Rada
Európskej únie

V Bruseli 16. decembra 2020
(OR. en)

14133/20

Medziinštitucionálny spis:
2020/0305(NLE)

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

SPRIEVODNÁ POZNÁMKA

Od:	Martine DEPREZOVÁ, riaditeľka, v zastúpení generálnej tajomníčky Európskej komisie
Dátum doručenia:	16. decembra 2020
Komu:	Jeppe TRANHOLM-MIKKELSEN, generálny tajomník Rady Európskej únie
Č. dok. Kom.:	JOIN(2020) 18 final
Predmet:	SPOLOČNÉ OZNÁMENIE EURÓPSKEMU PARLAMENTU A RADE Stratégia kybernetickej bezpečnosti EÚ v digitálnej dekáde

Delegáciám v prílohe zasielame dokument JOIN(2020) 18 final.

Príloha: JOIN(2020) 18 final

EURÓPSKA
KOMISIA

VYSOKÝ PREDSTAVITEĽ
ÚNIE PRE
ZAHRANIČNÉ VECI
A BEZPEČNOSTNÚ POLITIKU

V Bruseli 16. 12. 2020
JOIN(2020) 18 final

SPOLOČNÉ OZNÁMENIE EURÓPSKEMU PARLAMENTU A RADE

Stratégia kybernetickej bezpečnosti EÚ v digitálnej dekáde

SPOLOČNÉ OZNÁMENIE EURÓPSKEMU PARLAMENTU A RADE

Stratégia kybernetickej bezpečnosti EÚ v digitálnej dekáde

I. ÚVOD: KYBERNETICKY BEZPEČNÁ DIGITÁLNA TRANSFORMÁCIA V ZLOŽITOM KONTEXTE HROZIEB

Kybernetická bezpečnosť je neoddeliteľnou súčasťou celkovej bezpečnosti Európanov. Či už ide o pripojené zariadenia, elektrizačné sústavy, banky, lietadlá, verejnú správu alebo nemocnice, ktoré používajú alebo navštevujú, zaslúžia si istotu, že budú chránení pred kybernetickými hrozbami. Hospodárstvo, demokracia a spoločnosť EÚ viac než kedykoľvek predtým závisia od bezpečných a spoľahlivých digitálnych nástrojov a pripojiteľnosti. Kybernetická bezpečnosť je preto nevyhnutná na vybudovanie odolnej, zelenej a digitálnej Európy.

Doprava, energetika a zdravotníctvo, telekomunikácie, financie, bezpečnosť, demokratické procesy, vesmír aj obrana intenzívne využívajú siete a informačné systémy, ktoré sú čoraz prepojenejšie. Medziodvetvová previazanosť je veľmi silná, pretože fungovanie sietí a informačných systémov si zas vyžaduje stabilnú dodávku elektriny. Počet pripojených zariadení už presiahol počet ľudí na planéte a predpokladá sa, že do roku 2025 vzrastie na 25 miliárd[1] – a štvrtina z nich bude v Európe. Digitalizáciu pracovného režimu urýchlila pandémia COVID-19: 40 % pracovníkov EÚ počas nej presedlalo na prácu na diaľku, čo pravdepodobne trvalo ovplyvní každodenný život[2]. Rastie tým náchylnosť na kybernetické útoky[3]. Pripojené produkty sa často dodávajú spotrebiteľovi so známymi bezpečnostnými slabinami, čo ešte rozširuje „plochu útoku“ pre škodlivé kybernetické činnosti[4]. Čoraz viac sa digitalizuje a prepája aj priemyselná scéna EÚ, čo tiež znamená, že kybernetické útoky môžu mať oveľa väčší dosah na odvetvia a ekosystémy než kedykoľvek predtým.

Panorámu hrozieb ešte zhoršuje geopolitické napätie v otázkach globálneho a otvoreného internetu, ako aj kontroly nad technológiami v celom dodávateľskom reťazci[5]. Toto napätie sa odráža v rastúcom počte štátov, ktoré si stavajú digitálne hranice.

---

1 Odhad telekomunikačného záujmového združenia GSMA; https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf. Spoločnosť International Data Corporation predpovedá 42,6 miliardy pripojených zariadení, snímačov a kamier; https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

2 V prieskume z júna 2020 uviedlo 47 % vedúcich podnikov, že plánujú umožniť zamestnancom prácu na diaľku na plný úväzok, aj keď už bude možné vrátiť sa na pracovisko; 82 % plánovalo umožniť prácu na diaľku aspoň na časť pracovného času; 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 Jeden z doposiaľ najškodlivejších malvérov (známy ako Mirai) vytvoril botnety zahŕňajúce vyše 600 000 zariadení, ktoré narušili chod viacerých veľkých webových sídel v Európe a Spojených štátoch amerických.

5 Vrátane elektronických komponentov, dátovej analýzy, cloudu, rýchlejších a inteligentnejších sietí 5G a sietí ďalších generácií, šifrovania, umelej inteligencie (AI) a nových modelov výpočtov a dôveryhodného spracovania údajov, ako je blockchain, cloud-to-edge a kvantová výpočtová technika.

Obmedzovanie internetu ohrozuje globálny a otvorený kybernetický priestor, ako aj právny štát, základné práva, slobodu a demokraciu, ktoré sú základnými hodnotami EÚ. Kybernetický priestor sa čoraz častejšie zneužíva na politické a ideologické účely a nárast polarizácie na medzinárodnej úrovni bráni účinnému multilateralizmu. Hybridné hrozby kombinujú dezinformačné kampane s kybernetickými útokmi na infraštruktúru, hospodárske procesy a demokratické inštitúcie, pričom môžu spôsobiť fyzické škody, získať neoprávnený prístup k osobným údajom, ukradnúť priemyselné alebo štátne tajomstvá, vyvolať nedôveru a oslabiť sociálnu súdržnosť. Tieto činnosti oslabujú medzinárodnú bezpečnosť a stabilitu, ako aj prínosy kybernetického priestoru pre hospodársky, sociálny a politický rozvoj.

Veľkým globálnym rizikom sú zlovoľné útoky na kritickú infraštruktúru[6]. Internet má decentralizovanú architektúru bez ústrednej štruktúry a riadi ho viacero zainteresovaných strán. Hoci je neustále terčom zlovoľných pokusov o narušenie chodu, podarilo sa mu absorbovať exponenciálny nárast prenosových objemov[7]. Zároveň sa zvyšuje závislosť od základných funkcií globálneho a otvoreného internetu (napríklad systém doménových mien – DNS) a nevyhnutných internetových služieb v oblasti komunikácie, hostingu, aplikácií a údajov. Tieto služby sa čoraz viac sústreďujú v rukách niekoľkých súkromných spoločností[8]. Európske hospodárstvo a spoločnosť sú tak zraniteľné voči rušivým geopolitickým alebo technickým udalostiam, ktoré ovplyvňujú jadro internetu alebo jednu či viaceré z týchto spoločností. Nárast vo využívaní internetu a zmeny správania v dôsledku pandémie ešte viac odhalili krehkosť dodávateľských reťazcov, ktoré sú od tejto digitálnej infraštruktúry závislé.

Bezpečnostné obavy sú jedným z hlavných faktorov odrádzajúcich od využívania online služieb[9]. Zhruba dve pätiny používateľov v EÚ sa stretli s bezpečnostnými problémami a tri pätiny majú pocit, že sa pred kybernetickou kriminalitou nedokážu chrániť[10]. Tretina dostala za posledné tri roky podvodné e-maily alebo telefonáty so žiadosťou o osobné údaje, ale 83 % kybernetický zločin vôbec nenahlásilo. Kybernetické útoky postihli každý ôsmy podnik[11]. Vyše polovica podnikových a spotrebiteľských osobných počítačov, ktoré boli raz

---

6 Svetové ekonomické fórum, správa o globálnych rizikách 2020.

7 Podľa Organizácie pre hospodársku spoluprácu a rozvoj viedla pandémia k 60 % nárastu objemu dátových prenosov na internete; https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/. Orgán európskych regulátorov pre elektronické komunikácie a Komisia pravidelne uverejňujú správy o stave kapacity internetu počas opatrení na obmedzenie šírenia koronavírusu. Podľa správy agentúry ENISA vzrástol v treťom štvrťroku 2019 celkový počet distribuovaných útokov na vyradenie služby (DDoS) o 241 % oproti tretiemu štvrťroku 2018. Intenzita útokov DDoS rastie, pričom vo februári 2020 došlo k historicky najväčšiemu, ktorý dosiahol špičkový nápor 2,3 terabitov za sekundu. Pri výpadku firmy CenturyLink v auguste 2020 spôsobil problém so smerovačmi tohto amerického poskytovateľa internetových služieb prepad celosvetového internetového prenosu o 3,5 %; https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service.

8 Internet Society, *The Global Internet Report: Consolidation in the Internet Economy* (Globálna správa o internete: konsolidácia internetového hospodárstva); 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/en/data/dataset/S2249_92_2_499_ENG.

10 Index digitálnej ekonomiky a spoločnosti za rok 2020; https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020; https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG.

11 Tlačová správa Eurostatu, Bezpečnostné opatrenia IKT prijaté prevažnou väčšinou podnikov v EÚ, 6/2020 – 13. január 2020. „Kybernetické útoky na kritickú infraštruktúru sa stali novou normou v sektoroch ako energetika, zdravotníctvo a doprava“; Svetové ekonomické fórum, správa o globálnych rizikách 2020.

infikované malvérom, sa v tom istom roku infikuje opäť[12]. Každoročne sa pre narušenie ochrany údajov stratia milióny záznamov; priemerné náklady takéhoto narušenia pre jeden podnik v roku 2018 vzrástli na viac ako 3,5 milióna EUR[13]. Vplyv kybernetického útoku často nemožno izolovať – môže vyvolať reťazové reakcie v celom hospodárstve a spoločnosti, ktoré postihujú milióny ľudí[14].

Vyšetrovanie takmer všetkých druhov trestnej činnosti má aj digitálnu zložku. V roku 2019 sa nahlásený počet incidentov medziročne strojnásobil. Odhadom existuje 700 miliónov nových vzoriek malvéru, ktorý je najčastejším nosičom kybernetických útokov[15]. Počítačová kriminalita stála svetové hospodárstvo v roku 2020 odhadom 5,5 bilióna EUR, čo je dvojnásobok oproti roku 2015[16]. Ide o historicky najväčší transfer ekonomickej hodnoty – väčší než svetový obchod s drogami. Pri jednom veľkom incidente – ransomwarovom útoku WannaCry z roku 2017 – sa náklady pre svetové hospodárstvo odhadli na úrovni vyše 6,5 miliardy EUR[17].

Najčastejšie sú cieľom kybernetických útokov digitálne služby a finančný sektor, spolu s verejným sektorom a výrobou, no kybernetická pripravenosť a povedomie podnikov i jednotlivcov sú naďalej nízke[18] a pracovný trh trpí závažným nedostatkom kybernetickobezpečnostných zručností[19]. V roku 2019 došlo k takmer 450 kybernetickým incidentom, ktoré zasiahli kritickú európsku infraštruktúru ako finančný sektor a energetiku[20]. Zdravotnícke organizácie a zástupcovia tejto profesie boli obzvlášť zasiahnutí počas pandémie. Technológie sa neoddeliteľne prepájajú s fyzickým svetom a kybernetické útoky ohrozujú životy a blahobyt najzraniteľnejších skupín[21]. Viac ako dve tretiny firiem, najmä MSP, sa v kybernetickobezpečnostnej sfére považujú za „nováčikov“ a predpokladá sa, že európske spoločnosti sú slabšie pripravené než firmy v Ázii a Amerike[22]. Odhadom 291 000 pracovných miest pre odborníkov na kybernetickú bezpečnosť v Európe zostáva

---

12 Zdroj: Comparitech.

13 *Annual Cost of a Data Breach Report* (Správa o ročných nákladoch narušenia ochrany údajov), 2020 Ponemon Institute, vychádza z kvantitatívnej analýzy 524 nedávnych narušení v 17 geografických oblastiach a 17 odvetviach; https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf.

14 Správa Spoločného výskumného centra (JRC), Kybernetická bezpečnosť – naša digitálna opora; https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor.

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

16 JRC, Kybernetická bezpečnosť – naša digitálna opora.

17 Zdroj: Cyence.

18 Podnikateľské povedomie je naďalej nízke (aj pokiaľ ide o kybernetické krádeže obchodného tajomstva), najmä medzi MSP; štúdia PwC o rozsahu a vplyvoch priemyselnej špionáže a krádeže obchodného tajomstva prostredníctvom kybernetického priestoru: správa o opatreniach na boj proti kybernetickým krádežiam obchodného tajomstva a ich prevenciu, 2018.

19 Pozri ENISA, *Threat Landscape* (Panoráma hrozieb), 2020. Pozri tiež Verizon, *Data Breach Investigations Report* (Správa o vyšetrovaniach narušenia ochrany údajov), 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 Ransomware sa použil pri útokoch na nemocnice a zdravotné záznamy, napr. Rumunsko (jún 2020), Düsseldorf (september 2020) a Vastaamo (október 2020).

22 PwC, *The Global State of Information Security* (Globálny stav informačnej bezpečnosti), 2018; ESI Thoughtlab, The Cybersecurity Imperative, 2019.

neobsadených. Nábor a školenie odborníkov na kybernetickú bezpečnosť je pomalý proces, čo zvyšuje kybernetickobezpečnostné riziká pre organizácie[23].

EÚ chýba kolektívna situačná informovanosť o kybernetických hrozbách. Je to preto, že vnútroštátne orgány systematicky nezhromažďujú a nezdieľajú informácie (napríklad dostupné zo súkromného sektora), ktoré by mohli pomôcť vyhodnotiť stav kybernetickej bezpečnosti v EÚ. Členské štáty nahlasujú len zlomok incidentov a výmena informácií nie je ani systematická, ani komplexná[24]; kybernetické útoky môžu byť len jednou zo zložiek zosúladených zlovoľných útokov na európsku spoločnosť. Členské štáty si dnes vzájomne poskytujú len obmedzenú operačnú pomoc a neexistuje medzi nimi a inštitúciami, agentúrami a orgánmi EÚ žiaden operačný mechanizmus pre prípad rozsiahlych cezhraničných kybernetických incidentov alebo kríz[25].

