIŠLJATI GLOBALNO, DELOVATI EVROPSKO

Cilj te strategije je zagotoviti globalen in odprt internet z močnimi varovali za obravnavanje tveganj za varnost ter temeljne pravice in svoboščine prebivalcev Evrope. Izhajajoč iz napredka, doseženega v okviru prejšnjih strategij, vsebuje konkretne predloge za uvedbo **treh glavnih instrumentov – regulativnega in naložbenega instrumenta ter instrumenta politike** – za obravnavanje **treh področij delovanja EU – (1) odpornosti, tehnološke neodvisnosti in vodilne vloge, (2) krepitve operativne zmogljivosti za preprečevanje, odvratanje in odzivanje ter (3) spodbujanja globalnega in odprtega kibernetnega prostora**. EU je zavezana podpiranju te strategije z **doslej najvišjo ravno naložb v digitalni prehod EU v naslednjih sedmih letih** – ki bi bila lahko štirikrat tolikšna kot prejšnje ravni – v okviru novih tehnoloških in industrijskih politik ter programa okrevanja³².

Kibernetna varnost mora biti vključena v vse te digitalne naložbe, zlasti ključne tehnologije, kot so umetna inteligenca, šifriranje in kvantno računalništvo, pri tem pa je treba uporabiti spodbude, obveznosti in referenčne vrednosti. To lahko spodbudi rast evropske industrije kibernetne varnosti in poskrbi za gotovost, ki je potrebna za olajšanje postopne odprave starejših sistemov. Evropski obrambni sklad bo podprl evropske rešitve za kibernetno obrambo v okviru tehnološke in industrijske baze evropske obrambe. Kibernetna varnost je vključena v zunanje finančne instrumente za podpiranje naših partnerjev, zlasti instrument za sosedstvo ter razvojno in mednarodno sodelovanje. Preprečevanje zlorabe tehnologij, zaščita kritične infrastrukture in zagotavljanje celovitosti dobavnih verig prav tako omogočajo EU, da upošteva norme, pravila in načela OZN glede odgovornega ravnanja držav³³.

1. ODPORNOST, TEHNOLOŠKA NEODVISNOST IN VODILNI POLOŽAJ

Kritična infrastruktura EU in bistvene storitve so vse bolj soodvisne in digitalizirane. Vse z internetom povezane stvari v EU, naj so to avtomatizirani avtomobili, industrijski nadzorni sistemi ali gospodinjinski aparati, in celotne dobavne verige, ki jih dajejo na voljo, morajo imeti vgrajeno varnost, biti odporne proti kibernetnim incidentom in hitro popravljene, kadar se odkrijejo ranljivosti. To je temeljnega pomena, da se zasebnemu in javnemu sektorju EU omogoči izbiranje med najbolj varnimi infrastrukturami in storitvami. Prihodnje desetletje je priložnost za EU, da vodi razvoj varnih tehnologij v celotni dobavni verigi. Z zagotavljanjem odpornosti ter večjih industrijskih in tehnoloških zmogljivosti na področju kibernetne varnosti bi bilo treba mobilizirati vse potrebne regulativne in naložbene instrumente ter instrumente politike. Vgrajena kibernetna varnost za industrijske procese, dejavnosti in naprave lahko ublaži tveganja, potencialno zniža stroške za podjetja in širšo družbo ter s tem poveča odpornost.

³² Naložbe v celotni dobavni verigi digitalne tehnologije, ki prispevajo k digitalnemu prehodu ali obravnavanju izzivov, ki izhajajo iz njega, bi morale predstavljati vsaj 20 % – tj. 134,5 milijarde EUR – nepovratnih sredstev in posojil mehanizma za okrevanje in odpornost, katerega proračun znaša 672,5 milijarde EUR. Finančna sredstva EU v večletnem finančnem okviru za obdobje 2021–2027, ki so predvidena za kibernetno varnost v okviru programa za digitalno Evropo in za raziskave na področju kibernetne varnosti v okviru programa Obzorje Evropa, s posebnim poudarkom na podpori za MSP, bi lahko skupno znašala 2 milijardi EUR, temu pa je mogoče dodati naložbe držav članic in industrije.

³³ <https://undocs.org/A/70/174>.

1.1 Odporna infrastruktura in kritične storitve

Pravila EU o varnosti omrežij in informacijskih sistemov so v središču enotnega trga za kibernetško varnost. Komisija predlaga reformo teh pravil v okviru revidirane direktive o varnosti omrežij in informacij za zvišanje ravni **kibernetške odpornosti vseh ustreznih sektorjev, javnih in zasebnih, ki opravljajo pomembno funkcijo za gospodarstvo in družbo**³⁴. Potreben je pregled za zmanjšanje neskladnosti na notranjem trgu z uskladitvijo zahtev glede obsega, varnosti in poročanja o incidentih, nacionalnega nadzora in izvrševanja ter zmogljivosti pristojnih organov.

Reformirana direktiva o varnosti omrežij in informacij bo zagotovila podlago za natančnejša pravila, ki so potrebna tudi za strateško pomembne sektorje, vključno z energijo, prometom in zdravjem. Za zagotovitev usklajenega pristopa, kot je bil napovedan v okviru strategije za varnostno unijo za obdobje 2020–2025, je reformirana direktiva predlagana skupaj s pregledom zakonodaje o odpornosti kritične infrastrukture³⁵. Energetske tehnologije, ki vključujejo digitalne elemente, in varnost povezanih dobavnih verig so pomembne za kontinuiteto bistvenih storitev in strateški nadzor nad kritično energetske infrastrukturo. Komisija bo zato predlagala ukrepe, vključno z „omrežnim kodeksom“, ki bo določal pravila za kibernetško varnost pri čezmejnih tokovih električne energije, ki naj bi bila sprejeta do konca leta 2022. Finančni sektor mora tudi okrepiti digitalno operativno odpornost in zagotoviti zmožnost zoperstavljanja vsem vrstam motenj in groženj, povezanih z IKT, kot je predlagala Komisija³⁶. Na področju prometa je Komisija zakonodaji EU na področju varovanja v letalstvu dodala določbe o kibernetški varnosti³⁷ in si bo še naprej prizadevala povečati kibernetško odpornost pri vseh načinih prevoza. Okrepitev kibernetške odpornosti **demokratičnih procesov in institucij** je ključna sestavina akcijskega načrta za evropsko demokracijo za zaščito in spodbujanje svobodnih volitev ter demokratičnega dialoga in medijske pluralnosti³⁸. Nazadnje, za varnost infrastrukture in storitev v okviru prihodnjega vesoljskega programa bo Komisija še naprej poglobljala strategijo za kibernetško varnost v okviru sistema Galileo za naslednjo generacijo storitev globalnega satelitskega navigacijskega sistema in druge nove elemente vesoljskega programa³⁹.

1.2 Vzpostavitev evropskega kibernetškega ščita

S širitvijo poveztljivosti in vse večjo izpopolnjenostjo kibernetških napadov centri za izmenjavo in analizo informacij z omogočanjem izmenjave informacij o kibernetških grožnjah med več deležniki opravljajo dragoceno funkcijo, tudi na sektorski ravni⁴⁰. Poleg tega omrežja in računalniški sistemi zahtevajo stalno spremljanje in analizo za odkrivanje vdorov in anomalij v realnem času. Veliko zasebnih podjetij, javnih organizacij in

³⁴ [vstaviti sklic na predlog o varnosti omrežij in informacij].

³⁵ [vstaviti sklic na predlog direktive o odpornosti kritičnih subjektov].

³⁶ Predlog uredbe o digitalni operativni odpornosti finančnega sektorja ter spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014 in (EU) št. 909/2014 (COM(2020) 595 final).

³⁷ Izvedbena uredba Komisije (EU) 2019/1583.

³⁸ Sporočilo o akcijskem načrtu za evropsko demokracijo (COM(2020) 790). V skladu z načrtom bo evropska mreža za volilno sodelovanje, tj. volilne mreže držav članic, podpirala uvedbo skupnih skupin strokovnjakov za preprečevanje groženj, vključno s kibernetskimi napadi, za volilne procese; https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_sl.

³⁹ To vključuje novo vladno pobudo za satelitske komunikacije (GOVSATCOM) in vesoljske odpadke (SST).

⁴⁰ <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing>.

nacionalnih organov je zato ustanovilo skupine za odzivanje na incidente na področju računalniške varnosti in centre za varnostne operacije.

Centri za varnostne operacije so ključni za zbiranje dnevnikov⁴¹ in osamitev sumljivih dogodkov v komunikacijskih omrežjih, ki jih spremljajo. To počnejo z identifikacijo signalov in vzorcev ter pridobivanjem znanja o grožnjah iz velikih količin podatkov, ki jih je treba oceniti. Prispevali so k odkrivanju dejavnosti zlonamernih izvršljivih datotek in s tem pomagali omejevati kibernetike napade. V teh centrih je potrebno zelo zahtevno in hitro delo, zato lahko umetna inteligenca in zlasti tehnike strojnega učenja strokovnjakom zagotovijo neprecenljivo podporo⁴².

Komisija predlaga vzpostavitev **mreže centrov za varnostne operacije v EU**⁴³ za podpiranje izboljšanja obstoječih centrov in ustanovitve novih. Podpirala bo tudi usposabljanje ter razvoj znanj in spretnosti osebja, ki upravlja te centre. Na podlagi analize potreb, izvedene z ustreznimi deležniki in podprte s strani Agencije EU za kibernetiko varnost (agencija ENISA), bi lahko namenila več kot 300 milijonov EUR za podpiranje javno-zasebnega in čezmejnega sodelovanja pri ustvarjanju nacionalnih in sektorskih mrež, ki bo vključevalo tudi MSP, na podlagi ustreznega upravljanja, izmenjave podatkov in varnostnih določb.

Države članice so bile pozvane, naj prav tako vlagajo v ta projekt. Centri bi lahko zato učinkoviteje izmenjevali in povezovali zaznane signale ter ustvarjali visokokakovostne obveščevalne podatke o grožnjah, ki bi se delili s centri za izmenjavo in analizo informacij ter nacionalnimi organi, s čimer bi se omogočilo celovitejše situacijsko zavedanje. Cilj bi bil v več fazah povezati čim več centrov po vsej EU za ustvarjanje kolektivnega znanja in izmenjavo dobrih praks. Tem centrom bo na voljo podpora za izboljšanje odkrivanja incidentov in analize ter hitrejše odzivanje z najnovejšimi zmogljivostmi umetne inteligence in strojnega učenja, ki bo dopolnjena s superračunalniško infrastrukturo, ki jo je v EU razvilo Skupno podjetje za evropsko visokozmogljivostno računalništvo⁴⁴.

Ta mreža bo s stalnim sodelovanjem zagotavljala pravočasna opozorila o incidentih na področju kibernetike varnosti organom in vsem zainteresiranim deležnikom, vključno s skupno kibernetiko enoto (glej oddelek 2.1). **Delovala bo kot pravi ščit kibernetike varnosti za EU**, pri čemer bo zagotavljala trdno mrežo stražnih stolpov, ki bo lahko odkrila morebitne grožnje, preden bi lahko povzročile obsežno škodo.

1.3 Izjemno varna komunikacijska infrastruktura

Vladne satelitske komunikacije Evropske unije⁴⁵, ki so sestavni del vesoljskega programa, bodo zagotavljale varne in stroškovno učinkovite vesoljske komunikacijske zmogljivosti za misije, ki so pomembne za varnost in zaščito, ter operacije, ki jih upravljajo EU in njene

⁴¹Na tak način, da jih lahko organi kazenskega pregona in sodstvo uporabijo kot dokaz.

⁴²Vir: raziskava inštituta Ponemon Institute, „Improving the Effectiveness of the SOC, 2019“ (Izboljšanje učinkovitosti centrov za operativno varnost, 2019); za študije o uporabi umetne inteligence v centrih za operativno varnost glej na primer: Khraisat, A., Gondal, I., Vamplew, P., in drugi. Survey of intrusion detection systems: techniques, datasets and challenges (Raziskava o sistemih za odkrivanje vdorov: tehnike, nabori podatkov in izzivi), *Cybersecur* 2, 20 (2019).

