EVROPSKÝ ÚČETNÍ DVŮR

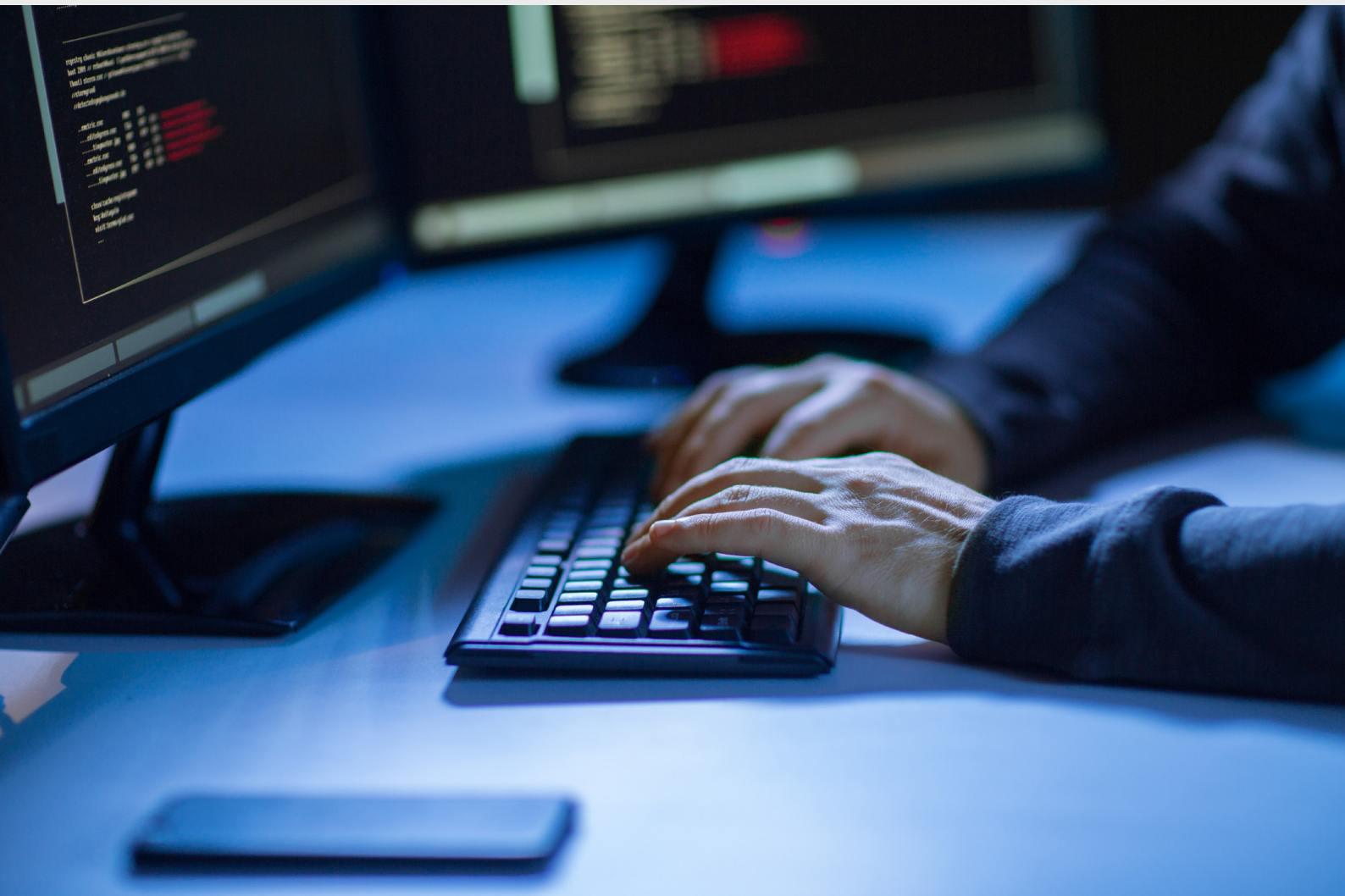
CS

2019

Výzvy týkající se účinné politiky EU v oblasti kybernetické bezpečnosti

Informační dokument

Březen 2019



O dokumentu:

Cílem tohoto informačního dokumentu, který není zprávou z auditu, je poskytnout přehled o komplexní politice EU v oblasti kybernetické bezpečnosti a identifikovat hlavní problémy při jejím účinném provádění. Zabývá se bezpečností sítí a informací, kyberkriminalitou, kybernetickou obranou a dezinformacemi. Tento dokument bude rovněž informovat o veškeré další auditorské činnosti v této oblasti.

Svou analýzu jsme založili na dokumentárním přezkumu veřejně dostupných informací v oficiálních dokumentech, stanoviscích a studiích třetích stran. Naše práce přímo na místě probíhala od dubna do září 2018 a byl zohledněn vývoj do prosince 2018. Svou práci jsme doplnili o průzkum vnitrostátních kontrolních úřadů jednotlivých členských států a rozhovory s klíčovými zúčastněnými stranami z institucí EU a se zástupci soukromého sektoru.

Problémy, které jsme zjistili, jsou seskupeny do čtyř širokých okruhů: i) rámec politiky v oblasti kybernetické bezpečnosti, ii) financování a výdaje, iii) budování kybernetické odolnosti, iv) účinná reakce na kybernetické bezpečnostní incidenty. Zcela zásadním úkolem zůstává dosažení vyšší úrovně kybernetické bezpečnosti v EU. Každou kapitolu tedy končíme řadou myšlenek určených k dalšímu uvážení pro tvůrce politik, zákonodárce a odborné pracovníky.

Rádi bychom ocenili konstruktivní zpětnou vazbu, kterou jsme obdrželi od jednotlivých útvarů Komise, Evropské služby pro vnější činnost, Rady Evropské unie, ENISA, Europolu, Evropské organizace pro kybernetickou bezpečnost a vnitrostátních kontrolních úřadů členských států.

Obsah

Shrnutí

I Technologie otevírá zcela nový svět příležitostí s novými produkty a službami, které se stávají nedílnou součástí našeho každodenního života. Na druhé straně se zvyšuje riziko, že se staneme obětí kyberkriminality nebo kybernetického útoku, jejichž společenský a hospodářský dopad se nadále zvyšuje. Současné směřování EU od roku 2017 k urychlení úsilí o posílení kybernetické bezpečnosti a její digitální nezávislost přichází proto v rozhodující době.

II Cílem tohoto informačního dokumentu, který není zprávou z auditu a je založen na veřejně dostupných informacích, je poskytnout přehled o složité a nevyrovnané situaci v této oblasti a identifikovat hlavní problémy účinného provádění dané politiky. Náš dokument se zabývá politikou EU v oblasti kybernetické bezpečnosti, kyberkriminality a kybernetické obrany a zahrnuje též úsilí o boj proti dezinformacím. Problémy, které jsme zjistili, jsou seskupeny do čtyř širokých okruhů: i) politika v oblasti kybernetické bezpečnosti a legislativní rámec, ii) financování a výdaje, iii) budování kybernetické odolnosti a iv) účinná reakce na kybernetické bezpečnostní incidenty. Každá kapitola obsahuje některé body k úvaze o uvedených problémech.

Politika v oblasti kybernetické bezpečnosti a legislativní rámec

III Vypracovat opatření, která jsou v souladu s rozsáhlými cíli strategie EU v oblasti kybernetické bezpečnosti stát se nejbezpečnějším digitálním prostředím na světě, je vzhledem k absenci měřitelných cílů a k nedostatku spolehlivých údajů velmi náročné. Výsledky jsou málokdy měřeny a hodnoceno je jen málo oblastí politiky. Klíčovým úkolem je tedy **zajistit smysluplné vyvozování odpovědnosti a hodnocení**, a to posunem směrem ke kultuře založené na výkonnosti se zabudovanými hodnotícími mechanismy.

IV Legislativní rámec zůstává neúplný. **Mezery v právních předpisech EU a jejich nedůsledné provádění do vnitrostátního práva** mohou ztížit dosažení plného potenciálu těchto předpisů.

Financování a výdaje

V **Sladění úrovně investic s cíli** je náročné: vyžaduje to nejen zvýšit celkové investice do kybernetické bezpečnosti, které jsou v EU nízké a roztříštěné, ale také zvyšovat dopad, zejména pokud jde o lepší využívání výsledků výdajů na výzkum a zajištění účinného nasměrování a financování začínajících podniků.

VI Pro EU a její členské státy je důležité **mít jasný přehled o výdajích EU**, aby věděly, které nedostatky odstranit, a bylo tak možné splnit stanovené cíle. Vzhledem k tomu, že neexistuje žádný zvláštní rozpočet EU na financování strategie kybernetické bezpečnosti, chybí jasná představa o tom, kam které peníze směřují.

VII V době zvýšených bezpečnostních politických priorit může **omezení dostatečného financování agentur EU, které se zabývají kybernetikou,** bránit tomu, aby byly naplněny ambice EU. Proto je potřeba hledat způsoby, jak přilákat a udržet talenty.

Budování kybernetické odolnosti

VIII Ve veřejném i soukromém sektoru v celé EU i na mezinárodní úrovni se často vyskytují nedostatky v řízení kybernetické bezpečnosti. To narušuje schopnost globálního společenství reagovat na kybernetické útoky a omezovat je a oslabuje soudržný přístup na úrovni celé EU. Důležitým úkolem je tedy **posílit řízení kybernetické bezpečnosti**.

IX **Zvyšování dovedností a povědomí** ve všech odvětvích a úrovních společnosti je nezbytné vzhledem k rostoucímu globálnímu nedostatku znalostí v oblasti kybernetické bezpečnosti. V současné době existují v celé EU pouze omezené normy pro odbornou přípravu, certifikaci nebo hodnocení kybernetického rizika.

X Vytvoření důvěry je rozhodující pro posílení celkové kybernetické odolnosti. Komise sama usoudila, že koordinace je obecně stále nedostatečná. Nadále je problémem **zlepšení výměny informací a koordinace** mezi veřejným a soukromým sektorem.

Účinná reakce na kybernetické bezpečnostní incidenty

XI Digitální systémy jsou natolik složité, že zabránit všem útokům je nemožné. Řešením tohoto problému je **rychlá detekce a reakce**. Kybernetická bezpečnost však ještě není plně začleněna do stávajících mechanismů koordinace reakcí na krizi na úrovni EU, což potenciálně omezuje schopnost EU reagovat na rozsáhlé, přeshraniční kybernetické bezpečnostní incidenty.

XII Prvořadá je **ochrana kritické infrastruktury a společenských funkcí**. Závažným problémem je případné zasahování do volebních procesů a dezinformační kampaně.

XIII Současné výzvy, jimž čelí EU a širší globální prostředí v souvislosti s kybernetickými hrozbami, vyžadují soustavné úsilí a stálé a vytrvalé dodržování základních hodnot EU.

Úvod

01 Technologie otevírá zcela nový svět příležitostí. Tak, jak přichází nové produkty a služby, stávají se nedílnou součástí našeho každodenního života. S každým novým rozvojem však roste naše závislost na technologiích, a tedy i význam kybernetické bezpečnosti. Čím více osobních údajů uvedeme na internet a čím více se připojujeme, tím spíše se můžeme stát obětí některé formy kyberkriminality nebo kybernetického útoku.

Co je to kybernetická bezpečnost?

02 Neexistuje žádná standardní, obecně přijímaná definice kybernetické bezpečnosti[1]. Obecně řečeno to jsou veškeré pojistky a opatření přijatá na ochranu informačních systémů a jejich uživatelů před nepovoleným přístupem, útokem a poškozením s cílem zajistit zachování důvěrnosti, integrity a dostupnosti údajů.

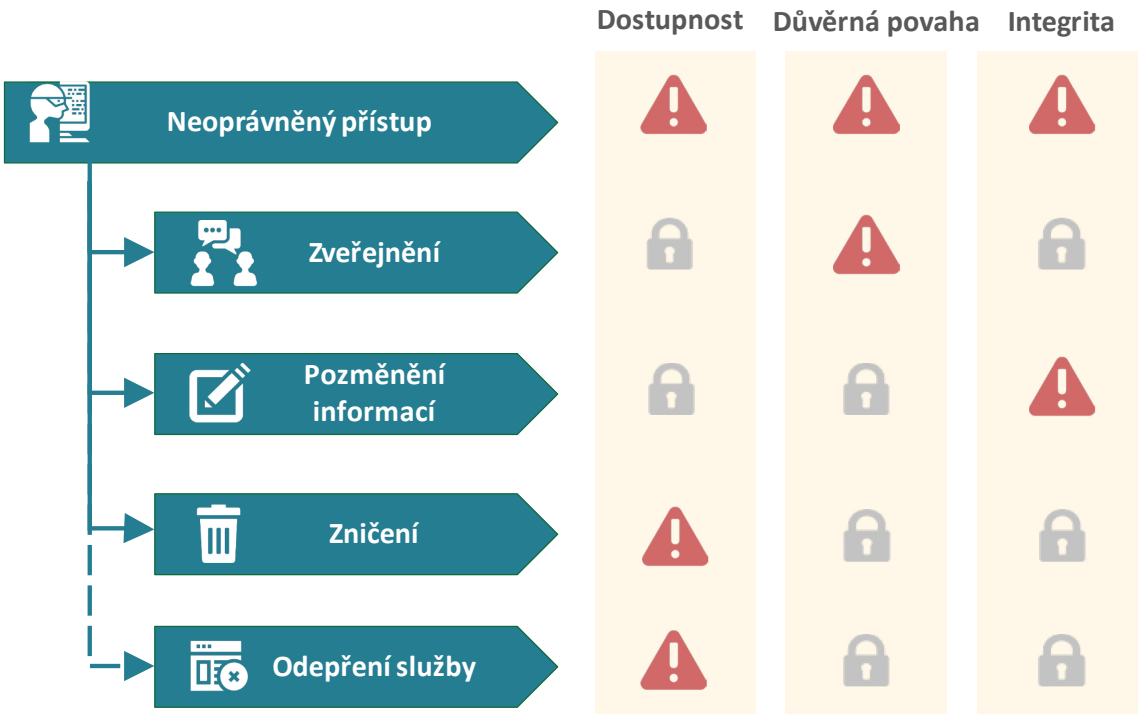
03 Kybernetická bezpečnost zahrnuje předcházení kybernetickým bezpečnostním incidentům, jejich odhalování, reakci na ně a zotavení. Incidenty mohou či nemusí být záměrné a mohou se například týkat náhodného zveřejnění informací, ale i útoků na podniky a kritickou infrastrukturu, krádeže osobních údajů a dokonce i zasahování do demokratických procesů. To vše může mít dalekosáhlé škodlivé účinky na jednotlivce, organizace a komunity.

04 Jako pojem používaný v odborných kruzích EU se kybernetická bezpečnost neomezuje pouze na bezpečnost sítí a informací. Zahrnuje veškeré protiprávní činnosti obnášející používání digitálních technologií v kybernetickém prostoru. Může se tedy jednat o kybernetické trestné činy, jako například útoky pomocí počítačových virů a bezhotovostní platební podvody, činnosti zasahující jak systémy, tak obsah, stejně jako šíření materiálů o sexuálním zneužívání dětí na internetu. Takové činnosti mohou spočívat také v dezinformačních kampaních, které ovlivňují online diskusi, a v možném zasahování do voleb. Europol navíc spatřuje úzký vztah mezi kyberkriminalitou a terorismem[2].

05 Kybernetické bezpečnostní incidenty podněcují různí aktéři – včetně států, zločineckých skupin a hacktivistů, přičemž jsou vedeni různými pohnutkami. Důsledky těchto incidentů se projevují na vnitrostátní, evropské a dokonce i globální úrovni. Nehmotná a převážně bezhraniční povaha internetu a použité nástroje a taktiky však často ztěžují identifikaci pachatele útoku (takzvaný „problém přiřazení pachatele“).

06 Řada druhů ohrožení kybernetické bezpečnosti může být klasifikována podle toho, co dělají s daty – zveřejnění, modifikaci, zničení nebo odepření přístupu, – nebo podle toho, které základní zásady bezpečnosti informací porušují, jak je znázorněno na ***obrázku 1***. Několik příkladů útoků je popsáno v ***rámečku 1***. Vzhledem k tomu, že útoky na informační systémy jsou stále promyšlenější, naše obranné mechanismy se stávají méně účinnými[3].

Obrázek 1 – Druhy ohrožení a zásady bezpečnosti, které jsou jimi ohroženy



Zdroj: EÚD upraveno ze studie Evropského parlamentu [4]. Zámek = bezpečnost není nijak ovlivněna; Vykřičník = bezpečnost je ohrožena

Rámeček 1

Druhy kybernetických útoků

Vždy, když se nové zařízení připojuje k internetu nebo se připojuje k jiným zařízením, zvětšuje se v rámci kybernetické bezpečnosti tzv. „prostor k útoku“. Exponenciální růst internetu věcí, cloudů, dat velkého objemu a digitalizace průmyslu jsou doprovázeny nárůstem expozice zranitelných míst, což umožňuje osobám s nekalými úmysly zaměřovat se na stále více obětí. V důsledku rozmanitosti typů útoků a jejich rostoucí promyšlenosti je skutečně obtížné udržet krok[5].