Zvýšenie kybernetickej bezpečnosti je preto kľúčom k tomu, aby ľudia dôverovali inováciám, prepojenosti a automatizácii, aby ich využívali vo svoj prospech a aby sa chránili základné práva a slobody vrátane práva na súkromie a ochranu osobných údajov, ako aj slobody prejavu a práva na informácie. Kybernetická bezpečnosť je nevyhnutná pre sieťovú pripojiteľnosť a globálny otvorený internet, na ktorom stojí transformácia hospodárstva a spoločnosti v 20. rokoch tohto storočia. Prispieva ku kvalite aj kvantite pracovných miest, flexibilnejším pracoviskám, efektívnejšej a udržateľnejšej doprave a poľnohospodárstvu, ako aj k ľahšiemu a spravodlivejšiemu prístupu k zdravotnej starostlivosti. Takisto je predpokladom prechodu na čistejšiu energiu v rámci Európskej zelenej dohody[26] vďaka cezhraničným sieťam, inteligentným meradlám a predchádzaniu zbytočnej duplicite uchovávania údajov. V neposlednom rade má zásadný význam aj pre medzinárodnú bezpečnosť a stabilitu, rozvoj hospodárstiev, demokracie a spoločenstiev na celom svete. Vlády, podniky aj jednotlivci preto musia používať digitálne nástroje zodpovedne a myslieť pri tom na bezpečnosť. Kybernetickobezpečnostné povedomie a hygiena musia byť základom digitálnej transformácie každodenných činností.

Nová stratégia kybernetickej bezpečnosti EÚ v digitálnej dekáde je kľúčovým prvkom formovania digitálnej budúcnosti Európy[27], Plánu obnovy pre Európu z dielne Komisie[28], Stratégie EÚ pre bezpečnostnú úniu na roky 2020 – 2025[29], globálnej stratégie pre zahraničnú a bezpečnostnú politiku EÚ[30] a strategického programu Európskej rady na roky 2019 – 2024[31]. Stanovuje sa v nej, ako bude EÚ chrániť svojich občanov, podniky a inštitúcie pred kybernetickými hrozbami, ako bude presadzovať medzinárodnú spoluprácu a ako sa ujme vedenia pri zabezpečovaní globálneho a otvoreného internetu.

---

23 Agentúra EÚ pre kybernetickú bezpečnosť – Rozvoj zručností v oblasti kybernetickej bezpečnosti v EÚ: certifikácia kybernetickobezpečnostných diplomov a databáza vysokoškolského vzdelávania agentúry ENISA, december 2019.

24 Od členských štátov sa vyžaduje, aby skupine pre spoluprácu predkladali výročnú súhrnnú správu o oznámeniach prijatých podľa článku 10 ods. 3 smernice o bezpečnosti sietí a informačných systémov [smernica (EÚ) 2016/1148].

25 Sú zavedené stále operačné postupy vzájomnej pomoci medzi členmi siete jednotiek CSIRT.

26 Európska zelená dohoda, COM(2019) 640 final.

27 Formovanie digitálnej budúcnosti Európy, COM(2020) 67 final.

28 Správny čas pre Európu: náprava škôd a príprava budúcnosti pre ďalšie generácie, COM(2020) 456 final.

29 Stratégia EÚ pre bezpečnostnú úniu na roky 2020 – 2025, COM(2020) 605 final.

30 https://eeas.europa.eu/topics/eu-global-strategy_en.

31 https://www.consilium.europa.eu/sk/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/#.

II. MYSLIEŤ GLOBÁLNE, KONAŤ EURÓPSKY

Cieľom tejto stratégie je zabezpečiť globálny a otvorený internet so silnými prvkami ochrany pred rizikami z hľadiska bezpečnosti a základných práv a slobôd Európanov. V nadväznosti na pokrok dosiahnutý predchádzajúcimi stratégiami obsahuje konkrétne návrhy na zavedenie **troch hlavných nástrojov – regulačného, investičného a politického**, s cieľom riešiť **tri oblasti činnosti EÚ – 1. odolnosť, technologická suverenita a vedúce postavenie; 2. budovanie operačnej kapacity na prevenciu, odrádzanie a reakciu a 3. presadzovanie globálneho a otvoreného kybernetického priestoru**. EÚ je odhodlaná podporiť túto stratégiu **bezprecedentnými investíciami do digitálnej transformácie EÚ v nasledujúcich siedmich rokoch** (pričom predošlá úroveň financovania sa môže až zoštvornásobiť) v rámci nových technologických a priemyselných politík a programu obnovy[32].

Kybernetická bezpečnosť sa musí začleniť do všetkých týchto digitálnych investícií, najmä do kľúčových technológií ako umelá inteligencia (AI), šifrovanie a kvantová výpočtová technika, pričom treba využiť stimuly, povinnosti a referenčné porovnávanie. Možno tak stimulovať rast európskeho odvetvia kybernetickej bezpečnosti a poskytnúť istotu potrebnú na uľahčenie postupného odstavovania starých systémov. Z Európskeho obranného fondu (EDF) sa podporia európske riešenia v oblasti kybernetickej obrany v rámci európskej obrannej technologickej a priemyselnej základne (EDTIB). Kybernetická bezpečnosť je na podporu našich partnerov zahrnutá aj v nástrojoch na financovanie vonkajšej činnosti, najmä Nástroji susedstva a rozvojovej a medzinárodnej spolupráce. Prevencia zneužívania technológií, ochrana kritickej infraštruktúry a zabezpečenie integrity dodávateľských reťazcov takisto umožňujú, aby EÚ dodržiavala normy, pravidlá a zásady zodpovedného správania štátov OSN[33].

1. ODOLNOSŤ, TECHNOLOGICKÁ SUVERENITA A VEDÚCE POSTAVENIE

Kritická infraštruktúra EÚ a základné služby sú čoraz viac vzájomne prepojené a digitalizované. Všetky veci pripojené k internetu v EÚ, či už automatizované autá, priemyselné kontrolné systémy alebo domáce spotrebiče, ako aj všetky dodávateľské reťazce, ktoré ich sprístupňujú, musia byť zabezpečené už v štádiu návrhu, odolné voči kybernetickým incidentom a v prípade zistenia zraniteľných miest rýchlo opravené. Je to nevyhnutné, aby si súkromný a verejný sektor EÚ mohol vybrať spomedzi tých najbezpečnejších infraštruktúr a služieb. Nadchádzajúce desaťročie je pre EÚ príležitosťou viesť vývoj zabezpečených technológií v celom dodávateľskom reťazci. Na zaistenie odolnosti a posilnenie priemyselných a technologických kapacít kybernetickej bezpečnosti treba mobilizovať všetky potrebné regulačné, investičné a politické nástroje. Kybernetická bezpečnosť priemyselných procesov, operácií a zariadení už v štádiu návrhu môže zmierniť riziká, potenciálne znížiť náklady pre spoločnosti, ako aj pre širšiu spoločnosť, a tým posilniť odolnosť.

---

[32] Investície do celého dodávateľského reťazca digitálnych technológií, ktoré prispievajú k digitálnej transformácii alebo k riešeniu súvisiacich problémov, by mali predstavovať aspoň 20 % (t. j. 134,5 miliardy eur) grantovej a úverovej podpory z Mechanizmu na podporu obnovy a odolnosti vo výške 672,5 miliardy eur. Financovanie EÚ vo viacročnom finančnom rámci na roky 2021 – 2027 je pre kybernetickú bezpečnosť naplánované v rámci programu Digitálna Európa a pre výskum kybernetickej bezpečnosti v rámci programu Horizont Európa, s osobitným zameraním na podporu MSP, a celkovo by mohlo dosiahnuť 2 miliardy eur, plus investície členských štátov a priemyslu.

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

1.1. Odolná infraštruktúra a kritické služby

Základom jednotného trhu kybernetickej bezpečnosti sú **pravidlá EÚ v oblasti sieťovej a informačnej bezpečnosti (NIS)**. Komisia navrhuje reformovať tieto pravidlá v rámci revidovanej smernice NIS s cieľom posilniť **kybernetickú odolnosť všetkých relevantných sektorov (verejných aj súkromných), ktoré plnia dôležitú funkciu pre hospodárstvo a spoločnosť**[34]. Preskúmanie je potrebné na zmiernenie nezrovnalostí na vnútornom trhu zosúladením rozsahu pôsobnosti, požiadaviek na podávanie správ o zabezpečení a incidentoch, vnútroštátneho dohľadu a presadzovania, ako aj kapacít príslušných orgánov.

Reformovaná smernica NIS poskytne základ pre konkrétnejšie pravidlá, ktoré sú potrebné aj pre strategicky dôležité odvetvia vrátane energetiky, dopravy a zdravotníctva. V záujme jednotného prístupu avizovaného v Stratégii EÚ pre bezpečnostnú úniu na roky 2020 – 2025 sa reformovaná smernica navrhuje spolu s preskúmaním legislatívy o odolnosti kritickej infraštruktúry[35]. Energetické technológie s digitálnymi prvkami a zabezpečenie súvisiacich dodávateľských reťazcov sú dôležité pre kontinuitu základných služieb a strategickú kontrolu nad kritickou energetickou infraštruktúrou. Komisia preto navrhne opatrenia vrátane tzv. sieťového predpisu, v ktorom sa stanovia pravidlá kybernetickej bezpečnosti cezhraničných tokov elektriny, ktoré predloží na prijatie do konca roka 2022. Digitálnu prevádzkovú odolnosť treba posilniť aj vo finančnom sektore, aby odolal všetkým typom narušení a hrozieb súvisiacich s IKT, ako to Komisia už navrhla[36]. Pokiaľ ide o dopravu, Komisia doplnila ustanovenia o kybernetickej bezpečnosti[37] do legislatívy EÚ o bezpečnostnej ochrane letectva a bude pokračovať vo svojom úsilí o posilnenie kybernetickej odolnosti všetkých druhov dopravy. Posilnenie kybernetickej odolnosti **demokratických procesov a inštitúcií** je základnou zložkou akčného plánu pre európsku demokraciu, ktorý má chrániť a podporovať slobodné voľby, demokratickú diskusiu a pluralitu médií[38]. A pokiaľ ide o bezpečnosť infraštruktúry a služieb v rámci budúceho vesmírneho programu, Komisia bude pokračovať v prehlbovaní stratégie kybernetickej bezpečnosti systému Galileo pre ďalšiu generáciu služieb globálneho navigačného satelitného systému, ako aj ďalších nových zložiek vesmírneho programu[39].

1.2. Budovanie európskeho kybernetického štítu

Vo svete, kde je pripojiteľnosť na vzostupe a kybernetické útoky sú čoraz sofistikovanejšie, zohrávajú hodnotnú funkciu strediská pre výmenu a analýzu informácií (ISAC), a to aj na odvetvovej úrovni, keďže umožňujú výmenu informácií o kybernetických hrozbách medzi rôznymi zainteresovanými stranami[40]. Okrem toho si siete a počítačové systémy vyžadujú neustále monitorovanie a analýzu, aby sa narušenia a anomálie zistili v reálnom čase. Mnohé

---

34 [*Vložiť odkaz na návrh NIS*]

35 [vložiť odkaz na *návrh* smernice o odolnosti kritických subjektov].

36 Návrh nariadenia o digitálnej prevádzkovej odolnosti finančného sektora, ktorým sa menia nariadenia (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014 a (EÚ) č. 909/2014, COM(2020) 595 final.

37 Vykonávacie nariadenie Komisie (EÚ) 2019/1583.

38 Oznámenie o akčnom pláne pre európsku demokraciu, COM(2020) 790. Európska sieť pre spoluprácu v oblasti volieb a volebné siete členských štátov budú v rámci plánu podporovať nasadzovanie spoločných tímov expertov na boj proti hrozbám (vrátane kybernetických) vo volebných procesoch; https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en.

39 Patrí sem nová iniciatíva vládnej satelitnej komunikácie (GOVSATCOM) a riešenie vesmírneho odpadu (SST).

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

súkromné spoločnosti, verejné organizácie a vnútroštátne orgány preto zriadili jednotky pre riešenie počítačových bezpečnostných incidentov (CSIRT) a centrá bezpečnostných operácií (SOC).

Centrá bezpečnostných operácií sú kľúčové pri zhromažďovaní logových záznamov[41] a izolácii podozrivých udalostí v komunikačných sieťach, ktoré monitorujú. Využívajú na to identifikáciu signálov a vzorov a extrakciu poznatkov o hrozbách z veľkého množstva údajov, ktoré treba vyhodnotiť. Prispeli k odhaleniu aktivity škodlivých spustiteľných súborov a tým pomohli obmedziť kybernetické útoky. Práca potrebná v týchto centrách je veľmi náročná a dynamická, takže pre ich pracovníkov môže byť neoceniteľnou podporou umelá inteligencia, a najmä techniky strojového učenia[42].

Komisia navrhla vybudovať **celoúnijnú sieť centier bezpečnostných operácií[43]** a podporiť zdokonaľovanie existujúcich centier a zriaďovanie nových. Bude podporovať aj odbornú prípravu a rozvoj zručností zamestnancov zabezpečujúcich prevádzku týchto centier. Na základe analýzy potrieb v spolupráci s príslušnými zainteresovanými stranami a s podporou Agentúry EÚ pre kybernetickú bezpečnosť (ENISA) by sa mohlo na podporu verejno-súkromnej a cezhraničnej spolupráce pri vytváraní národných a sektorových sietí zahŕňajúcich aj MSP vyčleniť vyše 300 miliónov EUR, pričom táto spolupráca by vychádzala z primeraných ustanovení o riadení, zdieľaní údajov a zabezpečení.

Členské štáty sa vyzývajú, aby do tohto projektu investovali tiež. Centrá by potom mohli účinnejšie zdieľať a korelovať zachytené signály a produkovať kvalitné spravodajské informácie o hrozbách, ktoré by sa mali poskytovať strediskám ISAC a vnútroštátnym orgánom v záujme získania komplexnejšieho situačného povedomia. Cieľom by bolo postupne prepojiť čo najviac centier v celej EÚ, budovať kolektívne vedomosti a vymieňať si osvedčené postupy. Centrá budú mať k dispozícii podporu na zrýchlenie odhaľovania incidentov, ich analýzy a reakcie na ne vďaka najmodernejším kapacitám umelej inteligencie a strojového učenia, ktoré doplní superpočítačová infraštruktúra, ktorú v EÚ vyvíja spoločný podnik pre európsku vysokovýkonnú výpočtovú techniku[44].

