Rada
Evropské unie

Brusel 16. prosince 2020
(OR. en)

14133/20

Interinstitucionální 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

PRŮVODNÍ POZNÁMKA

Odesílatel:	Martine DEPREZOVÁ, ředitelka, za generální tajemnici Evropské komise
Datum přijetí:	16. prosince 2020
Příjemce:	Jeppe TRANHOLM-MIKKELSEN, generální tajemník Rady Evropské unie
Č. dok. Komise:	JOIN(2020) 18 final
Předmět:	SPOLEČNÉ SDĚLENÍ EVROPSKÉMU PARLAMENTU A RADĚ Strategie kybernetické bezpečnosti EU pro digitální dekádu

Delegace naleznou v příloze dokument JOIN(2020) 18 final.

Příloha: JOIN(2020) 18 final

EVROPSKÁ
KOMISE

VYSOKÝ PŘEDSTAVITEL
UNIE PRO ZAHRANIČNÍ
VĚCI A BEZPEČNOSTNÍ
POLITIKU

V Bruselu dne 16.12.2020
JOIN(2020) 18 final

SPOLEČNÉ SDĚLENÍ EVROPSKÉMU PARLAMENTU A RADĚ

Strategie kybernetické bezpečnosti EU pro digitální dekádu

SPOLEČNÉ SDĚLENÍ EVROPSKÉMU PARLAMENTU A RADĚ

Strategie kybernetické bezpečnosti EU pro digitální dekádu

I. ÚVOD: KYBERNETICKY BEZPEČNÁ DIGITÁLNÍ TRANSFORMACE V PROSTŘEDÍ S KOMPLEXNÍMI HROZBAMI

Kybernetická bezpečnost je nedílnou součástí bezpečnosti Evropanů. Ať už jde o využívání zařízení připojených k internetu, elektrizačních soustav či letadel nebo návštěvy bank, orgánů veřejné správy či nemocnic, lidé si zaslouží, aby tak mohli činit s vědomím, že budou chráněni proti kybernetickým hrozbám. Ekonomika, demokracie a společnost v EU více než kdy jindy závisí na bezpečných a spolehlivých digitálních nástrojích a konektivitě. Kybernetická bezpečnost je proto zásadní pro budování odolné, zelené a digitální Evropy.

Doprava, energetika a zdravotnictví, telekomunikace, finance, bezpečnost, demokratické procesy a odvětví vesmíru a obrany jsou do velké míry závislé na sítích a informačních systémech, které jsou stále více propojeny. Vzájemné meziodvětvové závislosti jsou velmi silné, protože fungování sítí a informačních systémů zase závisí na stálém zásobování elektřinou. Zařízení připojená k internetu již převyšují počet lidí na planetě a podle odhadů se jejich počet do roku 2025 zvýší na 25 miliard[1]: čtvrtina z nich bude v Evropě. Digitalizaci pracovních režimů urychlila pandemie COVID-19, během níž 40 % pracovníků v EU přešlo na práci z domova, což pravděpodobně bude mít trvalé dopady na každodenní život[2]. To zvyšuje zranitelnost vůči kybernetickým útokům[3]. Předměty připojené k internetu jsou spotřebiteli často dodávány se známými chybami zabezpečení, což dále zvětšuje prostor k útokům pro nepřátelskou kybernetickou činnost[4]. Průmyslové prostředí v EU je stále více digitalizováno a propojeno, což také znamená, že kybernetické útoky mohou mít na průmyslová odvětví a ekosystémy mnohem větší dopad než kdykoli předtím.

Prostředí hrozeb je spojeno s geopolitickým napětím ohledně globálního a otevřeného internetu a ohledně kontroly technologií v celém dodavatelském řetězci[5]. Toto napětí se odráží v rostoucím počtu národních států budujících digitální hranice. Omezení internetu a na internetu ohrožuje globální a otevřený kyberprostor, jakož i právní stát, základní práva, svobodu a demokracii – základní hodnoty EU. Kyberprostor je stále více využíván pro

[1] Odhad telekomunikačního obchodního sdružení GSMA; https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf). Společnost International Data Corporation předpovídá 42,6 miliardy přístrojů, čidel a kamer připojených k internetu; https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2] Z průzkumu provedeného v červnu 2020 vyplývá, že 47 % předních podniků zamýšlí umožnit zaměstnancům práci z domova na plný úvazek, i když bude možné se na pracoviště vrátit; 82 % mělo v úmyslu povolit práci z domova alespoň částečně; 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 aktuálně nejškodlivějších malwarů známý pod názvem Mirai vytvořil botnety s více než 600 000 zařízeními, které narušily několik velkých internetových stránek v Evropě a ve Spojených státech.

[5] Včetně elektronických součástek, analýzy dat, cloudu, rychlejších a chytřejších sítí s technologií 5G a vyšší, šifrování, umělé inteligence (UI) a nových paradigmat pro výpočet a důvěryhodné zpracování dat, jako jsou blockchain, cloud-to-edge a kvantová výpočetní technika.

politické a ideologické účely a zvýšená polarizace na mezinárodní úrovni brání účinnému multilateralismu. Hybridní hrozby kombinují dezinformační kampaně s kybernetickými útoky na infrastrukturu, ekonomické procesy a demokratické instituce a mají potenciál způsobit fyzické škody, získat nezákonný přístup k osobním údajům, ukrást průmyslová nebo státní tajemství, zasít nedůvěru a oslabit sociální soudržnost. Tyto činnosti podkopávají mezinárodní bezpečnost a stabilitu a výhody, které kyberprostor přináší pro hospodářský, sociální a politický rozvoj.

Zacílení nepřátelské činnosti na kritickou infrastrukturu je závažným globálním rizikem[6]. Internet má decentralizovanou architekturu bez centrální struktury a je spravován různými zúčastněnými stranami. Podařilo se mu udržet exponenciální nárůst objemu provozu, zatímco je neustálým cílem zákeřných pokusů o narušení[7]. Zároveň se zvyšuje závislost na základních funkcích globálního a otevřeného internetu, jako je systém doménových jmen (DNS), a základní internetové služby pro komunikaci a hostování, aplikace a data. Tyto služby se stále více soustředí do rukou několika soukromých společností[8]. Evropská ekonomika a společnost jsou v důsledku toho zranitelné vůči rušivým geopolitickým nebo technickým událostem, které ovlivňují jádro internetu nebo jednu či více těchto společností. Zvýšené používání internetu a měnící se vzorce v důsledku pandemie dále odhalily křehkost dodavatelských řetězců, které závisí na této digitální infrastruktuře.

Obavy o bezpečnost jsou velkou překážkou používání on-line služeb[9]. Přibližně dvě pětiny uživatelů v EU zažily problémy související s bezpečností a tři pětiny mají dojem, že se nedokážou chránit před kyberkriminalitou[10]. Třetina uživatelů se za poslední tři roky setkala s podvodnými e-maily nebo telefonními hovory žádajícími o osobní údaje, 83 % z nich však kyberkriminalitu nikdy nenahlásilo. Každý osmý podnik byl zasažen kybernetickými útoky[11]. Více než polovina podnikových a spotřebitelských osobních počítačů, které jsou jednou infikovány malwarem, je opakovaně infikována ve stejném roce[12]. Každý rok se z důvodu porušení zabezpečení dat ztratí stovky milionů záznamů; průměrné náklady při narušení zabezpečení u jednoho podniku vzrostly v roce 2018 na více než 3,5 milionu EUR[13]. Dopad

---

[6] Světové ekonomické fórum, Zpráva o globálních rizicích z roku 2020.

[7] Podle Organizace pro hospodářskou spolupráci a rozvoj vedla pandemie k 60% nárůstu internetového provozu; https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/. Sdružení evropských regulačních orgánů v oblasti elektronických komunikací a Komise pravidelně zveřejňují zprávy o stavu kapacity internetu během opatření omezujících pohyb v souvislosti s koronavirem. Podle zprávy agentury ENISA došlo během třetího čtvrtletí roku 2019 k nárůstu celkového počtu útoků distribuovaným odmítnutím služby (DDoS) o 241 % ve srovnání s třetím čtvrtletím roku 2018. Útoky DDoS získávají na intenzitě, přičemž historicky největší útok proběhl v únoru 2020 a dosáhl maximálního provozu 2,3 terabitů za sekundu. Při „výpadku CenturyLink“ v srpnu 2020 vedl problém směrování u amerického poskytovatele internetových služeb k 3,5% poklesu globálního webového provozu; 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; 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 digitální ekonomiky a společnosti pro 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] Tisková zpráva Eurostatu, „ICT security measures taken by vast majority of enterprises in the EU“, 6/2020 – 13. ledna 2020. „Cyberattacks on critical infrastructure have become the new normal across sectors such as energy, healthcare and transportation“; Světové ekonomické fórum, Zpráva o globálních rizicích z roku 2020.

[12] Zdroj: Comparitech.

[13] Výroční zpráva o nákladech spojených s narušením bezpečnosti dat, 2020, Ponemon Institute a na základě kvantitativní analýzy 524 nedávných narušení v 17 zeměpisných oblastech a 17 průmyslových odvětvích:

kybernetického útoku často nelze izolovat a jeho důsledkem mohou být řetězové reakce v celé ekonomice a společnosti, které ovlivní miliony jednotlivců[14].

Vyšetřování téměř všech druhů trestné činnosti má digitální složku. V roce 2019 bylo oznámeno, že se počet incidentů meziročně ztrojnásobil. Odhaduje se, že existuje 700 milionů nových vzorků malwaru, který je nejčastějším prostředkem na podporu kybernetických útoků[15]. Roční náklady spojené s kybernetickou kriminalitou v globální ekonomice v roce 2020 se odhadují na 5,5 bilionu EUR, což je dvojnásobek oproti roku 2015[16]. To představuje největší přesun ekonomického bohatství v historii, větší než celosvětový obchod s drogami. U významného případu, jímž byl ransomwarový útok WannaCry v roce 2017, se náklady v globální ekonomice odhadovaly na více než 6,5 miliardy EUR[17].

Digitální služby a finanční sektor patří spolu s veřejným sektorem a výrobním průmyslem k nejčastějším cílům kybernetických útoků, avšak odborná způsobilost v oblasti kybernetické bezpečnosti a povědomí o tomto tématu zůstávají mezi podniky a jednotlivci nízké[18] a pracovní síly mají velké nedostatky v dovednostech v oblasti kybernetické bezpečnosti[19]. V roce 2019 došlo k téměř 450 incidentům v oblasti kybernetické bezpečnosti, které se týkaly evropských kritických infrastruktur, jako jsou finance a energetika[20]. Během pandemie byly obzvláště tvrdě zasaženy zdravotnické organizace společně s odborníky. Jelikož technologie jsou od fyzického světa neoddělitelné, ohrožují kybernetické útoky životy a blaho těch nejzranitelnějších[21]. Více než dvě třetiny společností, zejména malých a středních podniků, jsou v oblasti kybernetické bezpečnosti považovány za „nováčky“ a evropské společnosti jsou považovány za méně připravené než společnosti v Asii a Americe[22]. Odhaduje se, že v Evropě zůstává neobsazeno 291 000 pracovních míst pro odborníky v oblasti kybernetické bezpečnosti. Najímání a odborná příprava odborníků na kybernetickou bezpečnost je pomalý proces vedoucí k větším rizikům pro organizace v oblasti kybernetické bezpečnosti[23].

---

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

[14] Zpráva Společného výzkumného střediska (JRC), „Kybernetická bezpečnost – naše digitální 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 bezpečnost – naše digitální opora“.

[17] Zdroj: Cyence.

[18] Povědomí podniků zůstává nízké i v souvislosti s kybernetickými krádežemi obchodního tajemství, zejména mezi malými a středními podniky. PwC, The scale and impact of industrial espionage and theft of trade secrets through cyber: Dissemination report on measures to tackle and prevent cyber-theft of trade secrets, 2018. (Studie společnosti PwC, Rozsah průmyslové špionáže a krádeže obchodních tajemství v kyberprostoru a jejich dopad: zpráva o šíření informací o opatřeních pro boj proti kybernetickým krádežím obchodního tajemství a pro předcházení těmto krádežím, 2018.)

[19] Viz zpráva agentury ENISA o typech ohrožení pro rok 2020. Dále rovněž Verizon Data Breach Investigations Report 2020; https://enterprise.verizon.com/resources/reports/dbir/

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

[21] Ransomware je využíván k zaměření na nemocnice a zdravotní záznamy, jak k tomu došlo např. v Rumunsku (červen 2020), v Düsseldorfu (září 2020) a ve Vastaamu (říjen 2020).

[22] PwC, The Global State of Information Security 2018; ESI Thoughtlab, The Cybersecurity Imperative, 2019.

[23] Agentura EU pro kybernetickou bezpečnost, Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees and ENISA’s Higher Education Database, prosinec 2019.

EU chybí kolektivní znalost situace ohledně kybernetických hrozeb. Je tomu tak proto, že vnitrostátní orgány systematicky neshromažďují a nesdílejí informace (například ty, které jsou k dispozici od soukromého sektoru), které by mohly pomoci posoudit stav kybernetické bezpečnosti v EU. Ze strany členských států je hlášen jen zlomek incidentů a sdílení informací není systematické ani komplexní[24]; je možné, že kybernetické útoky jsou pouze jedním aspektem koordinovaných nepřátelských útoků proti evropským společnostem. Mezi členskými státy v současné době existuje pouze omezená vzájemná operační pomoc a mezi členskými státy a orgány, agenturami a orgány EU není zaveden žádný operační mechanismus pro případ rozsáhlých přeshraničních kybernetických incidentů nebo krizí[25].