Malware (škodlivý software) je navržen tak, aby poškozoval zařízení nebo sítě. Může jít o viry, trojské koně, ransomware, červy, adware a spyware. **Ransomware** šifruje údaje, brání uživatelům v přístupu k vlastním souborům, dokud není zaplaceno výkupné, zpravidla v kryptoměně, nebo proveden určitý krok. Podle Europolu jsou útoky ransomware převládajícím typem útoku a v posledních několika letech došlo doslova k explozi počtu druhů ransomware. Dochází také k nárůstu útoků **distribuovaného odepření služby** (DDoS), které znepřístupňuje služby nebo zdroje tím, že je zaplaví větším množstvím požadavků, než jsou schopny zvládnout. K tomuto typu útoku došlo v roce 2017 u jedné třetiny organizací[6].

Uživatelé mohou být vmanipulováni do nechtěného provedení určité akce nebo do zveřejnění důvěrných informací. Tento trik může být použit pro krádež údajů nebo kybernetickou špionáž a je známý jako **sociální inženýrství**. Existují různé způsoby, jak toho dosáhnout, ale běžnou metodou je **phishing**, kdy e-maily, které vypadají, jako by pocházely z důvěryhodných zdrojů, vybízejí uživatele k odhalení informací nebo kliknutí na odkazy, které pak infikují zařízení staženým malwarem. Více než polovina členských států informovala o vyšetřování síťových útoků[7].

Snad nejhanebnějšími typy hrozeb jsou **pokročilé trvalé hrozby** (APT). Páchají je sofistikovaní útočníci zabývající se dlouhodobým sledováním a krádežemi údajů, kteří někdy skrývají také destruktivní cíle. Cílem u těchto útoků je co nejdéle se udržet bez odhalení. Pokročilé trvalé hrozby se často týkají státu a jsou zaměřeny na obzvláště citlivá odvětví, jako je technologie, obrana a kritická infrastruktura. Kybernetická špionáž údajně představuje nejméně jednu čtvrtinu všech kybernetických bezpečnostních incidentů a většinu nákladů[8].

Jak vážný je to problém?

07 Přesně popsat dopad špatné připravenosti na kybernetický útok je obtížné vzhledem k nedostatku spolehlivých údajů. Hospodářský dopad kyberkriminality se v letech 2013 až 2017 zvýšil pětinásobně[9], zasáhl státy a společnosti, a to jak velké, tak malé. Tento trend odráží předpokládaný nárůst pojistného v oblasti kybernetiky ze 3 miliard EUR v roce 2018 na 8,9 miliardy EUR v roce 2020.

08 Zatímco finanční dopad kybernetických útoků nadále roste, existuje alarmující rozdíl mezi náklady na zahájení útoku a náklady na prevenci, vyšetřování a nápravu. Například útok DDoS může stát jen 15 EUR měsíčně, avšak ztráty, které utrpí cílový podnik, včetně poškození dobrého jména, jsou podstatně vyšší[10].

09 Přestože 80 % podniků z EU zaznamenalo v roce 2016 alespoň jeden incident v oblasti kybernetické bezpečnosti[11], je přiznání rizik stále znepokojivě nízké. Pokud jde o společnosti v EU, 69 % z nich nemá žádné, nebo má jen základní znalosti o vystavení kybernetickým hrozbám[12], a 60 % nikdy neodhadovalo případné finanční ztráty[13]. Navíc podle globálního průzkumu by jedna třetina organizací raději zaplatila hackerovi výkupné, než aby investovala do informační bezpečnosti[14].

10 Globální společné útoky ransomwaru *Wannacry* a wiperu *NotPetya* v roce 2017 postihly více než 320 000 obětí přibližně ve 150 zemích[15]. Tyto incidenty vedly k jakémusi celosvětovému uvědomění si hrozby představované kybernetickými útoky, čímž vznikl nový podnět, který vnesl kybernetickou bezpečnost do hlavního politického myšlení. Navíc 86 % občanů EU nyní věří, že riziko, že se stane obětí kyberkriminality, se stále zvyšuje[16].

Kroky EU v oblasti kybernetické bezpečnosti

11 V roce 2001 se EU stala pozorovatelskou organizací ve Výboru Rady Evropy pro Úmluvu o kyberkriminalitě[17] (Budapešťská úmluva). Od té doby EU používá politiku, právní předpisy a výdaje na to, aby zlepšila svou kybernetickou odolnost. Na pozadí rostoucího počtu velkých kybernetických útoků a incidentů se činnost od roku 2013 zrychluje, jak ukazuje ***obrázek 2***. Zároveň členské státy přijaly (a v některých případech již aktualizovaly) své první národní strategie v oblasti kybernetické bezpečnosti.

12 Hlavní aktéři EU s odpovědností za kybernetickou bezpečnost jsou popsáni v ***rámečku 2*** a v ***příloze I***.

Rámeček 2

Kdo je do činnosti zapojen?

Evropská komise si klade za cíl zvýšit schopnosti a spolupráci v oblasti kybernetické bezpečnosti, posílit EU jako hráče v oblasti kybernetické bezpečnosti a začlenit ji do dalších politik EU. Hlavními generálními ředitelstvími (GŘ) zodpovědnými za politiku kybernetické bezpečnosti jsou GŘ **CNECT** (kybernetická bezpečnost) a **HOME** (kyberkriminalita), která jsou odpovědná za jednotný digitální trh a bezpečnostní unii. GŘ **DIGIT** odpovídá za bezpečnost vlastních informačních systémů Komise.

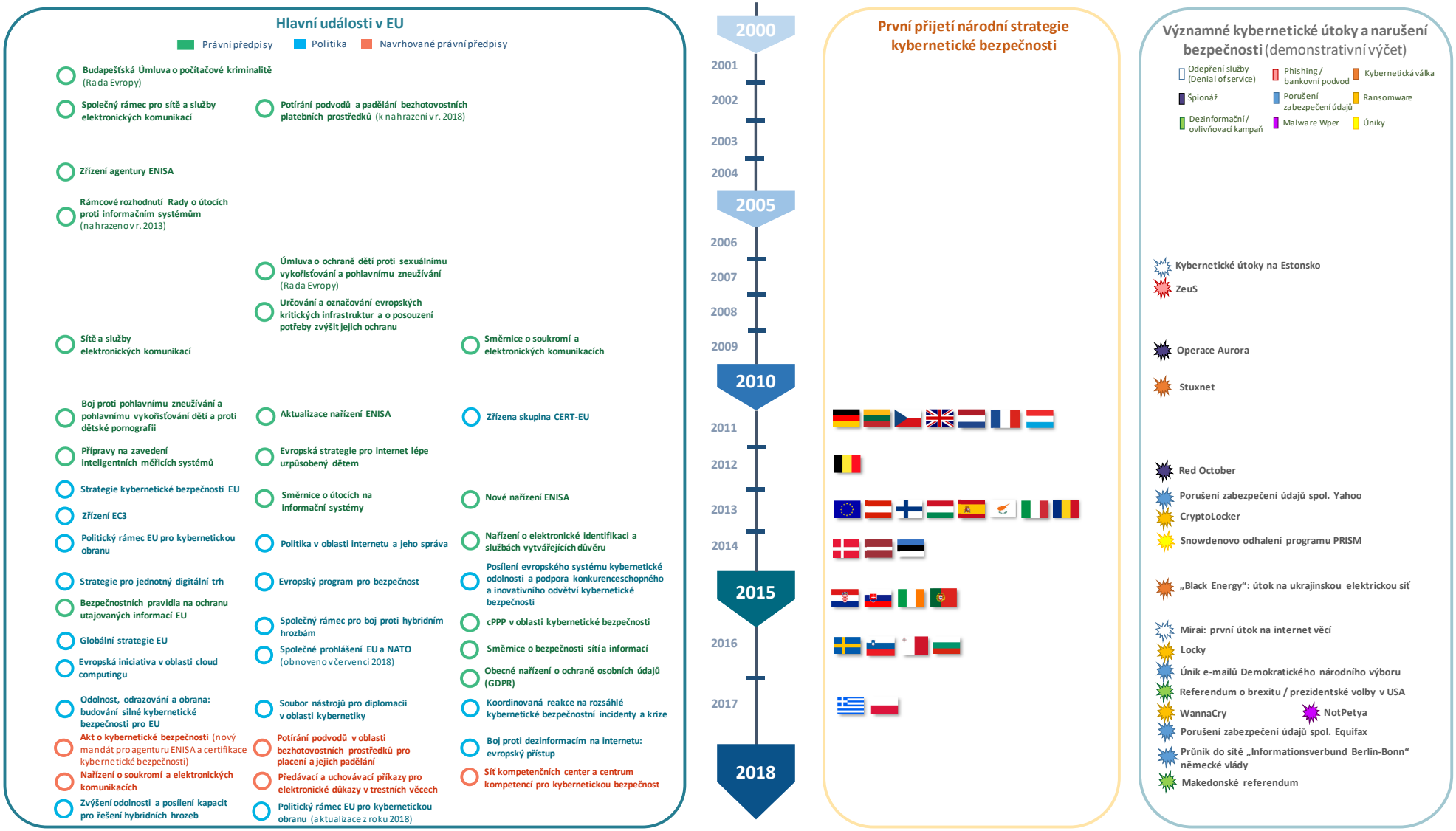
Řada agentur EU Komisi podporuje, zejména **ENISA** (Agentura Evropské unie pro bezpečnost sítí a informací), agentura EU pro kybernetickou bezpečnost – hlavní poradní orgán, který podporuje rozvoj politik, budování kapacit a zvyšování povědomí. Středisko Europolu pro boj proti kyberkriminalitě (**EC3**) bylo zřízeno za účelem posílení reakce EU při vymáhání práva v oblasti kyberkriminality. Skupina pro reakci na počítačové hrozby (**CERT-EU**), která podporuje všechny orgány, instituce a agentury Unie, je pod záštitou Komise.

Evropská služba pro vnější činnost (ESVČ) stojí v čele kybernetické obrany, kybernetické diplomacie a strategické komunikace a zaštiťuje zpravodajská a analytické střediska. **Evropská obranná agentura** (EDA) se zaměřuje na rozvoj schopností kybernetické obrany.

Členské státy jsou především zodpovědné za svou vlastní kybernetickou bezpečnost a na úrovni EU jednají prostřednictvím **Rady**, která má řadu orgánů pro koordinaci a sdílení informací (mezi něž patří Horizontální pracovní skupina pro kybernetické otázky). **Evropský parlament** jedná jako spolunormotvůrce.

Organizace soukromého sektoru, včetně průmyslu, orgánů správy internetu a akademické obce, jsou partnery a zároveň přispívají k tvorbě a provádění politik – a to i prostřednictvím smluvního partnerství veřejného a soukromého sektoru (**cPPP**).

Obrázek 2 – Urychlení vývoje v oblasti politiky a právních předpisů (ke dni 31. prosince 2018)



Zdroj: EÚD.

Politika

13 Kybernetický ekosystém EU je složitý a mnohovrstvý, prochází celou řadou oblastí vnitřních politik, jako je spravedlnost a vnitřní věci, jednotný digitální trh a politiky v oblasti výzkumu. Ve vnější politice se kybernetická bezpečnost vyznačuje diplomacií a je stále častěji součástí rozvíjející se obranné politiky EU.

14 Základním kamenem politiky EU je **Strategie kybernetické bezpečnosti z roku 2013**[18]. Cílem strategie je, aby se digitální prostředí EU stalo nejbezpečnějším na světě a současně obhajovalo základní hodnoty a svobody. Má pět základních cílů: i) zvýšení kybernetické odolnosti, ii) snížení kyberkriminality, iii) rozvoj politik a schopností kybernetické obrany, iv) rozvoj průmyslových a technologických zdrojů kybernetické bezpečnosti a v) vytvoření mezinárodní kyberprostorové politiky sladěné se základními hodnotami EU.

15 Strategie kybernetické bezpečnosti je propojena se třemi následně přijatými strategiemi:

— Cílem **Evropského programu pro bezpečnost** (2015) je zlepšit vymáhání práva a soudní reakci na kyberkriminalitu, zejména obnovením aktualizace stávajících politik a právních předpisů[19]. Rovněž se snaží identifikovat překážky vyšetřování trestné činnosti v oblasti kyberkriminality a posílit budování kapacit v oblasti kybernetiky.

— Cílem **Strategie pro jednotný digitální trh**[20] (2015) je vybudovat lepší přístup k digitálnímu boží a službám na základě vytvoření řádných podmínek, v nichž bude moci být maximalizován růstový potenciál digitální ekonomiky. Pro tento účel je nezbytné posílení online bezpečnosti, důvěry a začlenění.

— Cílem **globální strategie**[21] z roku 2016 je posílení úlohy EU ve světě. Kybernetická bezpečnost je základním pilířem obnoveného úsilí v oblasti kybernetických otázek, spolupráce s klíčovými partnery a rozhodnutí řešit kybernetické problémy ve všech oblastech politiky, včetně vyvrácení dezinformací prostřednictvím strategické komunikace.

16 V posledních letech, jak se kyberprostor stal stále více militarizovaným[22] a ozbrojeným[23], začal být považován za pátou oblast válčení[24]. Kybernetická obrana chrání kybernetické systémy, sítě a kritickou infrastrukturu před útoky vojenskými a jinými prostředky. **Rámec politiky v oblasti kybernetické obrany** byl přijat v roce 2014 a aktualizován byl v roce 2018[25]. Aktualizace v roce 2018 určuje šest priorit, včetně

rozvoje schopností kybernetické obrany i ochrany komunikačních a informačních sítí společné bezpečnostní a obranné politiky (SBOP). Kybernetická obrana je také součástí rámce stálé strukturované spolupráce (PESCO) a spolupráce mezi EU a NATO.

17 **Společný rámec EU pro boj proti hybridním hrozbám** (2016) řeší kybernetické hrozby pro kritickou infrastrukturu i pro soukromé uživatele, přičemž zdůrazňuje, že kybernetické útoky mohou být prováděny prostřednictvím dezinformačních kampaní na sociálních médiích[26]. Zaznamenává také potřebu zlepšit informovanost a posílit spolupráci mezi EU a NATO, jejíž základ byl dán ve společných prohlášeních EU-NATO z roku 2016 a 2018[27].

18 V roce 2017 Komise předložila nový balíček v oblasti kybernetické bezpečnosti, který odráží zvyšující se naléhavost digitální ochrany. Zahrnoval nové sdělení Komise, které aktualizuje strategii kybernetické bezpečnosti z roku 2013[28], návrh rychlé a koordinované reakce na rozsáhlý útok a rychlé provedení směrnice o bezpečnosti sítí a informací (směrnice NIS)[29]. Balíček dále zahrnoval řadu legislativních návrhů (viz bod ***22***).

Právní předpisy

19 Od roku 2002 byly přijaty právní předpisy s různou měrou významu pro kybernetickou bezpečnost.

20 Hlavním pilířem strategie kybernetické bezpečnosti z roku 2013 je ústřední právní předpis, jímž je **směrnice o bezpečnosti sítí a informací**[30] z roku 2016, která je prvním právním předpisem o kybernetické bezpečnosti platným v celé EU. Směrnice, která měla být provedena do května 2018, má za cíl dosáhnout minimální úrovně harmonizovaných kapacit tím, že zaváže členské státy k přijetí národních strategií bezpečnosti sítí a informací a k vytvoření jednotných kontaktních míst a skupin pro reakce na počítačové bezpečnostní incidenty (týmy CSIRT)[31]. Stanoví rovněž bezpečnostní požadavky a požadavky na hlášení incidentů pro poskytovatele základních služeb v kritických odvětvích a pro poskytovatele digitálních služeb.

21 Souběžně s tím vstoupilo v roce 2016 v platnost **nařízení o obecné ochraně osobních údajů**[32] (GDPR), které se uplatňuje od května 2018. Jeho cílem je chránit osobní údaje evropských občanů stanovením pravidel pro jejich zpracování a šíření. Zaručuje subjektům údajů určitá práva a ukládá povinnosti správcům údajů (poskytovatelům digitálních služeb), pokud jde o používání a přenos informací. Ukládá také požadavky na oznamování v případě porušení a v některých případech může

ukládat pokuty. ***Obrázek 3*** ukazuje, jak se směrnice o bezpečnosti sítí a informací a GDPR vzájemně doplňují v rámci svých cílů, jak posílit kybernetickou bezpečnost a zajistit ochranu údajů.

22 Návrh právního předpisu, o němž se v současné době diskutuje, zahrnuje navrhovaný akt o kybernetické bezpečnosti s cílem posílit ENISA a zavést celounijní certifikační mechanismus[33], navrhované nařízení o předávacích a uchovávacích příkazech pro elektronické důkazy[34] a navrhovanou směrnici o elektronických důkazech[35]. Návrh Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center (dále jen „síť center kompetencí pro kybernetickou bezpečnost a výzkumné centrum kompetencí“) z roku 2018 tvoří součást balíčku pro kybernetickou bezpečnost z roku 2017[36].