Vďaka trvalej spolupráci bude táto sieť poskytovať včasné varovania o kybernetickobezpečnostných incidentoch orgánom a všetkým zainteresovaným stranám vrátane spoločnej kybernetickej jednotky (pozri oddiel 2.1). **Bude pre EÚ skutočným kybernetickobezpečnostným štítom** s hustou sieťou strážnych veží, ktorá dokáže odhaliť potenciálne hrozby skôr, než budú môcť spôsobiť rozsiahle škody.

1.3. Ultrabezpečná komunikačná infraštruktúra

Vládna satelitná komunikácia Európskej únie[45], ktorá spadá pod vesmírny program, poskytne zabezpečené a nákladovo efektívne vesmírne komunikačné kapacity pre misie a operácie

---

41 Tak, aby ich orgány presadzovania práva a súdnictva mohli použiť ako dôkazy.

42 Zdroj: prieskum organizácie Ponemon Institute, *Improving the Effectiveness of the SOC* (Zefektívňovanie centier SOC), 2019; pokiaľ ide o štúdie využívania umelej inteligencie v centrách bezpečnostných operácií, pozri napríklad: Khraisat, A., Gondal, I., Vamplew, P. *et al. Survey of intrusion detection systems: techniques, datasets and challenges* (Prieskum systémov detekcie narušenia: techniky, dátové súbory a výzvy), *Cybersecur* 2**,** 20 (2019).

43 Mechanizmy riadenia, prevádzkové zásady a financovanie týchto centier, ako aj spôsob ich zasadenia do existujúcich štruktúr, ako sú centrá digitálnych inovácií, sa rozpracujú podrobnejšie.

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

45 GOVSATCOM je komponentom vesmírneho programu Únie.

kritické pre bezpečnosť riadené EÚ a jej členskými štátmi vrátane národných bezpečnostných aktérov, inštitúcií, orgánov a agentúr EÚ.

Členské štáty sa zaviazali spolupracovať s Komisiou na zavádzaní zabezpečenej kvantovej komunikačnej infraštruktúry (QCI) pre Európu[46]. Tá poskytne orgánom verejnej moci úplne nový spôsob prenosu dôverných informácií s použitím ultrabezpečnej formy šifrovania na ochranu pred kybernetickými útokmi, ktorá je postavená na európskych technológiách. Bude mať dve hlavné zložky: existujúce pozemské optické komunikačné siete spájajúce strategické miesta na vnútroštátnej a cezhraničnej úrovni a prepojené vesmírne satelity pokrývajúce celú EÚ vrátane jej zámorských území[47]. Táto iniciatíva zameraná na vývoj a zavádzanie nových zabezpečenejších foriem šifrovania a na navrhnutie nových spôsobov ochrany kritických komunikačných a dátových prostriedkov môže pomôcť ochrániť citlivé informácie a následne aj kritické infraštruktúry.

V tomto kontexte Komisia zájde ešte ďalej a preskúma možné zavedenie systému multiorbitálneho zabezpečeného spojenia. Vychádzal by zo systémov GOVSATCOM a QCI, pričom by integroval najmodernejšie technológie (kvantum, 5G, umelá inteligencia, edge computing) vyhovujúce tomu najprísnejšiemu kybernetickobezpečnostnému rámcu s cieľom podporiť služby zabezpečené už v štádiu návrhu; ide napríklad o spoľahlivú, zabezpečenú a nákladovo efektívnu pripojiteľnosť a šifrovanú komunikáciu pre kritické vládne činnosti.

1.4. Zabezpečenie ďalšej generácie širokopásmových mobilných sietí

Občania a firmy v EÚ, ktoré využívajú pokročilé a inovačné aplikácie s podporou **5G a ďalších generácií sietí**, by mali mať k dispozícii ten najvyšší štandard zabezpečenia. Členské štáty spolu s Komisiou a s podporou agentúry ENISA zaviedli v súbore nástrojov EÚ pre 5G[48] z januára 2020 komplexný a objektívny prístup ku kybernetickej bezpečnosti 5G na báze rizík, ktorý vychádza z vyhodnocovania možných plánov zmierňovania rizík a identifikácie najúčinnejších opatrení. EÚ navyše konsoliduje svoje kapacity v oblasti 5G a ďalších generácií, aby nevznikali závislosti a budoval sa udržateľný a diverzifikovaný dodávateľský reťazec.

Komisia v decembri 2020 uverejnila správu o vplyve odporúčania z 26. marca 2019 na kybernetickú bezpečnosť sietí 5G[49]. Ukázalo sa, že od schválenia súboru nástrojov došlo k veľkému pokroku a väčšine členských štátov sa podarí v blízkej budúcnosti zaviesť jeho

---

46 Deklaráciu EuroQCI už podpísala väčšina členských štátov, pričom rozvoj a zavádzanie infraštruktúry má prebehnúť v rokoch 2021 – 2027 s financovaním z programov Horizont Európa a Digitálna Európa, ako aj od Európskej vesmírnej agentúry, a predpokladom sú vhodné mechanizmy riadenia; https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network.

47 Rozvoj vesmírnej zložky je potrebný na dosiahnutie diaľkových prepojení typu bod – bod (> 1 000 km), ktoré pozemná infraštruktúra neumožňuje. Využitím vlastností kvantovej mechaniky QCI najskôr umožní stranám zabezpečenú výmenu náhodných tajných kľúčov, ktoré sa použijú na šifrovanie a dešifrovanie správ. Takisto bude zahŕňať zavedenie infraštruktúry na testovanie a overovanie súladu, ktorá bude vyhodnocovať súlad európskych kvantových komunikačných zariadení a systémov s infraštruktúrou QCI, ich certifikáciu a validáciu pred integrovaním do QCI. Bude navrhnutá tak, aby podporovala aj ďalšie nové aplikácie, ktoré dosiahnu potrebnú úroveň technologickej vyspelosti. Predchodcom tejto infraštruktúry na testovanie a overovanie súladu je v súčasnosti pilotný projekt OpenQKD (https://openqkd.eu/).

48 Oznámenie Komisie o bezpečnom zavádzaní 5G v EÚ – Vykonávanie súboru nástrojov, COM(2020) 50.

49 Správa Komisie o vplyve odporúčania Komisie z 26. marca 2019 na kybernetickú bezpečnosť sietí 5G, 15. december 2020.

podstatnú časť, aj keď v správe o pokroku z júla 2020[50] už sa identifikovali určité rozdiely a pretrvávajúce nedostatky.

V októbri 2020 Európska rada vyzvala EÚ a členské štáty, aby „v plnej miere využívali súbor nástrojov EÚ pre kybernetickú bezpečnosť 5G“ a aby „uplatňovali príslušné obmedzenia týkajúce sa vysokorizikových dodávateľov v prípade kľúčových aktív, ktoré sú v koordinovaných posúdeniach rizík EÚ vymedzené ako kritické a citlivé [...] na základe spoločných a objektívnych kritérií“[51].

EÚ a jej členské štáty by mali výhľadovo zabezpečiť, aby sa primerane a koordinovane zmiernili zistené riziká, najmä pokiaľ ide o cieľ minimalizovať vystavenie vysokorizikovým dodávateľom a zabrániť závislosti od týchto dodávateľov na vnútroštátnej aj únijnej úrovni, pričom sa musí zohľadniť akýkoľvek nový významný vývoj alebo riziko. Členské štáty sa vyzývajú, aby pri svojich investíciách do digitálnych kapacít a pripojiteľnosti súbor nástrojov plne využili.

Na základe správy o vplyvoch odporúčania z roku 2019 Komisia nabáda členské štáty, aby urýchlili prácu na zavedení hlavných opatrení súboru do druhého štvrťroka 2021. Zároveň ich vyzýva, aby naďalej spoločne monitorovali dosiahnutý pokrok a zabezpečovali ďalšie zosúlaďovanie prístupov. Na podporu tohto procesu sa na úrovni EÚ budú sledovať tri hlavné ciele: zaisťovanie ďalšej konvergencie prístupov k zmierňovaniu rizík v EÚ, podpora nepretržitej výmeny znalostí a budovania kapacít a podpora odolnosti dodávateľských reťazcov a ďalších strategických cieľov EÚ v oblasti bezpečnosti. Konkrétne opatrenia súvisiace s týmito kľúčovými cieľmi sú uvedené v osobitnom dodatku k tomuto oznámeniu.

Komisia bude naďalej úzko spolupracovať s členskými štátmi na plnení týchto cieľov a opatrení s podporou agentúry ENISA (pozri prílohu).

Prístup EÚ vychádzajúci zo súboru nástrojov pre 5G navyše vzbudil záujem krajín mimo EÚ, ktoré v súčasnosti rozvíjajú svoje prístupy k zabezpečeniu komunikačných sietí. Útvary Komisie sú spolu s Európskou službou pre vonkajšiu činnosť a sieťou delegácií EÚ pripravené na požiadanie poskytnúť orgánom na celom svete ďalšie informácie o jej komplexnom a objektívnom prístupe založenom na rizikách.

1.5. Internet zabezpečených vecí

Každé pripojené zariadenie má slabiny, ktoré sa dajú zneužiť s potenciálne rozsiahlymi dôsledkami. Pravidlá vnútorného trhu zahŕňajú ochranné opatrenia proti nezabezpečeným výrobkom a službám. Komisia už pracuje na **transparentných bezpečnostných riešeniach a certifikácii v rámci aktu o kybernetickej bezpečnosti**, ako aj na stimulovaní bezpečných produktov a služieb bez oslabovania funkčnosti[52]. V prvom štvrťroku 2021 prijme prvý

---

[50] Správa skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti o vykonávaní súboru nástrojov, 24. júl 2020.

[51] EUCO 13/20, mimoriadne zasadnutie Európskej rady (1. a 2. október 2020) – závery.

[52] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti). Aktom o kybernetickej bezpečnosti sa podporuje certifikácia IKT na úrovni EÚ; zahŕňa európsky rámec certifikácie kybernetickej bezpečnosti na zriaďovanie dobrovoľných európskych systémov certifikácie kybernetickej bezpečnosti s cieľom zabezpečiť primeranú úroveň kybernetickej bezpečnosti produktov, služieb a procesov IKT v Únii, ako aj zmierniť fragmentáciu vnútorného trhu, pokiaľ ide o systémy certifikácie kybernetickej bezpečnosti v Únii. Spoločnosti zaoberajúce sa „ratingom“ kybernetickej

priebežný pracovný program Únie (ktorý sa má aktualizovať aspoň raz za tri roky), aby sa priemysel, vnútroštátne a normalizačné orgány mohli vopred pripraviť na budúce európske systémy certifikácie kybernetickej bezpečnosti[53]. Internet vecí je v rozmachu a treba posilniť presaditeľné pravidlá – tak v záujme celkovej odolnosti, ako aj kybernetickej bezpečnosti.

Komisia zváži komplexný prístup vrátane možných **nových horizontálnych pravidiel na posilnenie kybernetickej bezpečnosti všetkých pripojených produktov a súvisiacich služieb umiestnených na vnútornom trhu**[54]. Takéto pravidlá by mohli zahŕňať **novú povinnosť náležitej starostlivosti výrobcov pripojených zariadení** na riešenie softvérových slabín vrátane kontinuálnych softvérových a bezpečnostných aktualizácií, ale aj na zaistenie toho, aby sa na konci životnosti vymazali všetky osobné a iné citlivé údaje. Tieto pravidlá by posilnili iniciatívu „práva na opravu zastaraného softvéru“ predstavenú v akčnom pláne EÚ pre obehové hospodárstvo, a zároveň by doplnili prebiehajúce opatrenia zamerané na osobitné druhy produktov, ako napríklad povinné požiadavky, ktoré sa majú navrhnúť pre prístup určitých bezdrôtových výrobkov na trh (formou delegovaného aktu na základe smernice o rádiových zariadeniach[55]), alebo cieľ zaviesť kybernetickobezpečnostné pravidlá pre všetky nové typy motorových vozidiel od júla 2022[56]. Okrem toho by vychádzali z navrhovanej revízie pravidiel všeobecnej bezpečnosti výrobkov, ktoré sa priamo netýkajú aspektov kybernetickej bezpečnosti[57].

1.6. Lepšie globálne zabezpečenie internetu

Funkčnosť a integritu internetu na celom svete zabezpečuje súbor základných protokolov a podpornej infraštruktúry[58]. Ten zahŕňa systém doménových mien (DNS) a jeho hierarchický a delegovaný systém zón, počnúc koreňovou zónou na vrchole hierarchie a trinástimi koreňovými servermi DNS[59], od ktorých závisí World Wide Web. Komisia má v úmysle vypracovať **s podporou financovania EÚ pohotovostný plán na riešenie extrémnych scenárov ovplyvňujúcich integritu a dostupnosť globálneho koreňového systému DNS**. Bude spolupracovať s agentúrou ENISA, členskými štátmi, oboma prevádzkovateľmi koreňových serverov DNS v EÚ[60] a s komunitou rôznych zainteresovaných strán, aby

---

bezpečnosti majú zároveň zvyčajne sídlo mimo EÚ, takže transparentnosť a dohľad sú obmedzené; https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings.

53 Vyžaduje sa v článku 47 ods. 5 aktu o kybernetickej bezpečnosti.

54 V záveroch Rady sa vyzýva na prijatie horizontálnych opatrení v oblasti kybernetickej bezpečnosti pripojených zariadení; 13629/20, 2. december 2020.

55 Smernica 2014/53/EÚ.

56 Riadi sa predpisom EHK OSN z júna 2020; http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf.

57 Revízia súčasných pravidiel všeobecnej bezpečnosti výrobkov (smernica 2001/95/ES); plánuje sa aj návrh úpravy pravidiel zodpovednosti výrobcov v digitálnom kontexte v rámci regulačného rámca EÚ týkajúceho sa zodpovednosti.