⁴³Razvite bodo podrobnejše ureditve za upravljanje, načela delovanja in financiranje teh centrov, pri čemer bo opredeljeno, kako bodo dopolnjevale obstoječe strukture, kot so vozlišča za digitalne inovacije.

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

⁴⁵Vladne satelitske komunikacije so sestavni del vesoljskega programa Unije.

države članice, vključno z akterji na področju nacionalne varnosti ter institucijami, organi in agencijami EU.

Države članice so se zavezale, da bodo sodelovale s Komisijo v prizadevanjih za uvedbo varne kvantne komunikacijske infrastrukture za Evropo⁴⁶. Kvantna komunikacijska infrastruktura bo javnim organom ponudila povsem nov način za pošiljanje zaupnih informacij z uporabo izjemno varne oblike šifriranja za zaščito pred kibernetскими napadi, vgrajene z evropsko tehnologijo. Imela bo dva glavna sestavna dela: obstoječa prizemna optična komunikacijska omrežja, ki bodo povezovala strateška območja na nacionalni in čezmejni ravni, ter povezane vesoljske satelite, ki bodo pokrivali celotno EU, vključno z njenimi čezmorskimi ozemlji⁴⁷. Ta pobuda za razvoj in uvedbo novih in varnejših oblik šifriranja ter oblikovanje novih načinov zaščite kritičnih komunikacijskih in podatkovnih sredstev lahko pomaga ohranjati varnost občutljivih informacij in s tem kritične infrastrukture.

V tem okviru in zunaj njega bo Komisija proučila morebitno uvedbo večorbitalnega sistema varne povezljivosti. Sistem, ki bi temeljil na vladnih satelitskih komunikacijah in kvantni komunikacijski infrastrukturi, bi vključeval najnovejše tehnologije (kvantna, 5G, umetna inteligenca, računalništvo na robu), pri čemer bi se upošteval najbolj omejevalen okvir kibernetiske varnosti za podpiranje storitev z vgrajeno varnostjo, kot sta zanesljiva, varna in stroškovno učinkovita povezljivost ter šifrirana komunikacija za kritične vladne dejavnosti.

1.4 Zavarovanje naslednje generacije širokopasovnih mobilnih omrežij

Državljeni in podjetja EU, ki uporabljajo napredne in inovativne aplikacije, ki jih omogočajo **tehnologija 5G in prihodnje generacije omrežij**, bi morali imeti korist od najvišjega varnostnega standarda. Države članice so skupaj s Komisijo in s podporo agencije ENISA z naborem orodij za tehnologijo 5G⁴⁸ z januarjem 2020 vzpostavile celovit in objektivni na tveganju temelječ pristop h kibernetiski varnosti tehnologije 5G, ki temelji na oceni možnih načrtov za zmanjšanje tveganj in opredelitvi najučinkovitejših ukrepov. Poleg tega EU utrjuje svoje zmogljivosti na področju tehnologije 5G in tehnologijah, ki ji bodo sledile, da bi preprečila odvisnosti ter spodbujala trajnostno in raznovrstno dobavno verigo.

Komisija je decembra 2020 objavila poročilo o vplivih priporočila z dne 26. marca 2019 z naslovom Kibernetiska varnost omrežij 5G⁴⁹. Poročilo je pokazalo, da je bil od dogovora o

⁴⁶Izjavo o kvantni komunikacijski infrastrukturi za Evropo je podpisala večina držav članic, razvoj in uvedba infrastrukture pa naj bi potekala v obdobju 2021–2027 s finančnimi sredstvi iz programa Obzorje Evropa in programa za digitalno Evropo ter finančnimi sredstvi Evropske vesoljske agencije na podlagi ustreznih dogovorov glede upravljanja; <https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network>.

⁴⁷Za vzpostavitev povezav od točke do točke na dolge razdalje (> 1 000 km), ki jih zemeljska infrastruktura ne more podpirati, je potreben razvoj vesoljske komponente. Kvantna komunikacijska infrastruktura bo z izkoriščanjem značilnosti kvantne mehanike najprej stranem omogočila varno izmenjavo naključnih skrivnih ključev za šifriranje in dešifriranje sporočil. Vključevala bo tudi vzpostavitev preskusne in usklajevalne infrastrukture za ocenjevanje skladnosti evropskih kvantnih komunikacijskih naprav in sistemov s kvantno komunikacijsko infrastrukturo ter njihovo certificiranje in potrjevanje pred njihovo vključitvijo v kvantno komunikacijsko infrastrukturo. Zasnovana bo za podpiranje dodatnih aplikacij, ko bodo dosegle potrebno raven tehnološke zrelosti. Sedanji pilotni projekt OpenQKD (<https://openqkd.eu/>) je predhodnik te preskusne in usklajevalne infrastrukture.

⁴⁸Sporočilo o varni uvedbi tehnologije 5G v EU – izvajanje nabora orodij, COM(2020) 50.

⁴⁹Poročilo Komisije o vplivih priporočila Komisije z dne 26. marca 2019 z naslovom Kibernetiska varnost omrežij 5G, 15. december 2020.

naboru orodij dosežen velik napredek in da je večina držav članic na dobri poti, da v bližnji prihodnosti dokonča velik del uvajanja nabora orodij, čeprav z nekaj odstopanji in preostalimi vrzelmi, kot so bile opredeljene že v poročilu o napredku, objavljenem julija 2020⁵⁰.

Evropski svet je oktobra 2020 pozval EU in države članice, „naj v celoti izkoristijo nabor orodij za kibernetško varnost omrežij 5G“ in „uporabijo ustrezne omejitve glede visoko tveganih dobaviteljev za ključna sredstva, ki so v usklajenih ocenah tveganja v EU, ki temeljijo na skupnih objektivnih merilih, opredeljena kot kritična in občutljiva“⁵¹.

V prihodnosti bi morale EU in države članice zagotoviti, da se opredeljena tveganja ustrezno in usklajeno zmanjšajo, zlasti kar zadeva cilj zmanjšanja izpostavljenosti visoko tveganim dobaviteljem in preprečevanja odvisnosti od teh dobaviteljev na nacionalni ravni in ravni Unije, ter da se upošteva vsaka nova pomembna sprememba ali tveganje. Države članice naj v celoti izkoristijo nabor orodij pri naložbah v digitalne zmogljivosti in povezanost.

Komisija na podlagi poročila o vplivih priporočila iz leta 2019 spodbuja države članice, naj pospešijo prizadevanja za dokončanje izvajanja glavnih ukrepov iz nabora orodij do drugega četrtertletja leta 2021. Poziva jih tudi, naj še naprej skupaj spremljajo doseženi napredek in zagotavljajo nadaljnje usklajevanje pristopov. Na ravni EU se bodo za podpiranje tega procesa uresničevali trije glavni cilji: zagotavljanje nadaljnega približevanja pri pristopih za zmanjšanje tveganj v EU, podpiranje stalne izmenjave znanja in krepitev zmogljivosti ter spodbujanje odpornosti dobavne verige, pa tudi drugi strateški cilji EU na področju varnosti. Konkretni ukrepi, povezani s temi ključnimi cilji, so opredeljeni v posebnem dodatku k temu sporočilu.

Komisija bo še naprej tesno sodelovala z državami članicami, da bi s podporo agencije ENISA izpolnile te cilje in izvedle ukrepe (glej Prilogo).

Poleg tega je pristop EU z naborom orodij za tehnologijo 5G povečal zanimanje v tretjih državah, ki trenutno razvijajo pristope, da bi zaščitile svoja komunikacijska omrežja. Službe Komisije so skupaj z Evropsko službo za zunanje delovanje in mrežo delegacij EU pripravljene na zahtevo organom po vsem svetu zagotoviti dodatne informacije o svojem celovitem, objektivnem in na tveganju temelječem pristopu.

1.5 Internet varnih stvari

Vsaka povezana stvar vsebuje ranljivosti, ki jih je mogoče izkoristiti s potencialno obsežnimi posledicami. Pravila notranjega trga vključujejo zaščitne ukrepe pred nevarnimi proizvodi in storitvami. Komisija si že prizadeva, da bi zagotovila **pregledne varnostne rešitve in certificiranje v skladu z Aktom o kibernetški varnosti** ter spodbudila varne proizvode in storitve, ne da bi ogrozila učinkovitost⁵². V prvem četrtertletju leta 2021 bo sprejela prvi tekoči

⁵⁰Poročilo Skupine za sodelovanje na področju varnosti omrežij in informacij o izvajanju nabora orodij z dne 24. julija 2020.

⁵¹EUCO 13/20, Izredno zasedanje Evropskega sveta (1. in 2. oktobra 2020) – sklepi.

⁵² Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetško varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetške varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetški varnosti). Akt o kibernetški varnosti spodbuja certificiranje IKT na ravni EU z evropskim certifikacijskim okvirom za kibernetško varnost za vzpostavitev prostovoljnih evropskih certifikacijskih shem za kibernetško varnost za zagotovitev ustrezne ravni kibernetške varnosti za proizvode, storitve in procese IKT v Uniji ter zmanjšanje razdrobljenosti notranjega trga, kar zadeva certifikacijske sheme za kibernetško varnost v Uniji. Hkrati imajo družbe za

delovni program Unije (ki se bo posodabljal vsaj vsaka tri leta), da bi industriji, nacionalnim organom in organom za standardizacijo omogočila, da se vnaprej pripravijo za prihodnje evropske certifikacijske sheme za kibernetsko varnost⁵³. S širjenjem interneta stvari je potrebna okrepitev izvršljivih pravil za zagotovitev splošne odpornosti in spodbujanje kibernetske varnosti.

Komisija bo razmislila o celovitem pristopu, vključno z možnimi **novimi horizontalnimi pravili za izboljšanje kibernetske varnosti vseh povezanih proizvodov in z njimi povezanih storitev, danih na notranji trg**⁵⁴. Taka pravila bi lahko vključevala **ново obveznost skrbi za proizvajalce povezanih naprav**, da bi se obravnavale ranljivosti programske opreme, vključno z nadaljnjimi posodobitvami programske opreme in varnostnimi posodobitvami ter z zagotavljanjem izbrisa osebnih in drugih občutljivih podatkov ob koncu življenjske dobe. Ta pravila bi okrepila pobudo za „pravico do popravila zastarele programske opreme“, predstavljeno v akcijskem načrtu za krožno gospodarstvo, in dopolnila sedanje ukrepe, s katerimi se obravnavajo posebne vrste proizvodov, kot so obvezne zahteve, ki jih je treba predlagati za dostop do trga nekaterih brezžičnih proizvodov (s sprejetjem delegiranega akta v skladu z direktivo o radijski opremi⁵⁵), ter cilj uvedbe pravil o kibernetski varnosti za motorna vozila za vse nove tipe vozil od julija 2022⁵⁶. Poleg tega bi temeljila na predlagani reviziji pravil o splošni varnosti proizvodov, ki ne obravnavajo neposredno vidikov kibernetske varnosti⁵⁷.

1.6 Večja varnost globalnega interneta

Funkcionalnost in celovitost interneta po vsem svetu zagotavlja sklop glavnih protokolov in podporne infrastrukture⁵⁸. Ta sklop vsebuje DNS ter njegov hierarhični in delegirani sistem območij, ki se na vrhu hierarhije začne s korenskim območjem in trinajstimi korenskimi strežniki DNS⁵⁹, od katerih je odvisen svetovni splet. Komisija namerava pripraviti **načrt izrednih ukrepov, ki bo podprt s financiranjem EU, za obravnavanje izrednih scenarijev, ki vplivajo na celovitost in razpoložljivost globalnega korenskega sistema DNS**. Sodelovala bo z agencijo ENISA, državami članicami, upravljavcema korenskih strežnikov DNS⁶⁰ v EU in večdeležniško skupnostjo, da bi ocenila vlogo teh upravljavcev pri zagotavljanju, da internet v vseh okoliščinah ostane dostopen po vsem svetu.

ocenjevanje kibernetske varnosti ponavadi sedež zunaj EU ter omejeno preglednost in nadzor; <https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings>.

⁵³ Kot se zahteva s členom 47(5) Akta o kibernetski varnosti.

⁵⁴ V sklepih Sveta se poziva k horizontalnim ukrepom na področju kibernetske varnosti povezanih naprav; 13629/20, 2. december 2020.

⁵⁵ Direktiva 2014/53/EU.

⁵⁶ Upošteva pravilnik OZN, sprejet junija 2020; <http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf>.