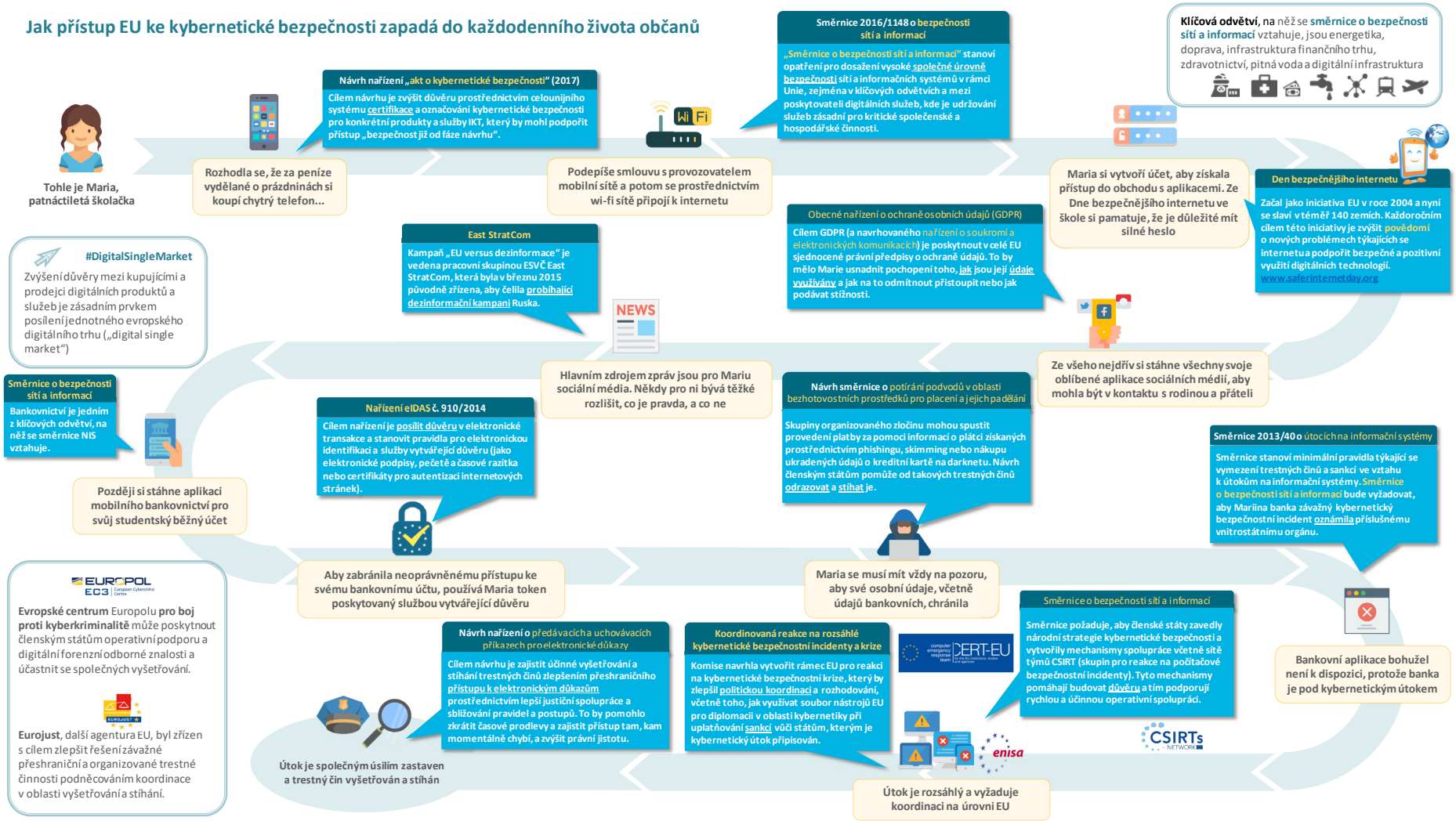
23 Může být obtížné získat představu o rozsahu politiky a legislativního rámce, který se dotýká kybernetické bezpečnosti a toho, jak ovlivňuje náš každodenní život.

24 ***Obrázek 4*** se pokouší mapovat průsečík různých legislativních aktů a dalších aktivit s životem fiktivního evropského občana.

Obrázek 3 – Jak se vzájemně doplňují směrnice o GDPR a směrnice o NIS

Zdroj: EÚD.

Obrázek 4 – Jak přístup EU ke kybernetické bezpečnosti zapadá do každodenního života občanů



Zdroj: EÚD.

Budování politiky a legislativního rámce

25 Kybernetický ekosystém EU je složitý a mnohovrstevnatý a zahrnuje mnoho zúčastněných stran (viz ***příloha I***). Spojení všech jeho nesourodých částí je velkou výzvou. Od roku 2013 probíhá soustředěná snaha o dosažení soudržnosti v oblasti kybernetické bezpečnosti EU[37].

Výzva 1: smysluplné hodnocení a odpovědnost

26 Stanovení příčinného vztahu mezi strategií na rok 2013 a všemi zřejmými změnami je obtížné, jak poznamenala Komise. Cíle strategie na rok 2013 byly formulovány velmi široce a „vyjádřily spíše vizi než měřitelný cíl“[38]. Vypracovat opatření v souladu s těmito širokými cíli je tam, kde neexistují měřitelné cíle, obtížné. Aktualizovaný rámec politiky pro kybernetickou obranu (2018) bude zaměřen na rozvoj cílů stanovujících minimální úroveň kybernetické bezpečnosti a důvěry, které je třeba dosáhnout. Bude se však omezovat na kybernetickou obranu. Nebyly stanoveny cíle vymezující požadovanou úroveň odolnosti pro EU jako celek.

27 Výsledky jsou málokdy měřeny a je hodnoceno jen málo oblastí politiky[39]. To je částečně způsobeno tím, že nedávno byla provedena řada opatření – legislativních nebo jiných, což brání úplnému vyhodnocení jejich dopadu. Úkolem je definovat smysluplná kritéria hodnocení, která mohou pomoci měřit dopad. Důkladné hodnocení se navíc ještě nestalo normou pro kybernetickou bezpečnost obecně. Proto je nutný posun směrem ke kultuře výkonnosti s vloženými postupy hodnocení a standardizovaným podáváním zpráv. Současný mandát agentury ENISA se nevztahuje na hodnocení a monitorování stavu kybernetické bezpečnosti a připravenosti EU.

28 Tvorba politiky založená na důkazech závisí na dostupnosti dostatečných spolehlivých údajů a statistik s cílem pomáhat monitorovat a analyzovat trendy a potřeby. Absence povinného a společného monitorovacího systému vede k nedostatku spolehlivých údajů. Ukazatele často nejsou snadno dostupné a jsou obtížně definovatelné[40]. V některých oblastech, jako je například cyklus politiky EU, byly vyvinuty specifické metrické funkce používané pro řešení závažné a organizované trestné činnosti.

29 Jen málo členských států pravidelně shromažďuje oficiální údaje o záležitostech souvisejících s kybernetikou, což znemožňuje srovnání. EU zatím projevila jen malou

potřebu konsolidace statistik na evropské úrovni[41]. Existuje také několik nezávislých celounijních analýz, které pokrývají klíčová témata, jako jsou[42]: ekonomika kybernetické bezpečnosti, včetně aspektů chování (nesoulad pobídek, informační asymetrie), porozumění dopadu kybernetických výpadků a kyberkriminality, makro-statistiky o kybernetických trendech a očekávaných výzvách a nejlepší způsoby řešení hrozeb.

30 S ohledem na chybějící konkrétní cíle a nedostatek spolehlivých údajů a řádně definovaných ukazatelů je dosavadní posouzení dosažených výsledků strategie do značné míry kvalitativní. Zprávy o pokroku často popisují prováděné činnosti nebo dosažené milníky bez důkladného měření výsledků. Navíc zatím nebyly stanoveny základy pro hodnocení odolnosti systémů. Vzhledem k chybějící kodifikované definici kyberkriminality je také téměř nemožné nalézt relevantní evropské ukazatele, které by napomohly sledování a hodnocení.

31 Nezávislý dohled nad prováděním politiky kybernetické bezpečnosti se v jednotlivých členských státech liší. Zkoumali jsme, jaké mají vnitrostátní kontrolní úřady zkušenosti s kontrolou této oblasti. Polovina všech respondentů[43] tuto oblast nikdy nekontrolovala. Pro ty, které kontrolu prováděly, byla hlavním cílem kontrol správa informací, ochrana kritické infrastruktury, výměna informací a koordinace mezi klíčovými zúčastněnými stranami, připravenost na incidenty, oznamování a reakce. Mezi méně pokrytá témata patřila opatření na zvyšování povědomí a nedostatek digitálních dovedností. Výsledky těchto kontrol nebo hodnocení nejsou vždy zveřejňovány z důvodů národní bezpečnosti. Seznam zveřejněných zpráv z kontrol podle vnitrostátních kontrolních úřadů je uveden v ***příloze III***.

32 Jako hlavní problémy při provádění kontrol správních opatření v této oblasti se jevila omezení v dovednostech týkajících se kybernetiky (viz též body ***82 až 90***) a obtíže při hodnocení pokroku v oblasti kybernetické bezpečnosti.

Výzva 2: řešení nedostatků v právních předpisech EU a jejich nevyrovnané provádění do vnitrostátních právních řádů

33 Rychlost, s jakou se objevují nové technologie a hrozby, výrazně překonává návrh a provádění právních předpisů EU. Postupy Unie nebyly zamýšleny v souvislosti s digitálním věkem: jedná se o kritickou prioritu při vývoji inovativních a flexibilních postupů, které zajistí politiku a účelový právní rámec[44] vhodný pro lepší předvídání a formování budoucnosti[45].

34 Navzdory snahám o větší soudržnost zůstává legislativní rámec pro kybernetickou bezpečnost neúplný (některé příklady viz ***tabulka 1***). Roztříštěnost a mezery brání dosažení celkových cílů politiky a vedou k neefektivitě. Mezi nedostatky, které Komise uvedla ve strategickém posouzení, patří internet věcí, rovnováha odpovědnosti mezi uživateli a poskytovateli digitálních produktů a některé aspekty, které směrnice o bezpečnosti sítí a informací neřeší. Navrhovaný akt o kybernetické bezpečnosti se pokouší tuto skutečnost částečně řešit podporou zabezpečení na základě návrhu prostřednictvím celounijního certifikačního systému. Některé zúčastněné subjekty se domnívají, že jasně definovaná kybernetická průmyslová politika a společný přístup k problematice kybernetické špionáže stále výrazně chybí[46].

Tabulka 1 – Nedostatky a nevyrovnané provádění do právního rámce (demonstrativní výčet)

Oblast politiky	Příklady
Jednotný digitální trh	o Stávající směrnice o prodeji spotřebitelům se nezabývá kybernetickou bezpečností. Cílem navrhovaných směrnic o digitálním obsahu[47] a o internetovém prodeji[48] je řešit tento nedostatek. o Existují omezené a rozmanité právní rámce pro povinnosti péče v členských státech EU, které vedou k právní nejistotě a potížím při vymáhání opravných právních prostředků[49]. o Politiky týkající se zveřejňování informací o zranitelnosti softwaru se rozvíjejí v různých členských státech různou rychlostí, přičemž na úrovni EU neexistuje zastřešující právní rámec, který by umožňoval koordinovaný přístup[50].
Posilování sítě a informační bezpečnosti	o Členské státy mohou dle svého uvážení zahrnovat odvětví, která směrnice o bezpečnosti sítí a informací opomíjí[51]. Oblasti ubytování, které nejsou pokryty, mohou být branou pro další trestnou činnost, včetně obchodování s lidmi a s drogami a nelegálního přistěhovalectví[52].
Boj proti kyberkriminalitě	o Mnohé členské státy nedefinovaly ve svých vnitrostátních právních předpisech elektronické důkazy[53] (viz též bod ***22***). o Současné rámcové rozhodnutí o bezhotovostních platebních podvodech výslovně nezahrnuje nefyzické platební nástroje, jako jsou virtuální měny, elektronické peníze a mobilní peníze, a nezahrnuje ani taková jednání, jako je phishing, skimming a držení a sdílení informací plátce[54]. o Směrnice o útoku proti informačním systémům se přímo nezaměřuje na nezákonné získávání údajů zevnitř (např. kybernetickou špionáž), což vede k problémům při vymáhání práva[55]. o Po rozsudku Soudního dvora Evropské unie o uchovávání údajů[56] zabránily rozdíly v uplatňování právního rámce mezi členskými státy prosazování práva, což může mít za následek ztrátu náskoku ve vyšetřování a narušení účinného stíhání trestné činnosti na internetu[57].

Zdroj: EÚD.

35 Uplatňování některých aspektů právních předpisů je i nadále dobrovolné jak pro vnitrostátní orgány, tak pro soukromé poskytovatele. Například v rámci skupiny pro spolupráci je hodnocení vnitrostátních strategií týkajících se bezpečnosti sítí a informací a účinnosti CSIRT dobrovolné. Dobrovolné bude také uplatňování certifikace pro produkty a služby IKT v rámci navrhovaného certifikačního schématu v aktu o kybernetické bezpečnosti.

36 V EU je kybernetická bezpečnost výsadou členských států. Navzdory tomu má EU klíčovou úlohu při vytváření podmínek pro zlepšení kapacit svých členských států a pro jejich spolupráci a vytváření důvěry. Přesto vzhledem k velkým rozdílům mezi členskými státy, pokud jde o kapacitu a zapojení[58], zůstane poskytování citlivých informací (o národní bezpečnosti) dobrovolné.

37 Nedůsledné provádění právních předpisů EU do vnitrostátního práva členských států může mít za následek právní a provozní nesoudržnost a brání tomu, aby právní předpisy dosáhly svého plného potenciálu. Například členské státy mají rozdílné výklady, jak by měly být uplatňovány kontroly vývozu zboží dvojího užití[59], takže některé společnosti se sídlem v EU mohou vyvážet technologie a služby, které mohou být používány pro kybernetický dohled a porušování lidských práv prostřednictvím cenzury nebo zachycování. Evropský parlament vyjádřil v souvislosti s tím své obavy[60].

38 Kromě toho ochrana soukromí a svoboda projevu vyžadují uzpůsobenou legislativní odpověď, aby bylo dosaženo nezbytné rovnováhy mezi ochranou základních hodnot a dosažením naléhavých bezpečnostních požadavků EU. Jak zajistíme například šifrování mezi koncovými body a zároveň nalezení nejlepšího způsobu, jak podpořit prosazování práva? Nebo jak bychom mohli splnit cíle GDPR a pochopit zároveň jeho dopady na veřejně dostupné informace o žadatelích o registraci doménových jmen a držitelů bloků IP adres? A jak to může negativně ovlivnit vyšetřování prosazování práva[61]?

39 Samotné právní předpisy nezaručují odolnost. Přestože cílem směrnice o bezpečnosti sítí a informací je dosáhnout vysokého stupně bezpečnosti v celé EU, otevřeně se soustředí na dosažení minimální, nikoli maximální harmonizace[62]. S tím, jak se kybernetické prostředí vyvíjí, budou se nedostatky objevovat i nadále.

Body k úvaze – rámec politiky

- Jaké kritické kroky jsou zapotřebí, aby se tvůrci politiky a zákonodárci posunuli směrem k intenzivnějšímu výkonu v oblasti kybernetické bezpečnosti, včetně definování celkové odolnosti?
- Jak může výzkum lépe přispívat ke generování potřebných údajů a statistik, které umožní smysluplné hodnocení?
- Jakým způsobem mohou být legislativní procesy EU přizpůsobeny tak, aby byly pružnější a lépe zohledňovaly rychlost technologického vývoje a vývoj hrozeb?
- Jak může být praxe rozvoje metrik (ukazatelů, cílů) v cyklu politik EU přizpůsobena, rozšířena a replikována pro oblast kybernetické bezpečnosti jako celku?
- Co se mohou vnitrostátní kontrolní úřady naučit ze vzájemných přístupů ke kontrole politik a opatření v oblasti kybernetické bezpečnosti?
- Jaké nesrovnalosti při provádění a uplatňování právního rámce EU oslabují účinnější reakci na nedostatky v oblasti kybernetické bezpečnosti a kyberkriminality a jak by to členské státy a orgány EU mohly nejlépe řešit?
- Jak efektivní jsou kontroly vývozu kybernetických výrobků a služeb EU při předcházení porušování lidských práv mimo EU?

Financování a výdaje

40 EU má své záměry stanovené tak, aby se stala nejbezpečnějším online prostředím na světě. Dosažení těchto cílů vyžaduje značné úsilí všech zúčastněných stran, včetně řádné a dobře řízené finanční základny.