Zlepšení kybernetické bezpečnosti je tedy zásadní pro to, aby lidé mohli důvěřovat inovacím, konektivitě a automatizaci, využívat je a mít z nich prospěch, a pro ochranu základních práv, včetně práv na soukromí a na ochranu osobních údajů, svobody projevu a informací. Kybernetická bezpečnost je nepostradatelná pro síťovou konektivitu a globální a otevřený internet, které musí podpořit transformaci ekonomiky a společnosti ve 20. letech 21. století. Přispívá k lepším dovednostem a většímu počtu pracovních míst, flexibilnějším pracovištím, efektivnějším a udržitelnějším odvětvím dopravy a zemědělství a snadnějšímu a spravedlivějšímu přístupu ke zdravotnickým službám. Je rovněž zásadní pro přechod na čistější energii v rámci Zelené dohody pro Evropu[26] prostřednictvím přeshraničních sítí a inteligentních měřičů a zamezení zbytečné duplikaci při ukládání dat. Navíc je nezbytná pro mezinárodní bezpečnost a stabilitu a pro rozvoj ekonomik, demokracií a společností na celém světě. Vládní instituce, podniky a jednotlivci proto musí používat digitální nástroje odpovědně a s vědomím dopadu na bezpečnost. Povědomí o kybernetické bezpečnosti a kybernetická hygiena musí být základem digitální transformace každodenních činností.

Nová strategie EU pro kybernetickou bezpečnost pro digitální dekádu tvoří klíčovou součást formování digitální budoucnosti Evropy[27], plánu Komise na podporu oživení pro Evropu[28], strategie bezpečnostní unie na období 2020–2025[29], globální strategie zahraniční a bezpečnostní politiky EU[30] a strategické agendy Evropské rady 2019–2024[31]. Stanoví, jak bude EU chránit své občany, podniky a instituce před kybernetickými hrozbami, jak bude podporovat mezinárodní spolupráci a stát v čele při zajišťování globálního a otevřeného internetu.

II. MYSLET GLOBÁLNĚ, JEDNAT EVROPSKY

Tato strategie si klade za cíl zajistit globální a otevřený internet se silnou ochranou k řešení rizik pro bezpečnost a základní práva a svobody lidí v Evropě. V návaznosti na pokrok dosažený v rámci předchozích strategií obsahuje konkrétní návrhy na zavedení **tří hlavních nástrojů – regulačních, investičních a politických** – k řešení **tří oblastí činnosti EU 1) odolnosti, technologické suverenity a vedoucího postavení, 2) budování operační**

[24] Členské státy jsou povinny poskytovat skupině pro spolupráci v oblasti bezpečnosti sítí a informací souhrnnou výroční zprávu o oznámeních přijatých podle čl. 10 odst. 3 směrnice o bezpečnosti sítí a informačních systémů (směrnice (EU) 2016/1148).
[25] Pro vzájemnou pomoc mezi členy sítě sdružující týmy CSIRT jsou zavedeny standardní operační postupy.
[26] Zelená dohoda pro Evropu, COM(2019) 640 final.
[27] Formování digitální budoucnosti Evropy, COM(2020) 67 final.
[28] Chvíle pro Evropu: náprava škod a příprava na příští generaci, COM (2020) 98 final.
[29] Strategie bezpečnostní unie EU 2020–2025, COM(2020) 605 final.
[30] https://eeas.europa.eu/topics/eu-global-strategy_en
[31] https://www.consilium.europa.eu/cs/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/#

kapacity s cílem předcházet, odrazovat a reagovat a 3) prosazování globálního a otevřeného kyberprostoru. EU je odhodlána podporovat tuto strategii prostřednictvím **bezprecedentní úrovně investic do digitální transformace EU v příštích sedmi letech** (která může být potenciálně čtyřikrát vyšší než předchozí úrovně) v rámci nových technologických a průmyslových politik a programu oživení[32].

Kybernetickou bezpečnost je třeba začlenit do všech těchto digitálních investic, zejména do klíčových technologií, jako je umělá inteligence (UI), šifrování a kvantová výpočetní technika, a to s využitím pobídek, závazků a měřítek. To může stimulovat růst evropského odvětví kybernetické bezpečnosti a poskytnout jistotu potřebnou k usnadnění postupného vyřazování starších systémů. Evropský obranný fond bude podporovat evropská řešení kybernetické obrany jako součást evropské obranné technologické a průmyslové základny. Kybernetická bezpečnost je součástí externích finančních nástrojů na podporu našich partnerů, zejména nástroje pro sousedství a rozvojovou a mezinárodní spolupráci. Prevence zneužití technologií, ochrana kritické infrastruktury a zajištění integrity dodavatelských řetězců také umožňuje EU dodržovat normy, pravidla a zásady odpovědného chování státu podle OSN[33].

1. ODOLNOST, TECHNOLOGICKÁ SUVERENITA A VEDOUCÍ POSTAVENÍ

Kritická infrastruktura a základní služby EU jsou stále více vzájemně závislé a digitalizované. Všechny předměty připojené k internetu v EU, ať už jsou to automatizované automobily, průmyslové řídicí systémy nebo domácí spotřebiče, a celé dodavatelské řetězce, které je zpřístupňují, musí být bezpečné již od fáze návrhu, odolné vůči kybernetickým incidentům a musí být rychle opravitelné v případě zjištění zranitelných míst. To je zásadní pro zajištění toho, aby soukromý a veřejný sektor v EU měl možnost vybrat si z nejbezpečnějších infrastruktur a služeb. Nadcházející desetiletí je pro EU příležitostí zaujmout vedoucí postavení ve vývoji bezpečných technologií v celém dodavatelském řetězci. Zajištění odolnosti a větších průmyslových a technologických kapacit v oblasti kybernetické bezpečnosti by mělo zmobilizovat všechny nezbytné regulační, investiční a politické nástroje. Kybernetická bezpečnost již od fáze návrhu pro průmyslové procesy, operace a zařízení může zmírnit rizika, potenciálně snížit náklady pro podniky i pro společnost, a tím zvýšit odolnost.

1.1 Odolná infrastruktura a kritické služby

Pravidla EU **týkající se bezpečnosti sítí a informačních systémů (NIS)** jsou jádrem jednotného trhu pro kybernetickou bezpečnost. Komise navrhuje změnit tato pravidla v rámci revidované směrnice o bezpečnosti sítí a informačních systémů s cílem zvýšit úroveň **kybernetické odolnosti všech příslušných odvětví, veřejných i soukromých, která plní důležitou funkci pro hospodářství a společnost[34].** Přezkum je nezbytný, aby se omezily

[32] Investice do celého dodavatelského řetězce digitálních technologií, které přispívají k digitální transformaci nebo k řešení výzev, které z ní vyplývají, by měly činit nejméně 20 % (což odpovídá 134,5 miliardám EUR) z facility na podporu oživení a odolnosti disponující rozpočtem 672,5 miliard EUR sestávajícím z grantů a půjček. Financování EU ve víceletém finančním rámci na období 2021–2027 předpokládané pro kybernetickou bezpečnost v rámci programu Digitální Evropa a pro výzkum v oblasti kybernetické bezpečnosti v rámci programu Horizont Evropa, se zvláštním zaměřením na podporu malých a středních podniků, by mohlo činit celkem 2 miliardy EUR plus investice ze strany členských států a průmyslu.

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

[34] [*vložit odkaz na návrh směrnice o bezpečnost sítí a informací*]

nesrovnalosti na vnitřním trhu sladěním požadavků na rozsah, bezpečnost a hlášení incidentů, vnitrostátního dohledu a prosazování práva a schopností příslušných orgánů.

Přepracovaná směrnice o bezpečnosti sítí a informací poskytne základ pro konkrétnější pravidla, která jsou rovněž nezbytná pro strategicky důležitá odvětví, včetně energetiky, dopravy a zdravotnictví. S cílem zajistit důsledný přístup oznámený v rámci strategie bezpečnostní unie na období 2020–2025 je přepracovaná směrnice navrhována spolu s přezkumem právních předpisů o odolnosti kritické infrastruktury[35]. Energetické technologie zahrnující digitální komponenty jsou spolu s bezpečností přidružených dodavatelských řetězců důležité pro kontinuitu základních služeb a pro strategické řízení kritické energetické infrastruktury. Komise proto navrhne opatření, včetně „kodexu sítě“, která stanoví pravidla pro kybernetickou bezpečnost přeshraničních toků elektřiny a která by měla být přijata do konce roku 2022. Finanční sektor musí rovněž posílit digitální provozní odolnost a zajistit schopnost odolat všem druhům narušení a hrozeb souvisejících s IKT, jak navrhla Komise[36]. V oblasti dopravy přidala Komise do právních předpisů EU o ochraně letectví před protiprávními činy ustanovení o kybernetické bezpečnosti[37] a bude pokračovat ve svém úsilí o zvýšení kybernetické odolnosti ve všech druzích dopravy. Posílení kybernetické odolnosti demokratických procesů a institucí je klíčovou součástí evropského akčního plánu pro demokracii zaměřeného na zajištění a podporu svobodných voleb a demokratické diskuse a plurality médií[38]. A konečně, pokud jde o bezpečnost infrastruktury a služeb v rámci budoucího vesmírného programu, bude Komise pokračovat v prohlubování strategie kybernetické bezpečnosti systému Galileo pro příští generaci služeb globálního navigačního satelitního systému a dalších nových složek vesmírného programu[39].

1.2 Budování evropského kybernetického štítu

S rozšiřováním konektivity a rostoucí sofistikovaností kybernetických útoků plní střediska pro sdílení a analýzu informací (ISAC) cennou funkci, a to i na odvětvové úrovni, jelikož umožňují výměnu informací o kybernetických hrozbách mezi různými zúčastněnými stranami[40]. Kromě toho sítě a počítačové systémy vyžadují neustálé monitorování a analýzu k odhalení neoprávněných vniknutí a neobvyklých chyb v reálném čase. Mnoho soukromých společností, veřejných organizací a vnitrostátních orgánů proto založilo skupiny pro reakce na počítačové bezpečnostní incidenty (týmy CSIRT) a bezpečnostní operační střediska neboli „SOC“.

Bezpečnostní operační střediska jsou zásadní pro shromažďování protokolů[41] a izolování podezřelých událostí, ke kterým dochází v jimi monitorovaných komunikačních sítích. Činí tak prostřednictvím identifikace signálu a vzorců a získávání znalostí o hrozbách z velkého množství dat, která je třeba vyhodnotit. Přispívají ke zjišťování aktivit škodlivých

[35] [vložit odkaz na *návrh* směrnice o odolnosti kritických subjektů]
[36] Návrh nařízení o digitální provozní odolnosti ve finančním sektoru, kterým se mění nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014 a (EU) č. 909/2014, COM/2020/595 final.
[37] Prováděcí nařízení Komise 2019/1583.
[38] Sdělení o evropském akčním plánu pro demokracii COM(2020) 790. V rámci plánu evropské sítě pro spolupráci při volbách budou volební sítě členských států podporovat nasazení společných týmů odborníků s cílem čelit hrozbám (včetně kybernetických hrozeb) při volebních procesech; https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en
[39] To zahrnuje novou družicovou komunikaci v rámci státní správy (GOVSATCOM) a kosmické smetí (SST)
[40] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing
[41] Takovým způsobem, aby je donucovací a soudní orgány mohly použít jako důkaz.

spustitelných souborů a následně pomáhají omezit kybernetické útoky. Práce vyžadovaná v těchto střediscích je velmi náročná a probíhá rychlým tempem, proto může umělá inteligence a zejména techniky strojového učení poskytnout provozovatelům neocenitelnou podporu[42].

Komise navrhuje vybudovat **síť bezpečnostních operačních středisek po celé EU**[43] a podporovat zdokonalování stávajících středisek a zakládání nových. Bude rovněž podporovat odbornou přípravu a rozvoj dovedností zaměstnanců provozujících tato střediska. Na základě analýzy potřeb provedené s příslušnými zúčastněnými stranami a podporované Agenturou EU pro kybernetickou bezpečnost (ENISA) by mohla vyčlenit více než 300 milionů EUR na podporu veřejného a soukromého sektoru a přeshraniční spolupráce při vytváření vnitrostátních a odvětvových sítí, do nichž budou zapojeny rovněž malé a střední podniky a které budou založeny na odpovídající správě, sdílení dat a bezpečnostních opatřeních.

Komise vyzývá členské státy, aby se podílely na investicích do tohoto projektu. Střediska by pak byla schopna efektivněji sdílet zjištěné signály a dávat je do souvislostí a vytvářet vysoce kvalitní informace o hrozbách, které by mohly být sdíleny se středisky ISAC a vnitrostátními orgány, což by umožnilo ucelenější znalost situace. Cílem by bylo fázově propojit co nejvíce středisek v celé EU za účelem vytváření kolektivních znalostí a sdílení osvědčených postupů. Těmto střediskům bude poskytnuta podpora s cílem zlepšit zjišťování, analýzu a rychlosti odezvy na incidenty prostřednictvím nejmodernější umělé inteligence a schopností strojového učení, která bude doplněna o superpočítačovou infrastrukturu vyvinutou v EU evropským společným podnikem pro vysoce výkonnou výpočetní techniku[44].

Díky trvalé spolupráci a společné činnosti bude tato síť poskytovat včasná varování o kybernetických bezpečnostních incidentech orgánům a všem zúčastněným stranám, včetně společné kybernetické jednotky (viz oddíl 2.1). **Bude sloužit jako skutečný štít kybernetické bezpečnosti pro EU** a poskytne pevnou síť pozorovatelen schopných odhalit případné hrozby dříve, než budou moci způsobit rozsáhlé škody.

1.3 Vysoce bezpečná komunikační infrastruktura

Program s názvem Družicová komunikace v rámci státní správy Evropské unie (GOVSATCOM)[45], součást vesmírného programu, poskytne bezpečné a nákladově efektivní schopnosti pro vesmírnou komunikaci misím a operacím kritickým z hlediska zajištění a bezpečnosti, které řídí EU a její členské státy, včetně vnitrostátních bezpečnostních aktérů a orgánů a agentur EU.