⁵⁷ Revizija veljavnih pravil o splošni varnosti proizvodov (Direktiva 2001/95/ES); predlagana prilagojena pravila so načrtovana tudi v zvezi z odgovornostjo proizvajalcev v digitalnem okolju znotraj regulativnega okvira EU o odgovornosti.

⁵⁸ „Javno jedro odprtega interneta, in sicer njegovi glavni protokoli in infrastruktura, ki so svetovno javno dobro, omogoča uporabo ključnih funkcij interneta kot celote in je podlaga za njegovo normalno delovanje. Agencija ENISA bi morala podpirati varnost javnega jedra odprtega interneta in stabilno delovanje, vključno s ključnimi protokoli (zlasti DNS, BGP in IPv6), ter delovanjem sistema domenskih imen (kot je delovanje vseh vrhnjih domen) in delovanjem korenskega območja,“ uvodna izjava 23 Akta o kibernetski varnosti.

⁵⁹ <https://www.iana.org/domains/root/servers>.

⁶⁰ Strežniki i.root, ki jih upravlja Netnod na Švedskem, in strežniki k.root, ki jih upravlja RIPE NCC na Nizozemskem.

Da lahko stranka dostopa do vira pod določenim domenskim imenom na internetu, mora biti njena zahteva (običajno za enotni naslov vira ali URL) prevedena ali „razrešena“ v naslov IP s sklicem na imenske strežnike DNS. Vendar se ljudje in organizacije v EU vse pogosteje zanašajo na nekaj javnih razreševalnikov DNS, ki jih upravljajo subjekti iz tretjih držav. Zaradi takšne konsolidacije razreševanja DNS, ki je v rokah nekaj podjetij⁶¹, je sam postopek razreševanja ranljiv v primeru pomembnih dogodkov, ki vplivajo na enega glavnega ponudnika, in organom EU otežuje obravnavanje morebitnih zlonamernih kibernetских napadov ter večjih geopolitičnih in tehničnih incidentov⁶².

Da bi zmanjšale težave v zvezi z varnostjo, ki so povezane s koncentracijo na trgu, bo Komisija spodbujala ustrezne deležnike, vključno s podjetji v EU, ponudniki internetnih storitev in prodajalci brskalnikov, naj sprejmejo strategijo za diverzifikacijo razreševanja DNS. Komisija namerava tudi prispevati k varni internetni poveztljivosti s podpiranjem razvoja javne storitve **evropskih razreševalnikov DNS**. Ta pobuda „DNS4EU“ bo ponujala alternativo, tj. evropsko storitev za dostop do globalnega interneta. DNS4EU bo pregledna, usklajena z najnovejšimi standardi in pravili glede varnosti, varstva podatkov in vgrajene zasebnosti ter privzetimi standardi in pravili ter bo del evropskega industrijskega zaveznštva za podatke in oblak⁶³.

Komisija bo v sodelovanju z državami članicami in industrijo tudi **pospešila sprejetje ključnih internetnih standardov, vključno z IPv6⁶⁴, in dobro uveljavljenimi standardi internetne varnosti ter dobrimi praksami za DNS, usmerjanje in varnost e-pošte⁶⁵**, pri čemer niso izključeni regulativni ukrepi, kot je evropska klavzula o časovni omejitvi veljavnosti za IPv4 za usmerjanje trga, če pri njihovem sprejemanju ni dosežen zadosten napredek. EU bi morala spodbujati (na primer v okviru strategije EU – Afrika⁶⁶) izvajanje teh standardov v partnerskih državah kot način podpiranja razvoja globalnega in odprtega interneta ter preprečevanja zaprtih in na nadzoru temelječih modelov interneta. Nazadnje, Komisija bo proučila potrebo po mehanizmu za bolj sistematično spremljanje in zbiranje zbirnih podatkov o internetnem prometu in za svetovanje glede morebitnih motenj⁶⁷.

1.7 Okrepljena prisotnost v dobavni verigi za tehnologijo

EU ima z načrtovano finančno podporo za kibernetško varno digitalno preobrazbo v okviru večletnega finančnega okvira za obdobje 2021–2027 edinstveno priložnost, da združi svoja

⁶¹Consolidation in the DNS resolver market – how much, how fast how dangerous? (Konsolidacija na trgu razreševalnikov DNS – koliko, kako hitro in kako nevarno?) [...], Evidence of decreasing Internet entropy – the lack of redundancy in DNS resolution by major websites and services (Dokazi o zmanjševanju entropije interneta – pomanjkanje redundance pri razreševanju DNS s strani glavnih spletnih mest in storitev) [...].

⁶² Obstajajo tudi dokazi, da se lahko podatki DNS uporabljajo za profiliranje, kar vpliva na pravice do zasebnosti in varstva podatkov.

⁶³ Skupna izjava: Izgradnja oblaka naslednje generacije za podjetja in javni sektor v EU; <https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe>.

⁶⁴Uvajanje IPv6 je zdaj naprednejše zaradi velikega zmanjšanja ponudbe in zvišanja stroškov naslovov IPv4. Vendar pri uvajanju IPv6 v EU obstajajo razlike.

⁶⁵Med takimi standardi so DNSSEC, HTTPS, DNS prek HTTPS (DoH), DNS prek TLS (DoT), SPF, DKIM, /DMARC, STARTTLS, DANE ter pravila usmerjanja in dobre prakse, npr. vzajemno dogovorjena pravila za varnost usmerjanja (MANRS).

⁶⁶Skupno sporočilo za celovito strategijo z Afriko z dne 9. marca 2020, JOIN(2020) 4 final.

⁶⁷Taka „internetna opazovalnica“ bi lahko spadala med dejavnosti Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetško varnost; Predlog uredbe o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetško varnost ter mreže nacionalnih koordinacijskih centrov (COM(2018) 630 final).

sredstva za uveljavitev svoje strategije za industrijo⁶⁸ ter vodilne vloge na področju digitalnih tehnologij in kibernetске varnosti v digitalni dobavni verigi (vključno s podatki in oblakom, tehnologijami procesorjev naslednje generacije, izjemno varno povezljivostjo in omrežji 6G) v skladu s svojimi vrednotami in prednostnimi nalogami. Posredovanje javnega sektorja bi moralo temeljiti na orodjih, zagotovljenih z regulativnim okvirom EU za javna naročila, in pomembnih projektih skupnega evropskega interesa. Poleg tega lahko sprostí zasebne naložbe prek javno-zasebnih partnerstev (tudi na podlagi izkušenj s pogodbenim javno-zasebnim partnerstvom na področju kibernetске varnosti in njegovim izvajanjem v okviru Evropske organizacije za kibernetско varnost), tveganega kapitala v podporo MSP ali industrijskih zavezništev in strategij za zmogljivosti na področju tehnologije.

Poseben poudarek bo tudi na instrumentu za tehnično podporo⁶⁹ in najboljši uporabi najnovejših orodij za kibernetско varnost s strani MSP, zlasti tistih, ki ne spadajo na področje uporabe revidirane direktive o varnosti omrežij in informacij, tudi z namenskimi dejavnostmi v okviru vozlišč za digitalne inovacije v programu za digitalno Evropo. Cilj je spodbuditi podoben znesek naložb držav članic, ki bi se mu dodal enak prispevek industrije v okviru partnerstva, ki ga soupravljajo države članice v predlaganem **industrijskem, tehnološkem in raziskovalnem strokovnem centru za kibernetско varnost ter mreži koordinacijskih centrov (CCCN)**. CCCN bi morala imeti ključno vlogo – ob prispevku industrije in akademskih skupnosti – pri razvoju tehnološke neodvisnosti EU na področju kibernetске varnosti, krepitvi zmogljivosti za zavarovanje občutljivih infrastruktur, kot je 5G, in zmanjšanje odvisnosti od drugih delov sveta, kar zadeva najpomembnejše tehnologije.

Komisija namerava podpreti, po možnosti s CCCN, razvoj posebnega magistrskega študijskega programa o kibernetски varnosti in prispevati k skupnemu evropskemu kažipotu za raziskave in inovacije na področju kibernetске varnosti po letu 2020. Naložbe prek CCCN bi temeljile tudi na sodelovanju pri raziskavah in razvoju, ki bi jih izvajale mreže centrov odličnosti na področju kibernetске varnosti, pri čemer bi se združile najboljše raziskovalne skupine v Evropi in industrija, da bi se v skladu s časovnim načrtom Evropske organizacije za kibernetско varnost oblikovali in izvajali skupni raziskovalni programi⁷⁰. Komisija se bo še naprej zanašala na raziskovalno delo agencije ENISA in Europol, v okviru programa Obzorje Evropa pa bo tudi še naprej podpirala posamezne internetne inovatorje pri razvoju varnih komunikacijskih tehnologij z okrepljenim varovanjem zasebnosti, ki temeljijo na odprtokodni programski in strojni opreml, kot jih trenutno v okviru pobude za internet naslednje generacije.

1.8 Kibernetско usposobljena delovna sila EU

Prizadevanja EU za izpopolnjevanje delovne sile, razvoj, privabljanje in zadržanje največjih talentov na področju kibernetске varnosti ter naložbe v vrhunske raziskave in inovacije so pomemben element splošne zaštite pred kibernetskimi grožnjami. To področje ima velik potencial. Zato je treba posebno pozornost nameniti razvoju, privabljanju in zadržanju bolj raznovrstnih talentov. Revidirani akcijski načrt za digitalno izobraževanje bo povečal ozaveščenost o kibernetски varnosti med posamezniki, zlasti otroci in mladimi, ter organizacijami, zlasti MSP⁷¹. Poleg tega bo spodbujal udeležbo žensk v izobraževanju na področju naravoslovja, tehnologije, inženirstva in matematike ter izpopolnjevanje in

⁶⁸Sporočilo o novi industrijski strategiji za Evropo (COM(2020) 102 final).

⁶⁹<https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=COM:2020:0409:FIN>.

⁷⁰<https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies>.

⁷¹https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_sl.

preusposabljanje na področju digitalnih znanj in spretnosti na delovnih mestih na področju IKT. Poleg tega bo Komisija skupaj z Uradom Evropske unije za intelektualno lastnino pri Europolu, agencijo ENISA, državami članicami in zasebnim sektorjem razvila orodja za ozaveščanje in smernice za povečanje odpornosti podjetij v EU **proti kibernetско omogočeni kraji intelektualne lastnine**⁷².

Izobraževanje, vključno s poklicnim izobraževanjem in usposabljanjem, ozaveščanjem in vajami, bi moralo tudi dodatno povečati znanja in spretnosti na področju kibernetiske varnosti in kibernetiske obrambe na ravni EU. V ta namen bi si morali ustrezni akterji EU, kot so agencija ENISA, Evropska obrambna agencija (EDA) in Evropska akademija za varnost in obrambo (ESDC)⁷³, prizadevati za sinergije med svojimi ustreznimi dejavnostmi.

Strateške pobude

EU bi morala zagotoviti:

- sprejetje revidirane direktive o varnosti omrežij in informacij;
- regulativne ukrepe za internet varnih stvari;
- prek CCCN naložbe v kibernetisko varnost (zlasti v okviru programov za digitalno Evropo in Obzorje Evropa ter mehanizma za okrevanje), da bi javne in zasebne naložbe v obdobju 2021–2027 dosegle 4,5 milijarde EUR;
- mrežo centrov za varnostne operacije s pomočjo umetne inteligence na ravni EU in ultravarno komunikacijsko infrastrukturo, ki izkorišča kvantne tehnologije;
- splošno sprejetje tehnologij za kibernetisko varnost z namensko podporo MSP v okviru vozlišč za digitalne inovacije;
- razvoj storitve EU za razreševanje DNS kot varne odprte alternative za dostopanje državljanov, podjetij in javnih uprav v EU do interneta ter
- dokončno uvedbo nabora orodij EU za kibernetisko varnost 5G do drugega četrtertletja leta 2021 (glej Prilogo).