Výzva 3: sladění míry investic s cíli

Zvýšení objemu investic

41 Celková míra výdajů na kybernetickou bezpečnost v celosvětovém měřítku jako procento HDP je odhadována na 0,1 %. Ve Spojených státech[63] tento objem představuje přibližně 0,35 % (včetně soukromého sektoru). Jako procento HDP představují výdaje federální vlády USA zhruba 0,1 % nebo přibližně 21 miliard USD plánovaných v rozpočtu na rok 2019[64].

42 Výdaje v EU jsou ve srovnání s tím nízké, roztříštěné a často nejsou podporované koordinovanými programy řízenými vládami. Údaje není snadné získat, ale odhaduje se, že veřejné výdaje EU na kybernetickou bezpečnost se pohybují mezi jednou a dvěma miliardami eur ročně[65]. Výdaje některých členských států jako procento HDP představují jednu desetinu objemu USA, nebo dokonce méně[66]. EU a její členské státy musí vědět, kolik investují kolektivně, aby věděly, které nedostatky je třeba vyřešit.

43 Je obtížné vytvořit komplexní obraz, protože chybí jasné údaje v důsledku průřezové povahy kybernetické bezpečnosti a protože kybernetickou bezpečnost a všeobecné výdaje na IT nelze často rozlišit[67]. Náš průzkum potvrdil, že je obtížné získat spolehlivé statistiky výdajů ve veřejném i soukromém sektoru. Tři čtvrtiny vnitrostátních kontrolních úřadů uvedly, že nemají centralizovaný přehled o vládních výdajích souvisejících s kybernetikou, a žádný členský stát neukládá veřejnoprávním subjektům povinnost vykazovat ve svých finančních plánech výdaje na kybernetickou bezpečnost samostatně.

44 Zvláštní výzvou je posílení veřejných a soukromých investic do evropských firem v oblasti kybernetické bezpečnosti. Veřejný kapitál je často dostupný pro počáteční fáze, ale již méně pro fáze růstu a expanze[68]. Existuje mnoho iniciativ na financování ze strany EU, které však nejsou využívány, a to převážně kvůli administrativní zátěži[69]. Celkově mají evropské firmy v oblasti kybernetické bezpečnosti nižší výkonnost oproti stejným mezinárodním firmám: je jich méně a průměrná výše finančních prostředků,

které získávají, je výrazně nižší[70]. Zajištění efektivního zaměření a financování začínajících podniků je proto klíčové pro dosažení cílů EU v oblasti digitální politiky.

Zvýšení dopadu

45 Vyřešení nedostatku investic do kybernetické bezpečnosti musí přinést užitečné výsledky. Například, navzdory síle odvětví výzkumu a inovací v EU nejsou výsledky dostatečně patentovány, komercializovány nebo rozšiřovány, aby pomohly posílit odolnost, konkurenceschopnost a digitální nezávislost[71]. To platí zejména v porovnání s globálními konkurenty EU. Nedostatek řádně využívaných výsledků vyplývá z řady faktorů[72], mezi něž patří:

- nedostatek konzistentní nadnárodní strategie, která by rozšířila přístup, jenž by odpovídal širším digitálním potřebám EU pro konkurenceschopnost a větší samostatnost;
- délka cyklu hodnotového řetězce, což znamená, že nástroje budou brzy zastaralé;
- nedostatek udržitelnosti, neboť projekty obvykle končí rozpuštěním projektového týmu a ukončením podpory, včetně aktualizací a opravných řešení.

46 Pokusem o překonání roztříštěnosti v oblasti výzkumu kybernetické bezpečnosti a podnícení investic v širším měřítku je návrh Komise na vytvoření sítě středisek pro kompetence v oblasti kybernetické bezpečnosti a výzkumného centra kompetencí[73]. Celkově je v celé EU 665 center odborných znalostí.

Výzva 4: jasný přehled rozpočtových výdajů EU

47 Centralizovaný přehled výdajů je důležitý pro transparentnost a lepší koordinaci. Bez této skutečnosti je pro tvůrce politik obtížné zjistit, jak výdaje souvisejí s potřebami pro splnění prioritních cílů.

48 Strategie kybernetické bezpečnosti není financována ze žádného zvláštního rozpočtu. Na úrovni EU pocházejí výdaje na kybernetickou bezpečnost spíše ze souhrnného rozpočtu EU a spolufinancování ze strany členských států. Naše analýza odhaluje složité uspořádání nejméně deseti různých nástrojů v rámci souhrnného rozpočtu EU, ale neposkytuje žádný jasný obraz o tom, kam které peníze směřují (viz ***příloha II***).

49 Vytvoření jasného přehledu výdajů v oblasti, která zasahuje do mnoha oblastí politik, je tedy značnou výzvou. Programy výdajů jsou řízeny různými složkami Komise, z nichž každá má své vlastní cíle, pravidla a časové plány. Tento obraz se dále komplikuje, pokud zohledníme spolufinancování členských států, podobně jako v rámci Fondu vnitřní bezpečnosti (policie)[74].

Identifikovatelné výdaje na oblast kybernetické bezpečnosti

50 V období 2014–2018 Komise vynaložila nejméně 1,4 miliardy EUR na provádění strategie[75], přičemž největší podíl přidělila na program Horizont 2020[76] („H2020“). Financování H2020 se provádí hlavně prostřednictvím programu Secure Societies Challenge a pro vedoucí postavení v oblasti projektů podporujících průmyslové technologie[77]. Do září roku 2018 jsme identifikovali 279 nasmlouvaných projektů týkajících se kybernetické bezpečnosti, přičemž celkové financování ze strany EU dosáhlo 786 milionů EUR[78]. ***Obrázek 5*** ukazuje typologii těchto projektů na základě této analýzy.

Obrázek 5 – Nasmlouvané výzkumné projekty H2020 v oblasti kybernetické bezpečnosti (v milionech EUR)

Zdroj: EÚD.

51 V roce 2016 bylo zřízeno smluvní partnerství veřejného a soukromého sektoru (cPPP), jehož cílem je podpořit evropskou oblast kybernetické bezpečnosti. Cílem bylo nasměrovat 450 milionů EUR z programu H2020 do partnerství cPPP a do roku 2020 získat dalších 1,8 miliardy EUR ze soukromého sektoru. V 18měsíčním období do 31. prosince 2017 bylo z H2020 směrováno 67,5 milionu EUR do partnerství cPPP a soukromý sektor investoval 1 miliardu EUR[79].

52 Boj proti kyberkriminalitě podporuje i Fond pro vnitřní bezpečnost – Policie (ISF-P). ISF-P podporuje studie, setkání odborníků a komunikační aktivity; v období od roku 2014 do roku 2017 činily náklady na ně téměř 62 milionů EUR. Členské státy mohou dále získat granty na vybavení, odbornou přípravu, výzkum a shromažďování údajů v rámci sdíleného řízení. Devatenáct členských států převzalo tyto granty za 42 milionů EUR.

53 Prostředky na podporu soudní spolupráce a fungování smluv o vzájemné právní pomoci se zvláštním zaměřením na výměnu elektronických údajů a finančních informací činily 9 milionů EUR v rámci programu spravedlnosti, který spravuje GŘ JUST.

54 Směrnice o bezpečnosti sítí a informací výslovně uvádí, že CSIRT musí mít k dispozici dostatečné zdroje pro účinné plnění svých úkolů[80]. Od roku 2016 do roku 2018 bylo z nástroje pro propojení Evropy každoročně k dispozici 13 milionů EUR, o něž by členské státy mohly požádat pro účely pomoci při provádění požadavků směrnice. Nebyla provedena žádná studie, která by určovala skutečné finanční potřeby sítě CSIRT a skupiny pro spolupráci tak, aby měly dopad.

55 Některé provozní náklady agentur byly zaměřeny konkrétně na aktivity v oblasti kybernetické bezpečnosti a kyberkriminality. Z údajů, které jsou k dispozici, je však obtížné získat přesné údaje.

56 Budapešťská úmluva (viz bod ***11***) tvoří páteř externích výdajů EU na kybernetické účely. EU vynaložila v období 2014–2018 přibližně 50 milionů EUR na posílení kybernetické bezpečnosti mimo své hranice. Téměř polovina z toho byla prostřednictvím nástroje přispívajícího ke stabilitě a míru s jedním hlavním projektem – GLACY+ ve výši 13,5 milionu EUR, jehož cílem je posílit celosvětové kapacity pro rozvoj a provádění právních předpisů v oblasti kyberkriminality a pro rozšíření mezinárodní spolupráce[81]. Jinde se zaměření výdajů z jiných finančních nástrojů EU týkalo převážně západního Balkánu[82] a evropského sousedství, například projekt Cybercrime @ EaP se

zeměmi Východního partnerství má za cíl zlepšit mezinárodní spolupráci v oblasti kyberkriminality a elektronických důkazů.

Další výdaje na oblast kybernetické bezpečnosti

57 V rámci programů EU není vždy možné určit konkrétní výdaje v oblasti kybernetické bezpečnosti:

- financování H2020 bylo také směřováno prostřednictvím společného podniku pro provádění společné technologické iniciativy pro elektronické součásti a systémy pro vedoucí postavení Evropy (ECSEL) pro kybernetické fyzické systémy. Během let 2015 až 2016 jsme však nemohli určit, co z 27 projektů v celkové výši 437 milionů EUR se konkrétně týká kybernetické bezpečnosti.

- V rámci evropských strukturálních a investičních fondů je až 400 milionů EUR k dispozici na výdaje na kybernetickou bezpečnost a služby vytvářející důvěru. To zahrnuje investice do bezpečnosti a ochrany údajů s cílem zlepšit interoperabilitu a vzájemné propojení digitální infrastruktury, elektronickou identifikaci, služby v oblasti ochrany soukromí a služby vytvářející důvěru.

58 Evropská investiční banka ve svém operačním plánu z roku 2018 oznámila svůj záměr zvýšit během tříletého období financování technologií dvojího užití, kybernetickou bezpečnost a civilní bezpečnost až na 6 miliard EUR[83].

Výhled do budoucna

59 Složka kybernetické bezpečnosti ve výši 2 miliard EUR navrženého nového programu Digitální Evropa[84] (DEP) na období 2021–2027 je určena k posílení oblasti kybernetické bezpečnosti EU a celkové ochrany společnosti, včetně podpory provádění směrnice o bezpečnosti sítí a informací. Navrhovaná síť středisek pro kompetence v oblasti kybernetické bezpečnosti a výzkumné centrum kompetencí, jehož cílem je racionalizovanější přístup, by měly být hlavním prováděcím mechanismem pro výdaje EU v rámci DEP.

60 Výdaje na obranu z rozpočtu EU se nedávno zvýšily prostřednictvím Evropského programu rozvoje obranného průmyslu, přičemž 500 milionů EUR bude přiděleno v letech 2019 a 2020[85]. Bude se zaměřovat na zlepšení koordinace a účinnosti výdajů členských států na obranu prostřednictvím pobídek pro společný rozvoj. Jeho cílem je vygenerovat celkem 13 miliard EUR na investice do obranných kapacit po roce 2020

prostřednictvím Evropského obranného fondu, z nichž některé se týkají kybernetické obrany[86].

Výzva 5: přiměřené financování agentur EU

61 Tři klíčové orgány, které jsou jádrem politiky EU v oblasti kybernetické bezpečnosti – ENISA, Europol EC3 a CERT-EU (viz ***rámeček 2***) – čelí výzvám v oblasti financování v době vyšších politických priorit na základě bezpečnosti. Při současném objemu lidských a finančních zdrojů do agentur EU je pro ně nadále obtížné splnit očekávání[87].

62 Žádosti agentur o dodatečné zdroje na pokrytí rostoucí poptávky nebyly plně uspokojeny, což by mohlo případně ohrozit (včasné) splnění cílů politiky. Například:

- Omezené zdroje byly faktorem, který zabránil tomu, aby agentura ENISA splnila v roce 2017 své cíle v celém rozsahu[88]. V balíčku z roku 2017 byly navrženy další zdroje, které odpovídají novému mandátu agentury ENISA.

- Nabídka analytiků a investice do schopností v IKT v Europolu EC3 nedrží krok s poptávkou[89]. Společná pracovní skupina Europolu pro kyberkriminalitu (J-CAT) rovněž disponuje odborníky z členských států a ze třetích zemí, kteří podporují vyšetřování prováděné zpravodajskými službami. Náklady však z velké části hradí vysílající státy, což odrazuje od nasazení většího počtu odborníků. Dočasné nasazení na jednotlivé případy bylo navrženo s částečným financováním ze strany Europolu nebo cyklu politiky EU tak, aby se mohlo účastnit více zemí.

63 Některá omezení vznikají sama o sobě. Mnoho pracovníků CERT-EU a ENISA je smluvními zaměstnanci, u nichž jsou postupy při náboru zpravidla pomalé. Jiná omezení, například získávání a udržení talentů, plynou z neschopnosti agentur konkurovat platům v soukromém sektoru, nebo jsou způsobena špatnými vyhlídkami na kariérní postup. Agentura ENISA si tedy v letech 2014–2016 najala externisty na značnou část své práce[90].

64 Nedostatek zaměstnanců a potřebných nástrojů s sebou může nést značné riziko, zejména pokud jde o shromažďování informací o hrozbách. Objem údajů z otevřených a uzavřených zdrojů se nadále zvětšuje a hrozí, že analytici již nebudou stačit provádět řádné analýzy hrozeb. Bez správných schopností a nástrojů k úspěšné integraci a vzájemnému propojení těchto údajů nedojde k efektivní přeměně na použitelné informace o hrozbách, které lze sdílet a analyzovat v celé EU[91].

Body k úvaze – Financování a výdaje

- Jakým způsobem může Komise a zákonodárci zefektivnit výdaje na kybernetickou bezpečnost v EU a přímo je sladit s jasně stanovenými cíli?
- Jak mohou být nedostatky ve financování agentur EU řešeny společně, s přihlédnutím k potřebám a cílům Unie?
- Jaká opatření jsou stanovena na úrovni EU a členských států, aby se omezily překážky, které brání malým a středním podnikům převzít investiční kapitál a rozšířit svou činnost?
- Jaké konkrétní a trvalé výsledky přinášejí fondy H2020 k řešení kybernetické bezpečnosti?
- Jak posiluje budování kapacit EU kapacity mimo hranice EU v souladu s hodnotami EU?

Budování společnosti odolné vůči kybernetickým hrozbám

65 Řízení kybernetické bezpečnosti znamená řízení hrozeb a rizik, posilování kapacity a informovanosti a koordinaci a sdílení informací postavené na důvěře.

Výzva 6: posílení správy a norem

Řízení informační bezpečnosti

66 Řízení informační bezpečnosti znamená zavedení struktur a politik, které zajistí důvěrnost, integritu a dostupnost údajů. Více než jen technické řešení vyžaduje efektivní vedení, spolehlivé procesy a strategie sladěné s organizačními cíli[92]. Podmnožinou je řízení kybernetické bezpečnosti, která se zabývá všemi druhy kybernetických hrozeb, včetně cílených, sofistikovaných útoků, narušení nebo incidentů, které lze obtížně rozpoznat nebo řešit.

67 Modely řízení kybernetické bezpečnosti se v jednotlivých členských státech liší a v rámci nich je odpovědnost za kybernetickou bezpečnost často rozdělena mezi mnoho subjektů. Tyto rozdíly by mohly bránit spolupráci potřebné k reakci na rozsáhlé, přeshraniční incidenty a k výměně informací o hrozbách na vnitrostátní úrovni, a tím spíše i na úrovni EU. Náš průzkum vnitrostátních kontrolních úřadů odhalil, že jako nejsilnější riziko jsou vnímány nedostatky ve správě u orgánů veřejné správy a řízení rizik.

68 V řízení kybernetické bezpečnosti je mnoho slabých míst, přestože důsledky pro organizace soukromého sektoru mohou být vážné. Téměř devět z deseti organizací tvrdí, že jejich funkce v oblasti kybernetické bezpečnosti celkově neplní jejich potřeby[93], a pracovníci v oblasti kybernetické bezpečnosti jsou často vyřazováni z vedení[94].

69 Směrnice EU o právu společností nestanoví žádné zvláštní požadavky na zveřejňování kybernetických rizik. Ve Spojených státech nedávno Komise pro cenné papíry vydala nezávazné pokyny pro pomoc veřejným společnostem při přípravě zveřejnění informací o rizicích a incidentech v oblasti kybernetické bezpečnosti[95]. Společný výbor evropských orgánů dohledu[96] (ESA) varoval před nárůstem

kybernetických rizik, vyzval finanční instituce, aby posílily křehké IT systémy a prozkoumaly přirozená rizika pro bezpečnost informací, konektivitu a outsourcing[97].

70 Posílení řízení informační bezpečnosti malých a středních podniků je obzvláště obtížné, neboť častěji nedokáží zavést příslušné systémy. Malým a středním podnikům chybí vhodné pokyny pro uplatňování požadavků na bezpečnost informací a soukromí a pro zmírnění technologických rizik[98]. Klíčovou výzvou je proto lepší pochopení jejich potřeb a poskytnutí potřebných pobídek a podpory.