Členské státy se zavázaly spolupracovat s Komisí na zavedení zabezpečené kvantové komunikační infrastruktury pro Evropu[46]. Kvantová komunikační infrastruktura nabídne

[42]Zdroj: průzkum Ponemon Institute Research, „Improving the Effectiveness of the SOC, 2019“; studie o využívání umělé inteligence v bezpečnostních operačních střediscích viz například: Khraisat, A., Gondal, I., Vamplew, P. a kol., Survey of intrusion detection systems: techniques, datasets and challenges, *Cybersecur* 2**,** 20 (2019).

[43]Budou vypracována podrobnější opatření pro správu, provozní zásady a financování těchto středisek a ohledně způsobu, jak budou doplňovat stávající struktury, jako jsou centra pro digitální inovace.

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

[45]Program GOVSATCOM je součástí vesmírného programu Unie

[46]Prohlášení EuroQCI dosud podepsala většina členských států, přičemž vývoj a rozmístění infrastruktury proběhne v letech 2021–2027 s financováním z programů Horizont Evropa a Digitální Evropa a z Evropské kosmické agentury, s výhradou příslušných ujednání o správě; https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network

orgánům veřejné správy zcela nový způsob přenosu důvěrných informací pomocí maximálně bezpečné formy šifrování na ochranu proti kybernetickým útokům, která je vytvořena s využitím evropské technologie. Bude mít dvě hlavní součásti: stávající pozemní komunikační sítě s optickými vlákny spojující strategická místa na vnitrostátní a přeshraniční úrovni a propojené vesmírné družice pokrývající celou EU, včetně jejích zámořských území[47]. Tato iniciativa zaměřená na vývoj a zavádění nových a bezpečnějších forem šifrování a na navrhování nových způsobů ochrany důležitých komunikačních a datových aktiv může pomoci udržet citlivé informace (a tím i kritickou infrastrukturu) v bezpečí.

Z tohoto pohledu a s výhledem do budoucna Komise prozkoumá možné zavedení zabezpečeného systému připojení na víceoběžných drahách. V návaznosti na program GOVSATCOM a kvantovou komunikační infrastrukturu by tento systém integroval nejmodernější technologie (kvantovou technologii, 5G, AI, edge computing) dodržující nejpřísnější rámec pro kybernetickou bezpečnost s cílem podporovat služby bezpečné již od fáze návrhu, jako je spolehlivé, bezpečné a nákladově efektivní připojení a šifrovaná komunikace pro kritické vládní činnosti.

1.4 Zabezpečení nové generace širokopásmových mobilních sítí

Občané EU a společnosti využívající pokročilé a inovativní aplikace umožněné **sítí 5G a příštími generacemi sítí** by měly těžit z nejvyššího standardu zabezpečení. Členské státy společně s Komisí a s podporou agentury ENISA zavedly v podobě souboru nástrojů EU pro sítě 5G[48] z ledna 2020 komplexní a objektivní přístup ke kybernetické bezpečnosti sítí 5G založený na posouzení rizik, který vychází z posouzení možných plánů zmírnění dopadů a identifikaci nejúčinnějších opatření. Kromě toho EU konsoliduje své schopnosti v oblasti 5G a dalších sítí, aby zabránila závislostem a podpořila udržitelný a rozmanitý dodavatelský řetězec.

V prosinci 2020 zveřejnila Komise zprávu o dopadech doporučení ze dne 26. března 2019 na kybernetickou bezpečnost sítí 5G[49]. Ukázalo se, že od doby, kdy byl schválen soubor nástrojů, bylo dosaženo značného pokroku a že většina členských států je na cestě k dokončení významné části provádění souboru nástrojů v blízké budoucnosti, i když s určitými odchylkami a zbývajícími mezerami, které již byly určeny ve zprávě o pokroku zveřejněné v červenci 2020[50].

V říjnu 2020 Evropská rada vyzvala EU a členské státy, aby „plně využívaly soubor nástrojů pro kybernetickou bezpečnost sítí 5G“ a „uplatňovaly příslušná omezení na vysoce rizikové

[47]Rozvoj vesmírné složky je nezbytný k dosažení dvoubodových spojení (> 1 000 km), které pozemní infrastruktura nemůže podporovat. Využitím vlastností kvantové mechaniky kvantová komunikační infrastruktura zpočátku umožní stranám bezpečně sdílet náhodné tajné klíče, které se použijí k šifrování a dešifrování zpráv. Rovněž bude zahrnovat zavedení testovací infrastruktury kontrolující dodržování předpisů pro hodnocení souladu evropských kvantových komunikačních zařízení a systémů s kvantovou komunikační infrastrukturou a jejich certifikaci a validaci před jejich začleněním do kvantové komunikační infrastruktury. Bude navržena tak, aby podporovala další aplikace, jakmile dosáhnou potřebné úrovně technologické vyspělosti. Aktuální pilotní projekt OpenQKD (https://openqkd.eu/) je předchůdcem této testovací infrastruktury pro kontrolu dodržování předpisů.

[48]Sdělení s názvem Bezpečné zavádění sítí 5G v EU – Implementace souboru opatření EU, COM(2020) 50.

[49] Zpráva Komise o dopadech doporučení Komise ze dne 26. března 2019 o kybernetické bezpečnosti sítí 5G, 15. prosinec 2020.

[50]Zpráva skupiny pro spolupráci v oblasti bezpečnosti sítí a informací o provádění souboru nástrojů ze dne 24. července 2020.

dodavatele pro klíčová aktiva definovaná jako kritická a citlivá v koordinovaném posouzení rizik EU na základě společných objektivních kritérií“[51].

S výhledem do budoucna by EU a její členské státy měly zajistit, aby byla zjištěná rizika přiměřeně a koordinovaně zmírňována, zejména pokud jde o cíl minimalizace expozice vysoce rizikovým dodavatelům a zamezení závislosti na těchto dodavatelích na vnitrostátní i unijní úrovni, a aby byl zohledněn jakýkoli nový významný vývoj nebo riziko. Komise vyzývá členské státy, aby při svých investicích do digitálních kapacit a konektivity plně využívaly soubor nástrojů.

Na základě zprávy o dopadech doporučení z roku 2019 Komise vyzývá členské státy, aby urychlily práci na dokončení provádění hlavních opatření v rámci souboru nástrojů do druhého čtvrtletí roku 2021. Rovněž vyzývá členské státy, aby společně sledovaly dosažený pokrok a zajistily další sladění přístupů. Na úrovni EU budou za účelem podpory tohoto procesu sledovány tři hlavní cíle: zajištění dalšího sbližování přístupů ke zmírňování rizik v celé EU, podpora nepřetržité výměny znalostí a budování kapacit a podpora odolnosti dodavatelského řetězce a dalších strategických cílů EU v oblasti bezpečnosti. Konkrétní opatření týkající se těchto klíčových cílů jsou uvedena ve zvláštním dodatku tohoto sdělení.

Komise bude i nadále úzce spolupracovat s členskými státy na plnění těchto cílů a kroků s podporou agentury ENISA (viz příloha).

Přístup EU v podobě souboru nástrojů pro sítě 5G navíc zvýšil zájem v zemích mimo EU, které v současné době rozvíjejí své přístupy k zabezpečení svých komunikačních sítí. Útvary Komise jsou spolu s Evropskou službou pro vnější činnost a sítí delegací EU připraveny poskytnout na požádání další informace o svém komplexním, objektivním a na riziku založeném přístupu orgánům po celém světě.

1.5 Internet zabezpečených věcí

Každý předmět připojený k internetu obsahuje chyby zabezpečení, které lze zneužít s potenciálně rozsáhlými následky. Pravidla vnitřního trhu zahrnují záruky proti nezabezpečeným výrobkům a službám. Komise již pracuje na zajištění **transparentních bezpečnostních řešení a certifikace podle aktu o kybernetické bezpečnosti** a na podpoře bezpečných produktů a služeb, aniž by byla ohrožena výkonnost[52]. V prvním čtvrtletí roku 2021 přijme svůj první průběžný pracovní program Unie (bude aktualizován nejméně jednou za tři roky), který umožní, aby se průmysl, vnitrostátní orgány a normalizační orgány mohly předem připravit na budoucí evropské systémy certifikace kybernetické bezpečnosti[53]. Jak se internet věcí rozrůstá, vynutitelná pravidla vyžadují posílení, a to jak k zajištění celkové odolnosti, tak k podpoře kybernetické bezpečnosti.

[51]EUCO 13/20, zvláštní jednání Evropské rady (1. a 2. října 2020) – závěry.

[52]Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“). Akt o kybernetické bezpečnosti podporuje certifikaci IKT na úrovni EU, přičemž evropský rámec pro certifikaci kybernetické bezpečnosti slouží k vytvoření dobrovolných evropských systémů certifikace kybernetické bezpečnosti za účelem zajištění odpovídající úrovně kybernetické bezpečnosti pro produkty IKT, služby IKT a procesy IKT v Unii a také ke snížení fragmentace vnitřního trhu, pokud jde o systémy certifikace kybernetické bezpečnosti v Unii. „Ratingové“ společnosti v oblasti kybernetické bezpečnosti zároveň obvykle sídlí mimo EU a vyznačují se omezenou transparentností a dohledem; https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings

[53]Ve smyslu požadavků čl. 47 odst. 5 aktu o kybernetické bezpečnosti.

Komise zváží komplexní přístup, včetně možných **nových horizontálních pravidel ke zlepšení kybernetické bezpečnosti všech produktů připojených k internetu a souvisejících služeb uváděných na vnitřní trh**[54]. Tato pravidla by mohla zahrnovat **novou povinnost řádné péče pro výrobce zařízení připojených k internetu** ohledně řešení chyb zabezpečení softwaru, včetně pokračování aktualizací softwaru a zabezpečení, jakož i zajištění vymazání osobních a jiných citlivých údajů na konci životnosti. Tato pravidla posílila iniciativu „právo na opravu zastaralého softwaru“ představenou v akčním plánu pro oběhové hospodářství a doplnila by probíhající opatření zaměřená na konkrétní typy produktů, jako jsou povinné požadavky navrhované pro přístup určitých bezdrátových výrobků na trh (prostřednictvím přijetí aktu v přenesené pravomoci v rámci směrnice o rádiových zařízeních[55]), a cíl zavést pravidla kybernetické bezpečnosti pro motorová vozidla, a to u všech nových typů vozidel od července 2022[56]. Kromě toho by se opírala o navrhovanou revizi obecných pravidel pro bezpečnost výrobků, která přímo neřeší aspekty kybernetické bezpečnosti[57].

1.6 Větší globální internetová bezpečnost

Soubor základních protokolů a podpůrné infrastruktury zajišťují funkčnost a integritu internetu po celém světě[58]. Tento soubor zahrnuje systém DNS a jeho hierarchický a delegovaný systém zón, počínaje kořenovou zónou a třinácti kořenovými servery DNS[59] v horní části hierarchie, na kterých závisí síť WWW. Komise má v úmyslu vypracovat **pohotovostní plán podporovaný financováním EU pro řešení extrémních scénářů ovlivňujících integritu a dostupnost globálního kořenového systému DNS**. Bude spolupracovat s agenturou ENISA, členskými státy, dvěma provozovateli kořenových serverů DNS v EU[60] a komunitou mnoha zúčastněných stran, aby vyhodnotila úlohu těchto provozovatelů při zajišťování toho, že internet zůstane za všech okolností globálně přístupný.

Aby měl klient přístup ke zdroji pod určitým doménovým jménem na internetu, musí být jeho požadavek (obvykle pro Uniform Resource Locator, neboli adresu URL) přeložen nebo „rozlišen“ do podoby adresy IP pomocí odkazu na jmenné servery DNS. Lidé a organizace v EU se však stále více spoléhají na několik veřejných resolverů (překladačů) DNS provozovaných subjekty mimo EU. V důsledku takové konsolidace služby rozlišení DNS v rukou několika společností[61] je samotný proces rozlišení zranitelný v případě významných

[54]Závěry Rady požadují horizontální opatření v oblasti kybernetické bezpečnosti zařízení připojených k internetu; 13629/20, 2. prosince 2020.
[55]Směrnice 2014/53/EU
[56] Řídí se nařízením OSN přijatým v červnu 2020; http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf
[57]Revize současných obecných pravidel bezpečnosti výrobků (směrnice 2001/95/ES); navrhovaná upravená pravidla jsou plánována také v oblasti odpovědnosti výrobců v digitálním kontextu v rámci regulačního rámce odpovědnosti EU.
[58]„Veřejné jádro otevřeného internetu, tedy hlavní protokoly a infrastruktura, jež jsou globálním veřejným statkem, zajišťuje základní funkci internetu jako celku a je základem pro jeho běžný provoz. Agentura ENISA by měla podpořit bezpečnost veřejného jádra otevřeného internetu a stabilitu jeho fungování, včetně klíčových protokolů (zejména DNS, BGP a IPv6), provozu systému doménových jmen (včetně provozu všech domén na vrcholné úrovni) a provozu root zone“; 23. bod odůvodnění aktu o kybernetické bezpečnosti.
[59]https://www.iana.org/domains/root/servers
[60]Servery i.root provozované společností Netnod ve Švédsku a servery k.root provozované společností RIPE NCC v Nizozemsku.
[61]Consolidation in the DNS resolver market – how much, how fast, how dangerous? (), Evidence of decreasing Internet entropy – the lack of redundancy in DNS resolution by major websites and services ()

událostí, které postihnou jednoho významného poskytovatele, a ztěžuje orgánům EU řešení možných zákeřných kybernetických útoků a velkých geopolitických a technických incidentů[62].