2. KREPITEV OPERATIVNE ZMOGLJIVOSTI ZA PREPREČEVANJE, ODVRAČANJE IN ODZIVANJE

Kibernetiski incidenti, ki so bodisi naključni bodisi namerna dejanja storilcev kaznivih dejanj, državnih in drugih nedržavnih akterjev, lahko povzročijo ogromno škodo. Njihov obseg in kompleksnost, ki pogosto vključujeta izkoriščanje storitev tretjih oseb, strojne opreme in programske opreme za poškodovanje končne tarče, otežujeta spoprijemanje z okoljem kolektivnih groženj v EU brez sistematične in celovite izmenjave informacij ter sodelovanja pri skupnem odzivanju. Cilj EU je **s polnim izvajanjem regulativnih orodij, mobilizacijo in sodelovanjem** podpirati države članice pri zaščiti njihovih državljanov ter njihovih gospodarskih in nacionalnih varnostnih interesov ob polnem spoštovanju temeljnih pravic in svoboščin ter pravne države. Več skupnosti, sestavljenih iz mrež, institucij, organov in agencij EU ter organov držav članic, je odgovornih za preprečevanje in preganjanje

⁷²https://ec.europa.eu/commission/presscorner/detail/sl/IP_20_2187.

⁷³Prek platforme za kibernetisko izobraževanje, usposabljanje, ocenjevanje in kibernetiske vaje (ETEE).

kibernetskih groženj, odvracanje od njih in odzivanje nanje, za kar uporabljajo ustrezne instrumente in pobude⁷⁴. Te skupnosti vključujejo: (i) organe za varnost omrežij in informacij, kot so skupine CSIRT in organi za odzivanje na nesreče, (ii) organe kazenskega pregona ter pravosodne organe, (iii) kibernetsko diplomacijo in (iv) kibernetsko obrambo.

2.1 Skupna kibernetska enota

Skupna kibernetska enota bi delovala kot virtualna in fizična platforma za sodelovanje različnih skupnosti na področju kibernetske varnosti v EU, osredotočena pa bi bila na operativno in tehnično usklajevanje v boju proti večjim čezmejnimi kibernetskimi incidentom in grožnjam.

Skupna kibernetska enota bi bila pomemben korak naprej pri dokončanju **evropskega okvira za krizno upravljanje kibernetske varnosti**. Kot je opisano v političnih smernicah predsednika Komisije⁷⁵, bi morala enota državam članicam ter institucijam, organom in agencijam EU omogočiti, da v celoti izkoristijo obstoječe strukture, sredstva in zmogljivosti ter spodbujajo miselnost, ki temelji na „**potrebi po izmenjavi**“. Zagotovila bi sredstva za utrditev doslej doseženega napredka pri izvajanju priporočila iz leta 2017 o usklajenem odzivu na velike kibernetske incidente in krize („načrt“)⁷⁶. Zagotovila bi tudi možnost nadaljnje krepitve sodelovanja na področju arhitekture načrta in izkoriščanja doseženega napredka, zlasti v okviru Skupine za sodelovanje na področju varnosti omrežij in informacij ter mreže CyCLONe.

S tem bi se lahko obravnavali **dve glavni vrzeli**, ki trenutno povečujeta ranljivosti in ustvarjata neučinkovitosti pri odzivanju na čezmejne grožnje in incidente, ki škodijo Uniji. Prvič, civilne, diplomatske in obrambne kibernetske **skupnosti** ter kibernetske **skupnosti** organov kazenskega pregona še nimajo skupnega prostora za spodbujanje strukturnega sodelovanja ter olajšanje operativnega in tehničnega sodelovanja. Drugič, ustrezni deležniki na področju kibernetske varnosti še niso bili sposobni izkoristiti celotnega **potenciala** operativnega sodelovanja in vzajemne pomoči v obstoječih mrežah in skupnostih. To vključuje neobstoj platforme, ki bi omogočala operativno sodelovanje z zasebnim sektorjem. Enota bi morala izboljšati in pospešiti usklajevanje ter omogočiti EU, da bi se soočila z velikimi kibernetskimi incidenti in krizami ter se odzvala nanje.

Skupna kibernetska enota ne bi bila dodaten samostojni organ niti ne bi vplivala na pristojnosti in pooblastila nacionalnih organov za kibernetsko varnost ali udeležencev iz EU. Pač pa bi delovala kot varovalni mehanizem, v okviru katerega bi se udeleženci lahko zanašali na medsebojno podporo in strokovno znanje drugih članov, zlasti če bi bilo potrebno

⁷⁴Vključno z Agencijo Evropske unije za kibernetsko varnost (agencija ENISA), ki podpira operativno sodelovanje in krizno upravljanje; mrežo skupin CSIRT; mrežo organizacij za povezovanje v kibernetski krizi (CyCLONe, ki naj bi postala mreža EU-CyCLONe, kot je predlagano v revidirani direktivi o varnosti omrežij in informacij); Skupino za sodelovanje na področju varnosti omrežij in informacij; „rescEU“; Evropskim centrom za boj proti kibernetski kriminaliteti in skupno delovno skupino za ukrepanje na področju kibernetske varnosti pri Europolu ter protokolom za odzivanje organov kazenskega pregona na izredne razmere; Obveščevalnim in situacijskim centrom EU (EU INTCEN) in zbirko orodij za kibernetsko diplomacijo; Enotno zmogljivostjo za analizo obveščevalnih podatkov (SIAC); kibernetskimi projekti v okviru stalnega strukturnega sodelovanja (PESCO), zlasti „enote za hitro posredovanje na kibernetskem področju in vzajemno pomoč pri kibernetski varnosti“.

⁷⁵„Bolj ambiciozna Unija: Moj načrt za Evropo“, politične usmeritve naslednje Evropske komisije za obdobje 2019–2024 kandidatke za predsednico Evropske komisije Ursule von der Leyen.

⁷⁶Načrt priporočila C(2017) 6100 final z dne 13. septembra 2017 o usklajenem odzivu na velike kibernetske incidente in krize.

tesno sodelovanje različnih kibernetских skupnosti. Hkrati nedavni dogodki kažejo, da mora EU povečati svoje ambicije in pripravljenost za spoprijemanje z okoljem in dejanskim stanjem na področju kibernetских groženj. Akterji EU (Komisija ter agencije in organi EU) bodo v okviru svojega prispevka k skupni kibernetски enoti zato pripravljeni znatno povečati svoja sredstva in zmogljivosti, da bi povečali svojo pripravljenost in odpornost.

Skupna kibernetска enota bi izpolnjevala tri glavne cilje. Prvič, zagotovila bi **pripravljenost** v skupnostih za kibernetсko varnost, drugič, z izmenjavo informacij bi zagotavljala stalno skupno situacijsko **zavedanje** in, tretjič, okrepila bi usklajeno **odzivanje** in okrevanje. Za doseganje teh ciljev bi morala enota graditi na dobro opredeljenih **blokih in ciljih**, kot so zagotavljanje **varne in hitre izmenjave informacij**, izboljšanje **sodelovanja** med udeleženci, vključno s sodelovanjem med državami članicami in ustreznimi subjekti EU, vzpostavitev strukturiranih **partnerstev z zaupanja vredno industrijsko** bazo in omogočanje usklajenega pristopa k **sodelovanju z zunanjimi partnerji**. V ta namen bi lahko enota na podlagi vzporejanja razpoložljivih zmogljivosti na nacionalni ravni in ravni EU olajšala razvoj okvira za sodelovanje.

Da bi skupna kibernetска enota postala središče operativnega sodelovanja na področju kibernetсke varnosti v EU, bo Komisija sodelovala z državami članicami ter ustreznimi institucijami, organi in agencijami EU, vključno z agencijo ENISA, skupino CERT-EU in Europolom, da bi spodbujala **postopen in vključujoč pristop** ob polnem spoštovanju pristojnosti in pooblastil vseh vključenih. V skladu s tem pristopom bi lahko enota prispevala k nadaljnjemu sodelovanju med tvorci posebne kibernetсke skupnosti, če bi se tem to zdelo potrebno.

Za vzpostavitev skupne kibernetсke enote se predlagajo štirje koraki:

- *opredelitev* z vzporejanjem razpoložljivih zmogljivosti na nacionalni ravni in ravni EU;
- *priprava* z vzpostavitvijo okvira za strukturirano sodelovanje in pomoč;
- *uvredba* z izvajanjem okvira, ki temelji na sredstvih, ki jih zagotovijo udeleženci, tako da skupna kibernetска enota začne delovati;
- *razširitev* z okrepitevijo zmogljivosti za usklajen odziv s prispevki industrije in partnerjev.

Komisija bo na podlagi izida posvetovanj z državami članicami ter institucijami, organi in agencijami EU⁷⁷ v sodelovanju z visokim predstavnikom v skladu z njegovimi pristojnostmi do februarja 2021 predstavila postopek, mejnike in časovnico za **opredelitev, pripravo, uvedbo in razširitev skupne kibernetсke enote**.

2.2 Boj proti kibernetски kriminaliteti

Zaradi naše odvisnosti od spletnih orodij se eksponentno povečuje napadna površina za storilce kaznivih dejanj v kibernetском prostoru, rezultat tega pa je stanje, ko preiskave skoraj vseh vrst kaznivih dejanj vključujejo digitalno komponento. Poleg tega jedrne dele

⁷⁷Posvetovanje z državami članicami (tudi med vajo Blue OLEx20, na kateri so se zbrali vodje nacionalnih organov za kibernetсko varnost) ter institucijami, organi in agencijami EU, izvedeno med julijem in novembrom 2020.

naše družbe ogrožajo kibernetiski akterji in tisti, ki uporabljajo kibernetiska orodja za načrtovanje in izvajanje svojih nezakonitih dejavnosti. Zato obstajajo tesne povezave s splošno varnostno politiko EU, kot se odraža v kibernetiskih elementih iz njene strategije za varnostno unijo iz leta 2020 in agendi EU za boj proti terorizmu⁷⁸.

Učinkovit boj proti kibernetiski kriminaliteti je ključni dejavnik pri zagotavljanju kibernetске varnosti: odvracanja ni mogoče doseči zgolj z odpornostjo, ampak sta potrebna tudi identifikacija in pregon storilcev. Zato je bistveno spodbujati sodelovanje in izmenjavo med akterji na področju kibernetске varnosti in organi kazenskega pregona. Na ravni EU sta zato Europol in agencija ENISA že vzpostavila tesno sodelovanje z organizacijo skupnih konferenc in delavnic ter zagotovila skupna poročila Komisiji, državam članicam in drugim deležnikom o kibernetiskih grožnjah in tehnoloških izzivih. Komisija bo še naprej podpirala ta celostni pristop, da bi zagotovila skladen in učinkovit odziv, temelječ na celovitih informacijah.

Eden od pomembnih elementov navedenega odziva je, da morajo EU in nacionalni organi povečati in izboljšati zmogljivost kazenskega pregona za preiskave kibernetске kriminalitete ob polnem spoštovanju temeljnih pravic ter prizadevanju za vzpostavitev ustreznega ravnovesja med različnimi pravicami in interesi. EU bi se morala biti sposobna boriti proti kibernetiski kriminaliteti z zakonodajo, ki je v celoti izvedena, ustreza svojemu namenu ter je posebej osredotočena na boj proti spolni zlorabi otrok na spletu in digitalne preiskave, vključno s kriminaliteto na „temnem omrežju“. Kazenski pregon mora biti popolnoma opremljen za digitalne preiskave. Komisija bo zato predstavila akcijski načrt za izboljšanje digitalne zmogljivosti organov kazenskega pregona z zagotovitvijo potrebnih znanj in spretnosti ter orodij tem organom. Poleg tega bo Europol nadalje razvijal svojo vlogo središča strokovnega znanja za podpiranje nacionalnih organov kazenskega pregona, ki se borijo proti kriminaliteti, ki jo omogoča kibernetiski prostor in ki je odvisna od kibernetskega prostora, ter bo prispeval k opredelitvi skupnih forenzičnih standardov (prek Europolovega inovacijskega laboratorija in središča). Vse te dejavnosti zahtevajo ustrezen začetek izvajanja v državah članicah, ki so pozvane, naj izkoristijo nacionalne programe Sklada za notranjo varnost in predlagajo projekte na podlagi razpisov za zbiranje predlogov v okviru tematskega instrumenta.