71 Absence soudržného mezinárodního rámce řízení kybernetické bezpečnosti narušuje schopnost mezinárodního společenství reagovat na kybernetické útoky a omezovat je. Proto je důležité nalézt konsensus ohledně takového rámce řízení, který nejlépe odráží zájmy a hodnoty EU[99]. Pokusy o stanovení závazných mezinárodních pravidel v oblasti kyberprostoru jsou stále náročnější, jak o tom svědčí absence konsensu v rámci skupiny odborníků vládních expertů OSN v roce 2017 na tom, jak by se mezinárodní právo mělo vztahovat na reakce státu na incidenty.

72 Za účelem posílení agendy o správě kyberprostoru EU formalizovala také šest partnerství v oblasti kybernetické bezpečnosti s cílem zavést pravidelný politický dialog zaměřený na budování důvěry a společných oblastí spolupráce[100]. Výsledky jsou smíšené, ale celkově nelze EU na mezinárodním poli považovat za „významného aktéra kybernetické bezpečnosti“, ačkoli její prestiž se zvýšila[101].

Informační bezpečnost v orgánech EU

73 Každý orgán EU má vlastní pravidla pro řízení informační bezpečnosti. Interinstitucionální dohoda zajišťuje pomoc Komise v oblasti informační bezpečnosti pro ostatní orgány a agentury. Orgány a instituce EU uznaly potřebu soudržného rozvoje svých kybernetických kapacit a přístupů k řízení rizik. Komise, Rada a ESVČ předloží do roku 2020 horizontální pracovní skupině pro kybernetické otázky zprávu týkající se správy věcí veřejných a pokroku dosaženého při objasňování a harmonizaci řízení kybernetické bezpečnosti v orgánech a agenturách EU[102].

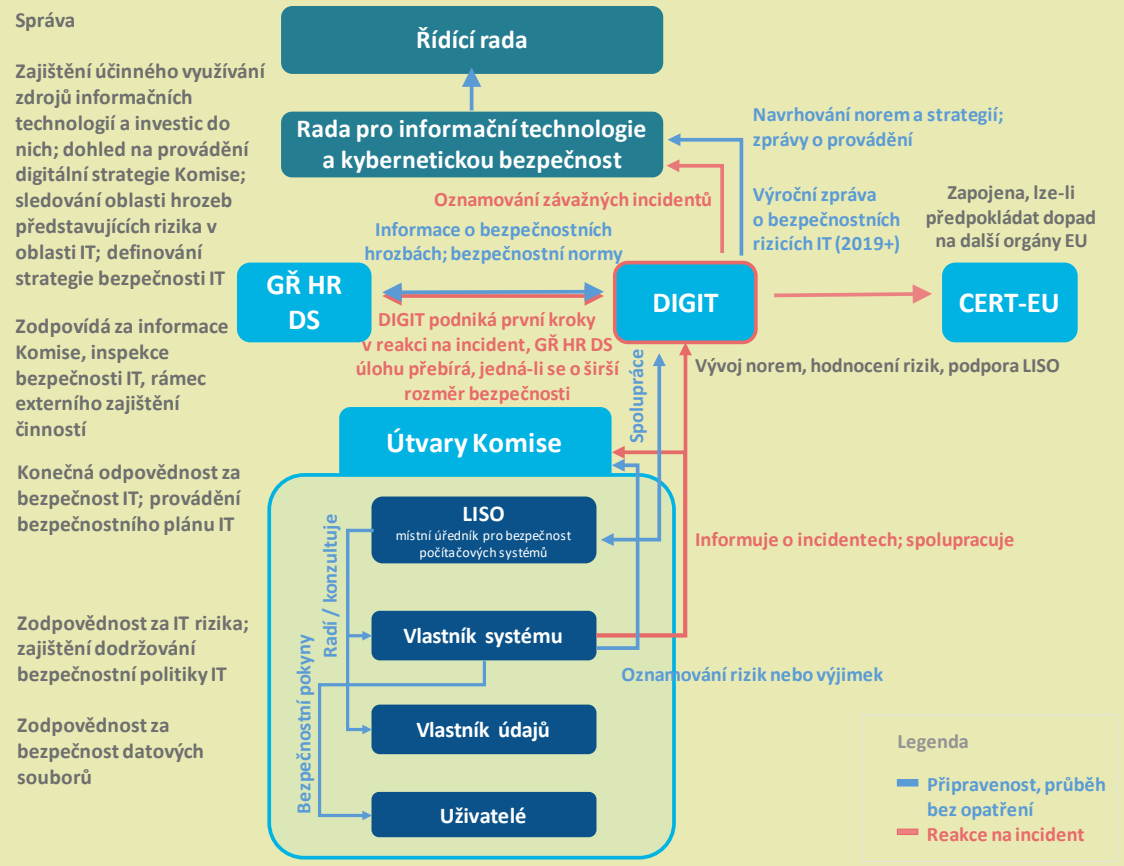
74 Generální ředitelství pro informatiku (DIGIT) je v rámci Komise odpovědné za bezpečnost IT infrastruktury a služeb (viz ***rámeček 3***). Hlavní cíle digitální strategie Komise v oblasti IT bezpečnosti zahrnují zabezpečení IT v řídících procesech, zajištění (nákladově) efektivní infrastruktury a odolnosti, rozšíření rozsahu zjišťování a řešení incidentů a integrace řízení IT a bezpečnosti[103]. Komise v rámci smlouvy o poskytovateli zajišťuje, aby téměř veškerý software byl aktivně udržován a aby byl používán pouze software podporovaný prodejcem[104].

75 Důležitost ochrany institucí se vztahuje i na mise a struktury EU v rámci SBOP na celém světě. Jednou z priorit rámce politiky EU v oblasti rámce politiky pro kybernetickou obranu (aktualizace z roku 2018) je posílit ochranu komunikačních a informačních systémů SBOP používaných subjekty EU. V současné době funguje interní rada pro správu kybernetických komunikací ESVČ, která se poprvé sešla v červnu roku 2017[105].

Rámeček 3

Ochrana informačních systémů Komise

Přibližně 1 300 systémů a 50 000 zařízení Komise je neustále cílem kybernetických útoků. Odpovědnost za IT je decentralizovaná, jak je znázorněno na následujícím obrázku. Bezpečnost informací a IT je založena na společném bezpečnostním plánu IT zavedeném GŘ DIGIT. Rada pro informační technologie a kybernetickou bezpečnost působí de facto jako hlavní orgán Komise pro informační bezpečnost a spojuje provozní stránku zabezpečení IT s vrcholovým vedením Komise zastoupeným správní radou společnosti.



Zdroj: EÚD na základě rozhodnutí Komise[106].

Hlavním úkolem GŘ pro lidské zdroje a bezpečnost (GŘ HR DS) je ochrana zaměstnanců, informací a majetku Komise. Provádí rovněž bezpečnostní vyšetřování incidentů, které mají širší bezpečnostní rozměr než pouze informační technologie, čímž přispívá k aktivitám v oblasti boje proti zpravodajským službám a proti terorismu.

GŘ DIGIT zodpovídá za zabezpečení IT a je hostitelem skupiny CERT-EU (skupina pro reakci na počítačové hrozby). Skupina CERT-EU, která byla založena v roce 2011, má roční rozpočet ve výši přibližně 2,5 milionu EUR ročně a přibližně 30 zaměstnanců. Je první, kdo reaguje v případě jakéhokoli incidentu v oblasti informační bezpečnosti, který se týká několika institucí, avšak nepracuje nepřetržitě. Je hostitelem platformy pro sdílení informací. V roce 2018 podepsala skupina CERT-EU nezávazné memorandum o porozumění s agenturou ENISA, EC3 a Evropskou obrannou agenturou s cílem posílit spolupráci a koordinaci. Má také technickou dohodu se složkou NATO pro schopnost reakce na počítačové incidenty (NCIRC).

Posouzení hrozeb a rizik

76 Řádné a soustavné hodnocení hrozeb a rizik je důležitým nástrojem pro veřejnoprávní i soukromoprávní organizace. Neexistuje však žádný standardní přístup ke klasifikaci a mapování kybernetických hrozeb nebo k hodnocení rizik, což znamená, že obsah hodnocení se značně liší a představuje výzvu k soudržnému celoevropskému přístupu ke kybernetické bezpečnosti[107]. Hodnocení navíc často vycházejí ze stejných zdrojů nebo dokonce jiných hodnocení hrozeb, v důsledku čehož se opakovaně objevují stejná zjištění[108] s tím rizikem, že nebude věnována dostatečná pozornost jiným hrozbám. To je ještě zhoršeno neustálou neochotou sdílet informace a neinformováním o událostech.

77 Středisko pro hybridní hrozby[109], které je součástí ESVČ, bylo zřízeno za účelem zlepšení povědomí o situaci a podpory rozhodování prostřednictvím sdílení analýz, ale potřebuje rozšířit své odborné znalosti, a to i v oblasti kybernetické bezpečnosti. CERT-EU zároveň poskytuje orgánům, institucím a agenturám EU zprávy a informace týkající se kybernetických hrozeb, které jsou na ně zaměřeny.

78 ENISA v minulosti poznamenala, že mnoho členských států má kvalitativní chápání hrozeb a že je zapotřebí širší modelování kybernetické hrozby[110]. Monitorování kapacity pro strategickou analýzu posílí celkové porozumění. Posouzení hrozeb by se však v zájmu ucelenějšího obrázku mohlo zaměřovat nejen na technologické hrozby, ale také na sociálně-politické a ekonomické hrozby a hnací síly a motivy aktérů.

Pobídky

79 Stále ještě existuje málo právních a ekonomických podnětů pro organizace, aby oznamovaly a sdílely informace o incidentech. Kvůli obavám z poškození dobrého jména mnoho organizací stále dává přednost diskrétnímu řešení kybernetických útoků nebo vyplacení pachatelů. Uvidí se, jak účinně bude směrnice o bezpečnosti sítí a informací zvyšovat míru oznamování. Komise očekává, že se zlepšení projeví především na vnitrostátní úrovni, ale akt o kybernetické bezpečnosti doplní celkový přehled celé EU[111].

80 Po zavedení určitých standardů do zadávání veřejných zakázek mají orgány veřejné moci významnou páku vůči dodavatelům jako pořizovatelé digitálních produktů a služeb prostřednictvím veřejných zakázek a financování výzkumu a programů (například tím, že vyžadují přijetí určitých technických norem, jako je internetový protokol IPv6 s cílem napomáhat boji proti kyberkriminalitě). V současné době však neexistuje společný rámec pro zadávání veřejných zakázek pro infrastrukturu kybernetické bezpečnosti[112]. Komise může v tomto ohledu hodně udělat. Navržený program Digitální Evropa pro příští víceletý finanční rámec je zaměřen na řešení dosud omezených investic veřejného sektoru při nákupu nejnovějších technologií kybernetické bezpečnosti.

81 Prostřednictvím své regulační kapacity může Komise zajistit, aby byly vytvořeny správné normy pro široké přijetí s cílem zvýšit bezpečnost. Komise a Europol pracují s orgány pro správu internetu, jako je ICANN (viz bod ***38***) a RIPE-NCC[113], což je nezbytné pro zavedení řádného systému v oblasti kyberkriminality na podporu donucovacích a soudních orgánů.

Výzva 7: zlepšování dovedností a informovanosti

82 ENISA poukázala na to, že uživatelé hrají klíčovou úlohu v boji proti kybernetickým útokům a že posilování dovedností, vzdělání a informovanosti je klíčem k vybudování společnosti odolné vůči kybernetickým hrozbám[114]. Jednotlivci, v práci nebo doma, kteří jsou zběhlí v pozorování varovných znamení a jsou vyzbrojeni správnými technikami, mohou zpomalit útoky nebo jim zabránit.

83 Zvláštní pozornost je třeba věnovat narůstající asymetrii mezi know-how potřebným k páchání kyberkriminality nebo ke spuštění kybernetického útoku a dovednostmi potřebnými k obraně proti tomuto útoku. Model „zločin jako služba“ snížil bariéry pro vstup na trh s kyberkriminalitou. Jedinci, kteří nemají technické

znalosti k tomu, aby sami mohli vyvinout škodlivé nástroje, si nyní mohou pronajmout botnety, využívat balíčky exploitů nebo balíčky ransomwaru.

Odborná příprava, dovednosti a rozvoj kapacit

84 Svět se potýká s rostoucím nedostatkem dovedností v oblasti kybernetické bezpečnosti, nedostatek pracovních sil se od roku 2015 prohloubil o 20 %[115]. Tradiční náborové kanály neodpovídají poptávce, a to ani pro manažerské a interdisciplinární pozice[116]. Téměř 90 % celosvětové pracovní síly v oblasti kybernetické bezpečnosti jsou muži a přetrvávající nedostatečná genderová rozmanitost tak ještě více omezuje sdílení talentů[117]. Navíc na univerzitách nejsou předměty týkající se kybernetiky v netechnických programech dostatečně zastoupeny.

85 Odborná příprava a vzdělávání je zapotřebí ve vedení, mezi státními úředníky, úředníky činnými v oblasti vymáhání práva, u soudních orgánů, ozbrojených sil a pedagogů. Například soudy musí být schopny řešit rychle se měnící technická specifika kyberkriminality a jejích obětí[118], neboť v současné době neexistují žádné celounijní normy pro odbornou přípravu a certifikaci[119]. V orgánech EU je důležité získat správnou kombinaci dovedností. Bez nich nemusí být instituce schopny správně definovat rozsah, určit správné partnery a bezpečnostní potřeby, nebo mohou postrádat schopnost řídit programy. To může ovšem oslabit účinnost programů EU nebo rozvoj politik.

86 Za vzdělávací politiky na úrovni EU odpovídají členské státy a probíhá již také řada vzdělávacích činností (viz ***tabulka 2***) a cvičení (viz ***rámeček 4***). EU může přispět k tomu, aby do učebních osnov byly začleněny celounijní normy ve všech relevantních oborech[120]. Například v oblasti digitálních forenzních činností jsou nezbytné společné normy pro odbornou přípravu, aby se usnadnila cesta k přípustnosti důkazů v členských státech. Kvůli přeshraničnímu charakteru kyberkriminality mohou být zapojeny různé jurisdikce, což vyžaduje odbornou přípravu na úrovni EU. A přesto CEPOL, agentura EU pro vzdělávání a výcvik v oblasti prosazování práva, uvedla, že více než dvě třetiny členských států neposkytují úředníkům v oblasti prosazování práva pravidelné vzdělávání v oblasti kybernetické bezpečnosti[121]. EU může také případně stanovit způsoby, jak sladit vzdělávání a odbornou přípravu mezi civilní a vojenskou sférou[122]. Agentura ENISA zjistila, že i když existující možnosti odborné přípravy v kritických odvětvích jsou široké, nejsou dostatečně zaměřeny na odolnost kritické infrastruktury[123].

Tabulka 2 – Některé iniciativy EU související s odbornou přípravou v oblasti kybernetické bezpečnosti

Projekty Evropské obranné agentury, např. podpora činnosti ze strany soukromého sektoru a projekt Cyber Ranges	Síť Evropské bezpečnostní a obranné školy (poskytující civilně-vojenskou přípravu), včetně kybernetického vzdělávání, odborné přípravy a hodnotící platformy	Odborná příprava agentury ENISA nabízející programy odborné přípravy, které komerční trh pravděpodobně nenabízí
Europol, CEPOL, programy odborné přípravy ECTEG[124] – včetně modelu řízení odborné přípravy a rámce odborné způsobilosti (včetně certifikace)	Síť center pro kompetenci a výzkumné centrum pro kompetenci (navržené)	Opatření na šifrování navržená v jedenácté zprávě o pokroku na cestě k bezpečnostní unii
Spolupráce EU-NATO v oblasti odborné přípravy a vzdělávání v oblasti kybernetické obrany	Vojenský program Erasmus	Evropská síť pro justiční vzdělávání

Zdroj: EÚD.

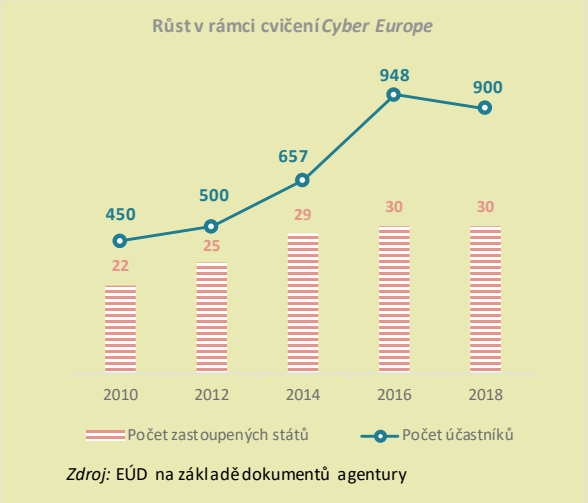
87 EU vyslala protiteroristické a bezpečnostní experty do 17 delegací za účelem posílení vazby mezi vnitřní a vnější bezpečností EU[125]. Bez ohledu na omezení zdrojů by širší kybernetické know-how mohlo napomoci při zavádění správných projektů a mohlo by též stanovit součinnost s jinými programy nebo zdroji financování[126]. Mohlo by také zvýšit prestiž kybernetické bezpečnosti v politickém dialogu, i když by musela konkurovat mnoha jiným prioritám, jako je migrace, organizovaná trestná činnost nebo navracení zahraničních bojovníků.