S cílem omezit bezpečnostní problémy spojené s koncentrací trhu bude Komise podporovat příslušné zúčastněné strany včetně společností z EU, poskytovatelů internetových služeb a prodejců prohlížečů, aby přijali strategii diverzifikace rozlišení DNS. Komise rovněž hodlá přispět k zabezpečenému připojení k internetu podporou rozvoje veřejné **evropské služby pro překlad DNS**. Tato iniciativa „DNS4EU" nabídne alternativní evropskou službu pro přístup na globální internet. Služba DNS4EU bude transparentní, bude odpovídat nejnovějšímu zabezpečení, ochraně dat a soukromí dané již samotným návrhem a obvyklým standardům a pravidlům a bude součástí Evropské průmyslové aliance pro data a cloud[63].

Komise rovněž ve spolupráci s členskými státy a průmyslovým odvětvím **urychlí zavádění klíčových internetových standardů včetně IPv6[64] a zavedených standardů zabezpečení internetu a osvědčených postupů pro zabezpečení DNS, směrování a e-mailů[65]**, nevyjímaje regulační opatření, jako je evropská doložka o skončení platnosti pro standard IPv4. za účelem řízení trhu, pokud k jejich přijetí nebude učiněn dostatečný pokrok. EU by měla prosazovat (například v rámci strategie EU–Afrika[66]) provádění těchto standardů v partnerských zemích jako způsob podpory rozvoje globálního a otevřeného internetu a boje proti uzavřeným a modelům internetu založeným na kontrole. Nakonec Komise zváží potřebu mechanismu pro systematičtější sledování a shromažďování souhrnných údajů o internetovém provozu a pro poradenství ohledně možných narušení[67].

1.7 Posílená přítomnost v technologickém dodavatelském řetězci

Díky plánované finanční podpoře kyberneticky zabezpečené digitální transformace ve víceletém finančním rámci na období 2021–2027 má EU jedinečnou příležitost spojit svá aktiva s cílem podpořit svou průmyslovou strategii[68] a vedoucí postavení v oblasti digitálních technologií a kybernetické bezpečnosti v celém digitálním dodavatelském řetězci (včetně dat a cloudu, procesorových technologií nové generace, maximálně zabezpečené konektivity a sítí 6G), a to v souladu se svými hodnotami a prioritami. Intervence veřejného sektoru by se měla opírat o nástroje poskytované regulačním rámcem EU pro zadávání veřejných zakázek a významnými projekty společného evropského zájmu. Kromě toho může uvolnit soukromé investice prostřednictvím partnerství veřejného a soukromého sektoru (včetně navázání na zkušenosti se smluvním partnerstvím veřejného a soukromého sektoru pro kybernetickou

[62] Existují také důkazy poukazující na to, že údaje DNS lze použít pro účely profilování, což má dopad na práva na ochranu soukromí a údajů.

[63] Společné prohlášení: Budování cloudu nové generace pro podniky a veřejný sektor v EU; https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe

[64] zavádění protokolu IPv6 je nyní pokročilejší v souvislosti s vážným vyčerpáním nabídky a zvýšením nákladů na adresy IPv4. Zavádění IPv6 je však v celé EU nerovnoměrné.

[65] Mezi takové standardy patří DNSSEC, HTTPS, DNS přes HTTPS (DoH), DNS přes TLS (DoT), SPF, DKIM, / DMARC, STARTTLS, DANE a směrovací normy a osvědčené postupy, např. vzájemně dohodnuté normy pro zabezpečení směrování (MANRS).

[66] Společné sdělení „Na cestě ke komplexní strategii pro Afriku" (JOIN(2020) 4 final) ze dne 9. března 2020.

[67] Takové „středisko pro sledování internetu" by mohlo spadat do rámce činností Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost; návrh nařízení, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center, COM(2018) 630.

[68] Sdělení Nová průmyslová strategie pro Evropu, COM/2020/102 final.

bezpečnost a jeho prováděním prostřednictvím Evropské organizace pro kybernetickou bezpečnost), rizikového kapitálu na podporu malých a středních podniků nebo průmyslových aliancí a strategií v oblasti technologických kapacit.

Zvláštní důraz bude kladen také na nástroj pro technickou podporu[69] a nejlepší využití nejnovějších nástrojů kybernetické bezpečnosti ze strany malých a středních podniků – zejména těch, které nespadají do oblasti působnosti revidované směrnice o bezpečnosti sítí a informací – mimo jiné prostřednictvím specializovaných činností v rámci center pro digitální inovace v programu Digitální Evropa. Cílem je aktivovat podobnou částku investic ze strany členských států, která by měla doplnit investice ze strany průmyslu v rámci partnerství řízeného společně s členskými státy v navrhovaném **průmyslovém, technologickém a výzkumném centru kompetencí pro kybernetickou bezpečnost a síti koordinačních center (CCCN)**. Síť CCCN by prostřednictvím vstupů ze strany průmyslu a akademických komunit měla hrát klíčovou úlohu při rozvoji technologické suverenity EU v oblasti kybernetické bezpečnosti, budování kapacit pro zabezpečení citlivých infrastruktur, jako jsou sítě 5G, a snižování závislosti nejdůležitějších technologií na jiných částech světa.

Komise má v úmyslu, případně spolu se sítí CCCN, podpořit rozvoj specializovaného magisterského programu v oblasti kybernetické bezpečnosti a přispět ke společnému evropskému plánu pro výzkum a inovace v oblasti kybernetické bezpečnosti po roce 2020. Investice prostřednictvím sítě CCCN by se rovněž opíraly o spolupráci ve výzkumu a vývoji prováděnou sítěmi středisek excelence v oblasti kybernetické bezpečnosti, která by spojovala nejlepší evropské výzkumné týmy s průmyslem, a to s cílem navrhovat a provádět společné výzkumné programy v souladu s plánem Evropské organizace pro kybernetickou bezpečnost[70]. Komise se bude i nadále spoléhat na výzkumnou práci prováděnou Agenturou Evropské unie pro bezpečnost sítí a informací a Europolem a v rámci programu Horizont Evropa bude i nadále podporovat jednotlivé internetové inovátory vyvíjející a zvyšující ochranu osobních údajů a bezpečné komunikační technologie založené na softwaru a hardwaru s otevřeným zdrojovým kódem, jak je tomu v současné době v rámci iniciativy Internet nové generace.

1.8 Pracovní síla EU se znalostí kybernetické bezpečnosti

Úsilí EU o zvyšování kvalifikace pracovní síly, o rozvoj, přilákání a udržení nejlepších talentů v oblasti kybernetické bezpečnosti a o investice do špičkového výzkumu a inovací tvoří důležitou součást ochrany před kybernetickými hrozbami obecně. Tato oblast nabízí velký potenciál. Proto je třeba věnovat zvláštní pozornost rozvoji, přilákání a udržení rozmanitějších talentů. Revidovaný akční plán digitálního vzdělávání zvýší informovanost o kybernetické bezpečnosti mezi jednotlivci, zejména dětmi a mladými lidmi, a organizacemi, zejména malými a středními podniky[71]. Podpoří také účast žen ve vzdělávání v oblasti přírodních věd, technologií, inženýrských oborů a matematiky („STEM“) a zvyšování a změnu kvalifikace u pracovních míst v oblasti IKT se zaměřením na digitální dovednosti. Kromě toho Komise společně s Úřadem EU pro duševní vlastnictví v rámci Europolu, s agenturou ENISA, členskými státy a soukromým sektorem vypracuje nástroje pro zvyšování

[69] https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=COM%3A2020%3A0409%3AFIN# .
[70] https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies
[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_cs

povědomí a pokyny ke zvýšení odolnosti podniků v EU proti **krádežím duševního vlastnictví způsobeným kybernetickými útoky**[72].

Vzdělávání – včetně odborného vzdělávání a přípravy, povědomí a výcviku – by rovněž mělo dále zvyšovat dovednosti v oblasti kybernetické bezpečnosti a kybernetické obrany na úrovni EU. Za tímto účelem by příslušné subjekty EU, jako je agentura ENISA, Evropská obranná agentura (EDA), Evropská bezpečnostní a obranná škola (EBOŠ)[73], měly usilovat o součinnost mezi svými příslušnými činnostmi.

Strategické iniciativy

EU by měla zajistit:

- přijetí revidované směrnice o bezpečnosti sítí a informací,
- regulační opatření pro internet zabezpečených věcí,
- prostřednictvím investic sítě CCCN do kybernetické bezpečnosti (zejména prostřednictvím programu Digitální Evropa, Horizont Evropa a facility na podporu oživení) dosáhnout v letech 2021–2027 veřejných a soukromých investic až 4,5 miliardy EUR,
- síť bezpečnostních operačních středisek EU s umělou inteligencí a maximálně bezpečnou komunikační infrastrukturu využívající kvantové technologie,
- široké přijetí technologií kybernetické bezpečnosti prostřednictvím specializované podpory pro malé a střední podniky v rámci středisek pro digitální inovace,
- vývoj služby resolveru DNS na úrovni EU jako bezpečné a otevřené alternativy pro občany EU, podniky a veřejnou správu pro přístup na internet a
- dokončení provádění souboru nástrojů pro 5G do druhého čtvrtletí roku 2021 (viz příloha).

2. BUDOVÁNÍ PROVOZNÍCH KAPACIT V OBLASTI PREVENCE, ODSTRAŠOVÁNÍ A REAKCE

Kybernetické incidenty, ať už se jedná o nehody nebo úmyslné jednání pachatelů trestné činnosti, státních a jiných nestátních subjektů, mohou způsobit obrovské škody. Vzhledem k jejich rozsahu a složitosti (zahrnují často zneužívání služeb, hardwaru a softwaru třetích stran za účelem ohrožení konečné cíle) je bojovat proti prostředí kolektivních hrozeb pro EU obtížné bez systematického a komplexního sdílení informací a spolupráce na společné reakci. Cílem EU je **prostřednictvím plného provedení regulačních nástrojů, mobilizace a spolupráce** podporovat členské státy při ochraně jejich občanů, jakož i jejich hospodářských a národních bezpečnostních zájmů, při plném respektování základních práv a svobod a právního státu. Za předcházení kybernetickým hrozbám, odrazování a odstrašování od těchto hrozeb a reakci na ně odpovídá několik komunit, které se skládají ze sítí, orgánů, institucí a agentur EU, jakož i orgánů členských států a které používají svých příslušné nástroje a

[72] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2187

[73] Prostřednictvím platformy pro vzdělávání, odbornou přípravu, výcvik a hodnocení v oblasti kybernetické bezpečnosti (ETEE).

iniciativy[74]. Mezi tyto komunity patří: i) orgány pro bezpečnost sítí a informací, jako jsou skupiny pro reakce na počítačové bezpečnostní incidenty (týmy CSIRT), a reakce na katastrofy; ii) donucovací a soudní orgány; iii) kybernetická diplomacie a iv) kybernetická obrana.

2.1 Společná kybernetická jednotka

Společná kybernetická jednotka by sloužila jako virtuální a fyzická platforma pro spolupráci různých komunit působících v EU v oblasti kybernetické bezpečnosti se zaměřením na operativní a technickou koordinaci postupu proti závažným přeshraničním kybernetickým incidentům a hrozbám.

Společná kybernetická jednotka by byla důležitým krokem na cestě k dokončení **evropského rámce pro řešení kybernetických bezpečnostních krizí**. Jak je uvedeno v politických směrech předsedkyně Komise[75], jednotka by členským státům a orgánům, institucím a agenturám EU měla umožnit, aby plně využívaly stávající struktury, zdroje a schopnosti, a podporovat způsob myšlení založený na pochopení „**potřeby sdílení**“. Poskytovala by prostředky na upevnění dosavadního pokroku, jehož bylo dosaženo při provádění doporučení z roku 2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize (dále jen „plán“)[76]. Nabízela by rovněž příležitosti pro další posilování spolupráce na bázi architektury tohoto plánu a využívání pokroku dosaženého zejména v rámci skupiny pro spolupráci v oblasti bezpečnosti sítí a informací (NIS) a v rámci sítě CyCLONe.

Bylo by tak možné odstranit **dva hlavní nedostatky**, které v současné době zvyšují zranitelnost a způsobují neefektivitu v odezvě na přeshraniční hrozby a incidenty, které Unii postihují. První nedostatek spočívá v tom, že **komunity** působící v civilní sféře, v diplomatické oblasti a v oblasti vymáhání práva a obrany, které se zaměřují na kybernetickou bezpečnost, zatím nemají společný prostor, který by vytvářel příznivé podmínky pro jejich strukturovanou spolupráci a usnadňoval jejich operativní a technickou spolupráci. Druhým nedostatkem je to, že příslušné zúčastněné strany působící v oblasti kybernetické bezpečnosti nebyly dosud schopny plně využít **potenciálu** operativní spolupráce a vzájemné pomoci v rámci stávajících sítí a komunit. Dosud také neexistuje platforma, která by umožňovala operativní spolupráci se soukromým sektorem. Jednotka by měla zlepšit a urychlit koordinaci a umožnit EU čelit rozsáhlým kybernetickým incidentům a krizím a reagovat na ně.

Společná kybernetická jednotka by nebyla dalším samostatným orgánem, ani by neovlivnila kompetence a pravomoci vnitrostátních orgánů pro kybernetickou bezpečnost nebo účastníků z EU. Fungovala by spíše jako společné zázemí, kde účastníci mohou využívat možností vzájemné podpory a odborných znalostí, zejména v případě, kdy je zapotřebí, aby různé

[74]Patří sem také podpora v oblasti operativní spolupráce a řešení krizí, kterou poskytuje Agentura Evropské unie pro kybernetickou bezpečnost (ENISA), síť týmů CSIRT, síť styčných organizací pro řešení kybernetických krizí (CyCLONe, ze které se podle návrhu revidované směrnice o bezpečnosti sítí a informací stane EU-CyCLONe), skupina pro spolupráci týkající se směrnice o bezpečnosti sítí a informací, rescEU, Evropské centrum pro boj proti kyberkriminalitě a společná pracovní skupina pro kyberkriminalitu při Europolu a nouzový protokol pro koordinovanou reakci prostřednictvím prosazování práva, Středisko EU pro analýzu zpravodajských informací (EU INTCEN) a soubor nástrojů pro diplomacii v oblasti kybernetiky, společná zpravodajsko-analytická složka (SIAC), kybernetické projekty v rámci stálé strukturované spolupráce (PESCO), zejména tzv. týmy rychlé reakce a vzájemná pomoc v oblasti kybernetické bezpečnosti (CRRT).