Komisija bo uporabila vsa ustrezna sredstva, vključno s postopki za ugotavljanje kršitev, da bi zagotovila popoln prenos direktive o napadih na informacijske sisteme iz leta 2013⁷⁹ v nacionalno zakonodajo in njeno izvajanje, vključno z zagotavljanjem statističnih podatkov s strani držav članic. Izboljšala bo preprečevanje zlorabe domenskih imen, po potrebi med drugim za distribucijo nezakonite vsebine, in si prizadevala za razpoložljivost točnih podatkov o registraciji z nadaljnjim sodelovanjem z Organizacijo za dodeljevanje spletnih imen in števil (ICANN) in drugimi deležniki v sistemu upravljanja interneta, zlasti prek delovne skupine za javno varnost pri Vladnem svetovalnem odboru ICANN. Predlog v revidirani direktivi o varnosti omrežij in informacij tako predvideva vzdrževanje točnih in popolnih podatkovnih zbirk domenskih imen in podatkov o registraciji ali „podatkov

⁷⁸Communication A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond (Sporočilo Agenda za boj proti terorizmu v EU: predvidevanje, preprečevanje, zaščita in odziv) z dne 9. decembra 2020 (COM(2020) 795 final).

⁷⁹Direktiva 2013/40/EU o napadih na informacijske sisteme.

WHOIS“ ter zagotavljanje zakonitega dostopa do teh podatkov kot bistvenega za zagotavljanje varnosti, stabilnosti in odpornosti sistema domenskih imen.

Komisija si bo tudi še naprej prizadevala za zagotavljanje ustreznih kanalov in pojasnitev pravil za pridobitev čezmejnega dostopa do elektronskih dokazov za kazenske preiskave (ki so potrebni v 85 % preiskav, pri čemer je 65 % vseh zahtevkov naslovljenih na ponudnike s sedežem v drugi jurisdikciji) z olajšanjem sprejetja ter poznejšega izvajanja „svežnja o elektronskih dokazih“ in praktičnih ukrepov⁸⁰. Hitro sprejetje predlogov o elektronskih dokazih s strani Evropskega parlamenta in Sveta je ključno, da se preiskovalcem zagotovi učinkovito orodje. Elektronski dokazi morajo biti berljivi, zato si bo Komisija še naprej prizadevala za podporo za zmogljivost kazenskega pregona na področju digitalnih preiskav, vključno z obravnavanjem šifriranja v kazenskih preiskavah, pri čemer bo v celoti ohranila svojo funkcijo varovanja temeljnih pravic in kibernetске varnosti.

2.3 Zbirka orodij EU za kibernetško diplomacijo

EU uporablja svojo **zbirko orodij za kibernetško diplomacijo**⁸¹ za preprečevanje in preganjanje zlonamernih kibernetских dejavnosti, odvracanje od njih ter odzivanje nanje. Po uvedbi pravnega okvira za ciljno usmerjene omejevalne ukrepe proti kibernetским napadom maja 2019⁸² je EU julija 2020 v okviru ureditve⁸³ uvrstila na seznam šest posameznikov in tri subjekte, odgovorne za ali vključene v kibernetские napade, ki škodijo EU in njenim državam članicam. Oktobra 2020 so bili na seznam uvrščeni še dva posameznika in en organ⁸⁴. Proti zlonamernim kibernetским dejavnostim, vključno s tistimi, ki se razvijajo počasi, bi se bilo treba boriti z učinkovitim in celovitim skupnim diplomatskim odzivom EU, pri tem pa uporabiti celoten nabor ukrepov, ki so na voljo na ravni EU.

Hiter in učinkovit skupni diplomatski odziv EU zahteva močno skupno situacijsko zavedanje in sposobnost hitre priprave skupnega stališča EU. Visoki predstavnik Unije za zunanje zadeve in varnostno politiko bo spodbujal in olajševal ustanovitev **delovne skupine obveščevalnih služb držav članic EU** v okviru Obveščevalnega in situacijskega centra EU (INTCEN) za spodbujanje strateškega sodelovanja obveščevalnih služb na področju kibernetских groženj in dejavnosti. To prizadevanje bo nadalje podpiralo situacijsko

⁸⁰COM(2018) 225 in 226; C(2020) 2779 final. Zlasti projekt SIRIUS je v okviru instrumenta partnerstva nedavno prejel dodatna sredstva za izboljšanje kanalov za pridobitev zakonitega čezmejnega dostopa do elektronskih dokazov za kazenske preiskave (ki so potrebni v 85 % preiskav hudih kaznivih dejanj, pri čemer je 65 % vseh zahtevkov naslovljenih na ponudnike s sedežem v drugi jurisdikciji) in vzpostavitev združljivih pravil na mednarodni ravni.

⁸¹<https://www.consilium.europa.eu/sl/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/>.

⁸²Sklep Sveta (SZVP) 2019/797 z dne 17. maja 2019 o omejevalnih ukrepih proti kibernetским napadom, ki ogrožajo Unijo ali njene države članice (UL L 129I, 17.5.2019, str. 13), in Sklep Sveta (EU) 2019/796.

z dne 17. maja 2019 o omejevalnih ukrepih proti kibernetским napadom, ki ogrožajo Unijo ali njene države članice (UL L 129I, 17.5.2019, str. 1).

⁸³ Sklep Sveta (SZVP) 2020/1127 z dne 30. julija 2020 o spremembi Sklepa Sveta (SZVP) 2019/797 o omejevalnih ukrepih proti kibernetским napadom, ki ogrožajo Unijo ali njene države članice (ST/9564/2020/INIT) (UL L 246, 30.7.2020, str. 12), in Izvedbena uredba Sveta (EU) 2020/1125 z dne 30. julija 2020 o izvajanju Uredbe (EU) 2019/796 o omejevalnih ukrepih proti kibernetским napadom, ki ogrožajo Unijo ali njene države članice (ST/9568/2020/INIT) (UL L 246, 30.7.2020, str. 4).

⁸⁴ Sklep Sveta (SZVP) 2020/1537 z dne 22. oktobra 2020 o spremembi Sklepa Sveta (SZVP) 2019/797 o omejevalnih ukrepih proti kibernetским napadom, ki ogrožajo Unijo ali njene države članice (UL L 351I, 22.10.2020, str. 5), in Izvedbena uredba Sveta (EU) 2020/1536 z dne 22. oktobra 2020 o izvajanju Uredbe (EU) 2019/796 o omejevalnih ukrepih proti kibernetским napadom, ki ogrožajo Unijo ali njene države članice (UL L 351I, 22.10.2020, str. 1).

zavedanje in odločanje EU o skupnem diplomatskem odzivu. Delovna skupina bo sodelovala z obstoječimi strukturami⁸⁵, po potrebi tudi s tistimi, ki zajemajo širšo grožnjo hibridnega in tujega vmešavanja, za zbiranje in ocenjevanje situacijskega zavedanja.

Visoki predstavnik bo za okrepitev svoje sposobnosti preprečevanja in preganjanja zlonamernega ravnanja v kibernetnem prostoru, odvracanja od njega ter odzivanja nanj z vključitvijo Komisije v skladu s svojimi pristojnostmi predstavil predlog, v skladu s katerim bi EU natančneje opredelila svoje **stališče do kibernetnega odvracanja**. Na podlagi dosedanjega dela v okviru zbirke orodij EU za kibernetno diplomacijo bi morale stališče prispevati k odgovornemu ravnanju držav in sodelovanju v kibernetnem prostoru ter zagotoviti natančne smernice za preprečevanje kibernetnih napadov z največjim vplivom, zlasti tistih, ki škodujejo naši kritični infrastrukturi, demokratičnim institucijam in procesom⁸⁶, ter napadov na dobavne verige in kraje intelektualne lastnine, ki jih omogoča kibernetni prostor. V stališču bi moralo biti opisano, kako bi lahko EU in države članice izkoristile svoja orodja za politično, ekonomsko, diplomatsko, pravno in strateško komuniciranje v boju proti zlonamernim kibernetnim dejavnostim, poleg tega pa bi morale biti v njem obravnavane, kako bi lahko EU in države članice izboljšale svojo sposobnost pripisovanja zlonamernih kibernetnih dejavnosti. Poleg tega namerava visoki predstavnik skupaj s Svetom in Komisijo proučiti **dodatne ukrepe v okviru zbirke orodij za kibernetno diplomacijo**, vključno z možnostjo dodatnih opcij za omejevalne ukrepe in proučitvijo **glasovanja s kvalificirano večino za uvrstitev na seznam v okviru režima horizontalnih sankcij proti kibernetnim napadom**. Poleg tega bi si morala EU nadalje prizadevati za **okrepitev sodelovanja z mednarodnimi partnerji**, vključno z zvezo NATO, za spodbujanje skupnega razumevanja okolja groženj, razvoj mehanizmov sodelovanja in opredelitev skupnih diplomatskih odzivov

Visoki predstavnik bo v sodelovanju s Komisijo predlagal tudi posodobitev **izvedbenih smernic zbirke orodij za kibernetno diplomacijo**⁸⁷, tudi za povečanje učinkovitosti postopka odločanja, ter še naprej redno organiziral vaje in ocenjevanja v zvezi z zbirko orodij za kibernetno diplomacijo. Poleg tega bi morala EU še naprej **vključevati zbirko orodij za kibernetno diplomacijo v krizne mehanizme** EU ter iskati sinergije s prizadevanji za preprečevanje hibridnih groženj, dezinformacij in tujega vmešavanja v skladu s skupnim okvirom o preprečevanju hibridnih groženj⁸⁸ in akcijskim načrtom za evropsko demokracijo. V zvezi s tem bi morala EU razmisliti o povezavi med zbirko orodij za kibernetno diplomacijo ter morebitno uporabo člena 42(7) PEU in člena 222 PDEU⁸⁹.

2.4 Povečevanje zmogljivosti kibernetne obrambe

EU in države članice morajo povečati svojo sposobnost preprečevanja kibernetnih groženj in odzivanja nanje v skladu s ciljem na ravni EU, ki izhaja iz globalne strategije EU iz leta 2016⁹⁰. V ta namen bo visoki predstavnik v sodelovanju s Komisijo predstavil **pregled okvira politike za kibernetno obrambo** za okrepitev nadaljnjega usklajevanja in

⁸⁵ Kot so enotna zmogljivost EU za analizo obveščevalnih podatkov (SIAC) in po potrebi ustrezni projekti, vzpostavljeni v okviru stalnega strukturnega sodelovanja (PESCO), in sistem hitrega obveščanja iz leta 2018, ki je bil vzpostavljen za podpiranje splošnega pristopa EU k boju proti dezinformacijam.

⁸⁶ Zlasti z iskanjem sinergij s pobudami v skladu z akcijskim načrtom za evropsko demokracijo.

⁸⁷ 13007/17.

⁸⁸ <https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:52016JC0018&from=SL>.

⁸⁹ Klavzula o vzajemni obrambi oziroma solidarnostna klavzula.

⁹⁰ Sklepi Sveta (14149/16) o izvajanju globalne strategije EU na področju varnosti in obrambe.

sodelovanja med akterji v EU⁹¹ ter z državami članicami in med njimi, tudi kar zadeva misije in operacije v okviru skupne varnostne in obrambne politike (SVOP). Okvir politike za kibernetško obrambo bi moral priskrbeti informacije za prihodnji strateški kompas⁹² in s tem zagotoviti nadaljnje vključevanje kibernetške varnosti in kibernetške obrambe v širšo agendo za varnost in obrambo.

EU je leta 2018 opredelila kibernetški prostor kot področje delovanja⁹³. V prihodnji „vojaški viziji in strategiji za kibernetški prostor kot področje delovanja“, ki jo bo pripravil Vojaški odbor EU, bi moralo biti podrobneje opredeljeno, kako kibernetški prostor kot področje delovanja omogoča vojaške misije in operacije EU v okviru SVOP. **Mreža vojaških skupin za odzivanje na računalniške grožnje**⁹⁴, ki jo ustanavlja Evropska obrambna agencija (EDA), bo še dodatno prispevala k bistvenemu povečanju sodelovanja med državami članicami. Poleg tega bosta za zagotovitev kibernetške varnosti kritičnih vesoljskih infrastruktur v okviru odgovornosti vesoljskega programa okrepljeni Agencija Evropske unije za vesoljski program in zlasti center za nadzor varnosti Galileo, njune pristojnosti pa bodo razširjene na druga kritična sredstva vesoljskega programa.