Rámeček 4

Cvičení

Cvičení jsou důležitými prvky kybernetického vzdělávání a odborné přípravy, nabízejí prvořadé příležitosti pro zvýšení připravenosti tím, že testují schopnosti, nabízejí odpovědi na scénáře v reálném životě a vytvářejí sítě pracovních vztahů. Od roku 2010 se jejich četnost výrazně zvýšila.

Účastníci se účastní na místě nebo dálkově. Provádí se hodnocení po cvičení s cílem identifikovat získané poznatky, ačkoli tyto poznatky nemusí být dosud plně součástí strategické/politické, provozní a technické roviny[127].



Zdroj: EÚD na základě dokumentů agentury

Hlavních cvičení EU a NATO – každé dva roky Cyber Europe (operační) a každoročního Locked Shields (technické) – se účastní více než 1 000 účastníků z přibližně 30 států. Obě cvičení se zaměřují na ochranu a udržování kritické infrastruktury v simulovaných scénářích útoku. Cvičení se značně rozrostla, obě nyní zahrnují média, prvky z právní a finanční politiky, které zlepšují informovanost odborných pracovníků o situaci. Paralelní a koordinovaná cvičení PACE (strategická) je zkouškou interakce EU a NATO ve scénáři hybridní krize.

Nejsou to jediná mezinárodní cvičení. ENISA organizuje každoroční kybernetickou výzvu, v níž týmy soutěží o řešení bezpečnostních problémů, jako je bezpečnost na internetu a v mobilním prostředí, kryptografické skládačky, reverzní inženýrství, etika a forenzní problematika. První cvičení na úrovni ministrů EU CYBRID se uskutečnilo v září roku 2017 a zaměřilo se na strategické rozhodování. V roce 2018 bylo zahájeno cvičení s názvem Crossed Swords, na němž se podílelo NATO, s cílem zlepšit útočné prvky jeho cvičení Locked Shields. NATO také organizuje cvičení Cyber Coalition.

Klíčovým úkolem je zajistit aktivní zapojení všech důležitých zúčastněných stran a koordinaci všech cvičení, vyhnout se duplicitě a efektivně sdílet získané poznatky.

Povědomí

88 Občané jsou často terčem útoků a šíření dezinformací, neboť jsou pravděpodobně nevědomky vystaveni zranitelným místům v levných a široce distribuovaných zařízeních a softwaru nebo se stávají obětí sociálního inženýrství. Zvyšování povědomí je proto zásadní pro budování účinné kybernetické odolnosti,

avšak v žádném případě není snadným úkolem, neboť pro neodborníky je obtížné pochopit složitost kybernetické bezpečnosti a související rizika.

89 Každoroční Evropský měsíc pro informovanost o kybernetické bezpečnosti (ECSM) a Den bezpečnějšího internetu jsou příklady zvyšování povědomí. Do ECSM se nyní zapojilo i sedm států, které nejsou členy EU[128]. Cílem kampaně Europolu *Say No!* (Řekni Ne!) je snížit riziko, že se děti stanou oběťmi sexuálního nátlaku a vydírání na internetu. Snižování rizika je důležité, protože v současné době jen málo obětí útoků hlásí tyto trestné činy policii[129]. Komise uznává, že strategie kybernetické bezpečnosti je při zvyšování povědomí občanů a podniků pouze „částečně účinná“[130]. To je dáno rozsahem úkolu, omezenými zdroji, nerovnoměrným zapojením členských států a nedostatkem vědeckých důkazů o tom, jak nejlépe zvýšit a měřit povědomí.

90 Výzvou pro Komisi a příslušné agentury je zajistit, aby opatření ke zvýšení povědomí byla řádně zaměřená a zveřejněná, inkluzivní, aby mapovala hrozby, vyhýbala se nežádoucím účinkům, jako je „únava z tématu bezpečnosti“[131], a vypracovat hodnotící metody a metriky pro posouzení jejich účinnosti. To by se mělo uplatňovat stejně v rámci samotných orgánů EU, kde je třeba zlepšit kulturu osvěty[132].

Výzva 8: lepší výměna informací a koordinace

91 Kybernetická bezpečnost vyžaduje spolupráci mezi veřejným a soukromým sektorem, především pokud jde o sdílení informací a výměnu osvědčených postupů. Důvěra je nezbytná na všech úrovních, aby se vytvořilo správné prostředí pro přeshraniční sdílení citlivých informací. Špatná koordinace vede k roztříštěnosti, zdvojování úsilí a rozptýlení odborných znalostí. Efektivní koordinace může vést k hmatatelným úspěchům, jako je uzavření obchodních míst na darkwebu[133]. Navzdory pokroku dosaženému v posledních letech je míra důvěry na úrovni EU a v některých členských státech[134] stále „nedostatečná“[135].

Koordinace mezi orgány EU a členskými státy

92 Jedním z cílů strategie kybernetické bezpečnosti a struktur pro spolupráci zavedených směrnicí o bezpečnosti sítí a informací bylo posílit důvěru mezi zúčastněnými stranami. Hodnocení strategie uznala, že byly položeny základy pro strategickou a operační spolupráci na úrovni EU[136]. Navzdory tomu je koordinace obecně „nedostatečná“[137]. Úkolem je zajistit, aby výměna informací nebyla jen smysluplná, ale aby také umožňovala mít úplný přehled o celé situaci. Dosažení

společného porozumění založeného na uznávané terminologii je v tomto ohledu důležitým faktorem (viz ***rámeček 5***).

93 V hodnocení agentury ENISA však bylo uvedeno, že přístup EU ke kybernetické bezpečnosti nebyl dostatečně koordinován, což vedlo k nedostatečné součinnosti mezi činnostmi agentury ENISA a činnostmi ostatních zúčastněných stran. Mechanismy spolupráce jsou stále poměrně nezralé[138], akt o kybernetické bezpečnosti má tuto situaci řešit posílením koordinační úlohy agentury ENISA. Snahou o posílení spolupráce bylo zdůvodněno memorandum o porozumění podepsané v roce 2018 mezi agenturou ENISA, EDA, Europolem EC3 a CERT-EU[139]. Prioritou Komise v příštích letech bude zajistit řádné sladění politických iniciativ, potřeb a investičních programů s cílem překonat roztříštěnost a vytvořit synergie[140].

94 Koordinační funkce jsou zakotveny v různých institucionálních orgánech. Byla zřízena pracovní skupina pro bezpečnostní unii, která bude hrát ústřední úlohu při koordinaci různých generálních ředitelství Komise s cílem podpořit program bezpečnostní unie[141]. GŘ CNECT předsedá podskupině pracovní skupiny pro kybernetickou bezpečnost.

95 V Radě je kybernetická bezpečnost řešena horizontální pracovní skupinou pro kybernetické otázky (HWP), která koordinuje strategické a horizontální kybernetické otázky a pomáhá připravovat cvičení a hodnotit jejich výsledky. Úzce spolupracuje s Politickým a bezpečnostním výborem, který má ústřední rozhodovací úlohu ve vztahu ke všem diplomatickým opatřením v oblasti kybernetické bezpečnosti (viz ***rámeček 6*** v následující kapitole). Vzhledem k tomu, že kybernetická bezpečnost je průřezové téma, koordinace všech relevantních zájmů není přímočará: otázkami souvisejícími s kybernetickou bezpečností se v nedávné době zabývalo nejméně 24 pracovních skupin a přípravných orgánů[142].

96 Poslední dva legislativní návrhy týkající se posílení agentury ENISA (2017) a vytvoření sítě středisek pro kompetence v oblasti kybernetické bezpečnosti a výzkumného centra kompetencí (2018) jsou speciálně navrženy tak, aby řešily roztříštěnost a zdvojení úsilí. Hnacím faktorem v síti středisek pro kompetence v oblasti kybernetické bezpečnosti a výzkumného centra kompetencí je potřeba zaplnit mezeru, kterou kooperativní struktury směrnice o bezpečnosti sítí a informací nevyplňují, protože nebyly navrženy tak, aby podporovaly vývoj „špičkových“ řešení.

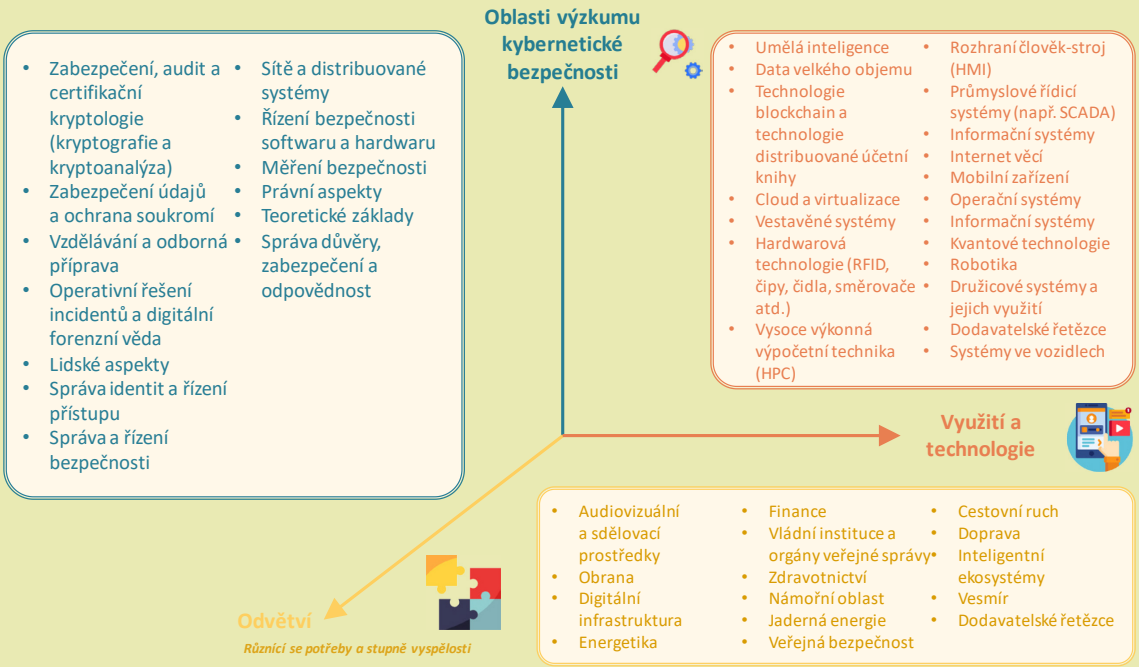
Rámeček 5

Snaha hovořit stejným kybernetickým jazykem: technologická soudržnost

Terminologická jasnost zlepšuje povědomí o situaci a koordinaci[143] a pomáhá přesně stanovit, co představuje hrozbu a riziko.

Společné výzkumné středisko Komise nedávno vypracovalo revidovanou výzkumnou taxonomii, která vychází z různých mezinárodních norem[144] . Jejím cílem je stát se referenčním bodem pro využití výzkumných subjektů v Evropě jako indexu.

Taxonomie kynernetické bezpečnosti



Zdroj: EÚD na základě údajů z Evropské komise.

Orgány a agentury EU neměly donedávna žádné společné definice. To se mění. V rámci svého návrhu skupina pro spolupráci vytvořila taxonomii incidentů s cílem usnadnit účinnou přeshraniční spolupráci.

Spolupráce a výměna informací se soukromým sektorem

97 Pro posílení celkové úrovně kybernetické bezpečnosti je nezbytná spolupráce mezi veřejnými orgány a soukromým sektorem. Navzdory tomu Komise ve svém hodnocení Strategie kybernetické bezpečnosti z roku 2017 zjistila, že výměna informací mezi soukromými zúčastněnými stranami a mezi veřejným a soukromým sektorem „nebyla dosud optimální“ kvůli „nedostatku důvěryhodných mechanismů podávání zpráv a podnětů ke sdílení informací“[145], což brání dosažení strategických cílů. Komise rovněž vzala na vědomí, že neexistuje účinný mechanismus spolupráce, pomocí něhož členské státy spolupracují na strategickém zvyšování trvale udržitelných průmyslových příslušných schopností[146].

98 Centra pro sdílení informací a analýzu (ISAC) jsou organizace, které jsou zřízeny tak, aby poskytovaly platformy a zdroje pro usnadnění sdílení informací mezi veřejným a soukromým sektorem, jakož i pro shromažďování informací o kybernetických hrozbách. Cílem je vybudovat důvěru prostřednictvím sdílení zkušeností, znalostí a analýz, zejména o příčinách, incidentech a hrozbách. V mnoha členských státech již existují vnitrostátní a odvětvová centra ISAC, ale na evropské úrovni jsou stále relativně omezená[147]. Přicházejí však s řadou výzev (omezení zdrojů, potíže s hodnocením jejich úspěchu, zajištění správných struktur pro zapojení veřejného i soukromého sektoru, zapojení orgánů prosazujících právo), které bude třeba překonat, pokud mají přispět k pomoci při provádění směrnice o bezpečnosti sítí a informací a vytvářet bezpečnostní kapacity na celoevropské úrovni[148].

99 Úzká spolupráce se soukromým sektorem je zvláště důležitá pro boj proti složité kyberkriminalitě, její účinnost je však v jednotlivých členských státech nevyrovnaná a závisí na úrovni důvěry[149]. Europol EC3 však vytvořil řadu poradních skupin s operátory ze soukromého sektoru, institucí a agentur EU a dalších mezinárodních organizací, aby zlepšil spolupráci prostřednictvím vytváření sítí, sdílení strategických zpráv od zpravodajských služeb a spolupráci. Pracují na plánech sladěných s cíli politického cyklu EU[150]. Trestní zneužívání šifrování je další oblastí plnou problémů, které vyzývají k větší spolupráci se soukromým sektorem. Europol EC3 v současné době zkoumá možnosti, jak hostit subjekty krátkodobě přidělené na konkrétní případy k J-CAT (viz bod ***62***) pro odborníky ze soukromého sektoru a akademické obce.

100 Nedostatek účinných mechanismů spolupráce postihuje civilní a obranná společenství – veřejná i soukromá. Mezi oblasti, které představují společnou výzvu, patří kryptografie, zabezpečené vestavěné systémy, detekce malwaru, simulační techniky, ochrana sítí a komunikačních systémů a autentizační technologie. Podpora civilně-vojenské spolupráce a podpora výzkumu a technologií (zejména formou

podpory malých a středních podniků) jsou dvě priority aktualizovaného rámce politiky EU v oblasti kybernetické obrany (aktualizace z roku 2018).

Body k úvaze – budování odolnosti

- Jak lze na úrovni EU dosáhnout vhodné rovnováhy mezi potřebou začlenit politiku kybernetické bezpečnosti a zajistit účinnou koordinaci mezi různými aktéry a rozptýlení odpovědnosti?
- Jak dobře jsou připraveny orgány a agentury EU na další velký útok, který bude veden přímo proti nim?
- Jak mohou být agentury EU, jichž se týká kybernetická bezpečnost, přitažlivější pro talentované odborníky?
- Jaké další kroky jsou zapotřebí, aby se zajistila přiměřená kapacita ve všech orgánech a agenturách EU s cílem umožnit soudržný rámec posuzování rizik a hrozeb?
- Jakým způsobem se evropské orgány dohledu (Evropský orgán pro bankovnictví, Evropský orgán pro cenné papíry a trhy a Evropský orgán pro pojišťovnictví a zaměstnanecké penzijní pojištění) zabývají kybernetickou zranitelností, která je součástí finančního sektoru, a jak se z toho lze poučit v jiných odvětvích?
- Jak může být vzhledem k celkovému nedostatku odborných znalostí nejlépe využita technická pomoc EU pro veřejné orgány k dosažení maximálního celkového dopadu na zlepšení kybernetické odolnosti?
- Jak mohou EU a členské státy zajistit smysluplnou přítomnost v mezinárodních diskusích s cílem utvářet řízení a normy kyberprostoru a podporovat hodnoty EU?
- Která opatření na zvýšení povědomí na úrovni EU a členských států (včetně úsilí v oblasti prevence) jsou opravdu významná a co může EU udělat, aby se tato opatření rozšířila?
- Jakou úlohu může hrát EU, aby napomohla genderové rozmanitosti v oblasti kybernetické bezpečnosti?
- Jak může EU a členské státy posílit součinnost mezi civilními a obrannými společenstvími v souladu s rámcem politiky kybernetické obrany (aktualizace z roku 2018)?

Účinná reakce na kybernetické bezpečnostní incidenty

101 Vytvoření účinné reakce na kybernetické útoky je zásadní pro jejich co nejrychlejší vystopování a zastavení. Zvláště důležité je, aby kritické sektory, členské státy a orgány EU byly schopny rychle a koordinovaně reagovat. Důležitá je včasná detekce.