58 „Verejným jadrom otvoreného internetu, najmä jeho hlavnými protokolmi a infraštruktúrou, ktoré sú celosvetovým verejným statkom, sa zabezpečuje základná funkčnosť internetu ako celku a jeho bežná prevádzka. Agentúra ENISA by mala podporovať bezpečnosť verejného jadra otvoreného internetu a stabilitu jeho fungovania vrátane napríklad kľúčových protokolov (najmä DNS, BGP a IPv6), prevádzky systému názvov domén (napríklad prevádzky všetkých domén najvyššej úrovne) a prevádzky koreňovej zóny.“ Odôvodnenie 23 aktu o kybernetickej bezpečnosti.

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

60 Servery i.root prevádzkované organizáciou Netnod vo Švédsku a servery k.root prevádzkované organizáciou RIPE NCC v Holandsku.

vyhodnotili rolu týchto prevádzkovateľov pri zaručovaní trvalej globálnej prístupnosti internetu za každých okolností.

Aby mal klient prístup k zdroju pod konkrétnym doménovým menom na internete, jeho požiadavka (zvyčajne o jednotnú adresu zdroja – URL) sa musí „preložiť“ na IP adresu s odkazom na servery DNS. Ľudia a organizácie v EÚ však čoraz intenzívnejšie využívajú niekoľko málo verejných resolverov („prekladačov“) DNS prevádzkovaných subjektmi mimo EÚ. Takáto konsolidácia prekladania DNS v rukách malého počtu spoločností[61] znamená, že samotný proces prekladania je zraniteľný voči závažným udalostiam, ak postihnú jedného veľkého poskytovateľa, a sťažuje orgánom EÚ zásah v prípade zlovoľných kybernetických útokov a veľkých geopolitických a technických incidentov[62].

Na zmiernenie bezpečnostných problémov spojených s koncentráciou trhu bude Komisia nabádať príslušné zainteresované strany vrátane spoločností EÚ, poskytovateľov internetových služieb a predajcov prehliadačov, aby prijali stratégiu diverzifikácie prekladu DNS. Komisia zároveň plánuje prispieť k zabezpečeniu internetového pripojenia podporou rozvoja verejnej **európskej služby prekladu DNS**. Táto iniciatíva DNS4EU ponúkne alternatívnu európsku službu prístupu k svetovému internetu. DNS4EU bude transparentná, bude v súlade s najnovšími normami a pravidlami integrovaného zabezpečenia, ochrany údajov a súkromia už v štádiu návrhu a bude súčasťou Európskej priemyselnej aliancie pre dáta a cloud[63].

Komisia takisto v spolupráci s členskými štátmi a priemyslom **urýchli zavádzanie kľúčových internetových noriem vrátane IPv6**[64] **a etablovaných noriem internetového zabezpečenia a osvedčených postupov pre DNS, smerovanie a zabezpečenie elektronickej pošty**[65], pričom na usmernenie trhu nevylučuje regulačné opatrenia, ako je európska doložka o ukončení platnosti IPv4, ak by sa nedosiahol dostatočný pokrok v ich zavádzaní. EÚ by mala presadzovať (ako napríklad v rámci stratégie EÚ – Afrika[66]) uplatňovanie týchto noriem v partnerských krajinách na podporu rozvoja globálneho a otvoreného internetu a predchádzanie uzavretým modelom internetu založeným na kontrole. Komisia napokon zváži potrebu mechanizmu na systematickejšie monitorovanie a zhromažďovanie súhrnných údajov o objeme dátových prenosov na internete a na konzultácie v prípade narušení[67].

---

61 *Consolidation in the DNS resolver market – how much, how fast how dangerous?* (Konsolidácia na trhu resolverov DNS – koľko, ako rýchlo a aké je to nebezpečné?) *Evidence of decreasing Internet entropy – the lack of redundancy in DNS resolution by major websites and services* (Dôkazy o klesajúcej internetovej entropii – nedostatok záložných možností prekladu DNS hlavnými webovými sídlami a službami).

62 Existujú aj dôkazy o tom, že údaje DNS možno použiť na profilovanie, čo zasahuje do práva na súkromie a ochranu údajov.

63 Spoločné vyhlásenie: Budovanie cloudu budúcej generácie pre podniky a verejný sektor v EÚ; https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe.

64 Zavádzanie IPv6 už je v pokročilejšej fáze, keďže adresy IPv4 sú značne vyčerpané a nákladnejšie. Zavádzanie IPv6 je však v rámci EÚ nerovnomerné.

65 Medzi takéto normy patria DNSSEC, HTTPS, DNS over HTTPS (DoH), DNS over TLS (DoT), SPF, DKIM, DMARC, STARTTLS, DANE, ako aj smerovacie normy a osvedčené postupy, napr. spoločne dohodnuté normy pre bezpečnosť smerovania (MANRS).

66 Spoločné oznámenie Na ceste ku komplexnej stratégii pre Afriku, JOIN(2020) 4 final z 9. marca 2020.

67 Takéto „internetové monitorovacie stredisko“ by mohlo spadať do rozsahu činností Európskeho centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti; Návrh nariadenia, ktorým sa zriaďuje Európske centrum odvetvových, technologických a výskumných

1.7. Posilnená prítomnosť v technologickom dodávateľskom reťazci

EÚ má vďaka plánovanej finančnej podpore kyberneticky zabezpečenej digitálnej transformácie v rámci viacročného finančného rámca na roky 2021 – 2027 jedinečnú príležitosť zlúčiť svoje zdroje na podporu priemyselnej stratégie[68] a vedúceho postavenia na poli digitálnych technológií a kybernetickej bezpečnosti v celom digitálnom dodávateľskom reťazci (vrátane údajov a cloudu, technológií procesorov novej generácie, ultrabezpečnej pripojiteľnosti a sietí 6G) v súlade so svojimi hodnotami a prioritami. Intervencia verejného sektora by sa mala opierať o nástroje, ktoré poskytuje regulačný rámec EÚ pre verejné obstarávanie a dôležité projekty spoločného európskeho záujmu. Okrem toho možno mobilizovať súkromné investície formou verejno-súkromných partnerstiev (vrátane využitia skúseností so zmluvným verejno-súkromným partnerstvom v oblasti kybernetickej bezpečnosti a jeho vykonávaním v rámci Európskej organizácie kybernetickej bezpečnosti), rizikového kapitálu na podporu MSP alebo odvetvových aliancií, ako aj stratégií v oblasti technologických kapacít.

Osobitný dôraz sa bude klásť aj na Nástroj technickej podpory[69] a optimálne využitie najnovších kybernetickobezpečnostných nástrojov zo strany MSP – najmä tých, ktoré nespadajú do rozsahu pôsobnosti revidovanej smernice NIS, a to aj prostredníctvom cielených činností centier digitálnych inovácií v rámci programu Digitálna Európa. Cieľom je vyvolať podobný objem investícií zo strany členských štátov a priemyslu v rámci partnerstva riadeného spoločne s členskými štátmi v rámci navrhovaného **centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a siete národných koordinačných centier (CCCN)**. CCCN by malo s podporou priemyslu a akademickej obce zohrávať kľúčovú úlohu pri rozvoji technologickej suverenity EÚ v oblasti kybernetickej bezpečnosti, budovaní kapacít na zabezpečenie citlivých infraštruktúr, ako je 5G, a znižovaní závislosti od kľúčových technológií z iných častí sveta.

Komisia plánuje (prípadne spoločne s CCCN) podporiť rozvoj špecializovaného magisterského programu v oblasti kybernetickej bezpečnosti a prispieť k spoločnému európskemu plánu výskumu a inovácií v oblasti kybernetickej bezpečnosti po roku 2020. Investície smerované cez CCCN by nadväzovali aj na spoluprácu vo výskume a vývoji medzi sieťami centier kybernetickobezpečnostnej excelentnosti, ktorá združuje najlepšie európske výskumné tímy s priemyslom pri návrhu a realizácii spoločných výskumných programov v súlade s plánom Európskej organizácie kybernetickej bezpečnosti[70]. Komisia bude pokračovať vo využívaní výskumu agentúry ENISA a Europolu a v rámci programu Horizont Európa bude naďalej podporovať jednotlivých internetových inovátorov, ktorí vyvíjajú technológie na posilnenie ochrany súkromia a zabezpečenie komunikácie založené na softvéri a hardvéri s otvoreným zdrojovým kódom, ako je to v súčasnosti v rámci iniciatívy Internet ďalšej generácie.

1.8. Kvalifikovaní kybernetickí experti v EÚ

Dôležitou súčasťou ochrany pred kybernetickými hrozbami vo všeobecnosti je snaha EÚ o zvýšenie kvalifikácie pracovnej sily, rozvoj, prilákanie a udržanie najlepších

---

kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier, COM(2018) 630 final.

68 Oznámenie o Novej priemyselnej stratégii pre Európu, COM(2020) 102 final.

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

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

kybernetickobezpečnostných talentov a investovanie do výskumu a inovácie svetovej triedy. Táto oblasť má veľký potenciál. Preto treba venovať osobitnú pozornosť rozvoju, prilákaniu a udržaniu rozmanitejších talentov. Revidovaný akčný plán digitálneho vzdelávania zvýši kybernetickobezpečnostné povedomie ľudí (najmä detí a mládeže) aj organizácií (najmä MSP)[71]. Zároveň podporí účasť žien na vzdelávaní v odboroch vedy, technológie, inžinierstva a matematiky (STEM), ako aj na zvyšovaní kvalifikácie na pozície v IKT a rekvalifikácii zahŕňajúcej digitálne zručnosti. Komisia navyše spolu s Úradom EÚ pre duševné vlastníctvo pri Europole, agentúrou ENISA, členskými štátmi a súkromným sektorom vypracuje nástroje na zvyšovanie informovanosti a usmernenia na zvýšenie odolnosti podnikov EÚ **voči kybernetickým krádežiam duševného vlastníctva**[72].

Vzdelávanie – vrátane odborného vzdelávania a prípravy (OVP), informovanosti a cvičení – by zároveň malo ďalej zvyšovať zručnosti v oblasti kybernetickej bezpečnosti a obrany na úrovni EÚ. Na tento účel by sa príslušní aktéri EÚ ako ENISA, Európska obranná agentúra (EDA), Európska akadémia bezpečnosti a obrany (EABO)[73] mali usilovať o vzájomné synergie činností.

Strategické iniciatívy

EÚ by mala zabezpečiť:

- prijatie revidovanej smernice NIS,
- regulačné opatrenia v záujme internetu zabezpečených vecí,
- prostredníctvom CCCN investície do kybernetickej bezpečnosti (najmä z programov Digitálna Európa a Horizont Európa a z mechanizmu obnovy), pričom verejné a súkromné investície by v rokoch 2021 – 2027 mali dosiahnuť až 4,5 miliardy eur,
- celoúnijnú sieť centier bezpečnostných operácií s kapacitami umelej inteligencie a ultrazabezpečenú komunikačnú infraštruktúru s využitím kvantových technológií,
- plošné zavádzanie kybernetickobezpečnostných technológií vďaka cielenej podpore MSP v rámci centier digitálnych inovácií,
- rozvoj služby EÚ na preklad DNS ako bezpečnej a otvorenej alternatívnej možnosti prístupu na internet pre občanov, podniky a verejné správy EÚ a
- dokončenie vykonávania súboru nástrojov 5G do druhého štvrťroka 2021 (pozri prílohu).

2. BUDOVANIE OPERAČNEJ KAPACITY NA PREVENCIU, ODRÁDZANIE A REAKCIU

Či už sú kybernetické incidenty dielom náhody alebo ide o úmyselné konanie zločincov, štátov a iných, neštátnych subjektov, môžu spôsobiť obrovské škody. Ich rozsah a zložitosť často zahŕňa zneužitie služieb, hardvéru a softvéru tretích strán na zasiahnutie konečného cieľa, takže bez systematickej a komplexnej výmeny informácií a spolupráce na spoločnej

[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_sk.
[72] https://ec.europa.eu/commission/presscorner/detail/sk/IP_20_2187.
[73] Na platforme pre vzdelávanie, odbornú prípravu, hodnotenie a cvičenia v kybernetickej oblasti (ETEE).

reakcii je kolektívne riešenie prostredia hrozieb v EÚ ťažké. EÚ chce **úplným vykonaním regulačných nástrojov, mobilizáciou a spoluprácou** podporovať členské štáty pri obrane svojich občanov, hospodárskych záujmov a záujmov národnej bezpečnosti pri plnom dodržiavaní základných práv, slobôd a právneho štátu. Za prevenciu, odrádzanie a reakciu na kybernetické hrozby nesie zodpovednosť niekoľko komunít, ktoré sa skladajú zo sietí, z inštitúcií, orgánov a agentúr EÚ, ako aj orgánov členských štátov a využívajú príslušné nástroje a iniciatívy[74]. Medzi tieto komunity patria: i) orgány NIS, ako sú jednotky CSIRT a útvary reakcie na katastrofy; ii) orgány presadzovania práva a justičné orgány; iii) kybernetická diplomacia a iv) kybernetická obrana.

2.1. Spoločná kybernetická jednotka

Spoločná kybernetická jednotka by slúžila ako virtuálna aj fyzická platforma spolupráce jednotlivých kybernetickobezpečnostných komunít v EÚ so zameraním na operačnú a technickú koordináciu v boji proti veľkým cezhraničným kybernetickým incidentom a hrozbám.

Spoločná kybernetická jednotka by bola dôležitým krokom k dokončeniu **európskeho rámca krízového riadenia kybernetickej bezpečnosti**. Jednotka vychádza z politických usmernení predsedníčky Komisie[75] a mala by členským štátom a inštitúciám, orgánom a agentúram EÚ umožniť plnohodnotné využívanie existujúcich štruktúr, zdrojov a kapacít a podporovať mentálne nastavenie „**potreby zdieľania**“ (need to share). Poskytla by prostriedky na konsolidáciu doterajšieho pokroku vo vykonávaní odporúčania z roku 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (ďalej len „koncepcia“)[76]. Takisto by bola príležitosťou na ďalšie posilnenie spolupráce na architektúre koncepcie a využitie dosiahnutého pokroku najmä v rámci skupiny pre spoluprácu v sieťovej a informačnej bezpečnosti a siete CyCLONe.