EU in države članice bi morale z različnimi politikami in instrumenti EU, zlasti okvirom politike za kibernetško obrambo, zagotoviti dodatno spodbudo za **razvoj najsodobnejših zmogljivosti za kibernetško obrambo** in po potrebi nadgraditi delo Evropske obrambne agencije. To zahteva veliko osredotočenost na razvoj in uporabo ključnih tehnologij, kot so umetna inteligenca, šifriranje in kvantno računalništvo. EU bi morala v skladu s prednostnimi nalogami EU glede razvoja zmogljivosti iz leta 2018⁹⁵ in na podlagi ugotovitev prvega celovitega poročila o usklajenem letnem pregledu na področju obrambe⁹⁶ nadalje olajševati sodelovanje med državami članicami pri **raziskavah, inovacijah in razvoju zmogljivosti na področju kibernetške obrambe**, pri tem pa spodbujati države članice, naj izkoristijo celoten potencial **stalnega strukturnega sodelovanja (PESCO)**⁹⁷ in **Evropskega razvojnega sklada (ERS)**⁹⁸.

Prihodnji **akcijski načrt Komisije za sinergije med civilno, obrambno in vesoljsko industrijo**, ki bo predstavljen v prvem četrtletju leta 2021, bo vključeval ukrepe za nadaljnje

⁹¹ Zlasti Evropska služba za zunanje delovanje (ESZD), vključno z Vojaškim štabom EU (VŠEU), Evropsko akademijo za varnost in obrambo (EAVO), Komisijo in agencijami EU, zlasti Evropsko obrambno agencijo (EDA).

⁹² Sklepi Sveta o varnosti in obrambi z dne 17. junija 2020 (8910/20).

⁹³ <https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/sl/pdf>.

⁹⁴ Vzpostavitev mreže vojaških skupin za odzivanje na računalniške grožnje v EU je odziv na cilj, opredeljen v okviru politike za kibernetško obrambo iz leta 2018, ter je namenjen spodbujanju dejavnega sodelovanja in izmenjave informacij med vojaškimi skupinami držav članic EU za odzivanje na računalniške grožnje.

⁹⁵ Junija 2018 so se države članice v usmerjevalnem odboru Evropske obrambne agencije dogovorile, da bodo vodile sodelovanje na področju obrambe na ravni EU.

⁹⁶ Ki so ga novembra 2020 odobrili ministri za obrambo v usmerjevalnem odboru Evropske obrambne agencije. [https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-\(card\)](https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card)).

⁹⁷ Trenutno se izvaja več projektov v okviru stalnega strukturnega sodelovanja, povezanih s kibernetiskim prostorom, zlasti platforma za izmenjavo informacij o kibernetiskih grožnjah in odzivih na incidente, enote za hitro posredovanje na kibernetiskem področju in vzajemna pomoč pri kibernetiski varnosti, Akademsko in inovacijsko vozlišče EU za kibernetško varnost ter Center za usklajevanje na kibernetiskem in informacijskem področju (CIDCC).

⁹⁸ Komisija je v okviru Evropskega obrambnega sklada že opredelila možnosti za morebitne ukrepe sodelovanja pri raziskavah in razvoju na področju kibernetške obrambe, namenjene krepitvi sodelovanja, inovacijske zmogljivosti in konkurenčnosti obrambne industrije.

podpiranje sinergij na ravni programov, tehnologij, inovacij in zagonskih podjetij v skladu z upravljanjem ustreznih programov⁹⁹.

Poleg tega bi bilo treba razviti ustrezne sinergije in vmesnike med pobudami za kibernetško varnost, ki se izvajajo v drugih okvirih, vključno s skupnimi projekti, povezanimi s kibernetiskim prostorom¹⁰⁰, ki jih države članice izvajajo v okviru stalnega strukturnega sodelovanja, ter s strukturami EU za kibernetško varnost za podpiranje izmenjave informacij in vzajemne pomoči.

Strateške pobude

EU bi morala:

- dopolniti evropski okvir za krizno upravljanje kibernetške varnosti ter določiti postopek, mejnike in časovnico za vzpostavitev skupne kibernetške enote;
- še naprej izvajati agendo za kibernetško varnost v okviru strategije za varnostno unijo;
- spodbujati in olajšati ustanovitev delovne skupine obveščevalnih služb držav članic v okviru Obveščevalnega in situacijskega centra EU;
- razviti stališče EU glede kibernetškega odvrčanja za preprečevanje in preganjanje zlonamernih kibernetških dejavnosti, odvrčanje od njih ter odzivanje nanje;
- pregledati okvir politike za kibernetško obrambo;
- olajšati razvoj „vojaške vizije in strategije EU za kibernetški prostor kot področje delovanja“ za vojaške misije in operacije v okviru SVOP;
- podpirati sinergije med civilno, obrambno in vesoljsko industrijo ter
- okrepiti kibernetško varnost kritične vesoljske infrastrukture v okviru vesoljskega programa.

3. SPodbujanje globalnega in odprtega kibernetškega prostora

EU bi morala še naprej sodelovati z mednarodnimi partnerji pri spodbujanju političnega modela in vizije kibernetškega prostora, ki temeljita na pravni državi, človekovih pravicah, temeljnih svoboščinah in demokratičnih vrednotah, ki prinašajo socialni, ekonomski in politični razvoj na svetovni ravni ter prispevajo k varnostni uniji. Mednarodno sodelovanje je bistveno za ohranjanje globalnega, odprtega, stabilnega in varnega kibernetškega prostora. EU bi morala v ta namen še naprej sodelovati s tretjimi državami, mednarodnimi organizacijami in večdeležniško skupnostjo pri oblikovanju in izvajanju skladne in celostne mednarodne kibernetške politike, ob tem pa upoštevati vse večje medsebojno povezovanje med ekonomskimi vidiki novih tehnologij, notranje varnosti ter zunanje, varnostne in obrambne politike. EU kot močen gospodarski in trgovinski blok, ustanovljen na temeljnih demokratičnih vrednotah, spoštovanju pravne države in temeljnih pravic, ima tudi edinstveno

⁹⁹ Kot so program Obzorje Evropa, program za digitalno Evropo in Evropski obrambni sklad.

¹⁰⁰ <https://pesco.europa.eu/>.

priložnost, da prevzame vodilno vlogo pri določanju in spodbujanju mednarodnih norm in standardov.

3.1 Vodilna vloga EU pri oblikovanju standardov, norm in okvirov v kibernetnem prostoru

Okrepitev mednarodne standardizacije

Da bi lahko EU spodbujala in zagovarjala svojo vizijo kibernetnega prostora na mednarodni ravni, mora **okrepiti sodelovanje in vodilno vlogo v mednarodnih postopkih standardizacije ter povečati zastopanost v mednarodnih in evropskih organih za standardizacijo ter drugih organizacijah za razvoj standardov**¹⁰¹. Zaradi hitrega razvoja digitalnih tehnologij so mednarodni standardi vse pomembnejši pri dopolnjevanju tradicionalnih regulativnih prizadevanj na področjih, kot so umetna inteligenca, oblak, kvantno računalništvo in kvantna komunikacija. Mednarodna standardizacija se vse pogosteje uporablja v tretjih državah za spodbujanje njihovega političnega in ideološkega programa, ki pogosto ni skladen z vrednotami EU. Poleg tega se povečuje tveganje konkurenčnih okvirov za mednarodno standardizacijo, ki povzroča razdrobljenost.

Oblikovanje mednarodnih standardov na področju nastajajočih tehnologij in osnovne internetne arhitekture v skladu z vrednotami EU je bistveno za zagotovitev, da internet ostane globalen in odprt, da so tehnologije osredotočene na človeka in zasebnosti ter da je njihova uporaba zakonita, varna in etična. EU bi morala v okviru prihodnje strategije za standardizacijo opredeliti svoje **cilje za mednarodno standardizacijo** ter izvajati proaktivno in usklajeno razširjanje za njihovo spodbujanje na mednarodni ravni. Prizadevati bi si morala za tesnejše sodelovanje in porazdelitev bremena z enako mislečimi partnerji in evropskimi deležniki.

Spodbujanje odgovornega ravnanja držav v kibernetnem prostoru

EU še naprej sodeluje z mednarodnimi partnerji za uveljavljanje in spodbujanje globalnega, odprtega, stabilnega in varnega kibernetnega prostora, v katerem se spoštujejo **mednarodno pravo, zlasti Ustanovna listina Združenih narodov**¹⁰², ter upoštevajo **prostovoljne nezavezujoče norme, pravila in načela odgovornega ravnanja držav**¹⁰³. Zaradi zmanjševanja učinkovite večstranske razprave o mednarodni varnosti v kibernetnem prostoru obstaja jasna potreba po tem, da EU in države članice zavzamejo bolj proaktivno stališče v razpravah v okviru OZN in drugih ustreznih mednarodnih forumih. EU ima najboljše možnosti za **spodbujanje, usklajevanje in povezovanje stališč držav članic v mednarodnih forumih** ter bi morala **oblikovati stališče EU do uporabe mednarodnega prava v kibernetnem prostoru**. Visoki predstavnik namerava skupaj z državami članicami tudi nadaljevati oblikovanje svojega vključujočega in na soglasju temelječega predloga za politično zavezanost **programu ukrepov za spodbujanje odgovornega ravnanja držav v**

¹⁰¹ Na primer v [Mednarodni organizaciji za standardizacijo](#) (ISO), [Mednarodni elektrotehniški komisiji](#) (IEC), [Mednarodni telekomunikacijski zvezi](#) (ITU), [Evropskem odboru za standardizacijo](#) (CEN), [Evropskem odboru za elektrotehniško standardizacijo](#) (CENELEC), [Evropskem inštitutu za telekomunikacijske standarde](#) (ETSI), delovni skupini za internetsko inženirstvo (IETF), partnerskemu projektu tretje generacije (3GPP) ter [Inštitutu inženirjev elektrotehnike in elektronike](#) (IEEE).

¹⁰² <https://www.un.org/en/sections/un-charter/un-charter-full-text/>.

¹⁰³ Kot se odraža v ustreznih poročilih skupin vladnih strokovnjakov za razvoj na področju informacij in telekomunikacij v okviru mednarodne varnosti, ki jih je potrdila Generalna skupščina Združenih narodov, zlasti poročilih za leta 2015, 2013 in 2010.

kibernetskem prostoru¹⁰⁴ v okviru OZN. Program ukrepov za spodbujanje odgovornega ravnanja držav v kibernetskem prostoru, ki temelji na veljavnem pravnem redu, kot ga je potrdila Generalna skupščina Združenih narodov¹⁰⁵, ponuja platformo za sodelovanje in izmenjavo dobrih praks v okviru OZN ter predlaga vzpostavitev mehanizma za prenos norm odgovornega ravnanja držav v prakso in spodbujanje krepitve zmogljivosti. Poleg tega namerava visoki predstavnik okrepiti in spodbujati izvajanje **ukrepov za krepitev zaupanja** med državami, tudi z izmenjavo dobrih praks na regionalni in večstranski ravni ter s prispevanjem k medregionalnemu sodelovanju.

Večja globalna povezljivost ne bi smela voditi do cenzure, množičnega nadzora, kršitev zasebnosti podatkov ter zatiranja civilne družbe, akademikov in državljanov. EU bi morala še naprej imeti vodilno vlogo pri varstvu in spodbujanju **človekovih pravic in temeljnih svoboščin** na spletu. V ta namen bi morala spodbujati nadaljnje usklajevanje z mednarodnim pravom in standardi s področja človekovih pravic¹⁰⁶, izvajati svoj Akcijski načrt za človekove pravice in demokracijo za obdobje 2020–2024¹⁰⁷ ter uresničevati smernice o človekovih pravicah glede svobode izražanja na spletu in drugje¹⁰⁸, **pri tem pa ponuditi novo spodbudo za praktično uporabo instrumentov EU**. EU bi si morala vztrajno prizadevati za **zaščito zagovornikov človekovih pravic, civilne družbe in akademikov, ki se ukvarjajo z vprašanji, kot so kibernetska varnost, zasebnost podatkov, nadzor in spletna cenzura**. V ta namen bi morala zagotoviti dodatne praktične usmeritve, spodbujati dobre prakse in okrepiti prizadevanje za preprečevanje zlorabe nastajajočih tehnologij, zlasti z uporabo diplomatskih ukrepov, če so potrebni, in nadzorom nad izvozom takih tehnologij. EU bi se morala tudi še naprej boriti za zaščito najranljivejših članov družbe na spletu s predlaganjem zakonodaje za boljšo zaščito otrok pred spolno zlorabo in spolnim izkoriščanjem ter strategije o otrokovih pravicah.