Výzva 9: účinná detekce a reakce

Detekce a oznámení

102 Běžné detekční nástroje pomáhají překazit velkou většinu útoků denně[151]. Nicméně digitální systémy jsou nyní tak složité, že předcházení každému jednotlivému útoku je nemožné. Jejich sofistikovanost znamená, že útoky se často po dlouhou dobu vyhýbají detekci. Odborníci proto tvrdí, že důraz by měl být kladen na rychlou detekci a obranu[152]. Některé detekční nástroje, jako je automatizace, strojové učení a analýza chování, které se zaměřují na snižování rizik a na analýzu a poučení se ze systémového chování, však trpí tím, že podniky si je dostatečně neosvojí[153]. To je částečně způsobeno vytvářením falešných pozitivních záznamů, kdy se neohrožující aktivity mylně považují za škodlivé.

103 Jakmile je porušení zjištěno a analyzováno, je nezbytné rychlé oznámení a podání zprávy tak, aby ostatní veřejné a soukromé subjekty mohly podniknout preventivní kroky a příslušné orgány mohly těm, jichž se to týká poskytnout podporu. Mnoho organizací se zdráhá uznat a hlásit kybernetické bezpečnostní incidenty[154]. Zásadní je rovněž včasné zapojení orgánů vymáhajících právo do počáteční reakce na podezření na kyberkriminalitu a proaktivní výměna informací s CSIRT.

104 Předchozí absence společných požadavků EU na oznamování mimořádných událostí mohla způsobovat zpoždění při informování o porušení předpisů a brzdění reakce, kterou mělo řešit zavedení směrnice o bezpečnosti sítí a informací (viz bod ***20***). V návaznosti na útoky Wannacry v roce 2017 dospěla Komise k závěru, že síťový systém CSIRT „nebyl dosud plně funkční“[155]. Vzhledem k tomu, že provádění směrnice pokračuje, je třeba zjistit, zda pokyny vypracované skupinou pro spolupráci budou účinné a překonají neochotu hlásit incidenty[156].

105 Provozovatelé základních služeb v některých odvětvích mají v rámci stávajících předpisů EU řadu oznamovacích povinností (včetně informování spotřebitelů), které mohou narušit účinnost procesu. Například provozovatelé ve finančním a bankovním sektoru podléhají různým oznamovacím kritériím, standardům, prahům a časovým rámcům podle GDPR, směrnice o bezpečnosti sítí a informací, směrnice o platebních službách, ECB/SSM, cíle 2 a nařízení o eIDAS[157]. Proto je důležité tyto povinnosti zefektivnit, neboť kromě toho, že představují zbytečnou administrativní zátěž, mohla by taková nesourodost vést k roztříštěnému vykazování.

Koordinovaná reakce

106 Rozvoj evropského rámce pro krizovou spolupráci v oblasti kybernetické bezpečnosti je stále nedokončený. Byl proto zaveden související „plán“[158] (viz bod ***18***), který má zavést kybernetickou perspektivu do mechanismu integrovaných opatření pro politickou reakci na krize (IPCR), zlepšit informovanost o situaci a zajistit lepší integraci s dalšími mechanismy EU pro řešení krizí[159]. Projekt zahrnuje orgány, agentury a členské státy EU. Bezproblémová integrace všech těchto mechanismů reakce na krize je náročná[160]. Současná absence společné bezpečné komunikační sítě mezi orgány EU je rovněž významným nedostatkem[161].

107 Schopnost EU reagovat na kybernetické útoky na operační a politické úrovni v případě rozsáhlého přeshraničního incidentu byla označena za „omezenou“, částečně proto, že kybernetická bezpečnost není dosud začleněna do současných koordinačních mechanismů na úrovni EU na řešení krizí[162]. Směrnice o bezpečnosti sítí a informací se tímto nezabývala.

108 Nedávno navržená reforma agentury ENISA, která předpokládala větší operační úlohu při řešení rozsáhlých incidentů v oblasti kybernetické bezpečnosti, nebyla podporována členskými státy a upřednostňovala, aby úloha agentury podporovala a doplňovala vlastní operační opatření[163]. Existuje již mnoho CERT/CSIRT na úrovni členských států, ale jejich kapacity se značně liší. To představuje překážku účinné přeshraniční spolupráce potřebné pro rozsáhlé reakce na incidenty[164].

109 Snažili jsme se zmapovat různé úlohy připisované různým aktérům uvedeným v plánu, ale existovaly mezery, které budou muset být zaplněny tak, jak pokročí provádění. Jedna z oblastí, která byla zpočátku nedostatečně řešena, byla vymáhání práva, ačkoli v prosinci 2018 vstoupil v platnost Protokol o reakci na mimořádné situace v EU v oblasti vymáhání práva[165]. Je třeba zajistit, aby návrh byl praktický a aby

všechny strany věděly, co dělat, což je klíčem k jeho úspěchu. V příštích letech budou třeba rozsáhlé zkoušky.

110 Účinná odezva je víc než zamezit poškození, důležité je i určení odpovědnosti za útoky. Sledování a identifikace pachatelů, především při hybridním útoku, může být velmi obtížné kvůli narůstajícímu zneužívání anonymních nástrojů, kryptoměn a šifrování. To je známé jako problém přiřazení pachatele. Náprava tohoto problému není jen technickou záležitostí, je to také problém trestního soudnictví. Právní a procesní rozdíly mezi zeměmi mohou bránit vyšetřování trestných činů a stíhání podezřelých. Řešení problému s přidělením bude vyžadovat formalizovanější operační výměnu informací pomocí jasnějších postupů, například s Europolem nebo evropskou justiční sítí pro boj proti kyberkriminalitě Eurojustu.

111 Na politické úrovni byla vytvořena sada nástrojů pro kybernetickou diplomacii (viz ***rámeček 6***) s cílem podpořit urovnání mezinárodních sporů v kyberprostoru mírovými prostředky. Vytvoření týmů rychlé kybernetické reakce a vzájemná pomoc v oblasti kybernetické bezpečnosti představuje dva projekty podporující zdokonalené sdílení informací, které jsou rozvíjeny v rámci rámce PESCO[166].

Rámeček 6

Soubor nástrojů pro diplomacii v oblasti kybernetiky

Společná diplomatická reakce EU na škodlivé kybernetické aktivity[167] nebo „soubor nástrojů pro diplomacii v oblasti kybernetiky“ vyrostla na závěrech Rady o diplomacie v oblasti kybernetiky v roce 2015[168]. Cílem diplomacie v oblasti kybernetiky je vyvinout a zavést společný a komplexní přístup ke kyberprostoru založený na hodnotách EU, právním státě, budování kapacit a partnerství, podpoře modelu správy internetových stránek pro více zúčastněných stran a zmírnění hrozeb pro kybernetickou bezpečnost a větší stabilitu v mezinárodních vztazích.

Soubor nástrojů umožňuje EU a jejím členským státům vytvořit společnou diplomatickou reakci na škodlivé kybernetické aktivity, která plně využívá opatření v rámci společné zahraniční a bezpečnostní politiky. Mohou zahrnovat preventivní opatření (např. zvyšování povědomí, budování kapacit), spolupráci, stabilizační a omezující opatření (např. zákaz cestování, zbrojní embarga, zmrazení finančních prostředků) nebo podporu reakcí členských států[169]. Tato myšlenka spočívá v tom, že další spolupráce s cílem zmírnění hrozeb a jasná signalizace pravděpodobných důsledků společné reakce může (potenciálně) odradit od agresivního chování.

Společná reakce EU na škodlivé činnosti v kyberprostoru bude přiměřená rozsahu, míře, době trvání, intenzitě, složitosti, propracovanosti a dopadu dané činnosti v kyberprostoru.

Součástí úspěchu souboru nástrojů bude skutečnost, jak dobře je propojen s plánem a IPCR (viz bod ***106***), jak dobře je vytvořeno povědomí o situaci prostřednictvím rychlého a nepřetržitého sdílení informací (včetně prvků přidělení)[170] a nakonec i účinná spolupráce. Klíčem k úspěšnému nasazení souboru nástrojů je také účinná a koordinovaná komunikace. Doposud byl tento soubor nástrojů použit dvakrát: k zahájení dialogu se Spojenými státy po útoku *Wannacry*[171] a k vypracování závěrů Rady odsuzujících škodlivé používání IKT[172]. Zprovoznění souboru nástrojů právě probíhá a je třeba počkat, jak efektivní bude při dosahování svých cílů.

Výzva 10: ochrana kritické infrastruktury a společenské funkce

Ochrana infrastruktury

112 Většina kritické infrastruktury EU je provozována prostřednictvím průmyslových řídicích systémů (ICS)[173]. Mnoho z nich bylo navrženo jako samostatné systémy s omezeným připojením k vnějšímu světu. Vzhledem k tomu, že součásti systému ICS jsou připojeny k internetu, jsou citlivé na vnější rušení. Udržování a opravy stávajících systémů již nemusí být možné, ale jejich aktualizace není ani rychlá, ani levná. Úsilí o zvýšení bezpečnosti kritické infrastruktury proto musí zahrnovat modernizaci systému ICS.

113 Vzhledem k tomu, že průmysl se dále digitalizuje (situace je obecně známa jako „Průmysl 4.0“), dopad rozsáhlého incidentu v jednom průmyslovém sektoru může mít řetězový účinek jinde. Agentura ENISA vzala na vědomí význam mapování dopadu vzájemných závislostí kritických odvětví[174]. To je nezbytné pro pochopení případného rozšíření incidentu a podporuje dobře koordinované reakce.

114 Cílem směrnice o bezpečnosti sítí a informací je zvýšit připravenost v klíčových odvětvích odpovědných za kritickou infrastrukturu. Nejedná se však o všechna odvětví (viz ***tabulka 1***)[175]což „snižuje účinnost strategie“[176]. Zvláštní pozornost v tomto ohledu zasluhuje ochrana demokratické integrity voleb před zasahováním do volební infrastruktury a před dezinformacemi (viz ***rámeček 7***). Kromě revize stávajících právních předpisů bude proto klíčovou výzvou, jak zapojit tato odvětví do účinných reakcí na rozsáhlé incidenty.

115 Zranitelnosti v kritické infrastruktuře nekončí na hranicích Evropy. Zvláštním zájmem Komise je podněcovat kandidátské země, aby přijaly stejné normy jako členské

státy, například v oblastech, jako jsou právní předpisy týkající se kybernetické bezpečnosti nebo ochrany kritické infrastruktury.

Rámeček 7

Ochrana kriticky důležitých společenských funkcí: *boj proti zasahování do voleb*

V květnu 2019 bude přibližně 400 milionů voličů hlasovat ve volbách do Evropského parlamentu, prvních, které se uskuteční podle GDPR. Volby se budou konat bezprostředně po skandálech okolo zneužívání osobních údajů k politickému ovlivňování a k bezpříkladně koordinovaným dezinformačním kampaním („Fake News“). Komise varovala před pravděpodobnými kybernetickými zásahy v těchto volbách[177], boj proti tomu bude vyžadovat celostátní a celospolečenský přístup.

Volební infrastruktura

Organizování voleb je složité a zajištění jejich ochrany a integrity je odpovědností členských států. Zásahy do voleb a volební infrastruktury se mohou snažit ovlivňovat preference voličů, volební účast nebo samotný volební proces, včetně skutečného hlasování, zanášení výsledků do tabulek a komunikace. Ve volbách do Evropského parlamentu je ochrana tzv. „poslední míle“ (sdělování výsledků z jednotlivých hlavních měst do Bruselu) zvláště významnou problematikou vzhledem k tomu, že neexistuje nebo nebyl pro tento účel testován žádný společný bezpečnostní přístup[178].

V nedávném volebním balíčku Komise byla zahrnuta opatření na posílení kybernetické bezpečnosti voleb, jako je stanovení vnitrostátních kontaktních míst pro koordinaci a výměnu informací v době před volbami. Sdílení osvědčených postupů a získaných zkušeností má zvláštní význam[179].

Volební systémy se nepovažují za součást kritické infrastruktury[180] a nejsou zahrnuty ani do směrnice o bezpečnosti sítí a informací. Navzdory tomu skupina pro spolupráci vypracovala praktické pokyny týkající se bezpečnosti volebních technologií s cílem podpořit veřejné orgány. Očekává se, že zástupci vnitrostátních kontaktních míst se setkají počátkem roku 2019[181]. Členským státům je také doporučováno, aby prováděly hodnocení rizik týkajících se kybernetického ohrožení jejich volebních procesů.

Dezinformace

Dezinformace jsou stále důležitějším prvkem hybridních útoků, které zahrnují kybernetické útoky a hacking sítí. Mohou být použity k rozdělení společností, mohou zasít nedůvěru a podkopávat důvěru v demokratické procesy nebo v jiné záležitosti (například odpor proti očkování nebo změna klimatu). Rozrůstá se jejich rozsah, rychlost a rozmezí a představují pro EU skutečnou bezpečnostní hrozbu.

EU přijala řadu opatření k řešení dezinformací. Počínaje rokem 2015 byla vytvořena pracovní skupina East StratCom se základnou v ESVČ, která vyzývá k boji proti ruským dezinformačním kampaním[182]. Odborníci ocenili její činnost při podpoře politik EU, podpoře nezávislých sdělovacích prostředků v sousedství a její prognózování, sledování a řešení dezinformací[183]. Zdroje pracovní skupiny jsou však omezeny vzhledem k rozsahu a složitosti dezinformačních kampaní[184]. Je zapotřebí systematičtější interakce se stávajícími strukturami EU a lepší strategická komunikační spolupráce[185]. Nový akční plán[186] byl schválen Evropskou radou v prosinci 2018.

Komise v nedávné době vypracovala na základě svého sdělení z dubna 2018 o řešení dezinformací na internetu[187] dobrovolný, samoregulační kodex postupů[188] založený na stávajících politických nástrojích, k němuž se přihlásily on-line platformy a reklamní průmysl[189]. Akce zahrnují pomoc při zvyšování důvěryhodnosti obsahu a podpoře úsilí o zvýšení mediální a zpravodajské gramotnosti. Byla také zřízena nezávislá evropská síť ověřovatelů faktů.

Komise uvedla, že v případě nedodržení kodexu postupů mohou následovat další regulační opatření. Stanovení účinnosti opatření se ukáže jako klíčové, zejména pokud jde o to, jak měřit zlepšení důvěry, transparentnosti a odpovědnosti.

Dalším úkolem bude nalezení způsobů, jak zlepšit detekci, analýzu a zveřejňování dezinformací[190]. Je také zapotřebí aktivní a strategické sledování a analýza otevřených zdrojů údajů[191]. Pokusy o lepší pochopení prostředí ohrožení by se měly týkat i nových trendů, jako jsou „hluboké dezinformace“ (falešná videa vyrobená pomocí umělé inteligence a hlubokého strojového učení), stejně jako nástroje potřebné k jejich odhalení.

Posilování samostatnosti

116 EU je čistým dovozcem produktů a služeb v oblasti kybernetické bezpečnosti, čímž se zvyšuje riziko technologické závislosti a zranitelnosti subjektů mimo EU[192]. Zejména tato skutečnost podkopává bezpečnost kritické infrastruktury EU, která je rovněž podporována komplexními globálními dodavatelskými řetězci. Riziko se dále zhoršuje, pokud subjekty mimo EU získávají evropské podniky zabývající se kybernetickou bezpečností. Členské státy jsou odpovědné za prověřování přímých zahraničních investic a v současné době neexistuje mechanismus prověřování pro celou EU[193].

117 Větší strategická autonomie je cílem ve sdělení z roku 2017 o globální strategii EU *Odolnost, odrazování a obrana*[194]. Řešení nesčetných problémů uvedených v této zprávě pomůže zvýšit tuto požadovanou autonomii. Žádné jednotlivé opatření samo o sobě toho nedosáhne.

Body k úvaze – účinná reakce

- Jak směrnice o bezpečnosti sítí a informací zlepšila oznamování kybernetických bezpečnostních incidentů v kritických odvětvích i mimo ně?
- Jak dobře fungují instituce EU pro internalizaci koordinace krizové reakce na závažný kybernetický bezpečnostní incident?
- Jak může diplomacie v oblasti kybernetiky hrát významnější úlohu v rámci vnější činnosti EU?
- Jsou současné struktury a opatření EU, které se mají zabývat dezinformacemi, úměrné rozsahu a složitosti problému?

Závěrečné poznámky

118 V posledních letech EU a její členské státy posílily kybernetickou bezpečnost a učinily z ní agendu s cílem zlepšit celkovou kybernetická odolnost. Dosažení vyšší úrovně kybernetické bezpečnosti v Unii však zůstává obrovským úkolem. V této stručné zprávě jsme se snažili zdůraznit některé z hlavních obtíží spojených s ambicí EU stát se nejbezpečnějším digitálním prostředím na světě.