[75]„Unie, která si klade vyšší cíle: Moje agenda pro Evropu“, Politické směry pro příští Evropskou komisi (2019–2024) kandidátky na funkci předsedkyně Evropské komise Ursuly von der Leyenové.

[76]Doporučení C(2017) 6100 final ze dne 13.9.2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize.

kybernetické komunity úzce spolupracovaly. Nedávné události zároveň poukazují na to, že je nezbytné, aby EU zvýšila svou úroveň ambicí a připravenost čelit kybernetickým hrozbám a souvisejícím skutečnostem. V rámci svého příspěvku pro společnou kybernetickou jednotku budou tedy aktéři EU (Komise a agentury a subjekty EU) připraveni výrazně navýšit své zdroje a schopnosti, a tím i svoji připravenost a odolnost.

Společná kybernetická jednotka by plnila tři hlavní cíle. Zaprvé by zajišťovala **připravenost** všech komunit působících v oblasti kybernetické bezpečnosti; zadruhé by sdílením informací umožňovala nepřetržité získávání sdílených **poznatků o situaci**; zatřetí by zvyšovala koordinovanost **odezvy** a odstraňování škod. S ohledem na naplňování těchto cílů by jednotka měla vycházet z přesně definovaných **oblastí a dílčích cílů**, jako je zajištění **bezpečného a rychlého sdílení informací**, zlepšení **spolupráce** mezi účastníky, včetně interakce mezi členskými státy a příslušnými subjekty EU, vytváření strukturovaných **partnerství s důvěryhodnou průmyslovou základnou** a usnadnění koordinovaného přístupu ke **spolupráci se zahraničními partnery**. V zájmu toho by pak jednotka na základě mapování dostupných schopností na vnitrostátní úrovni a na úrovni EU mohla usnadnit rozvoj určitého rámce pro spolupráci.

S ohledem na to, aby se společná kybernetická jednotka stala jádrem operační spolupráce EU v oblasti kybernetické bezpečnosti, bude Komise spolupracovat s členskými státy a příslušnými orgány, institucemi a agenturami EU, včetně ENISA, CERT-EU a Europolu, na prosazování **přírůstkového a inkluzivního přístupu**, který bude v plné míře respektovat pravomoci a mandáty všech zúčastněných. Na základě tohoto přístupu by jednotka mohla přispět k posílení spolupráce mezi složkami konkrétní kybernetické komunity, budou-li to tyto složky považovat za nezbytné.

Činnost společné kybernetické jednotky předpokládá čtyři hlavní navrhované kroky:

- *Vymezení* – na základě zmapování dostupných kapacit na vnitrostátní úrovni a na úrovni EU,
- *Příprava* – vytvořením rámce pro strukturovanou spolupráci a pomoc,
- *Zavedení* – provedením rámce vycházejícího ze zdrojů poskytnutých účastníky, který umožní uvést společnou kybernetickou jednotku do provozu,
- *Rozšíření* – posilováním schopnosti koordinované odezvy reakce s využitím vstupům ze strany průmyslu a partnerů.

Na základě výsledků konzultací s členskými státy a orgány, institucemi a agenturami EU[77] představí Komise za účasti vysokého představitele pro zahraniční věci a bezpečnostní politiku a v souladu se svými pravomocemi do února 2021 postup, milníky a časový plán pro **vymezení, přípravu, zavedení a rozšíření společné kybernetické jednotky**.

2.2 Potírání kybernetické kriminality

Naše závislost na on-line nástrojích exponenciálně rozšířila prostor k útoku pro pachatele kybernetické kriminality a vedla k situaci, kdy vyšetřování téměř všech typů trestné činnosti

[77]Konzultace s členskými státy (které se uskutečnily i v rámci cvičení Blue OLEx20, platformy pro setkávání představitelů vnitrostátních orgánů pro kybernetickou bezpečnost) a orgány, institucemi a agenturami EU, které proběhly v období od července do listopadu 2020.

má nějakou digitální složku. Základní součásti naší společnosti jsou navíc ohroženy kybernetickými aktéry a subjekty, které používají kybernetické nástroje k plánování a provádění svých nelegálních činností. Existují proto úzké vazby na celkovou bezpečnostní politiku EU, jak je zohledněna v bodech její strategie bezpečnostní unie z roku 2020, které se týkají kybernetické bezpečnosti, a v protiteroristické agendě EU[78].

Účinné potírání kybernetické kriminality je klíčovým faktorem pro zajištění kybernetické bezpečnosti: odstrašení od páchání kybernetické trestné činnosti je na základě pouhé odolnosti nedosažitelné: vyžaduje také zjišťování totožnosti a stíhání pachatelů. Je proto nezbytné podporovat spolupráci a výměnu mezi aktéry v oblasti kybernetické bezpečnosti a donucovacími orgány. Na úrovni EU se tak již podařilo vybudovat úzkou spolupráci mezi agenturami Europol a ENISA, které pořádají společné konference a pracovní setkání a podávají Komisi, členským státům a dalším zúčastněným stranám společné zprávy o kybernetických hrozbách a technologických výzvách. Komise bude tento integrovaný přístup k zajištění soudržné a účinné odezvy na základě celkového obrazu situace i nadále podporovat.

EU a vnitrostátní orgány by měly rozšířit kapacity a zlepšit schopnosti v oblasti prosazování práva, které umožní vyšetřování kybernetické kriminality, což je jedním z důležitých prvků takové odezvy, s tím, že přitom musí plně respektovat základní práva a usilovat o nalezení požadované rovnováhy mezi různými právy a zájmy. EU by měla být schopna potírat kybernetickou kriminalitu na základě plně provedených a pro tento účel vhodných právních předpisů, přičemž by se měla zvlášť zaměřit na boj proti pohlavnímu zneužívání dětí na internetu a na digitální vyšetřování, včetně vyšetřování kriminality na „darknetu“. Donucovací orgány musí mít k dispozici veškeré prostředky, které jsou pro digitální vyšetřování potřebné. Komise proto předloží akční plán pro zlepšení digitální kapacity donucovacích orgánů zajištěním potřebných dovedností a nástrojů. Zároveň s tím bude agentura Europol dále rozvíjet svou úlohu střediska odborných znalostí schopného poskytovat vnitrostátním donucovacím orgánům podporu v boji proti trestné činnosti, která je umožněná kybernetickými technologiemi a na nich závislá, a přispěje tak k vymezení společných forenzních norem (díky práci laboratoře a střediska agentury Europol pro inovace). Je zapotřebí, aby všechny tyto činnosti byly v členských státech náležitým způsobem přijímány, a členské státy by proto měly využívat vnitrostátních programů Fondu pro vnitřní bezpečnost a reagovat svými projekty na výzvy k předkládání návrhů, které jsou v rámci daného tematického nástroje vydávány.

Komise bude využívat všech vhodných prostředků, včetně řízení o nesplnění povinnosti, aby zajistila plné provedení směrnice z roku 2013 o útocích na informační systémy[79] ve vnitrostátním právu a její uplatňování, včetně povinnosti členských států poskytovat své statistiky. Bude důsledněji předcházet zneužívání doménových jmen, a to i případnému šíření nezákonného obsahu, a bude usilovat o zajištění dostupnosti přesných údajů o registraci. Za tímto účelem bude nadále spolupracovat s Internetovým sdružením pro přidělování jmen a čísel (ICANN), jakož i s dalšími zúčastněnými stranami systému správy internetu, a to zejména prostřednictvím Pracovní skupiny pro veřejnou bezpečnost Vládního poradního výboru sdružení ICANN. Návrh, který obsahuje revidovaná směrnice o opatřeních k zajištění

[78]Sdělení o protiteroristické agendě pro EU: předvídání, prevence, ochrana, reakce, 9.12.2020, COM(2020) 795 final.
[79]Směrnice 2013/40/EU o útocích na informační systémy.

vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, proto předpokládá udržování přesných a úplných databází doménových jmen a registračních údajů nebo „údajů typu WHOIS“ a poskytuje zákonný přístup k takovým údajům jako nezbytnou podmínku zajištění bezpečnosti, stability a odolnosti DNS.

Komise bude rovněž nadále pracovat na vytváření vhodných způsobů a vyjasnění pravidel získávání přeshraničního přístupu k elektronickým důkazům pro účely vyšetřování trestné činnosti (které jsou potřebné v 85 % vyšetřovaných případů, přičemž 65 % z celkového počtu žádostí míří na poskytovatele usazené v jiné jurisdikci) a za tímto účelem chce usnadnit přijetí a následné provádění „balíčku pro elektronické důkazy“ a praktických opatření[80]. Je velmi důležité, aby Evropský parlament a Rada rychle přijaly návrhy o elektronických důkazech a odborníci z praxe tak získali účinný nástroj. Elektronické důkazy musí být čitelné, takže Komise bude pokračovat v podpoře schopnosti donucovacích orgánů v oblasti digitálního vyšetřování, včetně zacházení s šifrovanými daty, pokud se s nimi při vyšetřování trestné činnosti setkají, při úplném zachování jejich funkce, pokud jde o ochranu základních práv a kybernetické bezpečnosti.

2.3 Soubor nástrojů pro diplomacii v oblasti kybernetiky

EU používá svůj **soubor nástrojů pro diplomacii v oblasti kybernetiky**[81] k předcházení nepřátelské kybernetické činnosti, odrazování a odstrašování od této činnosti a reakci na ni. EU po zavedení právního rámce pro cílená omezující opatření proti kybernetickým útokům v květnu 2019[82] uvedla v červenci 2020 v rámci tohoto režimu jména šesti osob a tří subjektů, které byly odpovědné za kybernetické útoky namířené proti EU a jejím členským státům nebo které se na těchto útocích podílely[83]. Další dvě osoby a jedna organizace byly na tento seznam zařazeny v říjnu 2020[84]. Nepřátelskou kybernetickou činnost, včetně dlouhodobých činností založených na pozvolném působení, je třeba potírat v rámci účinné a komplexní společné diplomatické reakce EU, a to s využitím celé škály opatření, která jsou na úrovni EU k dispozici.

---

[80]COM(2018) 225 a 226; C(2020) 2779 final. Zejména projekt SIRIUS získal nedávno v rámci nástroje partnerství další finanční prostředky na zlepšení možností získávání zákonného přeshraničního přístupu k elektronickým důkazům pro účely vyšetřování trestné činnosti (které jsou potřebné v 85 % vyšetřovaných případů, přičemž 65 % z celkového počtu žádostí míří na poskytovatele usazené v jiné jurisdikci) a stanovení slučitelných pravidel na mezinárodní úrovni.

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

[82]Rozhodnutí Rady (SZBP) 2019/797 ze dne 17. května 2019 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy (Úř. věst. L 129 I, 17.5.2019, s. 13) a nařízení Rady (EU) 2019/796
ze dne 17. května 2019 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy (Úř. věst. L 129 I, 17.5.2019, s. 1).

[83]Rozhodnutí Rady (SZBP) 2020/1127 ze dne 30. července 2020, kterým se mění rozhodnutí (SZBP) 2019/797 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy (ST/9564/2020/INIT) (Úř. věst. L 246, 30.7.2020, s. 12), a prováděcí nařízení Rady (EU) 2020/1125 ze dne 30. července 2020, kterým se provádí nařízení (EU) 2019/796 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy (ST/9568/2020/INIT)(Úř. věst. L 246, 30.7.2020, s. 4).

[84] Rozhodnutí Rady (SZBP) 2020/1537 ze dne 22. října 2020, kterým se mění rozhodnutí (SZBP) 2019/797 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy (Úř. věst. L 351 I , 22.10.2020, s. 5), a prováděcí nařízení Rady (EU) 2020/1536 ze dne 22. října 2020, kterým se provádí nařízení (EU) 2019/796 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy (Úř. věst. L 351 I, 22.10.2020, s. 1).

Rychlá a účinná společná diplomatická reakce EU vyžaduje solidní sdílenou znalost situace a schopnost rychle připravit společný postoj EU. Vysoký představitel Unie pro zahraniční věci a bezpečnostní politiku podpoří a usnadní **zřízení pracovní skupiny členských států EU pro kybernetické zpravodajské informace**, která bude sídlit ve Středisku EU pro analýzu zpravodajských informací (INTCEN), a to s cílem rozvíjet strategickou zpravodajskou spolupráci v oblasti kybernetických hrozeb a aktivit. Tato práce v EU dále podpoří získávání poznatků o situaci a rozhodování o společné diplomatické reakci. Pracovní skupina má spolupracovat se stávajícími strukturami[85], v případě potřeby i se strukturami, do jejichž působnosti spadá obecnější hrozba hybridního a zahraničního vměšování, na shromažďování a vyhodnocování poznatků o situaci.