Tým by sa dali vyriešiť **dva hlavné nedostatky**, ktoré v súčasnosti zvyšujú zraniteľnosť a znižujú efektívnosť reakcie na cezhraničné hrozby a incidenty, ktoré postihujú Úniu. Po prvé, civilné a diplomatické kruhy, orgány presadzovania práva a obranné kybernetickobezpečnostné **komunity** zatiaľ nemajú spoločný priestor na podporu štruktúrovanej operačnej a technickej spolupráce. Po druhé, príslušní kybernetickobezpečnostní aktéri zatiaľ nemali príležitosť naplno využiť **potenciál** operačnej spolupráce a vzájomnej pomoci v rámci existujúcich sietí a komunít. Sem spadá aj absencia platformy, ktorá by umožňovala operačnú spoluprácu so súkromným sektorom. Jednotka by mala zlepšiť a urýchliť koordináciu a umožniť EÚ postaviť sa a čeliť rozsiahlym kybernetickým incidentom a krízam.

---

[74] Sem patrí podpora operačnej spolupráce a krízového riadenia zo strany Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA); sieť jednotiek CSIRT; organizačná sieť kontaktných miest pre kybernetické krízy (CyCLONe, má sa podľa revidovanej smernice NIS premenovať na EU-CyCLONe); skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti; „rescEU“; Európske centrum boja proti počítačovej kriminalite a spoločná pracovná skupina Europolu pre boj proti počítačovej kriminalite a protokol o reakcii na núdzové situácie v rámci presadzovania práva; Spravodajské a situačné centrum EÚ (EU INTCEN) a súbor nástrojov kybernetickej diplomacie; jednotná kapacita na analýzu spravodajských informácií (SIAC); kybernetické projekty v rámci stálej štruktúrovanej spolupráce (PESCO), najmä „tímy rýchlej kybernetickej reakcie a vzájomná pomoc v oblasti kybernetickej bezpečnosti“ (CRRT).

[75] Ambicióznejšia Únia – Môj plán pre Európu, Politické usmernenia pre budúcu Európsku komisiu (2019 – 2024) kandidátky na predsedníčku Európskej komisie Ursuly von der Leyen.

[76] Koncepčné odporúčanie C(2017) 6100 final z 13. 9. 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu.

Spoločná kybernetická jednotka by nebola ďalším samostatným orgánom, ani by nezasahovala do právomocí vnútroštátnych kybernetickobezpečnostných orgánov či aktérov na úrovni EÚ. Skôr by bola zabezpečovacím mechanizmom, v ktorom by účastníci mohli využívať vzájomnú podporu a expertízu, najmä v prípadoch, kde sa vyžaduje úzka spolupráca rôznych kybernetických komunít. Najnovšie dianie zároveň ukazuje, že EÚ musí posilniť svoje ambície a pripravenosť čeliť panoráme a realite kybernetických hrozieb. Aktéri EÚ (Komisia a agentúry a orgány EÚ) budú preto v rámci svojho príspevku do spoločnej kybernetickej jednotky pripravení výrazne navýšiť svoje zdroje a kapacity v záujme posilnenia pripravenosti a odolnosti.

Spoločná kybernetická jednotka by sledovala tri hlavné ciele. Po prvé, zabezpečovala by **pripravenosť** všetkých kybernetickobezpečnostných komunít, po druhé, výmenou informácií by poskytovala nepretržité spoločné situačné **povedomie** a po tretie by posilňovala koordinovanú **reakciu** a obnovu. Na dosiahnutie týchto cieľov by jednotka mala vychádzať z dobre vymedzených **blokov a čiastkových cieľov** – napríklad zaručenie **zabezpečenej a rýchlej výmeny informácií**, zlepšovanie **spolupráce** účastníkov (vrátane interakcie medzi členskými štátmi a príslušnými subjektmi na úrovni EÚ), vytváranie štruktúrovaných **partnerstiev s dôveryhodnou odvetvovou** základňou a podpora koordinovaného prístupu k **spolupráci s externými partnermi**. Na to by jednotka mohla na základe mapovania dostupných kapacít na vnútroštátnej a únijnej úrovni podporiť rozvoj rámca spolupráce.

Aby sa spoločná kybernetická jednotka stala stredobodom operačnej spolupráce EÚ v oblasti kybernetickej bezpečnosti, Komisia bude spolupracovať s členskými štátmi a príslušnými inštitúciami, orgánmi a agentúrami EÚ vrátane agentúry ENISA, tímu CERT-EU a Europolu na presadzovaní **inkrementálneho a inkluzívneho prístupu**, ktorý bude plne rešpektovať právomoci a mandáty všetkých zúčastnených aktérov. V súlade s týmto prístupom by jednotka mohla prispieť k ďalšej spolupráci medzi zložkami konkrétnej kybernetickej komunity tam, kde to považujú za potrebné.

Na vytvorenie spoločnej kybernetickej jednotky sa navrhujú štyri hlavné kroky:

- *vymedzenie* zmapovaním dostupných kapacít na vnútroštátnej a únijnej úrovni,
- *príprava* vytvorením rámca štruktúrovanej spolupráce a pomoci,
- *zavedenie* implementáciou tohto rámca s využitím zdrojov poskytnutých účastníkmi tak, aby sa spoločná kybernetická jednotka stala prevádzkyschopnou,
- *rozšírenie* posilnením koordinovanej schopnosti reakcie za pomoci priemyslu a partnerov.

Na základe výsledkov konzultácií s členskými štátmi, inštitúciami, orgánmi a agentúrami EÚ[77] Komisia za účasti vysokého predstaviteľa a v súlade s jeho právomocami do februára 2021 predstaví proces, míľniky a harmonogram **vymedzenia, prípravy, zavedenia a rozšírenia spoločnej kybernetickej jednotky**.

[77] Konzultácie s členskými štátmi (aj počas cvičenia Blue OLEx20, kde sa zišli vedúci predstavitelia vnútroštátnych kybernetickobezpečnostných orgánov), inštitúciami, orgánmi a agentúrami EÚ prebehli v období od júla do novembra 2020.

2.2. *Boj proti počítačovej kriminalite*

Naša závislosť od online nástrojov exponenciálne zvýšila plochu útoku dostupnú počítačovým kriminálnikom a viedla k situácii, keď vyšetrovanie takmer všetkých druhov trestnej činnosti zahŕňa digitálnu zložku. Okrem toho sú kľúčové časti našej spoločnosti ohrozované kybernetickými aktérmi a tými, ktorí využívajú kybernetické nástroje na plánovanie a realizáciu nezákonnej činnosti. Preto existuje úzke prepojenie s celkovou bezpečnostnou politikou EÚ, ktoré sa odráža v kybernetických prvkoch jej Stratégie pre bezpečnostnú úniu z roku 2020 a v jej programe boja proti terorizmu[78].

Účinný boj proti počítačovej kriminalite je kľúčovým faktorom kybernetickej bezpečnosti: odrádzajúci účinok nemožno dosiahnuť len odolnosťou – vyžaduje si aj identifikáciu a stíhanie páchateľov. Preto je nevyhnutné posilniť spoluprácu a výmenu medzi kybernetickobezpečnostnými aktérmi a orgánmi presadzovania práva. Na úrovni EÚ preto Europol a ENISA už nadviazali úzku spoluprácu, v rámci ktorej organizovali spoločné konferencie a semináre a Komisii, členským štátom a iným zainteresovaným stranám predložili spoločné správy o kybernetickobezpečnostných hrozbách a technologických výzvach. Komisia bude tento integrovaný prístup naďalej podporovať s cieľom zabezpečiť koherentnú a účinnú reakciu na základe komplexného prehľadu informácií.

Ako jeden z dôležitých prvkov tejto reakcie musia orgány EÚ a vnútroštátne orgány rozšíriť a zlepšiť možnosti orgánov presadzovania práva vyšetrovať počítačovú kriminalitu, pričom treba plne rešpektovať základné práva a usilovať sa o požadovanú rovnováhu medzi rôznymi právami a záujmami. EÚ by mala byť schopná bojovať proti počítačovej kriminalite plne uplatňovanou legislatívou, ktorá je primeraná svojmu účelu, s osobitným dôrazom na boj proti sexuálnemu zneužívaniu detí online a na digitálne vyšetrovanie vrátane trestnej činnosti na tzv. darknete. Orgány presadzovania práva musia byť na digitálne vyšetrovanie plne vybavené. Komisia preto predloží akčný plán na zlepšenie digitálnej kapacity orgánov presadzovania práva tým, že im poskytne potrebné zručnosti a nástroje. Europol bude okrem toho ďalej rozvíjať svoju rolu centra expertízy na podporu vnútroštátnych orgánov presadzovania práva v boji proti trestnej činnosti umožnenej počítačom a trestnej činnosti závislej od počítača, pričom prispeje k vymedzeniu spoločných forenzných noriem (prostredníctvom inovačného laboratória a centra Europolu). Všetky tieto činnosti si vyžadujú primerané využitie v členských štátoch, ktoré by mali využiť národné programy Fondu pre vnútornú bezpečnosť a navrhnúť projekty v rámci výziev na predkladanie návrhov spadajúcich pod príslušný tematický nástroj.

Komisia využije všetky vhodné prostriedky vrátane konaní o nesplnení povinnosti, aby zabezpečila úplnú transpozíciu a vykonávanie smernice z roku 2013 o útokoch na informačné systémy[79] vrátane poskytovania štatistík členskými štátmi. Bude lepšie brániť zneužívaniu doménových mien (vrátane prípadného šírenia nezákonného obsahu) a presadzovať sprístupňovanie presných registračných údajov, a to pokračujúcou spoluprácou s Internetovou korporáciou pre prideľovanie mien a čísel (ICANN) a ďalšími zainteresovanými stranami v systéme správy internetu, najmä prostredníctvom pracovnej skupiny pre verejnú bezpečnosť v rámci vládneho poradného výboru ICANN. V návrhu revidovanej smernice NIS sa preto predpokladá udržiavanie presných a úplných databáz doménových mien a registračných

[78] Oznámenie o programe EÚ v oblasti boja proti terorizmu: predvídať, predchádzať, chrániť a reagovať; 9. 12. 2020, COM(2020) 795 final.

[79] Smernica 2013/40/EÚ o útokoch na informačné systémy.

údajov (tzv. údajov WHOIS) a poskytovanie zákonného prístupu k takýmto údajom, čo je nevyhnutné na zaistenie bezpečnosti, stability a odolnosti DNS.

Komisia bude okrem toho aj naďalej pracovať na zabezpečení vhodných kanálov a objasnení pravidiel na získanie cezhraničného prístupu k elektronickým dôkazom na účely vyšetrovania trestných činov (potreba v 85 % vyšetrovaní, pričom 65 % celkového objemu žiadostí je adresovaných poskytovateľom so sídlom v inej jurisdikcii), a to podporou prijatia a následného vykonávania „balíka predpisov o elektronických dôkazoch“ a praktických opatrení[80]. Urýchlené prijatie návrhov o elektronických dôkazoch Európskym parlamentom a Radou je kľúčové, aby mali pracovníci v tejto oblasti účinný nástroj. Elektronické dôkazy musia byť čitateľné, takže Komisia bude ďalej pracovať na podpore kapacít presadzovania práva v oblasti digitálnych vyšetrovaní vrátane otázok šifrovania, ak sa naň pri vyšetrovaní trestných činov narazí, pričom plne zachová svoju funkciu chrániť základné práva a kybernetickú bezpečnosť.

2.3. Súbor nástrojov kybernetickej diplomacie EÚ

EÚ využíva svoj **súbor nástrojov kybernetickej diplomacie**[81] na prevenciu škodlivých kybernetických činností, odrádzanie od nich a reakciu na ne. Po zavedení právneho rámca cielených reštriktívnych opatrení proti kybernetickým útokom v máji 2019[82] EÚ v júli 2020 zostavila zoznam šiestich fyzických osôb a troch subjektov, ktoré boli zodpovedné za kybernetické útoky postihujúce EÚ a jej členské štáty alebo do nich boli zapojené[83]. Ďalšie dve fyzické osoby a jeden orgán boli do zoznamu zaradené v októbri 2020[84]. Škodlivé kybernetické činnosti vrátane tých „pomaly kvasiacich“ by sa mali riešiť účinnou, komplexnou a jednotnou diplomatickou reakciou EÚ s využitím všetkých druhov opatrení dostupných na úrovni EÚ.

Rýchla a účinná spoločná diplomatická reakcia EÚ si vyžaduje spoľahlivé spoločné situačné povedomie a schopnosť rýchlo pripraviť spoločnú pozíciu EÚ. Vysoký predstaviteľ Únie pre zahraničné veci a bezpečnostnú politiku bude podporovať a presadzovať zriadenie **pracovnej skupiny členských štátov EÚ pre kybernetické spravodajstvo** v rámci Spravodajského a

---

80 COM(2018) 225 a 226; C(2020) 2779 final. Konkrétne projekt SIRIUS nedávno získal dodatočné financovanie z nástroja partnerstva na zdokonalenie kanálov získavania zákonného cezhraničného prístupu k elektronickým dôkazom na účely vyšetrovania trestných činov (potrebné v 85 % vyšetrovaní závažných trestných činov, pričom 65 % celkového objemu žiadostí je adresovaných poskytovateľom so sídlom v inej jurisdikcii) a stanovenie kompatibilných pravidiel na medzinárodnej úrovni.

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

82 Rozhodnutie Rady (SZBP) 2019/797 zo 17. mája 2019 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty (Ú. v. EÚ L 129I, 17.5.2019, s. 13) a nariadenie Rady (EÚ) 2019/796 zo 17. mája 2019 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty (Ú. v. EÚ L 129I, 17.5.2019, s. 1).

83 Rozhodnutie Rady (SZBP) 2020/1127 z 30. júla 2020, ktorým sa mení rozhodnutie (SZBP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty (ST/9564/2020/INIT) (Ú. v. EÚ L 246, 30.7.2020, s. 12 – 17) a vykonávacie nariadenie Rady (EÚ) 2020/1125 z 30. júla 2020, ktorým sa vykonáva nariadenie (EÚ) 2019/796 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty (ST/9568/2020/INIT) (Ú. v. EÚ L 246, 30.7.2020, s. 4 – 9).