Budimpeška konvencija o kibernetski kriminaliteti

EU še naprej podpira tretje države, ki želijo pristopiti h Konvenciji **Sveta Evrope o kibernetski kriminaliteti iz Budimpešte**, in si prizadeva dokončati **Drugi dodatni protokol k Budimpeški konvenciji**, ki vključuje zaščitne in druge ukrepe za izboljšanje mednarodnega sodelovanja med organi kazenskega pregona in pravosodnimi organi ter med organi in ponudniki storitev iz drugih držav ter za katere Komisija sodeluje v pogajanjih v imenu EU¹⁰⁹. Pri sedanji pobudi za nov pravni instrument o kibernetski kriminaliteti na ravni OZN obstaja tveganje širjenja razhajanj ter upočasnitve prepotrebnih nacionalnih reform in z njimi povezanih prizadevanj za krepitev zmogljivosti, kar bi lahko oviralo učinkovito mednarodno sodelovanje na področju boja proti kibernetski kriminaliteti: EU ne vidi potrebe po novem pravnem instrumentu o kibernetski kriminaliteti na ravni OZN. EU še naprej sodeluje pri **večstranskih izmenjavah o kibernetski kriminaliteti**, da bi zagotovila spoštovanje človekovih pravic in temeljnih svoboščin z vključenostjo in preglednostjo ter ob

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 Kot se odraža v ustreznih poročilih skupin vladnih strokovnjakov za razvoj na področju informacij in telekomunikacij v okviru mednarodne varnosti, ki jih je potrdila Generalna skupščina Združenih narodov, zlasti: poročila za leta 2015, 2013 in 2010.

¹⁰⁶ Zlasti Ustanovno listino Združenih narodov in Splošno deklaracijo o človekovih pravicah.

¹⁰⁷ <https://www.consilium.europa.eu/sl/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 Sklep Sveta iz junija 2019 (sklic 9116/19).

upoštevanju razpoložljivega strokovnega znanja, cilj tega sodelovanja pa je ustvarjanje dodane vrednosti za vse.

3.2 Sodelovanje s partnerji in večdeležniško skupnostjo

EU bi morala **okrepiti in razširiti svoje kibernetiske dialoge s tretjimi državami** za spodbujanje svojih vrednot in vizije za kibernetiski prostor z izmenjavo dobrih praks in prizadevanjem za učinkovitejše sodelovanje. Poleg tega bi morala vzpostaviti **strukturirane izmenjave z regionalnimi organizacijami**, kot so Afriška unija, regionalni forum ASEAN, Organizacija ameriških držav in Organizacija za varnostno sodelovanje v Evropi. Hkrati bi si morala prizadevati za doseg skupnih stališč, kjer bo to mogoče in primerno, z drugimi partnerji na podlagi vprašanj skupnega interesa. EU bi morala v sodelovanju z delegacijami EU, in kjer bo ustrezno, veleposlaništvu držav članic po vsem svetu oblikovati neformalno **mrežo EU za kibernetisko diplomacijo** za spodbujanje svoje vizije kibernetskega prostora, izmenjave informacij ter rednega usklajevanja v zvezi s spremembami v kibernetiskem prostor¹¹⁰.

EU bi morala na podlagi skupnih izjav z dne 8. julija 2016¹¹¹ in 10. julija 2018¹¹² še naprej spodbujati **sodelovanje med EU in zvezo NATO**, zlasti v zvezi z zahtevami po interoperabilnosti kibernetiske obrambe. V tem okviru bi si morala še naprej prizadevati za povezovanje ustreznih struktur SVOP z mreženjem federativnih misij zveze NATO, da bi se po potrebi omogočila interoperabilnost mreže z zvezo NATO in partnerji. Poleg tega bi bilo treba dodatno proučiti sodelovanje med EU in zvezo NATO na področju izobraževanja, usposabljanja in vaj, vključno z iskanjem sinergij med Evropsko akademijo za varnost in obrambo ter centrom odličnosti zveze NATO za kibernetisko obrambo.

EU v skladu s svojimi vrednotami močno podpira in spodbuja **večdeležniški model za upravljanje interneta**. Posamezni subjekti, vlade ali mednarodne organizacije ne bi smeli poskušati pridobiti nadzora nad internetom. EU bi morala še naprej sodelovati v forumih¹¹³, da bi okrepila sodelovanje ter zagotovila varstvo temeljnih pravic in svoboščin, zlasti pravico do dostojanstva in zasebnosti ter svobodo izražanja in obveščanja. Za spodbuditev večdeležniškega sodelovanja pri vprašanjih, povezanih s kibernetisko varnostjo, nameravata Komisija in visoki predstavnik v skladu s svojimi ustreznimi pristojnostmi okrepiti **redne in strukturirane izmenjave z deležniki**, vključno z zasebnim sektorjem, akademiki in civilno družbo, pri čemer poudarjata, da medsebojna povezanost kibernetskega prostora zahteva izmenjave med vsemi deležniki, ki morajo prevzeti posebne odgovornosti za ohranjanje globalnega, odprtega, stabilnega in varnega kibernetskega prostora. Ta prizadevanja bodo zagotovila dragocen prispevek za morebitne ključne ukrepe na ravni EU.

3.3 Krepitev globalnih zmogljivosti za povečanje globalne odpornosti

Za zagotovitev, da lahko vse države izkoristijo socialne, ekonomske in politične prednosti, ki jih prinašata internet in uporaba tehnologij, EU še naprej podpira svoje partnerje pri povečevanju njihovih kibernetiske odpornosti in zmogljivosti za preiskovanje in pregon kibernetiske kriminalitete ter obravnavanje kibernetiskih groženj. Za zagotovitev splošne

¹¹⁰ Kjer je ustrezno, bi lahko spodbudila tudi dejavnosti neformalne mreže EU za digitalno diplomacijo, ki vključuje zunanja ministrstva držav članic.

¹¹¹ <http://www.consilium.europa.eu/sl/press/press-releases/2016/07/08-eu-nato-joint-declaration/>.

¹¹² <https://www.consilium.europa.eu/sl/press/press-releases/2018/07/10/eu-nato-joint-declaration/>.

¹¹³ Kot sta Organizacije za dodeljevanje spletnih imen in števil (ICANN) in forum o upravljanju interneta.

skladnosti bi morala razviti **agendo EU za krepitev zunanjih kibernetских zmogljivosti**, da bi ta prizadevanja usmerjala v skladu s svojimi smernicami za krepitev zunanjih kibernetских zmogljivosti¹¹⁴ in agendo za trajnostni razvoj do leta 2030¹¹⁵. Agenda bi morala izkoristiti strokovno znanje držav članic ter ustreznih institucij, organov in agencij EU ter pobude, vključno z mrežo EU za krepitev kibernetских zmogljivosti¹¹⁶, v skladu z njihovimi ustreznimi pooblastili. Ustanovi se **odbor EU za krepitev kibernetске zmogljivosti**, ki bo vključeval vse ustrezne institucionalne deležnike EU in spremljal napredek, ter opredelitev dodatnih sinergij in morebitnih vrzeli. Poleg tega lahko podpira okrepljeno sodelovanje z državami članicami, partnerji iz javnega in zasebnega sektorja ter drugimi ustreznimi mednarodnimi organi za zagotovitev usklajevanja prizadevanj in preprečevanje podvajanj.

Krepitev kibernetске zmogljivosti EU bi se morala še naprej osredotočati na Zahodni Balkan in sosedstvo EU ter partnerske države, ki doživljajo hiter digitalni razvoj. Prizadevanja EU bi morala podpirati razvoj zakonodaje in politik partnerskih držav v skladu z ustreznimi politikami in standardi EU na področju kibernetске diplomacije. V tem okviru bi morala prizadevanja EU za krepitev zmogljivosti na področju digitalizacije vključevati kibernetско varnost kot standardni element. V ta namen bi morala EU razviti program usposabljanja, namenjen osebju EU, pristojnemu za izvajanje prizadevanj EU za krepitev zunanjih digitalnih in kibernetских zmogljivosti. EU bi morala v skladu s prizadevanji v okviru akcijskega načrta za evropsko demokracijo tem državam pomagati tudi pri spoprijemanju z vse večjim izzivom zlonamernih kibernetских dejavnosti, ki škodujejo razvoju njihovih družb ter **celovitosti in varnosti demokratičnih sistemov**. V zvezi s tem bi lahko bilo še posebno koristno vzajemno učenje med državami članicami EU ter ustreznimi agencijami EU in tretjimi državami.

Nazadnje, v okviru pakta o civilnih vidikih SVOP iz leta 2018¹¹⁷ lahko civilne misije SVOP prispevajo tudi k širšemu odzivu EU za spoprijemanje z izzivi na področju kibernetске varnosti, zlasti s krepitvijo pravne države v partnerskih državah ter zmogljivosti kazenskega pregona in civilne uprave teh držav.

Strateške pobude

EU bi morala:

- opredeliti sklop ciljev v mednarodnih postopkih standardizacije in jih spodbujati na mednarodni ravni;
- spodbujati mednarodno varnost in stabilnost v kibernetском prostoru, zlasti s predlogom EU in njenih držav članic za program ukrepov za spodbujanje odgovornega ravnanja držav v kibernetском prostoru v okviru Združenih narodov;
- ponuditi praktične smernice o uporabi človekovih pravic in temeljnih svoboščin v kibernetском prostoru;
- bolje zavarovati otroke pred spolno zlorabo in izkoriščanjem ter pripraviti strategijo o otrokovih pravicah;

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/sl/pdf>.

- okrepiti in spodbujati Budimpeško konvencijo o kibernetški kriminaliteti, tudi s pripravo Drugega dodatnega protokola k Budimpeški konvenciji;
- razširiti kibernetški dialog EU s tretjimi državami ter regionalnimi in mednarodnimi organizacijami, tudi prek neformalne mreže EU za kibernetško diplomacijo;
- okrepiti izmenjavo z večdeležniško skupnostjo, zlasti z rednimi in strukturiranimi izmenjavami z zasebnim sektorjem, akademiki in civilno družbo, ter
- predlagati agendo EU za krepitev zunanjih kibernetških zmogljivosti in odbor EU za krepitev kibernetške zmogljivosti.

III. KIBERNETSKA VARNOST V INSTITUCIJAH, ORGANIH IN AGENCIJAH EU

Institucije, organi in agencije EU so zaradi svojega velikega političnega pomena, kritičnih misij za usklajevanje zelo občutljivih vprašanj in vloge pri upravljanju velikih zneskov javnega denarja **redno tarča kibernetških napadov**, zlasti kibernetškega vohunjenja. Vendar se raven kibernetške odpornosti ter sposobnost odkrivanja zlonamernih kibernetških dejavnosti in odzivanja nanje med temi subjekti po zrelosti močno razlikujeta. Zato je treba s skladnimi in enotnimi pravili izboljšati splošno raven kibernetške varnosti.

Na področju informacijske varnosti je bil dosežen napredek pri doseganju večje skladnosti **pravil za varovanje tajnih podatkov in občutljivih netajnih podatkov EU**. Vendar interoperabilnost sistemov tajnih podatkov ostaja omejena, kar preprečuje nemoten prenos podatkov med različnimi subjekti. Doseči bi bilo treba nadaljnji napredek za omogočanje medinstitucionalnega pristopa k obravnavanju tajnih podatkov in občutljivih netajnih podatkov EU, ki bi se lahko uporabljal tudi kot vzorec za interoperabilnost med državami članicami. Določiti bi bilo treba tudi izhodišče za poenostavitev postopkov z državami članicami. EU bi morala tudi nadalje razvijati svojo sposobnost varnega komuniciranja z ustreznimi partnerji, pri čemer bi morala čim bolj upoštevati obstoječe ureditve in postopke.

Kot je napovedano v strategiji za varnostno unijo, bo Komisija zato pripravila predloge za **skupna zavezujoča pravila o informacijski varnosti ter skupna zavezujoča pravila o kibernetški varnosti za vse institucije, organe in agencije EU v letu 2021**, pri čemer bo izhajala iz razprav, ki med institucijami EU potekajo o kibernetški varnosti¹¹⁸.