V zájmu posílení schopnosti předcházet nepřátelskému jednání v kyberprostoru, odrazovat a odstrašovat od takového jednání a reagovat na ně předloží vysoký představitel pro zahraniční věci a bezpečnostní politiku v součinnosti s Komisí a v souladu se svými pravomocemi návrh, aby EU dále pracovala na vymezení svého **postoje ke kybernetickému odrazování**. Na základě práce, která byla dosud v rámci souboru nástrojů pro diplomacii v oblasti kybernetiky odvedena, by tento postoj měl přispět k odpovědnému chování států a jejich spolupráci v kyberprostoru a měl by klást důraz na obranu před kybernetickými útoky, které mají nejcitelnější dopady, tedy zejména před útoky, které ovlivňují naši kritickou infrastrukturu, demokratické instituce a procesy[86], jakož i útoky na dodavatelské řetězce a kybernetické krádeže duševního vlastnictví. Z uvedeného postoje by mělo vyplynout, jak by EU a členské státy mohly využívat své politické, ekonomické, diplomatické, právní a strategické komunikační nástroje pro účely boje proti nepřátelské kybernetické činnosti, a jeho předmětem by měla být také otázka, jak by EU a členské státy mohly zlepšit svou schopnost určovat původce nepřátelské kybernetické činnosti. Kromě toho se vysoký představitel pro zahraniční věci a bezpečnostní politiku společně s Radou a Komisí snaží prozkoumat **další opatření v rámci souboru nástrojů pro diplomacii v oblasti kybernetiky**, včetně prostoru pro další možnosti omezujících opatření, mimo jiné prozkoumáním hlasování kvalifikovanou většinou pro zařazení na seznam v rámci horizontálního sankčního režimu pro boj proti kybernetickým útokům. Dále by EU měla vyvinout další úsilí k **posílení spolupráce s mezinárodními partnery**, včetně NATO, s cílem pokročit ve společném chápání problematiky hrozeb, rozvíjet mechanismy spolupráce a identifikovat diplomatické reakce založené na spolupráci.

Vysoký představitel pro zahraniční věci a bezpečnostní politiku v součinnosti s Komisí rovněž navrhne aktualizaci **prováděcích pokynů k souboru nástrojů pro diplomacii v oblasti kybernetiky[87]**, jejímž cílem by mělo být mimo jiné zvýšení účinnosti rozhodovacího procesu, a nadále bude organizovat pravidelná školení a hodnocení, jejichž předmětem bude soubor nástrojů pro diplomacii v oblasti kybernetiky. EU by kromě toho měla v ještě větší míře **učinit soubor nástrojů pro diplomacii v oblasti kybernetiky součástí krizových mechanismů EU** a hledat možnosti synergií v oblasti boje proti hybridním hrozbám, dezinformacím a zahraničnímu vměšování ve společném rámci pro boj proti hybridním hrozbám[88] a v rámci evropského akčního plánu pro demokracii. V této souvislosti by EU

[85]Jako je například společná zpravodajsko-analytická složka (SIAC) a v případě potřeby příslušné projekty, které byly vytvořeny v rámci PESCO, jakož i systém včasného varování (RAS), který byl zřízen v roce 2018 na podporu celkového přístupu EU k boji proti dezinformacím.
[86] Zejména hledáním součinnosti s iniciativami v rámci evropského akčního plánu pro demokracii.
[87] 13007/17
[88] https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

měla zvážit možnosti interakce mezi souborem nástrojů pro diplomacii v oblasti kybernetiky a případným použitím čl. 42 odst. 7 Smlouvy o EU a článku 222 Smlouvy o fungování EU[89].

2.4 Posílení schopností v oblasti kybernetické obrany

EU a členské státy musí zvýšit svou schopnost předcházet kybernetickým hrozbám a reagovat na ně v souladu s úrovní ambicí EU, která vyplývá z globální strategie EU z roku 2016[90]. Za tímto účelem předloží vysoký představitel pro zahraniční věci a bezpečnostní politiku ve spolupráci s Komisí **přezkum politického rámce EU pro kybernetickou obranu (CDPF)**, který by měl posílit další koordinaci a spolupráci mezi aktéry EU[91], jakož i s jednotlivými členskými státy a mezi nimi navzájem, včetně misí a operací probíhajících v rámci společné bezpečnostní a obranné politiky (SBOP). Rámec CDPF by měl určit podobu chystaného strategického kompasu[92] a měl by zajistit, aby se kybernetická bezpečnost a kybernetická obrana staly ještě pevnější součástí obecnější bezpečnostní a obranné agendy.

V roce 2018 EU určila kybernetický prostor jako oblast operací[93]. Chystaná **„Vojenská vize a strategie pro kyberprostor jako oblast operací“** Vojenského výboru EU by měla blíže určit, jak kyberprostor jakožto oblast operací umožňuje vojenské mise a operace EU v rámci SBOP. **Vojenská síť CERT**[94], kterou zřizuje Evropská obranná agentura (EDA), dále přispěje k výraznému posílení spolupráce mezi členskými státy. V zájmu zajištění kybernetické bezpečnosti kritických infrastruktur v kosmickém prostoru spadajících do působnosti kosmického programu bude navíc posílena Evropská agentura pro vesmírný program, a zejména bezpečnostní středisko systému Galileo, a její mandát bude rozšířen i na další kriticky významné součásti kosmického programu.

EU a členské státy by měly vytvářet další podněty k **rozvoji nejmodernějších schopností v oblasti kybernetické obrany**, zejména rámce CDPF, a za tímto účelem by měly využívat různých politik a nástrojů EU a případně čerpat i z práce Evropské obranné agentury. S ohledem na to je třeba klást silný důraz na vývoj a používání klíčových technologií, jako je umělá inteligence, šifrování a kvantová výpočetní technika. V souladu s prioritami rozvoje schopností EU z roku 2018[95] a na základě zjištění uvedených v první zprávě o úplném koordinovaném každoročním přezkumu v oblasti obrany (CARD)[96] by EU měla dále podporovat spolupráci mezi členskými státy na poli **výzkumu, inovací a rozvoje schopností v oblasti kybernetické obrany** a podněcovat členské státy k využívání plného potenciálu **stálé strukturované spolupráce (PESCO)[97]** a **Evropského obranného fondu[98]**.

---

[89] Resp. doložka o vzájemné obraně a doložka solidarity.

[90] Závěry Rady (14149/16) o provádění globální strategie EU v oblasti bezpečnosti a obrany.

[91] Zejména ESVČ, včetně Vojenského štábu EU (EUMS), Evropské bezpečnostní a obranné školy (ESDC), Komise a agentury EU, především Evropská obranná agentura (EDA).

[92] Závěry Rady ze dne 17. června 2020 o bezpečnosti a obraně (8910/20).

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

[94] Zřízení vojenské sítě CERT EU odpovídá cíli vymezenému v politickém rámci EU pro kybernetickou obranu z roku 2018 a jejím účelem je podporovat aktivní interakci a výměnu informací mezi vojenskými skupinami členských států EU pro reakci na počítačové hrozby (CERT).

[95] V červnu 2018 se členské státy v Řídícím výboru Evropské obranné agentury dohodly, že svou obrannou spolupráci povedou na úrovni EU.

[96] Schváleno ministry obrany v Řídícím výboru Evropské obranné agentury v listopadu 2020. https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card)

[97] V současné době existuje několik projektů PESCO, které se týkají kybernetické bezpečnosti. Je to zejména platforma pro sdílení informací o kybernetických hrozbách a reakci na incidenty, týmy rychlé kybernetické

Připravovaný **akční plán Komise pro součinnost mezi civilním, obranným a kosmickým průmyslem**, který má být představen v prvním čtvrtletí roku 2021 , bude zahrnovat opatření, která dále podpoří synergie na úrovni programů, technologií, inovací a začínajících podniků v souladu s řízením příslušných programů[99].

Kromě toho je třeba rozvíjet příslušné synergie a rozhraní mezi jednotlivými iniciativami v oblasti kybernetické obrany realizovanými v jiných rámcích, včetně projektů spolupráce týkajících se kybernetiky,[100] které uskutečňují členské státy v rámci platformy PESCO, jakož i se strukturami kybernetické bezpečnosti EU, přičemž cílem by mělo být podpořit sdílení informací a vzájemnou podporu.

Strategické iniciativy

EU by měla:

- dokončit evropský rámec pro řešení kybernetických bezpečnostních krizí a stanovit proces, milníky a časový plán pro vytvoření společné kybernetické jednotky,
- pokračovat v provádění agendy pro potírání kybernetické kriminality v rámci strategie bezpečnostní unie,
- podpořit a usnadnit zřízení pracovní skupiny členských států pro kybernetické zpravodajské informace v rámci Střediska EU pro analýzu zpravodajských informací (INTCEN),
- pokročit v práci na přípravě postoje EU ke kybernetickému odrazování s cílem předcházet nepřátelské kybernetické činnosti, odrazovat a odstrašovat od této činnosti a reagovat na ni,
- přezkoumat politický rámec pro kybernetickou obranu,
- usnadnit rozvoj „Vojenské vize a strategie pro kyberprostor jako oblast operací“ EU pro účely vojenských misí a operací SBOP,
- podporovat součinnost mezi civilním, obranným a kosmickým průmyslem a
- posílit kybernetickou bezpečnost kritických kosmických infrastruktur v rámci kosmického programu.

3. PROSAZOVÁNÍ GLOBÁLNÍHO A OTEVŘENÉHO KYBERPROSTORU

EU by měla i nadále spolupracovat s mezinárodními partnery na prosazování politického modelu a vize kybernetického prostoru vybudovaného na základě právního státu, lidských práv, základních svobod a demokratických hodnot, které přinášejí celosvětový sociální, hospodářský a politický rozvoj a přispívají k bezpečnostní unii. Mezinárodní spolupráce je

reakce a vzájemná pomoc v oblasti kybernetické bezpečnosti, Akademické a inovační středisko EU pro kybernetickou oblast (EU CAIH) a Koordinační středisko pro kybernetický a informační prostor (CIDCC).

[98] V rámci Evropského obranného fondu již Komise určila možnosti spolupráce na poli výzkumu a vývoje v oblasti kybernetické obrany se zaměřením na posilování spolupráce, inovační kapacity a konkurenceschopnost obranného průmyslu.

[99] Například program Horizont Evropa, Digitální Evropa a Evropský obranný fond.

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

pro udržení globálního, otevřeného, stabilního a bezpečného kyberprostoru nezbytná. Za tímto účelem by EU měla pokračovat ve spolupráci se třetími zeměmi, mezinárodními organizacemi a komunitou více zúčastněných stran na rozvoji a provádění soudržné a ucelené mezinárodní politiky v oblasti kybernetické bezpečnosti při vědomí stále větší provázanosti hospodářských aspektů nových technologií, vnitřní bezpečnosti a zahraniční, bezpečnostní a obranné politiky. Jakožto silný hospodářský a obchodní blok opírající se o stěžejní demokratické hodnoty, respekt k právnímu státu a základní práva má EU rovněž jedinečné předpoklady k tomu, aby stála v čele procesu vymezování a prosazování mezinárodních standardů a norem.

3.1 Vedoucí postavení EU v oblasti standardů, norem a rámců v kybernetickém prostoru

Zintenzivnění úsilí v procesu stanovování mezinárodních norem

Má-li být EU schopna prosazovat a hájit svou vizi kyberprostoru na mezinárodní úrovni, musí se **ve větší míře podílet na procesech stanovování mezinárodních norem a ve větší míře se v této oblasti ujímat vedení a posílit své zastoupení v mezinárodních a evropských normalizačních orgánech, jakož i v jiných organizacích působících v oblasti vytváření standardů**[101]. Vzhledem k rychlému tempu vývoje digitálních technologií mají mezinárodní normy stále větší význam, protože doplňují tradiční regulační úsilí v oblastech, jako je umělá inteligence, cloud, kvantová výpočetní technika a kvantová komunikace. Mezinárodní normalizace je ve stále větší míře využívána třetími zeměmi k prosazování jejich politické a ideologické agendy, která často neodpovídá hodnotám EU. Existuje navíc rostoucí riziko vznikání konkurenčních rámců pro mezinárodní normy, jehož důsledkem je roztříštěnost.

Utváření mezinárodních norem v oblastech nově vznikajících technologií a základní architektury internetu v souladu s hodnotami EU je nezbytné pro zajištění toho, aby internet zůstal globální a otevřený, aby se technologie řídily potřebami lidí, aby byly používány v souladu s ochranou soukromí a ve shodě se zákonem a bezpečně a eticky. V rámci své připravované strategie pro normalizaci by EU měla vymezit své **cíle pro stanovování mezinárodních norem** a aktivním a koordinovaným způsobem se zasazovat o prosazování těchto cílů na mezinárodní úrovni. Je třeba usilovat o silnější spolupráci a sdílení zátěže s podobně smýšlejícími partnery a evropskými zúčastněnými stranami.

Prosazování odpovědného chování států v kybernetickém prostoru

EU nadále spolupracuje s mezinárodními partnery na prosazování a podporování globálního, otevřeného, stabilního a bezpečného kyberprostoru, v němž **je respektováno mezinárodní právo, zejména Charta Organizace spojených národů (OSN)**[102], a kde jsou dodržovány **dobrovolné nezávazné normy, pravidla a zásady odpovědného chování státu**[103]. Vzhledem ke zhoršování účinné mnohostranné diskuse o mezinárodní bezpečnosti v

---

[101] Například Mezinárodní organizace pro normalizaci (ISO), Mezinárodní elektrotechnická komise (IEC), Mezinárodní telekomunikační unie (ITU), Evropský výbor pro normalizaci (CEN), Evropský výbor pro normalizaci v elektrotechnice (CENELEC), Evropský ústav pro telekomunikační normy (ETSI), pracovní skupiny IETF, Projekt partnerství třetí generace (3GPP) a Institut pro elektrotechnické a elektronické inženýrství (IEEE).