84 Rozhodnutie Rady (SZBP) 2020/1537 z 22. októbra 2020, ktorým sa mení rozhodnutie (SZBP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty (Ú. v. EÚ L 351I, 22.10.2020, s. 5 – 7) a vykonávacie nariadenie Rady (EÚ) 2020/1536 z 22. októbra 2020, ktorým sa vykonáva nariadenie (EÚ) 2019/796 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty (Ú. v. EÚ L 351I, 22.10.2020, s. 1 – 4).

situačného centra EÚ (INTCEN) s cieľom podporiť strategickú spravodajskú spoluprácu v otázkach kybernetických hrozieb a činností. Táto práca bude ďalej zvyšovať situačné povedomie EÚ a podporovať jej rozhodovanie o jednotnej diplomatickej reakcii. Pracovná skupina má spolupracovať s existujúcimi štruktúrami[85], v prípade potreby vrátane štruktúr, ktoré sa zaoberajú širšou hrozbou hybridného narúšania a zahraničného zasahovania, s cieľom získavať a vyhodnocovať situačné povedomie.

Na posilnenie schopnosti prevencie zlovoľného správania v kybernetickom priestore, odrádzania od neho a reakcie naň vysoký predstaviteľ s podporou Komisie v rámci jej právomocí predloží návrh, aby EÚ podrobnejšie vymedzila svoju **pozíciu v otázke odrádzania od kybernetických útokov**. V nadväznosti na doterajšiu prácu v rámci súboru nástrojov kybernetickej diplomacie by táto pozícia mala prispieť k zodpovednému správaniu štátov a spolupráci v kybernetickom priestore a mala by zahŕňať konkrétne smerovanie v boji proti kybernetickým útokom s najzávažnejšími dôsledkami, najmä proti útokom, ktoré ovplyvňujú našu kritickú infraštruktúru, demokratické inštitúcie a procesy[86], ako aj proti útokom na dodávateľské reťazce a kybernetickým krádežiam duševného vlastníctva. Pozícia by mala uvádzať, ako by EÚ a členské štáty mohli využiť svoje politické, hospodárske, diplomatické, právne a strategické komunikačné nástroje proti škodlivým kybernetickým činnostiam, a mala by sa zaoberať aj tým, ako by EÚ a členské štáty mohli posilniť svoju schopnosť pripisovať zodpovednosť za škodlivé kybernetické činnosti. Okrem toho má vysoký predstaviteľ spolu s Radou a Komisiou zámer preskúmať **ďalšie opatrenia v súbore nástrojov kybernetickej diplomacie** vrátane ďalších prípadných reštriktívnych opatrení, a zároveň preskúmať **hlasovanie kvalifikovanou väčšinou pri zaraďovaní osôb do zoznamu v rámci horizontálneho režimu sankcií proti kybernetickým útokom**. EÚ by okrem toho mala vyvinúť ďalšie úsilie na **posilnenie spolupráce s medzinárodnými partnermi** vrátane NATO s cieľom posilniť spoločné chápanie panorámy hrozieb, rozvíjať mechanizmy spolupráce a identifikovať kooperatívne diplomatické reakcie.

Vysoký predstaviteľ za účasti Komisie navrhne aj aktualizáciu **vykonávacích usmernení k súboru nástrojov kybernetickej diplomacie[87]** (aj s cieľom zefektívniť rozhodovací proces) a bude naďalej pravidelne organizovať cvičenia a hodnotenia súboru nástrojov kybernetickej diplomacie. EÚ by navyše mala **pokračovať v integrácii súboru nástrojov kybernetickej diplomacie do krízových mechanizmov EÚ**, hľadať synergie s bojom proti hybridným hrozbám, dezinformáciám a zahraničnému zasahovaniu v kontexte spoločného rámca pre boj proti hybridným hrozbám[88] a akčného plánu pre európsku demokraciu. V tejto súvislosti by EÚ mala zvážiť vzťah medzi súborom nástrojov kybernetickej diplomacie a prípadným uplatnením článku 42 ods. 7 ZEÚ a článku 222 ZFEÚ[89].

2.4. Posilňovanie kapacít kybernetickej obrany

EÚ a členské štáty musia zlepšiť svoju schopnosť predchádzať kybernetickým hrozbám a reagovať na ne v súlade s úrovňou ambícií EÚ odvodenou z jej globálnej stratégie z roku 2016[90]. Na tento účel vysoký predstaviteľ v spolupráci s Komisiou predloží **preskúmanie**

---

85 Napríklad jednotná kapacita EÚ na analýzu spravodajských informácií (SIAC) a v prípade potreby príslušné projekty zriadené v rámci spolupráce PESCO, ako aj systém včasného varovania (RAS) z roku 2018, ktorý bol zriadený na podporu celkového prístupu EÚ k boju proti dezinformáciám.

86 Najmä hľadaním synergií s iniciatívami v rámci akčného plánu pre európsku demokraciu.

87 13007/17.

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

89 Doložka o vzájomnej obrane, doložka o solidarite.

90 Závery Rady (14149/16) o vykonávaní globálnej stratégie EÚ v oblasti bezpečnosti a obrany.

politického rámca kybernetickej obrany (CDPF) s cieľom posilniť ďalšiu koordináciu a spoluprácu medzi aktérmi EÚ[91], ako aj s členskými štátmi a medzi nimi, a to aj pokiaľ ide o misie a operácie spoločnej bezpečnostnej a obrannej politiky (SBOP). Rámec CDPF by mal slúžiť ako vstup pre nadchádzajúci Strategický kompas[92] a zabezpečiť, aby sa kybernetická bezpečnosť a kybernetická obrana ďalej integrovali do širšej agendy bezpečnosti a obrany.

V roku 2018 EÚ identifikovala kybernetický priestor ako samostatnú operačnú oblasť[93]. V nadchádzajúcej **„vojenskej vízii a stratégii pre kybernetický priestor ako operačnú oblasť“** z dielne Vojenského výboru EÚ by sa malo podrobnejšie vymedziť, ako bude kybernetický priestor ako operačná oblasť podporovať vojenské misie a operácie SBOP EÚ. **Vojenská sieť CERT**[94], ktorú zriaďuje Európska obranná agentúra (EDA), takisto výrazne posilní spoluprácu medzi členskými štátmi. Okrem toho sa v záujme kybernetickej bezpečnosti kritických vesmírnych infraštruktúr v gescii Vesmírneho programu Únie posilní Agentúra EÚ pre vesmírny program, a najmä Stredisko na monitorovanie bezpečnosti systému Galileo, a jeho mandát sa rozšíri aj na ďalšie kritické aktíva vesmírneho programu.

EÚ a členské štáty by mali poskytnúť ďalší impulz pre **rozvoj najmodernejších kapacít kybernetickej obrany** prostredníctvom rôznych politík a nástrojov EÚ, najmä CDPF, a v prípade potreby by mali vychádzať z práce EDA. To si vyžaduje silný dôraz na vývoj a využívanie kľúčových technológií, ako je umelá inteligencia, šifrovanie a kvantová výpočtová technika. V súlade s prioritami rozvoja spôsobilostí EÚ z roku 2018[95] a na základe zistení prvej úplnej správy z koordinovaného ročného hodnotenia obrany (CARD)[96] by EÚ mala ďalej podporovať spoluprácu členských štátov na **výskume, inovácii a rozvoji spôsobilostí v oblasti kybernetickej obrany** a nabádať ich, aby naplno využili potenciál **stálej štruktúrovanej spolupráce (PESCO)[97]** a **Európskeho obranného fondu[98]**.

Pripravovaný **akčný plán Komisie o synergiách medzi civilným, obranným a vesmírnym sektorom**, ktorý sa má predložiť v prvom štvrťroku 2021, bude zahŕňať opatrenia na ďalšiu podporu synergií na úrovni programov, technológií, inovácií a startupov v súlade s riadením príslušných programov[99].

---

91 Najmä ESVČ so zapojením Vojenského štábu EÚ (VŠEÚ), Európskej akadémie bezpečnosti a obrany (EABO), Komisie a agentúr EÚ, najmä Európskej obrannej agentúry (EDA).

92 Závery Rady o bezpečnosti a obrane zo 17. júna 2020 (8910/20).

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

94 Zriadenie vojenskej siete CERT EÚ je reakciou na cieľ identifikovaný v politickom rámci EÚ pre kybernetickú obranu z roku 2018, pričom má podporovať aktívnu interakciu a výmenu informácií medzi vojenskými tímami CERT členských štátov EÚ.

95 V júni 2018 sa členské štáty v riadiacom výbore EDA dohodli, že budú usmerňovať obrannú spoluprácu na úrovni EÚ.

96 Ministri obrany ju schválili v riadiacom výbore EDA v novembri 2020. https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card).

97 S kybernetickou problematikou sa spája viacero prebiehajúcich projektov PESCO, najmä platforma na výmenu informácií v oblasti reakcie na kybernetické hrozby a incidenty, tímy rýchlej kybernetickej reakcie a vzájomná pomoc v oblasti kybernetickej bezpečnosti, Akademické a inovačné centrum EÚ pre kybernetickú oblasť a Koordinačné centrum pre kybernetickú a informačnú oblasť (CIDCC).

98 V rámci Európskeho obranného fondu už Komisia identifikovala príležitosti na potenciálne spoločné výskumné a vývojové akcie v oblasti kybernetickej obrany zamerané na posilnenie spolupráce, inovačnej kapacity a konkurencieschopnosti obranného priemyslu.

99 Napríklad programy Horizont Európa, Digitálna Európa a Európsky obranný fond.

Okrem toho by sa mali rozvíjať relevantné synergie a rozhrania s iniciatívami kybernetickej obrany prebiehajúcimi v iných kontextoch vrátane projektov[100] spolupráce členských štátov v kybernetickej sfére v rámci stálej štruktúrovanej spolupráce, ako aj s kybernetickobezpečnostnými štruktúrami EÚ, aby sa podporila výmena informácií a vzájomná podpora.

Strategické iniciatívy

EÚ by mala:

- dokončiť európsky rámec krízového riadenia kybernetickej bezpečnosti a určiť postup, míľniky a harmonogram zriadenia spoločnej kybernetickej jednotky,
- pokračovať vo vykonávaní programu boja proti počítačovej kriminalite v rámci Stratégie EÚ pre bezpečnostnú úniu,
- podporovať a uľahčovať zriadenie pracovnej skupiny členských štátov pre kybernetické spravodajstvo v rámci centra EU INTCEN,
- pokročiť vo vymedzovaní pozície EÚ v otázke odrádzania od kybernetických útokov v záujme prevencie škodlivých kybernetických činností, odrádzania od nich a reakcie na ne,
- preskúmať politický rámec EÚ pre kybernetickú obranu,
- napomôcť prípravu „vojenskej vízie a stratégie pre kybernetický priestor ako operačnú oblasť“ EÚ na podporu vojenských misií a operácií SBOP,
- podporovať synergie medzi civilným, obranným a vesmírnym sektorom a
- posilniť kybernetickú bezpečnosť kritických vesmírnych infraštruktúr v rámci vesmírneho programu.

3. PRESADZOVANIE GLOBÁLNEHO A OTVORENÉHO KYBERNETICKÉHO PRIESTORU

EÚ by mala naďalej spolupracovať s medzinárodnými partnermi na presadzovaní politického modelu a vízie kybernetického priestoru založeného na zásadách právneho štátu, ľudských právach, základných slobodách a demokratických hodnotách, ktoré prinášajú sociálny, hospodársky a politický rozvoj na celom svete a prispievajú k bezpečnostnej únii. Medzinárodná spolupráca je kľúčová pre zachovanie globálneho, otvoreného, stabilného a bezpečného kybernetického priestoru. EÚ by preto mala pokračovať v spolupráci s tretími krajinami, medzinárodnými organizáciami a so širokou komunitou zainteresovaných strán na rozvoji a uplatňovaní koherentnej a holistickej medzinárodnej kybernetickej politiky, pričom treba mať na zreteli silnejúce väzby medzi hospodárskymi aspektmi nových technológií, vnútornou bezpečnosťou a zahraničnou, bezpečnostnou a obrannou politikou. EÚ ako silný hospodársky a obchodný blok založený na základných demokratických hodnotách, dodržiavaní zásad právneho štátu a základných práv má zároveň jedinečné postavenie na to, aby sa chopila iniciatívy pri definovaní a presadzovaní medzinárodných noriem a štandardov.

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

3.1. Vedúce postavenie EÚ v oblasti štandardov, noriem a rámcov v kybernetickom priestore

Zintenzívnenie medzinárodnej normalizácie

Na podporu a obranu svojej vízie kybernetického priestoru na medzinárodnej úrovni musí EÚ **zintenzívniť svoju angažovanosť a vedúce postavenie v medzinárodných normalizačných procesoch a posilniť svoje zastúpenie v medzinárodných a európskych normalizačných orgánoch, ako aj v iných organizáciách, ktoré vyvíjajú normy**[101]. Digitálne technológie rýchlo napredujú a medzinárodné normy čoraz významnejšie dopĺňajú tradičnú reguláciu v oblastiach ako umelá inteligencia, cloud, kvantová výpočtová technika a kvantová komunikácia. Tretie krajiny čoraz viac využívajú medzinárodnú normalizáciu na presadzovanie svojej politickej a ideologickej agendy, ktorá často nezodpovedá hodnotám EÚ. Okrem toho rastie riziko konkurenčných rámcov medzinárodnej normalizácie, čo vedie k fragmentácii.

Formovanie medzinárodných noriem v oblasti vznikajúcich technológií a základnej internetovej architektúry v súlade s hodnotami EÚ je nevyhnutné na zabezpečenie toho, aby internet zostal globálny a otvorený, aby boli technológie zamerané na človeka a na ochranu súkromia a aby ich používanie bolo zákonné, bezpečné a etické. EÚ by mala vo svojej pripravovanej stratégii normalizácie vymedziť svoje **ciele v oblasti medzinárodnej normalizácie** a mala by proaktívne a koordinovane komunikovať pri ich propagácii na medzinárodnej úrovni. Treba sa usilovať o intenzívnejšiu spoluprácu a rozdelenie zaťaženia s podobne zmýšľajúcimi partnermi a európskymi zainteresovanými stranami.