Sedanji in prihodnji trendi dela na daljavo bodo zahtevali tudi dodatne naložbe v varno opremo, infrastrukturo in orodja, ki omogočajo delo na daljavo z občutljivimi in tajnimi datotekami.

Poleg tega so zaradi vse bolj sovražnega okolja kibernetških groženj in večje pojavnosti izpopolnjenih kibernetških napadov, ki škodijo institucijam, organom in agencijam EU, potrebne večje naložbe za doseganje visoke ravni kibernetške zrelosti. Za vse institucije, organe in agencije EU se vzpostavlja program za kibernetško ozaveščanje za povečanje ozaveščenosti in kibernetške higijene osebja ter podpiranje skupne kulture kibernetške varnosti.

¹¹⁸ Redne razprave med institucijami EU o kibernetški varnosti so del širših izmenjav o priložnostih in izzivih, ki jih digitalna preobrazba prinaša institucijam EU.

Skupino CERT-EU je treba okrepiti z izboljšanim mehanizmom financiranja, da bi se povečala njena sposobnost zagotavljanja pomoči institucijam, organom in agencijam EU pri uporabi novih pravil o kibernetiki varnosti za izboljšanje njihove kibernetike odpornosti. Poleg tega je treba okrepiti mandat skupine CERT-EU, da ji bodo zagotovljena stalna sredstva za doseganje teh ciljev.

Strateške pobude

1. Uredba o informacijski varnosti v institucijah, organih in agencijah EU
2. Uredba o skupnih pravilih o kibernetiki varnosti za institucije, organe in agencije EU
3. Nova pravna podlaga za okrepitev mandata in financiranja skupine CERT-EU

IV. SKLEPNE UGOTOVITVE

Usklajeno izvajanje te strategije bo prispevalo h kibernetiki varnemu digitalnemu desetletju za EU, dokončanju varnostne unije in okrepitvi položaja EU v svetu.

EU bi morala biti vodilna pri standardih in normah za vrhunske rešitve in standarde kibernetike varnosti za bistvene storitve in kritično infrastrukturo ter razvoj in uporabo novih tehnologij. Vsaka organizacija in posameznik, ki uporablja internet, je del rešitve pri zagotavljanju kibernetiki varne digitalne preobrazbe.

Komisija in visoki predstavnik bosta v skladu s svojimi pristojnostmi spremljala napredek na podlagi te strategije ter pripravila merila za ocenjevanje. Prispevki k temu spremljanju bi morali vključevati poročila agencije ENISA in redna poročila Komisije o varnostni uniji. Rezultati bodo prispevali k ciljem za prihodnje digitalno desetletje¹¹⁹. Komisija in visoki predstavnik se bosta v skladu s svojimi pristojnostmi še naprej povezovala z državami članicami, da bi opredelila praktične ukrepe za povezovanje na štirih področjih kibernetike varnosti v EU: odpornost kritične infrastrukture in notranjega trga, pravosodje in kazenski pregon, kibernetika diplomacija in kibernetika obramba, po potrebi. Poleg tega bosta še naprej sodelovala z večdeležniško skupnostjo ter opozarjala na potrebo, da vsi, ki uporabljajo internet, prispevajo k ohranjanju globalnega, odprtega, stabilnega in varnega kibernetikega prostora, v katerem lahko vsi živijo varno digitalno življenje.

¹¹⁹ Kot je napovedano v delovnem programu Komisije za leto 2021.

Dodatek: Naslednji koraki za kibernetško varnost omrežij 5G

Glede na rezultate pregleda priporočila Komisije o kibernetški varnosti omrežij 5G¹²⁰ bi se morali naslednji koraki pri usklajenem delu na ravni EU osredotočiti na tri ključne cilje ter glavne kratko- in srednjeročne ukrepe, opredeljene v spodnji preglednici, ki bi jih morali izvesti organi držav članic, Komisija in agencija ENISA.

Prva prednostna naloga za naslednjo fazo je **dokončna uvedba nabora orodij na nacionalni ravni in obravnavanje vprašanj, opredeljenih v poročilu o napredku iz julija 2020**. V tem okviru bi imeli nekateri od strateških ukrepov iz nabora orodij korist od **okrepljenega usklajevanja ali izmenjave informacij** v okviru delovnih postopkov skupine za sodelovanje na področju varnosti omrežij in informacij, kot je opredeljeno že v poročilu o napredku, kar bi lahko privedlo do razvoja **dobrih praks ali smernic**. Kar zadeva tehnične ukrepe, bi lahko agencija ENISA zagotovila dodatno podporo, pri čemer bi izhajala iz že opravljenega dela in temeljiteje proučila nekatere teme ter **pripravila celovit pregled vseh ustreznih smernic o zahtevah glede kibernetške varnosti 5G za operaterje mobilnih omrežij**.

Drugič, države članice so poudarile, kako pomembno je iti v korak z razvojem s **stalnim spremljanjem razvoja na področju tehnologije, arhitekture 5G, groženj in primerov uporabe ter aplikacij 5G, pa tudi zunanjih dejavnikov**, da se lahko **opredelijo in obravnavajo nova ali nastajajoča tveganja**. Poleg tega bi bilo treba nadalje proučiti več vidikov iz prvotne analize tveganja, zlasti za zagotovitev, da bi obravnavala celotni ekosistem 5G, vključno z vsemi ustreznimi deli omrežne infrastrukture in dobavne verige 5G. Čeprav je nabor orodij zasnovan kot prožen in prilagodljiv instrument, bi se lahko srednjeročno po potrebi sprejeli ukrepi za njegovo dopolnitev ali spremembo, da bi se zagotovilo ohranjanje njegove celovitosti in aktualnosti.

Tretjič, še naprej bi bilo treba sprejemati **ukrepe na ravni EU** za podpiranje in dopolnjevanje ciljev nabora orodij ter njihovo popolno vključevanje v ustrezne politike Unije in Komisije, zlasti na podlagi ukrepov, ki jih je Komisija napovedala v sporočilu o naboru orodij z dne 29. januarja 2020¹²¹, na najrazličnejših področjih (npr. sredstva EU za varna omrežja 5G, naložbe v tehnologije 5G in tehnologije naslednic 5G, instrumenti trgovinske zaščite in konkurenca za preprečevanje izkrivljanj na dobavnem trgu 5G itd.).

Po potrebi bi se morali glavni akterji v začetku leta 2021 dogovoriti o podrobnih ureditvah in mejnikih za glavne ukrepe, ki so navedeni v nadaljevanju.

Ključni cilj 1: zagotovitev usklajenih nacionalnih pristopov za učinkovito zmanjševanje tveganj v EU		
Področja	Glavni kratko- in srednjeročni ukrepi	Glavni akterji
Izvajanje nabora orodij v državah članicah	Dokončanje izvajanja ukrepov, priporočenih v sklepih o naboru orodij, do drugega četrtletja leta 2021, z rednimi pregledi v okviru delovnih postopkov skupine za	Organi držav članic

¹²⁰ Poročilo Komisije o vplivih priporočila Komisije 2019/534 z dne 26. marca 2019 z naslovom Kibernetška varnost omrežij 5G.

¹²¹ Sporočilo Komisije COM(2020) 50, Varna uvedba tehnologije 5G v EU – izvajanje nabora orodij EU, 29. januar 2020.

	sodelovanje na področju varnosti omrežij in informacij.	
Izmenjava informacij in dobrih praks o strateških ukrepih, povezanih z dobavitelji	Okrepitev izmenjav informacij in proučitev morebitnih dobrih praks, zlasti o: - omejitvah za visoko tvegane dobavitelje (SM03) in ukrepih, povezanih z zagotavljanjem upravljanih storitev (SM04); - varnosti in odpornosti dobavne verige, zlasti na podlagi raziskave, ki jo je organ BEREC izvedel o SM05 in SM06.	Organi držav članic, Komisija
Krepitev zmogljivosti in smernice o tehničnih ukrepih	Izvedba poglobljene tehnične analize ter razvoj skupnih smernic in orodij, vključno s: - celovito in dinamično matriko varnostnega nadzora in dobrih praks za varnost 5G; smernicami v podporo izvajanju izbranih tehničnih ukrepov iz nabora orodij.	Agencija ENISA, organi držav članic
Ključni cilj 2: Podpiranje stalne izmenjave znanja in krepitev zmogljivosti		
Področja	Glavni kratko- in srednjeročni ukrepi	Glavni akterji
Nenehno pridobivanje znanja	Organizacija dejavnosti za pridobivanje znanja o tehnologiji in z njo povezanih izzivih (odprte arhitekture, značilnosti 5G – npr. virtualizacija, shranjevanje podatkov v vsebnikih, rezinjenje itd.), razvoj okolja groženj, dejanski incidenti itd.	Agencija ENISA, organi držav članic, drugi deležniki
Ocene tveganja	Posodobitev in izmenjava informacij o posodobljenih nacionalnih ocenah tveganja	Organi držav članic, Komisija, agencija ENISA
Skupni projekti s financiranjem EU za podporo izvajanja nabora orodij	Zagotavljanje finančne podpore projektom, ki podpirajo izvajanje nabora orodij z uporabo sredstev EU, zlasti v okviru programa za digitalno Evropo (npr. projekti krepitev zmogljivosti za nacionalne organe, preskuševalne naprave ali druge napredne zmogljivosti itd.)	Organi držav članic, Komisija
Sodelovanje med deležniki	Spodbujanje sodelovanja med nacionalnimi organi, ki se ukvarjajo s kibernetsko varnostjo 5G (npr. Skupina za sodelovanje na področju varnosti omrežij in informacij, organi za kibernetsko varnost, regulativni organi za telekomunikacije), in zasebnimi deležniki	Organi držav članic, Komisija, agencija ENISA
Ključni cilj 3: Spodbujanje odpornosti dobavne verige in drugi strateški varnostni cilji EU		
Področja	Glavni kratko- in srednjeročni ukrepi	Glavni akterji
Standardizacija	Opredelitev in izvajanje konkretnega akcijskega načrta za povečanje zastopanosti EU v organih za določanje standardov v okviru naslednjega koraka pri prizadevanjih podskupine za standardizacijo varnosti omrežij in informacij za doseganje določenih varnostnih ciljev, vključno s spodbujanjem interoperabilnih vmesnikov za olajševanje diverzifikacije dobaviteljev.	Organi držav članic
Odpornost dobavne verige	– Izvedba poglobljene analize ekosistema in dobavne verige 5G za boljšo opredelitev in spremljanje ključnih sredstev in morebitnih kritičnih odvisnosti – Zagotovitev delovanja trga in dobavne verige 5G v skladu	Organi držav članic, Komisija

	s pravili trgovanja in konkurence ter cilji EU, kot so opredeljeni v sporočilu Komisije z dne 29. januarja, in uporabe pregleda neposrednih tujih naložb pri razvoju naložb, ki bi lahko vplival na vrednostno verigo 5G, ob upoštevanju ciljev nabora orodij. – Spremljanje obstoječih in pričakovanih tržnih trendov ter ocena tveganj in priložnosti na področju odprtega radijskega dostopnega omrežja (RAN), zlasti na podlagi neodvisne študije	
Certificiranje	Začetek priprave certifikacijskih shem za ustrezne kandidate za ključne komponente 5G in postopke dobaviteljev za pomoč pri obravnavanju nekaterih tveganj, povezanih s tehničnimi šibkimi točkami, kot je opredeljeno v načrtih nabora orodij za zmanjšanje tveganja.	Komisija, agencija ENISA, nacionalni organi, drugi deležniki
Zmogljivosti EU in varna uvedba omrežij	– Naložbe v raziskave in inovacije ter zmogljivosti, zlasti s sprejetjem partnerstva za pametna omrežja in storitve. – Izvedba ustreznih varnostnih pogojev za programe financiranja in finančne instrumente EU (notranje in zunanje), kot je napovedano v sporočilu Komisije z dne 29. januarja.	Države članice, Komisija, deležniki iz industrije 5G
Zunanji vidiki	Pozitiven odziv na zahteve tretjih držav, ki želijo razumeti in morda uporabljati pristop nabora orodij, ki ga je razvila EU.	Države članice, Komisija, ESZD, delegacije EU