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

[103] Jak je zohledněn v příslušných zprávách skupin vládních expertů o vývoji v oblasti informací a telekomunikací v kontextu mezinárodní bezpečnosti (UNGGE), které schválilo Valné shromáždění OSN, zejména ve zprávách za roky 2015, 2013 a 2010.

kybernetickém prostoru je zřejmé, že EU a členské státy musí zaujímat aktivnější postoj v diskusích probíhajících na půdě OSN i v dalších příslušných mezinárodních fórech. EU má nejlepší předpoklady pro to, **aby prosazovala, koordinovala a posilovala postoje členských států na mezinárodních fórech** a měla by **vypracovat svůj vlastní postoj k uplatňování mezinárodního práva v kybernetickém prostoru**. Vysoký představitel pro zahraniční věci a bezpečnostní politiku má spolu s členskými státy rovněž v úmyslu nadále prosazovat inkluzivní a konsensuální návrh politického závazku ohledně **programu činnosti zaměřené na prosazování odpovědného chování států v kybernetickém prostoru**[104] v rámci OSN. Tento program, vytvořený na základě platného *acquis* schváleného Valným shromážděním OSN[105], nabízí platformu pro spolupráci a výměnu osvědčených postupů na půdě OSN a jeho součástí je návrh na zavedení mechanismu, který by umožňoval zavádět normy odpovědného chování státu a podporovat budování kapacit. Vysoký představitel pro zahraniční věci a bezpečnostní politiku se zaměřuje též na posílení a podporu provádění **opatření pro budování důvěry** mezi státy, včetně sdílení osvědčených postupů na regionální a mnohostranné úrovni a přispívání k meziregionální spolupráci.

Zvýšená globální konektivita by neměla vést k cenzuře, hromadnému dohledu, narušování ochrany osobních údajů a represím namířeným proti občanské společnosti, akademické obci a občanům. EU by měla i nadále zaujímat vedoucí postavení, pokud jde o ochranu a prosazování **lidských práv a základních svobod** na internetu. Za tímto účelem by EU měla prosazovat důslednější dodržování mezinárodního práva a norem v oblasti lidských práv[106] a realizovat svůj akční plán pro lidská práva a demokracii na období 2020–2024[107] a měla by pokročit v práci na svých obecných zásadách v oblasti lidských práv ohledně svobody projevu online a offline[108] a **nabídnout tak nový podnět k praktickému uplatňování nástrojů EU.** EU by měla vynakládat trvalé úsilí na **ochranu obránců lidských práv, občanské společnosti a akademické obce zabývajících se otázkami, jako je kybernetická bezpečnost, ochrana soukromých údajů, dohled a cenzura na internetu**. Za tímto účelem by EU měla vydávat další praktické pokyny, podporovat osvědčené postupy a zintenzivnit své úsilí o zamezení zneužívání nově vznikajících technologií, přičemž by v případech, kdy je to nezbytné, měla využívat diplomatických opatření a kontrolovat vývoz těchto technologií. EU by měla také pokračovat v boji za ochranu nejzranitelnějších členů společnosti na internetu a navrhnout za tím účelem právní předpisy, které budou lépe chránit děti před pohlavním zneužíváním a vykořisťováním, a strategii o právech dítěte.

Budapešťská úmluva o počítačové kriminalitě

EU nadále podporuje třetí země, které si přejí přistoupit k **Budapešťské úmluvě Rady Evropy o počítačové kriminalitě**, a pokračuje v práci na dokončení **Druhého dodatkového protokolu k Budapešťské úmluvě**, který obsahuje opatření a záruky pro zlepšení mezinárodní spolupráce mezi donucovacími a soudními orgány, jakož i mezi orgány a poskytovateli služeb v jiných zemích. Těchto jednání se jménem EU účastní Komise[109].

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

[105] Jak je zohledněno v příslušných zprávách skupin vládních expertů o vývoji v oblasti informací a telekomunikací v kontextu mezinárodní bezpečnosti (UNGGE), které schválilo Valné shromáždění OSN: 2015, 2013 and 2010 reports.

[106] Zejména Charta OSN a Všeobecná deklarace lidských práv.

[107] https://www.consilium.europa.eu/cs/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] Rozhodnutí Rady z června 2019 (ref 9116/19).

Současná iniciativa pro nový právní nástroj pro potírání kybernetické kriminality na úrovni OSN s sebou nese riziko dalšího rozdělení a zpomalí tolik potřebné vnitrostátní reformy a související úsilí o budování kapacit, což může bránit účinné mezinárodní spolupráci v boji proti kybernetické kriminalitě: EU si nemyslí, že by bylo zapotřebí nového právního nástroje pro potírání kybernetické kriminality na úrovni OSN. EU se nadále podílí na **mnohostranných výměnách informací v oblasti boje proti kybernetické kriminalitě** ve své snaze zajistit dodržování lidských práv a základních svobod prostřednictvím začleňování, transparentnosti a zohlednění dostupných odborných znalostí, přičemž cílem je vytvořit přidanou hodnotu pro všechny.

3.2 Spolupráce s partnery a komunitou více zúčastněných stran

EU by měla **posílit a rozšířit své dialogy se třetími zeměmi o otázkách kybernetické bezpečnosti** a prosazovat prostřednictvím těchto dialogů své hodnoty a svou vizi kybernetického prostoru, sdílet osvědčené postupy a usilovat o účinnější spolupráci. EU by měla rovněž zavést strukturované výměny informací s regionálními organizacemi, jako je Africká unie, regionální fórum ASEAN, Organizace amerických států a Organizace pro bezpečnost a spolupráci v Evropě. Kdykoli je to možné a je k tomu vhodná příležitost, měla by také na základě záležitostí společného zájmu usilovat o nalezení společných východisek s dalšími partnery. Ve spolupráci s delegacemi EU a případně s velvyslanectvími členských států po celém světě by měla vybudovat neformální **síť EU pro kybernetickou diplomacii**, která by podporovala unijní vizi kybernetického prostoru a umožňovala by výměnu informací a pravidelnou koordinaci vývoje, k němuž v kybernetickém prostoru dochází[110].

Na základě společných prohlášení ze dne 8. července 2016[111] a ze dne 10. července 2018[112] by EU měla pokračovat v rozvoji **spolupráce mezi EU a NATO**, zejména pokud jde o požadavky na interoperabilitu v oblasti kybernetické obrany. V této souvislosti by EU měla dále usilovat o přičlenění příslušných struktur SBOP k síti budované v rámci iniciativy NATO Federated Mission Networking, což v případě potřeby umožní interoperabilitu sítí s NATO a s partnery. Kromě toho by měly být důkladněji prozkoumány možnosti spolupráce mezi EU a NATO v oblasti vzdělávání, odborné přípravy a cvičení, mimo jiné hledáním možností součinnosti mezi Evropskou bezpečnostní a obrannou školou a Střediskem excelence NATO pro spolupráci v oblasti kybernetické obrany.

V **otázce správy internetu** EU v souladu se svými hodnotami jednoznačně podporuje a prosazuje **model více zúčastněných stran**. Žádný subjekt, vláda nebo mezinárodní organizace by neměly vyvíjet snahu o vlastní kontrolu internetu s vyloučením ostatních. EU by se měla na fórech[113] nadále podílet na posilování spolupráce a zajišťování ochrany základních práv a svobod, zejména práva na důstojnost, soukromí a svobodu projevu a svobodu informací. V zájmu prosazování spolupráce více zúčastněných stran v otázkách kybernetické bezpečnosti Komise a vysoký představitel pro zahraniční věci a bezpečnostní politiku v souladu se svými pravomocemi usilují o posílení **pravidelné a strukturované výměny se zúčastněnými stranami**, včetně soukromého sektoru, akademické obce a občanské společnosti, a zdůraznění toho, že s ohledem na propojenost kybernetického prostoru je nezbytné, aby si všechny zúčastněné strany vyměňovaly informace a přijaly

[110] V příslušných případech by také bylo možné využívat činností probíhajících v rámci neformální sítě EU pro digitální diplomacii, jejíž součástí jsou ministerstva zahraničních věcí členských států.
[111] http://www.consilium.europa.eu/cs/press/press-releases/2016/07/08-eu-nato-joint-declaration/
[112] https://www.consilium.europa.eu/cs/press/press-releases/2018/07/10/eu-nato-joint-declaration/
[113] Např. Internetové sdružení pro přidělování jmen a čísel (ICANN) a Fórum pro správu internetu (IGF).

konkrétní odpovědnost za udržení globálního, otevřeného, stabilního a bezpečného kybernetického prostoru. Toto úsilí bude cenným vstupem pro potenciální klíčová opatření na úrovni EU.

3.3 Posílení globálních kapacit pro zvýšení globální odolnosti

S ohledem na to, aby všechny země byly schopny využívat sociálních, hospodářských a politických přínosů internetu a využívání technologií, EU nadále podporuje své partnery, aby zvyšovali svou kybernetickou odolnost a schopnost vyšetřovat a stíhat kybernetickou kriminalitu a řešit kybernetické hrozby. Pro zajištění celkové soudržnosti by EU měla vypracovat **agendu EU pro budování vnějších kybernetických kapacit**, která by umožňovala řídit toto úsilí v souladu s jejími pokyny pro budování vnějších kybernetických kapacit[114] a v souladu s Agendou pro udržitelný rozvoj 2030[115]. Uvedená agenda by měla využívat odborných znalostí členských států a příslušných orgánů, institucí, agentur a iniciativ EU, včetně sítě EU pro budování kybernetických kapacit[116], a to v souladu s jejich příslušnými mandáty. Zřídí se **Rada EU pro budování kybernetických kapacit**, která bude zahrnovat příslušné zúčastněné instituce EU, sledovat dosažený pokrok a určovat možnosti dalších součinností i případné nedostatky. Kromě toho může podporovat posilování spolupráce s členskými státy, jakož i s partnery z veřejného a soukromého sektoru a dalšími příslušnými mezinárodními orgány, a to s cílem zajistit koordinaci úsilí a zabránit jeho zbytečnému zdvojování.

Budování kybernetických kapacit EU by se mělo i nadále zaměřovat na země západního Balkánu a na sousedství EU, jakož i na partnerské země, které procházejí rychlým digitálním rozvojem. EU by svým úsilím měla podporovat, aby v partnerských zemích vznikaly právní předpisy a politiky, které jsou v souladu s příslušnými politikami a normami kybernetické diplomacie EU. V této souvislosti by standardní součástí úsilí EU týkající se budování kapacit v oblasti digitalizace měla být kybernetická bezpečnost. Za tímto účelem by EU měla připravit program odborné přípravy určený úředníkům EU, kteří mají na starost realizaci snah EU v oblasti budování vnějších digitálních a kybernetických kapacit. EU by těmto zemím měla rovněž pomáhat při řešení stále většího problému, který představuje nepřátelská kybernetická činnost, jež narušuje rozvoj jejich společností a **integritu a bezpečnost demokratických systémů**, přičemž by měla postupovat v souladu s úsilím vyvíjeným v rámci akčního plánu pro demokracii. Velmi užitečné by v tomto ohledu mohlo být vzájemné učení mezi členskými státy a příslušnými agenturami EU a třetími zeměmi.

A konečně v rámci paktu pro civilní SBOP z roku 2018[117] mohou civilní mise SBOP rovněž přispět k širší reakci EU, pokud jde o řešení problémů kybernetické bezpečnosti, a to zejména posílením právního státu v partnerských zemích, jakož i jejich schopností v oblasti vymahatelnosti práva a civilní správy.

Strategické iniciativy

EU by měla:

- vymezit soubor cílů v oblasti mezinárodních normalizačních procesů a prosazovat tyto

[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/cs/pdf

cíle na mezinárodní úrovni,

- prosazovat mezinárodní bezpečnost a stabilitu v kybernetickém prostoru, a to zejména prostřednictvím návrhu programu činnosti zaměřeného na prosazování odpovědného chování států v kybernetickém prostoru v rámci OSN, který by EU předložila společně se svými členskými státy,
- nabídnout praktické pokyny k uplatňování lidských práv a základních svobod v kybernetickém prostoru,
- lépe chránit děti před pohlavním zneužíváním a vykořisťováním a navrhnout strategii o právech dítěte,
- posílit a prosazovat Budapešťskou úmluvu o počítačové kriminalitě, mimo jiné prací na Druhém dodatkovém protokolu k Budapešťské úmluvě,
- rozšířit kybernetický dialog EU s třetími zeměmi a s regionálními a mezinárodními organizacemi, mimo jiné prostřednictvím neformální sítě EU pro kybernetickou diplomacii,
- posílit výměny s komunitou více zúčastněných stran, zejména formou pravidelných a strukturovaných výměn informací se soukromým sektorem, akademickou obcí a občanskou společností, a
- navrhnout agendu EU pro budování vnějších kybernetických kapacit a Radu pro budování kybernetických kapacit EU.

III. KYBERNETICKÁ BEZPEČNOST V ORGÁNECH, INSTITUCÍCH A AGENTURÁCH EU

Vzhledem ke svému politickému významu, kriticky důležitým misím, kdy koordinují velmi citlivé otázky, a vzhledem k úloze, kterou plní jako správci velkého objemu veřejných prostředků, **se orgány, instituce a agentury EU stávají pravidelným cílem kybernetických útoků**, zejména kybernetické špionáže. Jejich kybernetická odolnost a schopnost odhalovat nepřátelské kybernetické aktivity a reagovat na ně je však u těchto subjektů na velmi různé úrovni vyspělosti. Celkovou míru kybernetické bezpečnosti je proto nutné zvýšit zavedením soudržných a jednotných pravidel.

V oblasti bezpečnosti informací bylo dosaženo pokroku, pokud jde o soudržnost **pravidel ochrany utajovaných informací EU, jakož i citlivých informací, které nespadají do kategorie utajovaných informací**. Interoperabilita systémů utajovaných informací však zůstává omezená a brání plynulému přenosu informací mezi jednotlivými subjekty. Mělo by být dosaženo dalšího pokroku, který umožní ve vztahu k zacházení s utajovanými informacemi a citlivými neutajovanými informacemi EU uplatňovat interinstitucionální přístup, jenž by mohl sloužit také jako vzor pro interoperabilitu mezi členskými státy. Stanoven by měl být rovněž základní scénář, který by zjednodušil postupy při jednání s členskými státy. EU by také měla dále rozvíjet svou schopnost vést zabezpečenou komunikaci s příslušnými partnery a v co největší míře přitom vycházet z již existujících ujednání a postupů.