Podpora zodpovedného správania štátov v kybernetickom priestore

EÚ naďalej spolupracuje s medzinárodnými partnermi na presadzovaní a podpore globálneho, otvoreného, stabilného a zabezpečeného kybernetického priestoru, kde **sa dodržiava medzinárodné právo, najmä Charta OSN**[102], a **dobrovoľné nezáväzné normy, pravidlá a zásady zodpovedného správania štátov**[103]. Účinnosť multilaterálnych debát o medzinárodnej bezpečnosti v kybernetickom priestore slabne, takže EÚ a členské štáty musia jednoznačne zaujať proaktívnejší postoj v diskusiách v rámci OSN a na iných príslušných medzinárodných fórach. EÚ má najlepšie postavenie **na presadzovanie, koordináciu a konsolidáciu pozícií členských štátov na medzinárodných fórach** a mala by vypracovať **pozíciu EÚ k uplatňovaniu medzinárodného práva v kybernetickom priestore**. Vysoký predstaviteľ má zároveň spolu s členskými štátmi v pláne presadiť na pôde OSN ich inkluzívny a konsenzuálny návrh politického záväzku v podobe **akčného programu na posilnenie zodpovedného správania štátov v kybernetickom priestore**[104]. Akčný program

---

101 Napr. Medzinárodná organizácia pre normalizáciu (ISO), Medzinárodná elektrotechnická komisia (IEC), Medzinárodná telekomunikačná únia (ITU), Európsky výbor pre normalizáciu (CEN), Európsky výbor pre normalizáciu v elektrotechnike (CENELEC), Európsky inštitút pre telekomunikačné normy (ETSI), Osobitná skupina pre internetovú techniku (IETF), projekt partnerstva 3. generácie (3GPP) a Inštitút elektrotechnických a elektronických inžinierov (IEEE).

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

103 Ako sa uvádza v príslušných správach skupín vládnych expertov na vývoj v oblasti informácií a telekomunikácií v kontexte medzinárodnej bezpečnosti (UNGGE), ktoré schválilo Valné zhromaždenie OSN – konkrétne v správach z rokov 2015, 2013 a 2010.

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

vychádza z existujúceho *acquis*, ktoré schválilo Valné zhromaždenie OSN[105], ponúka platformu na spoluprácu a výmenu osvedčených postupov v rámci OSN a navrhuje zavedenie mechanizmu na uplatňovanie noriem zodpovedného správania štátov v praxi, ako aj na podporu budovania kapacít. Vysoký predstaviteľ chce okrem toho posilniť a podporiť vykonávanie **opatrení na budovanie dôvery** medzi štátmi vrátane výmeny osvedčených postupov na regionálnej a multilaterálnej úrovni a podpory medziregionálnej spolupráce.

Zvýšená globálna prepojenosť by nemala viesť k cenzúre, hromadnému sledovaniu, porušovaniu ochrany osobných údajov či represiám voči občianskej spoločnosti, akademickej obci a občanom. EÚ by mala aj naďalej viesť v otázkach ochrany a presadzovania **ľudských práv a základných slobôd** online. Na to by mala ďalej podporovať dodržiavanie medzinárodného práva a noriem v oblasti ľudských práv[106], zaviesť do praxe svoj akčný plán pre ľudské práva a demokraciu na roky 2020 – 2024[107] a pokročiť v uplatňovaní Usmernení EÚ v oblasti ľudských práv týkajúcich sa slobody prejavu online a offline[108], **čím ponúkne nový impulz pre praktické uplatňovanie nástrojov EÚ**. EÚ by sa mala trvalo usilovať o **ochranu obhajcov ľudských práv, občianskej spoločnosti a akademickej obce pri práci na otázkach ako kybernetická bezpečnosť, ochrana údajov, sledovanie a online cenzúra.** Na to by EÚ mala poskytnúť ďalšie praktické usmernenia, podporovať osvedčené postupy a zintenzívniť úsilie o prevenciu zneužívania nových technológií, v náležitých prípadoch najmä diplomatickými opatreniami, ako aj kontrolou vývozu takýchto technológií. EÚ by zároveň mala pokračovať v boji za ochranu najzraniteľnejších členov spoločnosti online tým, že predloží legislatívu na lepšiu ochranu detí pred sexuálnym zneužívaním a vykorisťovaním, ako aj stratégiu v oblasti práv dieťaťa.

Budapeštiansky dohovor o počítačovej kriminalite

EÚ naďalej podporuje tretie krajiny, ktoré chcú pristúpiť k **Budapeštianskemu dohovoru Rady Európy o počítačovej kriminalite**, a pracuje na finalizácii **druhého dodatkového protokolu k Budapeštianskemu dohovoru**, ktorý obsahuje opatrenia a záruky na zlepšenie medzinárodnej spolupráce medzi orgánmi presadzovania práva a justičnými orgánmi, ako aj medzi orgánmi a poskytovateľmi služieb v iných krajinách, o ktorom Komisia rokuje v mene EÚ[109]. Hrozí, že súčasná iniciatíva o novom právnom nástroji v oblasti počítačovej kriminality na úrovni OSN prehĺbi rozpory a spomalí veľmi potrebné vnútroštátne reformy a súvisiace budovanie kapacít, čo by mohlo poškodiť účinnú medzinárodnú spoluprácu v boji proti počítačovej kriminalite: EÚ nevidí potrebu žiadneho nového právneho nástroja v oblasti počítačovej kriminality na úrovni OSN. EÚ sa naďalej zapája do **multilaterálnych debát v oblasti počítačovej kriminality** s cieľom zabezpečiť dodržiavanie ľudských práv a základných slobôd prostredníctvom inkluzívnosti, transparentnosti a zohľadnením dostupnej expertízy s cieľom zabezpečiť pridanú hodnotu pre všetkých.

---

105 Ako sa uvádza v príslušných správach skupín vládnych expertov na vývoj v oblasti informácií a telekomunikácií v kontexte medzinárodnej bezpečnosti (UNGGE), ktoré schválilo Valné zhromaždenie OSN – konkrétne v správach z rokov 2015, 2013 a 2010.

106 Najmä Charta OSN a Všeobecná deklarácia ľudských práv.

107 https://www.consilium.europa.eu/sk/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 Rozhodnutie Rady z júna 2019 (ref. 9116/19).

3.2. Spolupráca s partnermi a rozmanitou komunitou zainteresovaných strán

EÚ by mala **posilniť a rozšíriť kybernetický dialóg s tretími krajinami** s cieľom presadzovať svoje hodnoty a víziu kybernetického priestoru, vymieňať si osvedčené postupy a usilovať sa o účinnejšiu spoluprácu. EÚ by tiež mala nadviazať **štruktúrovanú komunikáciu s regionálnymi organizáciami**, ako je Africká únia, regionálne fórum ASEAN-u, Organizácia amerických štátov a Organizácia pre bezpečnosť a spoluprácu v Európe. Pokiaľ je to možné a vhodné, EÚ by sa zároveň mala usilovať o nájdenie spoločných východísk s ostatnými partnermi na základe otázok spoločného záujmu. V spolupráci s delegáciami EÚ a v relevantných prípadoch aj s veľvyslanectvami členských štátov na celom svete by Únia mala vytvoriť neformálnu **sieť kybernetickej diplomacie EÚ** na podporu únijnej vízie kybernetického priestoru, výmenu informácií a pravidelnú koordináciu v nadväznosti na dianie v kybernetickom priestore[110].

Vychádzajúc zo spoločných vyhlásení z 8. júla 2016[111] a 10. júla 2018[112] by EÚ mala naďalej podporovať **spoluprácu medzi EÚ a NATO**, najmä pokiaľ ide o požiadavky na interoperabilitu kybernetickej obrany. V tejto súvislosti by sa EÚ mala ďalej usilovať o pridruženie príslušných štruktúr SBOP k iniciatíve NATO s názvom Federated Mission Networking, čo by v prípade potreby umožnilo sieťovú interoperabilitu s NATO a partnermi. Okrem toho by sa mali hlbšie preskúmať možnosti spolupráce medzi EÚ a NATO v oblasti vzdelávania, odbornej prípravy a cvičení, vrátane hľadania synergií medzi Európskou akadémiou bezpečnosti a obrany a centrom excelentnosti NATO pre spoluprácu v oblasti kybernetickej obrany.

EÚ v súlade so svojimi hodnotami dôrazne podporuje a presadzuje **model správy internetu založený na viacerých zainteresovaných stranách**. O kontrolu nad internetom by sa nemal usilovať žiadny subjekt, vláda ani medzinárodná organizácia. EÚ by sa mala naďalej angažovať na fórach[113] s cieľom posilňovať spoluprácu a zaisťovať ochranu základných práv a slobôd, najmä práva na dôstojnosť a súkromie, slobody prejavu a práva na informácie. S cieľom pokročiť v multilaterálnej spolupráci v otázkach kybernetickej bezpečnosti sa Komisia a vysoký predstaviteľ v rámci svojich kompetencií budú usilovať o posilnenie **pravidelných a štruktúrovaných výmen so zainteresovanými stranami** vrátane súkromného sektora, akademickej obce a občianskej spoločnosti, pričom zdôrazňujú, že prepojenosť kybernetického priestoru si vyžaduje, aby všetky zainteresované strany o tejto problematike diskutovali a prevzali svoj diel zodpovednosti za zachovanie globálneho, otvoreného, stabilného a zabezpečeného kybernetického priestoru. Toto úsilie bude cenným vstupom do možných kľúčových krokov na úrovni EÚ.

3.3. Posilnenie globálnych kapacít na zvýšenie globálnej odolnosti

Aby mohli všetky krajiny využívať sociálne, hospodárske a politické prínosy internetu a využívania technológií, EÚ naďalej podporuje svojich partnerov pri zvyšovaní ich kybernetickej odolnosti a kapacít na vyšetrovanie a stíhanie počítačovej kriminality a riešenie kybernetických hrozieb. S cieľom zabezpečiť celkovú koherentnosť by EÚ mala vypracovať

---

110 V relevantných prípadoch by sa dali využiť aj činnosti neformálnej siete digitálnej diplomacie EÚ, ktorá zahŕňa ministerstvá zahraničných vecí členských štátov.

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

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

113 Napríklad Internetová korporácia pre prideľovanie mien a čísel (ICANN) a Fórum pre správu internetu (IGF).

program EÚ pre budovanie externých kybernetických kapacít, ktorý by toto úsilie riadil v súlade s usmerneniami EÚ v oblasti budovania externých kybernetických kapacít[114] a Agendou 2030 pre udržateľný rozvoj[115]. Program by mal využívať expertízu členských štátov a príslušných inštitúcií, orgánov, agentúr a iniciatív EÚ vrátane siete EÚ na budovanie kybernetických kapacít[116] v rámci ich príslušných mandátov. Zriadi sa **výbor EÚ pre budovanie kybernetických kapacít**, ktorý bude zahŕňať príslušných inštitucionálnych aktérov EÚ, bude monitorovať pokrok a identifikovať ďalšie synergie a prípadné medzery. Okrem toho môže podporovať posilnenú spoluprácu s členskými štátmi, ako aj s partnermi verejného a súkromného sektora a inými relevantnými medzinárodnými orgánmi s cieľom zabezpečiť koordináciu úsilia a zabrániť duplicite.

Budovanie kybernetických kapacít EÚ by sa malo naďalej zameriavať na západný Balkán a susedstvo EÚ, ako aj na partnerské krajiny, ktoré prechádzajú rýchlym digitálnym rozvojom. Úsilie EÚ by malo v partnerských krajinách podporovať tvorbu legislatívy a politík v súlade s príslušnými politikami a normami kybernetickej diplomacie EÚ. V tejto súvislosti by únijné budovanie kapacít v oblasti digitalizácie malo zahŕňať kybernetickú bezpečnosť ako štandardný prvok. Na to by EÚ mala vypracovať program školenia tých zamestnancov EÚ, ktorí sú zodpovední za budovanie digitálnych a kybernetických kapacít mimo EÚ. EÚ by mala týmto krajinám pomáhať aj pri riešení narastajúceho problému škodlivých kybernetických činností, ktoré poškodzujú rozvoj ich spoločnosti, ako aj **integritu a bezpečnosť demokratických systémov**, v súlade s úsilím v rámci akčného plánu pre európsku demokraciu. V tejto súvislosti by mohlo byť obzvlášť užitočné partnerské učenie medzi členskými štátmi EÚ, ako aj príslušnými agentúrami EÚ a tretími krajinami.

A napokon v kontexte paktu o civilnej SBOP z roku 2018[117] môžu aj civilné misie v rámci SBOP prispieť k celkovej reakcii EÚ na riešenie problémov kybernetickej bezpečnosti, najmä posilnením právneho štátu v partnerských krajinách, ako aj posilnením kapacít ich orgánov presadzovania práva a civilnej štátnej správy.

Strategické iniciatívy

EÚ by mala:

- vymedziť súbor cieľov v medzinárodných procesoch normalizácie a presadzovať ich na medzinárodnej úrovni,
- presadzovať medzinárodnú bezpečnosť a stabilitu v kybernetickom priestore, najmä tým, že EÚ a jej členské štáty navrhnú na pôde OSN akčný program na posilnenie zodpovedného správania štátov v kybernetickom priestore,
- poskytovať praktické usmernenia o uplatňovaní ľudských práv a základných slobôd v kybernetickom priestore,
- lepšie chrániť deti pred sexuálnym zneužívaním a vykorisťovaním, a zaviesť stratégiu v oblasti práv dieťaťa,
- posilniť a podporovať Budapeštiansky dohovor o počítačovej kriminalite, a to aj

[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/sk/pdf.

prácou na druhom dodatkovom protokole k nemu,

- rozšíriť kybernetický dialóg EÚ s tretími krajinami, regionálnymi a medzinárodnými organizáciami – aj prostredníctvom neformálnej siete kybernetickej diplomacie EÚ,
- posilniť komunikáciu s komunitou rôznych zainteresovaných strán, najmä pravidelnými a štruktúrovanými výmenami so súkromným sektorom, akademickou obcou a občianskou spoločnosťou a
- navrhnúť program EÚ pre budovanie externých kybernetických kapacít a výbor EÚ pre budovanie kybernetických kapacít.

III. KYBERNETICKÁ BEZPEČNOSŤ V INŠTITÚCIÁCH, ORGÁNOCH A AGENTÚRACH EÚ

Vzhľadom na ich politický profil, kritické poslanie koordinácie veľmi citlivých otázok a rolu v spravovaní veľkých objemov verejných financií **sú inštitúcie, orgány a agentúry EÚ pravidelným terčom kybernetických útokov**, najmä kybernetickej špionáže. Vyspelosť kybernetickej odolnosti a schopnosti odhaľovať škodlivé kybernetické činnosti a reagovať na ne je však v týchto subjektoch veľmi rôznorodá. Celkovú úroveň kybernetickej bezpečnosti preto treba zvýšiť konzistentnými a jednotnými pravidlami.