Jak bylo oznámeno ve strategii bezpečnostní unie, Komise proto **v roce 2021** předloží návrhy **společných závazných pravidel pro bezpečnost informací a společných závazných**

pravidel pro kybernetickou bezpečnost platných pro všechny orgány, instituce a agentury EU, která budou odrážet probíhající interinstitucionální diskuse EU o kybernetické bezpečnosti[118].

Současné a budoucí trendy v oblasti práce na dálku budou rovněž vyžadovat další investice do zabezpečeného vybavení, infrastruktury a nástrojů, jež umožní pracovat na dálku i na citlivých a utajovaných souborech.

Stále agresivnější formy kybernetických hrozeb a stále častější výskyt sofistikovanějších kybernetických útoků, jejichž terčem se stávají orgány, instituce a agentury EU, vytváří potřebu větších investic s cílem dosáhnout vysokého stupně vyspělosti kybernetického zabezpečení. Pro všechny orgány, instituce a agentury EU je nyní zaváděn program, který má zvýšit kybernetickou informovanost jejich zaměstnanců a jejich kybernetickou hygienu a podporovat společnou kulturu v oblasti kybernetické bezpečnosti.

Je třeba vytvořit **lepší mechanismus financování, který posílí skupinu CERT EU**, aby se zvýšila její schopnost pomáhat orgánům, institucím a agenturám EU s uplatňováním nových pravidel kybernetické bezpečnosti a zlepšit jejich kybernetickou odolnost. Posílit je třeba také mandát skupiny CERT EU, aby měla k naplnění těchto cílů stále dostupné prostředky.

Strategické iniciativy

1. Nařízení o bezpečnosti informací v orgánech, institucích a agenturách EU
2. Nařízení o společných pravidlech kybernetické bezpečnosti pro orgány, instituce a agentury EU
3. Nový právní základ pro skupinu CERT EU za účelem posílení jejího mandátu a financování.

IV. ZÁVĚRY

Společné provádění této strategie přispěje k naplnění cílů kyberneticky bezpečné digitální dekády EU, k uskutečnění bezpečnostní unie a k posílení postavení EU ve světě.

EU by měla prosazovat standardy a normy nabízející řešení na světové úrovni a standardy kybernetické bezpečnosti pro základní služby a kritické infrastruktury, a zároveň být hnací silou vývoje a uplatňování nových technologií. Součástí řešení problému, který představuje zajištění kybernetické bezpečnosti digitální transformace, je každá organizace i každá jednotlivá osoba využívající internet.

Komise a vysoký představitel pro zahraniční věci a bezpečnostní politiku budou v souladu se svými pravomocemi sledovat pokrok dosažený při uskutečňování této strategie a vypracují kritéria pro jeho hodnocení. Podkladem pro toto monitorování by měly být zprávy Evropské agentury pro bezpečnost sítí a informací (ENISA) a pravidelné zprávy Komise o bezpečnostní unii. Výsledky přispějí k naplnění cílů nadcházející evropské digitální dekády[119]. V souladu se svými pravomocemi budou Komise a vysoký představitel pro zahraniční věci a bezpečnostní politiku i nadále spolupracovat s členskými státy s cílem určit praktická opatření, jež umožní propojit čtyři komunity, které se v EU zabývají kybernetickou

[118] Pravidelné interinstitucionální diskuse EU o kybernetické bezpečnosti jsou součástí širších výměn informací o příležitostech a výzvách digitální transformace pro orgány EU.

[119] Oznámeno v pracovním programu Komise na rok 2021.

bezpečností, tj. v oblasti kritické infrastruktury a odolnosti vnitřního trhu, spravedlnosti a prosazování práva a popřípadě též v oblasti kybernetické diplomacie a kybernetické obrany. Komise a vysoký představitel pro zahraniční věci a bezpečnostní politiku budou i nadále spolupracovat s komunitou více zúčastněných stran, přičemž důraz by měl být kladen na to, aby každý, kdo používá internet, plnil příslušnou úlohu při udržování globálního, otevřeného, stabilního a bezpečného kyberprostoru, kde každý může vést bezpečný digitální život.

Dodatek: Další kroky v oblasti kybernetické bezpečnosti sítí 5G

Na základě výsledků přezkumu doporučení Komise o kybernetické bezpečnosti sítí 5G[120] by se další kroky koordinované práce na úrovni EU měly směřovat pozornost ke třem hlavním cílům a hlavním krátkodobým a střednědobým opatřením uvedeným v následující tabulce, jež mají provádět orgány členských států, Komise a Agentura Evropské unie pro bezpečnost sítí a informací (ENISA).

První prioritou pro další fázi je **dokončení provádění souboru opatření na vnitrostátní úrovni a řešení otázek uvedených ve zprávě o pokroku z července 2020**. V této souvislosti by s ohledem na některá strategická opatření, která jsou součástí souboru opatření, prospělo **posílení koordinační práce nebo výměny informací** v rámci činnosti skupiny pro spolupráci v oblasti bezpečnosti sítí a informací, jak již bylo uvedeno ve zprávě o pokroku, což by mohlo vést k rozvoji **osvědčených postupů nebo** vytvoření **pokynů**. V oblasti technických opatření by mohla poskytnout další podporu Evropská agentura pro bezpečnost sítí a informací (ENISA) na základě práce, kterou již vykonala, a některá témata by mohla prošetřit důkladněji a mohla by rovněž **sestavit ucelený přehled všech příslušných pokynů o požadavcích na kybernetickou bezpečnost sítí 5G pro operátory mobilních sítí**.

Členské státy zadruhé zdůraznily, že je důležité držet krok s vývojem prostřednictvím **neustálého sledování vývoje v oblasti technologií, architektury sítí 5G, hrozeb a jednotlivých způsobů použití technologie 5G a příslušných aplikací, ale i vývoje vnějších faktorů**, aby bylo možné **odhalovat nová nebo nově vznikající rizika a nacházet řešení**. Některé aspekty v rámci počáteční analýzy rizik by kromě toho měly být prošetřeny důkladněji, zejména proto, aby bylo zajištěno, že tato analýza obsáhne celý ekosystém 5G, včetně všech příslušných částí síťové infrastruktury a dodavatelského řetězce 5G. Soubor opatření byl navržen tak, aby byl flexibilní a přizpůsobitelný, ale ve střednědobém horizontu by bylo možné podniknout v případě potřeby kroky k jeho rozšíření nebo vylepšení, aby i nadále obsahoval vše potřebné a vyhovoval budoucím nárokům.

Zatřetí je důležité, aby **na úrovni EU** byly i nadále podnikány **kroky**, které budou podporovat uskutečňování cílů stanovených v rámci souborů opatření a doplňovat je, a které umožní, aby se tyto cíle staly v plné míře součástí příslušných politik Unie a Komise, zejména v návaznosti na kroky, které Komise oznámila ve svém sdělení o souboru opatření ze dne 29. ledna 2020[121] a které se týkají celé řady oblastí (např. poskytování prostředků EU na financování bezpečných sítí 5G, investic do technologií 5G i technologií dalších generací, nástrojů na ochranu obchodu a hospodářské soutěže, které zabrání narušování trhu dodávek v oblasti technologií 5G atd.).

V případě potřeby by na začátku roku 2021 měli hlavní aktéři dohodnout podrobné podmínky a milníky pro hlavní opatření, která jsou uvedena níže.

Hlavní cíl 1: Zajistit sblížení vnitrostátních přístupů k účinnému zmírňování rizik v celé EU

[120] Zpráva Komise o dopadech doporučení Komise 2019/534 ze dne 26. března 2019 o kybernetické bezpečnosti sítí 5G.

[121] Sdělení Komise COM(2020) 50 nazvané „Bezpečné zavádění sítí 5G v EU – Implementace souboru opatření EU“, 29. ledna 2020.

Oblasti	Hlavní krátkodobá a střednědobá opatření	Hlavní aktéři
Provádění souboru opatření v členských státech	Dokončit provádění opatření doporučených v závěrech souboru opatření do druhého čtvrtletí roku 2021 a v rámci činnosti skupiny pro spolupráci v oblasti bezpečnosti sítí a informací provádět jejich pravidelnou inventuru.	Orgány členských států
Zajistit výměnu informací a osvědčených postupů o strategických opatřeních ve vztahu k dodavatelům	Zintenzívnit výměnu informací a zvážit možné osvědčené postupy, zejména s ohledem na: – omezení vysoce rizikových dodavatelů (SM03) a opatření související s poskytováním spravovaných služeb (SM04), – bezpečnost a odolnost dodavatelských řetězců, zejména v návaznosti na průzkum, který provedlo Sdružení evropských regulačních orgánů v oblasti elektronických komunikací (BEREC) o SM05–SM06.	Orgány členských států, Komise
Budování kapacit a pokyny k technickým opatřením	Provádět hloubkové technické sondy a pracovat na společných pokynech a nástrojích, včetně: – komplexní a dynamické struktury bezpečnostních kontrol a osvědčených postupů pro bezpečnost technologií 5G, pokynů na podporu provádění vybraných technických opatření uvedených v souboru opatření.	Evropská agentura pro bezpečnost sítí a informací, orgány členských států
Hlavní cíl 2: Podporovat průběžnou výměnu znalostí a budování kapacit		
Oblasti	**Hlavní krátkodobá a střednědobá opatření**	**Hlavní aktéři**
Průběžné rozšiřování znalostí	Organizovat činnosti zaměřené na rozšiřování znalostí o technologiích a výzvách, které s nimi souvisejí (otevřené architektury, funkce technologií 5G, jako je např. virtualizace, kontejnerizace, plátkování atd.), formy hrozeb a jejich vývoj, faktické incidenty atd.	Evropská agentura pro bezpečnost sítí a informací, orgány členských států, další zúčastněné strany
Posuzování rizik	Aktualizovat a vyměňovat si informace o aktuálních vnitrostátních posouzeních rizik.	Orgány členských států, Komise, Evropská agentura pro bezpečnost sítí a informací (ENISA)
Společné projekty financované z prostředků EU na podporu provádění souboru opatření	S využitím finančních prostředků EU podporovat projekty podporující provádění souboru opatření, a to zejména v rámci programu Digitální Evropa (např. projekty budování kapacit pro vnitrostátní orgány, zkušební zařízení nebo jiné pokročilé kapacity atd.).	Orgány členských států, Komise
Spolupráce mezi	Podporovat součinnost a spolupráci mezi vnitrostátními	Orgány

zúčastněnými stranami	orgány zabývajícími se kybernetickou bezpečností technologií 5G (např. skupina pro spolupráci v oblasti bezpečnosti sítí a informací, orgány pro kybernetickou bezpečnost, telekomunikační regulační orgány) a se soukromými zúčastněnými stranami.	členských států, Komise, Evropská agentura pro bezpečnost sítí a informací (ENISA)
Hlavní cíl 3: Podporovat odolnost dodavatelského řetězce a prosazovat další strategické cíle EU v oblasti bezpečnosti		
Oblasti	**Hlavní krátkodobá a střednědobá opatření**	**Hlavní aktéři**
Normalizace	Vymezit a provést konkrétní akční plán, který v rámci další činnosti podskupiny pro spolupráci v oblasti bezpečnosti sítí a informací pro normalizaci posílí zastoupení EU v orgánech zabývajících se stanovováním norem s cílem dosáhnout konkrétních bezpečnostních cílů, včetně podpory interoperabilních rozhraní, která usnadní diverzifikaci dodavatelů.	Orgány členských států
Odolnost dodavatelských řetězců	– Provést hloubkovou analýzu ekosystému a dodavatelského řetězce 5G, aby bylo možné lépe určit a sledování jejich klíčové součásti a případné kritické závislosti. – Zajistit, aby fungování trhu a dodavatelského řetězce sítí 5G bylo v souladu s pravidly a cíli EU v oblasti obchodu a hospodářské soutěže, jak jsou definovány ve sdělení Komise ze dne 29. ledna, a aby vývoj investic, které by mohly ovlivnit hodnotový řetězec sítí 5G, byl předmětem prověřování PZI, přičemž je třeba přihlížet k účelům souboru opatření. – Sledovat stávající a očekávané tržní trendy a posuzovat rizika a příležitosti v oblasti Open RAN, zejména na základě nezávislé studie.	Orgány členských států, Komise
Certifikace	Zahájit přípravu příslušného návrhu či návrhů certifikačních systémů pro klíčové komponenty sítí 5G a dodavatelské procesy a napomoci tak překonání určitých rizik, která jsou spojena s technologickými slabinami a která jsou vymezeny v plánech zmírňování rizik souboru opatření.	Komise, Agentura Evropské unie pro bezpečnost sítí a informací (ENISA), vnitrostátní orgány, ostatní zúčastněné strany
Kapacity EU a bezpečné zavádění sítí	– Investovat do výzkumu a vývoje a do kapacit, zejména prostřednictvím přijetí partnerství pro inteligentní sítě a služby. – Zavést příslušné bezpečnostní podmínky pro programy financování EU a finanční nástroje (vnitřní i vnější), jak bylo oznámeno ve sdělení Komise ze dne 29. ledna.	Členské státy, Komise, zúčastněné strany v odvětví 5G

Vnější aspekty	Vstřícně reagovat na žádosti třetích zemí, které se chtějí seznámit s přístupem uplatňovaným v rámci zmiňovaného souboru opatření, který vytvořila EU, a případně tento soubor opatření používat.	Členské státy, Komise ESVČ, delegace EU