Pokiaľ ide o informačnú bezpečnosť, došlo k pokroku vo zvyšovaní konzistentnosti **pravidiel ochrany utajovaných skutočností EÚ, ako aj citlivých neutajovaných skutočností**. Interoperabilita systémov utajovaných skutočností je však naďalej obmedzená, čo bráni plynulému prenosu informácií medzi jednotlivými subjektmi. Treba urobiť viac v záujme medziinštitucionálneho prístupu k nakladaniu s utajovanými skutočnosťami EÚ a citlivými neutajovanými skutočnosťami, ktorý by mohol slúžiť aj ako vzor pre interoperabilitu medzi členskými štátmi. Zároveň by sa malo stanoviť východisko na zjednodušenie postupov s členskými štátmi. EÚ by okrem toho mala ďalej rozvíjať svoju schopnosť zabezpečenej komunikácie s relevantnými partnermi, pričom by mala podľa možností vychádzať z existujúcich mechanizmov a postupov.

Ako sa uvádza v Stratégii pre bezpečnostnú úniu, Komisia preto **v roku 2021 predloží návrhy spoločných záväzných pravidiel v oblasti informačnej a kybernetickej bezpečnosti pre všetky inštitúcie, orgány a agentúry EÚ**, a to na základe prebiehajúcich medziinštitucionálnych diskusií EÚ o kybernetickej bezpečnosti[118].

Súčasné a budúce trendy telepráce si budú zároveň vyžadovať ďalšie investície do zabezpečeného vybavenia, infraštruktúry a nástrojov, ktoré umožnia prácu na citlivých a utajovaných spisoch na diaľku.

Okrem toho je panoráma kybernetických hrozieb čoraz nebezpečnejšia a rastie frekvencia sofistikovanejších kybernetických útokov s vplyvom na inštitúcie, orgány a agentúry EÚ, takže treba viac investovať do vysokej úrovne kybernetickej vyspelosti. Zriaďuje sa program na zvýšenie kybernetickobezpečnostného povedomia vo všetkých inštitúciách, orgánoch a agentúrach EÚ s cieľom zlepšiť informovanosť a kybernetickú hygienu zamestnancov a podporiť spoločnú kultúru kybernetickej bezpečnosti.

[118] Pravidelné medziinštitucionálne diskusie EÚ o kybernetickej bezpečnosti sú súčasťou všeobecnejšej komunikácie o príležitostiach a výzvach digitálnej transformácie pre inštitúcie EÚ.

Tímu CERT-EU treba zlepšiť mechanizmus financovania, aby dokázal lepšie pomáhať inštitúciám, orgánom a agentúram EÚ s uplatňovaním nových kybernetickobezpečnostných pravidiel a so zvyšovaním ich kybernetickej odolnosti. Mandát CERT-EU sa musí tiež posilniť, aby mal k dispozícii stabilné prostriedky na dosiahnutie týchto cieľov.

Strategické iniciatívy

1. Nariadenie o informačnej bezpečnosti v inštitúciách, orgánoch a agentúrach EÚ;
2. nariadenie o spoločných pravidlách kybernetickej bezpečnosti pre inštitúcie, orgány a agentúry EÚ;
3. nový právny základ pre CERT-EU na posilnenie jeho mandátu a financovania.

IV. ZÁVERY

Koordinované vykonávanie tejto stratégie prispeje ku kyberneticky zabezpečenej digitálnej dekáde pre EÚ, k dosiahnutiu bezpečnostnej únie a k posilneniu pozície EÚ vo svete.

Únia by mala presadzovať štandardy a normy špičkových kybernetickobezpečnostných riešení pre základné služby a kritickú infraštruktúru, ako aj vývoj a zavádzanie nových technológií. V kyberneticky zabezpečenej digitálnej transformácii zohrá svoju rolu každá organizácia a jednotlivec, ktorí používajú internet.

Komisia a vysoký predstaviteľ budú v rámci svojich právomocí monitorovať pokrok v plnení tejto stratégie a vypracujú kritériá hodnotenia. Vstupy do tohto monitorovania by mali zahŕňať správy agentúry ENISA a pravidelné správy Komisie o bezpečnostnej únii. Výsledky prispejú k nadchádzajúcim cieľom digitálnej dekády[119]. Komisia a vysoký predstaviteľ budú v rámci svojich právomocí podľa potreby naďalej spolupracovať s členskými štátmi pri identifikácii praktických opatrení na prepojenie štyroch kybernetickobezpečnostných komunít v EÚ: kritickej infraštruktúry a odolnosti vnútorného trhu, spravodlivosti a presadzovania práva, kybernetickej diplomacie a kybernetickej obrany. Okrem toho sa Komisia a vysoký predstaviteľ budú naďalej angažovať v komunite rôznych zainteresovaných strán, pričom zdôrazňujú, že všetci používatelia internetu musia priložiť ruku k dielu v záujme zachovania globálneho, otvoreného, stabilného a zabezpečeného kybernetického priestoru, kde si môže každý bezpečne žiť svoj digitálny život.

[119] Ako bolo ohlásené v pracovnom programe Komisie na rok 2021.

Dodatok: Ďalšie kroky v oblasti kybernetickej bezpečnosti sietí 5G

Na základe výsledkov preskúmania odporúčania Komisie o kybernetickej bezpečnosti sietí 5G[120] by sa ďalšie koordinované kroky na úrovni EÚ mali zamerať na tri kľúčové ciele a hlavné krátko- a strednodobé opatrenia uvedené v nasledujúcej tabuľke, ktoré majú vykonať orgány členských štátov, Komisia a ENISA.

Prvou prioritou ďalšej fázy je **dokončiť vykonávanie súboru nástrojov na vnútroštátnej úrovni a riešiť problémy identifikované v správe o pokroku z júla 2020**. V tejto súvislosti by niektorým strategickým opatreniam zo súboru nástrojov pomohla **posilnená koordinácia alebo výmena informácií** v rámci pracovného okruhu sieťovej a informačnej bezpečnosti, ako sa už uviedlo v správe o pokroku, čo by mohlo potenciálne viesť k vypracovaniu **osvedčených postupov alebo usmernení**. Pokiaľ ide o technické opatrenia, agentúra ENISA by mohla poskytnúť ďalšiu podporu vychádzajúc zo svojej doterajšej činnosti a mohla by podrobnejšie preskúmať určité témy, ako aj **vypracovať komplexný prehľad všetkých relevantných usmernení o požiadavkách na kybernetickú bezpečnosť 5G kladených na prevádzkovateľov mobilných sietí**.

Po druhé, členské štáty zdôraznili, že je dôležité držať krok s dianím a **nepretržite monitorovať vývoj technológií, architektúry 5G, hrozieb a možností a aplikácií využitia 5G, ako aj externých faktorov**, aby bolo možné **identifikovať a riešiť nové alebo vznikajúce riziká**. Navyše by sa v počiatočnej analýze rizík malo hlbšie preskúmať viacero aspektov, najmä aby sa zamerala na celý ekosystém 5G vrátane všetkých relevantných častí sieťovej infraštruktúry a dodávateľského reťazca 5G. Hoci súbor nástrojov bol navrhnutý flexibilne a prispôsobivo, v prípade potreby by sa v strednodobom horizonte mohli prijať opatrenia na jeho rozšírenie alebo zmenu s cieľom zabezpečiť, aby zostal komplexný a aktuálny.

Po tretie, naďalej by sa mali prijímať **opatrenia na úrovni EÚ** s cieľom podporiť a doplniť ciele súboru nástrojov a plne ich začleniť do príslušných politík Únie a Komisie, najmä v nadväznosti na opatrenia oznámené Komisiou v jej oznámení o súbore nástrojov z 29. januára 2020[121] v širokej škále oblastí (napr. financovanie zabezpečených sietí 5G zo strany EÚ, investície do technológií 5G a post-5G, nástroje na ochranu obchodu a nástroje hospodárskej súťaže s cieľom zabrániť narušeniam na trhu dodávok 5G atď.).

Podľa potreby by vedúci aktéri mali začiatkom roka 2021 odsúhlasiť podrobné mechanizmy a míľniky pre hlavné opatrenia uvedené nižšie.

Kľúčový cieľ č. 1: Zabezpečenie konvergentných národných prístupov k účinnému zmierňovaniu rizík v celej EÚ		
Oblasti	**Hlavné krátko- a strednodobé opatrenia**	**Hlavní aktéri**
Vykonávanie súboru	dokončiť vykonávanie opatrení odporúčaných v záveroch	orgány

[120] Správa Komisie o vplyve odporúčania Komisie 2019/534 z 26. marca 2019 na kybernetickú bezpečnosť sietí 5G.

[121] Oznámenie Komisie COM(2020) 50, Bezpečné zavádzanie 5G v EÚ – Vykonávanie súboru nástrojov, 29. január 2020.

nástrojov členskými štátmi	súboru nástrojov do druhého štvrťroka 2021 s pravidelnou kontrolou v rámci pracovného okruhu sieťovej a informačnej bezpečnosti	členských štátov
Výmena informácií a osvedčených postupov v oblasti strategických opatrení zameraných na dodávateľov	zintenzívniť výmenu informácií a zvážiť možné osvedčené postupy, najmä pokiaľ ide o: – obmedzenia vysokorizikových dodávateľov (strategické opatrenie SM03) a opatrenia týkajúce sa poskytovania riadených služieb (SM04), – zabezpečenie a odolnosť dodávateľského reťazca, najmä v nadväznosti na prieskum orgánu BEREC o SM05 – SM06	orgány členských štátov, Komisia
Budovanie kapacít a usmernenia týkajúce sa technických opatrení	vykonávať hĺbkové technické prieskumy a vypracovať spoločné usmernenia a nástroje vrátane: – komplexnej a dynamickej matice bezpečnostných kontrol a osvedčených postupov v otázkach zabezpečenia 5G, usmernenia na podporu vykonávania vybraných technických opatrení zo súboru nástrojov.	ENISA, orgány členských štátov
Kľúčový cieľ č. 2: Podpora nepretržitej výmeny znalostí a budovania kapacít		
Oblasti	**Hlavné krátko- a strednodobé opatrenia**	**Hlavní aktéri**
Nepretržité budovanie znalostí	organizovať činnosti zamerané na budovanie znalostí o technológiách a súvisiacich výzvach (otvorené architektúry, prvky 5G – napr. virtualizácia, kontajnerizácia, vrstvená architektúra – tzv. slicing atď.), vývoj panorámy hrozieb, incidenty v reálnom svete atď.	ENISA, orgány členských štátov, iné zainteresované strany
Posudzovanie rizík	aktualizovať a vymieňať si informácie o aktualizovaných vnútroštátnych posúdeniach rizík	orgány členských štátov, Komisia, ENISA
Spoločné projekty financované z EÚ na podporu vykonávania súboru nástrojov	finančne podporovať projekty, ktoré podporujú vykonávanie súboru nástrojov, s využitím financovania EÚ, najmä v rámci programu Digitálna Európa (napr. projekty budovania kapacít vnútroštátnych orgánov, testovacie zariadenia alebo iné pokročilé kapacity atď.)	orgány členských štátov, Komisia
Spolupráca zainteresovaných strán	podporovať spoluprácu medzi vnútroštátnymi orgánmi zapojenými do kybernetickej bezpečnosti 5G (napr. skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, orgány kybernetickej bezpečnosti, telekomunikačné regulačné orgány) a so súkromnými zainteresovanými stranami	orgány členských štátov, Komisia, ENISA
Kľúčový cieľ č. 3: Podpora odolnosti dodávateľského reťazca a iných bezpečnostných strategických cieľov EÚ		
Oblasti	**Hlavné krátko- a strednodobé opatrenia**	**Hlavní aktéri**
Normalizácia	vymedziť a realizovať konkrétny akčný plán na posilnenie zastúpenia EÚ v normalizačných orgánoch ako súčasť ďalšej práce podskupiny NIS pre normalizáciu, aby sa dosiahli konkrétne bezpečnostné ciele vrátane podpory interoperabilných rozhraní s cieľom uľahčiť diverzifikáciu dodávateľov	orgány členských štátov
Odolnosť	– vykonať hĺbkovú analýzu ekosystému a	orgány

dodávateľského reťazca	dodávateľského reťazca 5G s cieľom lepšie identifikovať a monitorovať kľúčové aktíva a potenciálne kritické závislosti, – zabezpečiť, aby fungovanie trhu a dodávateľského reťazca 5G bolo v súlade s pravidlami a cieľmi EÚ v oblasti obchodu a hospodárskej súťaže vymedzenými v oznámení Komisie z 29. januára, a aby sa na investície, ktoré môžu ovplyvniť hodnotový reťazec 5G, uplatňovalo preverovanie PZI, pričom treba zohľadniť ciele súboru nástrojov, – monitorovať existujúce a očakávané trendy na trhu a vyhodnotiť riziká a príležitosti v oblasti otvorenej rádiovej prístupovej siete (Open RAN) formou nezávislej štúdie	členských štátov, Komisia
Certifikácia	začať s prípravou príslušných kandidátskych systémov certifikácie kľúčových komponentov 5G a dodávateľských procesov s cieľom pomôcť riešiť určité riziká súvisiace s technickými zraniteľnými miestami, ako sa vymedzuje v plánoch zmierňovania rizika v rámci súboru nástrojov	Komisia, ENISA, vnútroštátne orgány, iné zainteresované strany
Kapacity EÚ a bezpečné zavádzanie sietí	– investovať do výskumu, inovácie a kapacít, najmä prijatím partnerstva pre inteligentné siete a služby, – zaviesť príslušné bezpečnostné podmienky pre programy financovania a finančné nástroje EÚ (vnútorné aj vonkajšie), ako sa uvádza v oznámení Komisie z 29. januára	členské štáty, Komisia, zainteresované strany z odvetvia 5G
Vonkajšie aspekty	priaznivo reagovať na žiadosti tretích krajín, ktoré by chceli pochopiť a potenciálne využiť prístup založený na súbore nástrojov, ktorý vypracovala EÚ	členské štáty, Komisia, ESVČ, delegácie EÚ