119 Z našeho přehledu vyplývá, že pro zajištění **odpovědnosti a hodnocení** je nutný posun směrem ke kultuře založené na výkonnosti se zabudovanými hodnotícími mechanismy. Některé **mezery v právních předpisech nadále přetrvávají a stávající právní předpisy nejsou členskými státy důsledně prováděny do vnitrostátních právních řádů**. To může ztížit dosažení plného potenciálu právních předpisů. Další zjištěná výzva se týká **sladění objemu investic se strategickými cíli**, což vyžaduje zvýšení úrovně investic a jejich dopadu. To je náročnější, pokud EU a její členské státy nemají **jasný přehled o výdajích EU** v oblasti kybernetické bezpečnosti. Jsou rovněž zaznamenána **omezení, pokud jde o přiměřené financování agentur EU v oblasti kybernetiky,** včetně obtížného získávání a udržení talentovaných odborníků.

120 Dostupné studie dospěly k závěru, že **řízení kybernetické bezpečnosti může být posíleno,** aby se zvýšila schopnost celosvětového společenství reagovat na kybernetické útoky a incidenty. Není možné zabránit současně všem útokům. **Rychlá detekce a reakce a ochrana kritické infrastruktury a společenských funkcí** spolu s lepší **výměnou informací a koordinací** mezi veřejným a soukromým sektorem jsou proto klíčovými otázkami, které je třeba řešit. A v neposlední řadě narůstající globální nedostatek znalostí v oblasti kybernetické bezpečnosti znamená, že zásadním úkolem je **zvyšování dovedností a povědomí** ve všech odvětvích a na všech společenských úrovních.

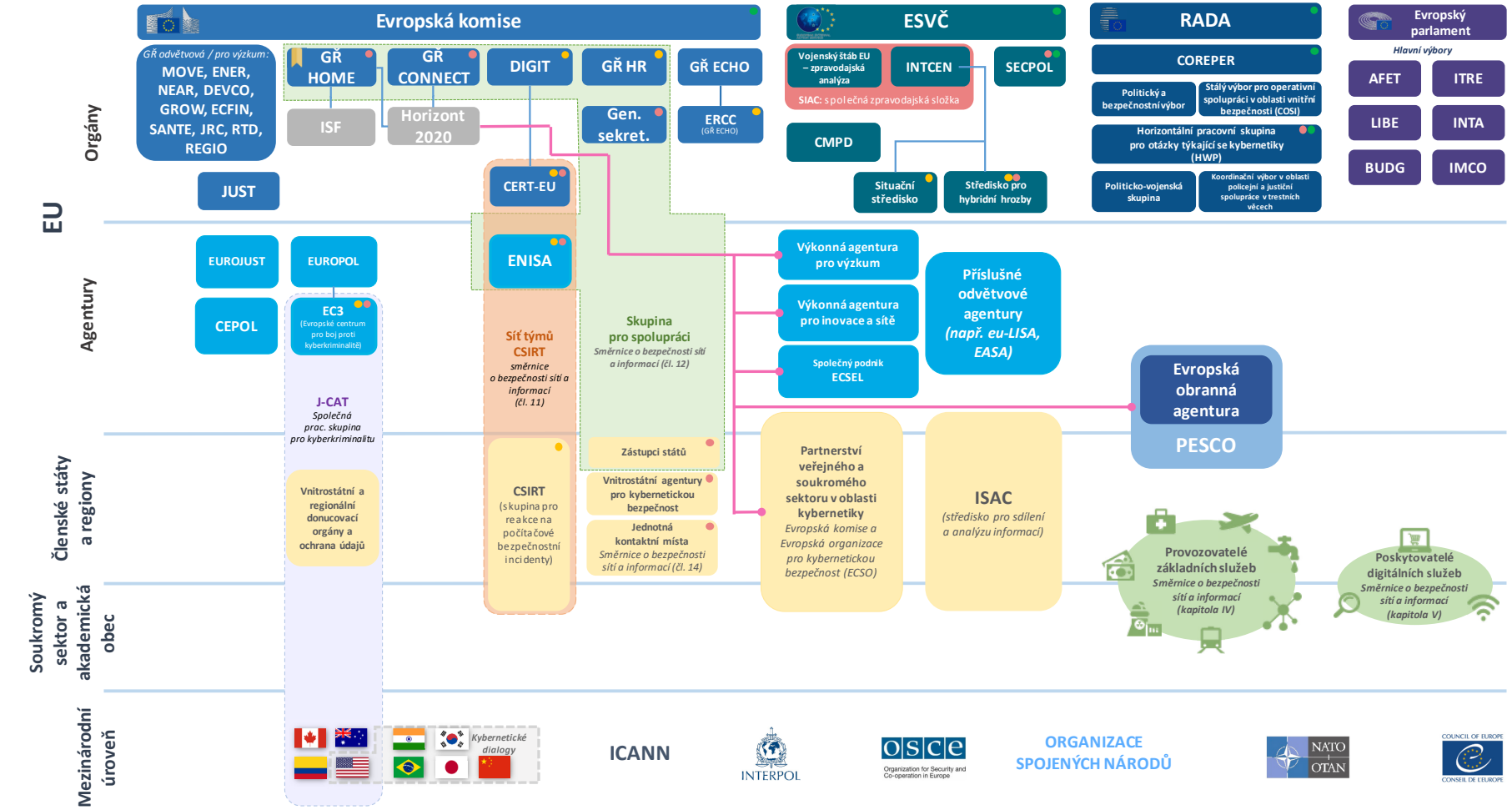
121 Tyto výzvy, jimž čelí EU a širší globální prostředí v důsledku kybernetických hrozeb, vyžadují soustavné úsilí a stálé a vytrvalé dodržování základních hodnot EU.

Tento informační dokument přijal senát III na svém zasedání dne 14. února 2019.

Za Účetní dvůr

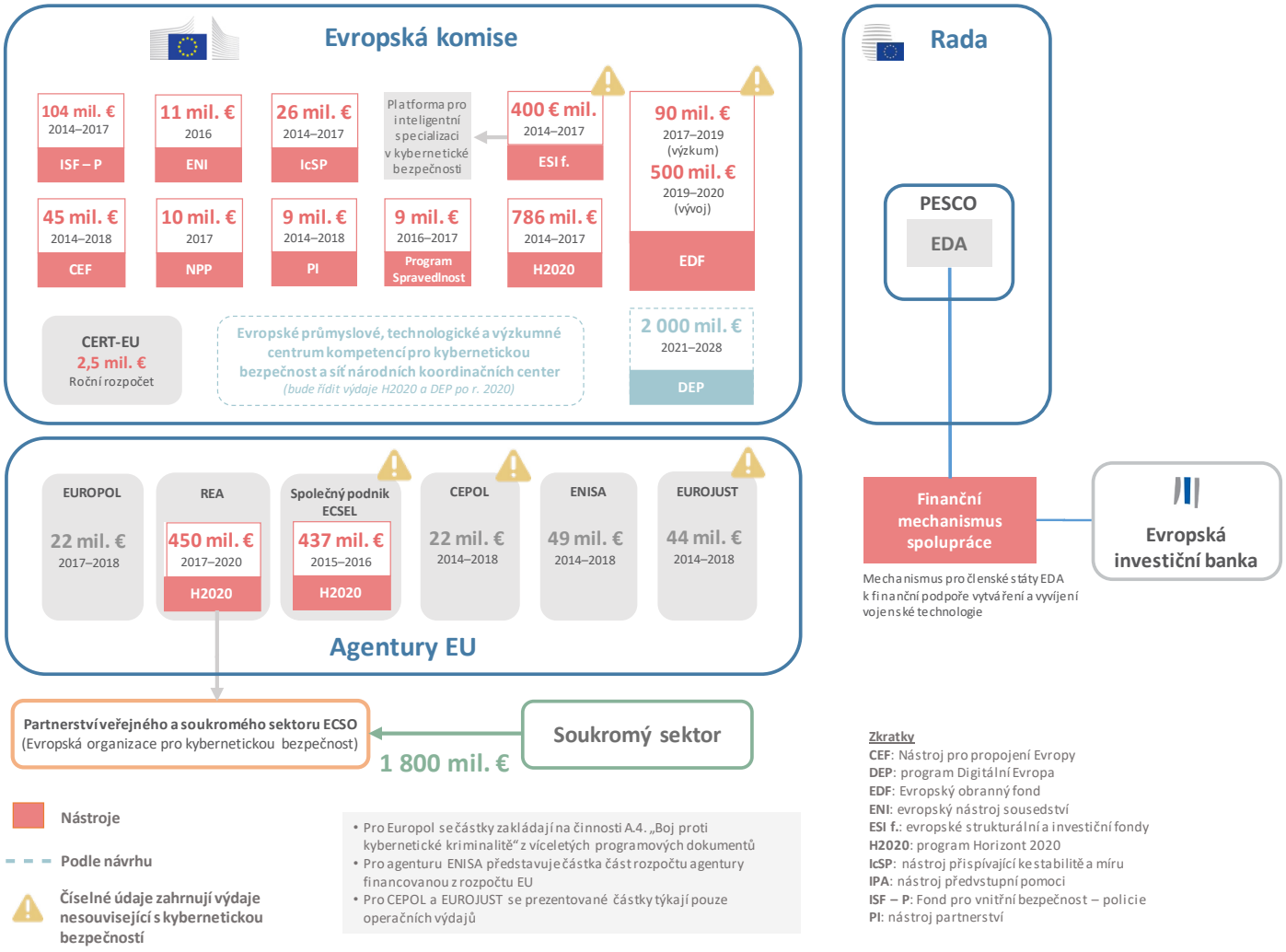
Klaus-Heiner Lehne
předseda

Příloha I — Složité, mnohovrstevnaté prostředí s mnoha aktéry



Zdroj: EÚD.

Příloha II — Výdaje EU na kybernetickou bezpečnost od roku 2014



Zdroj: EÚD podle dokumentů Evropské komise a agentur EU.

Příloha III — Zprávy kontrolních úřadů členských států EU

Druh	Název (s hypertextovým odkazem)	Rok	Čl. s.
Audity souladu s předpisy	Hodnotící zpráva vnitřní kontroly	2014	FR
	Zpráva o osvědčení účetní závěrky obecného systému sociálního zabezpečení (obrana, zahraniční věci)	2016	FR
	Osvědčení státní účetní závěrky	2016	FR
	Zajištění bezpečnosti a ochrany estonských vnitrostátních databází zásadního významu	Dok. 2018 / dosud nezveřejněno	EE
	Účinnost vnitřních kontrol při ochraně osobních údajů ve vnitrostátních databázích	2008	EE
Audity výkonnosti / optimálního vynaložení prostředků	Zpráva o zmírňování kybernetických útoků	2013	DK
	Bezpečnost informací ve veřejné správě (RiR 2014:23)	2014	SE
	Zpráva o zpracovávání důvěrných údajů o osobách a společnostech ze strany vlády	2014	DK
	Národní program kybernetické bezpečnosti	2014	UK
	Zpráva rozpočtovému výboru německého Spolkového sněmu podle § 88 odst. 2 zákona o státním rozpočtu – konsolidace IT, spolková vláda	2015	DE
	Zpráva o přístupu k informačním systémům, které podporují poskytování nezbytných služeb dánské společnosti	2015	DK
	Orgán veřejného plánování oblasti Plaine de France	2015	FR
	„Prostředí kybernetické bezpečnosti v Litvě“ litevské znění shrnutí přeložené do angličtiny	2015	LT
	Provádění úkolů v oblasti kybernetické bezpečnosti Polské republiky ze strany veřejných subjektů (polsky)	2015	PL
	Kyberkriminalita – policie a státními zástupci mohou být účinnější (RiR 2015:21)	2015	SE
	Nedostatek v oblasti digitálních dovedností ve vládě (zjišťování)	2015	UK
	Zpráva federálnímu parlamentu: Federální finance: výběr dědické daně	2016	BE
	Zpráva o řízení bezpečnosti IT v systémech zajišťovaných externími dodavateli	2016	DK
	Zpráva o auditu úvěrové činnosti Úřadu pro poskytování úvěrů z roku 2016	2016	ES
	Řízení vládní bezpečnostní sítě	2016	FI
	Zajištění bezpečnosti IT systémů používaných pro veřejné úkoly	2016	PL
	Prevence kyberšikany a boj proti ní mezi dětmi a mládeží	2016	PL
	Práce v oblasti bezpečností informací v devíti agenturách – další audit bezpečnosti informací ve státě (RiR 2016:8)	2016	SE
	Ochrana informací v celé veřejné správě	2016	UK
	Zpráva o ochraně informačních systémů a údajů o zdravotním stavu ve třech dánských regionech	2017	DK

Druh	Název (s hypertextovým odkazem)	Rok	Čl. s.
	Zpráva o výsledcích mezinárodního paralelního auditu „Účinnost vnitřních kontrol při ochraně osobních údajů ve vnitrostátních databázích“	2017	EE
	Zajištění kybernetické ochrany	2017	FI
	Řízení provozní spolehlivosti elektronických služeb	2017	FI
	Síť zemědělských komor (syntéza)	2017	FR
	Obchodní a průmyslová komora departamentu Vaucluse (od regionální účetní komory regionu Provence-Alpy-Azurové pobřeží)	2017	FR
	Zajištění bezpečnosti a ochrany estonských vnitrostátních databází zásadního významu	Dok. 2018 / dosud nezveřejněno	EE
	„Rozvoj státní elektronické komunikační infrastruktury“ litevské znění shrnutí přeložené do angličtiny	2017	LT
	Audit informačních technologií:kybernetická bezpečnost ve státních orgánech	2017	MT
	Systém vnitrostátních rejstříků: bezpečnost, fungování a použitelnost	2017	PL
	Incident „WannaCry“	2017	UK
	Podvody na internetu	2017	UK
	Zpráva o ochraně před ransomwarem	2018	DK
	Nemocnice v Arpajonu (od regionální komory regionu Île-de-France)	2018	FR
	„Kritické řízení státních informačních zdrojů“	2018	LT
	„Elektronické zločiny“	2019	LT
	Bezpečnost informací v Polsku	2019	PL
Jiné	Databáze veřejných subjektů	–	BE
	Dotazník ohledně politik bezpečnosti a analýzy rizik (stále probíhá)	–	BE

Zkratková slova a zkratky

CERT-EU: skupina pro reakci na počítačové hrozby v orgánech, institucích a jiných subjektech EU (*Computer Emergency Response Team*)

cPPP: smluvní partnerství veřejného a soukromého sektoru

CSIRT: skupina pro reakce na počítačové bezpečnostní incidenty (*Computer Security Incident Response Team*)

DDoS: distribuované odepření služby (*Distributed Denial of Service*)

DEP: program Digitální Evropa (*Digital Europe programme*)

DIGIT: Generální ředitelství pro informatiku

EC3: Evropské centrum pro boj proti kyberkriminalitě (součást Europolu)

ECSEL: elektronické součásti a systémy pro vedoucí postavení Evropy (*Electronic Components and Systems for European Leadership*)

ECSM: Evropský měsíc pro informovanost o kybernetické bezpečnosti (*European Cyber Security Awareness Month*)

ECSO: Evropská organizace pro kybernetickou bezpečnost (*European Cyber Security Organisation*)

EDA: Evropská obranná agentura

ENISA: Agentura Evropské unie pro bezpečnost sítí a informací

ESA: evropský orgán dohledu (*European Supervisory Authority*)

ESIF: evropský strukturální a investiční fond

ESVČ: Evropská služba pro vnější činnost

EU: Evropská unie

EÚD: Evropský účetní dvůr

GDPR: obecné nařízení o ochraně údajů (*General Data Protection Regulation*)

GŘ CONNECT: Generální ředitelství pro komunikační sítě, obsah a technologie

GŘ HOME: Generální ředitelství pro migraci a vnitřní věci

GŘ JUST: Generální ředitelství pro spravedlnost a spotřebitele

HWPCI: Horizontální pracovní skupina pro otázky týkající se kybernetiky (*Horizontal Working Party on Cyber Issues*)

ICS: průmyslové řídicí systémy (*Industrial Control Systems*)

ISF - P: Fond pro vnitřní bezpečnost - policie

ISSB: Rada pro řízení informační bezpečnosti

JRC: Společné výzkumné středisko

LISO: místní úředník pro bezpečnost informací (*Local Information Security Officer*)

NCIRC: složka NATO pro schopnost reakce na počítačové incidenty (*NATO Computer Incident Response Capability*)

NKI: národní kontrolní instituce

PESCO: rámec stálé strukturované spolupráce

PZI: přímé zahraniční investice

SBOP: společná bezpečnostní a obranná politika

SME: malé a střední podniky

Směrnice NIS: směrnice o bezpečnosti sítí a informací (*Network and Information Security Directive*)

Glosář

Adware: Škodlivý software zobrazující reklamní bannery nebo vyskakovací okna, které obsahují kód pro sledování chování obětí on-line.

Balíček exploitů („exploit kit“): Jeden ze souborů nástrojů, který pachatelé kybernetické kriminality využívají k útoku na zranitelná místa v síťových a informačních systémech, aby mohli šířit malware nebo provádět jiné škodlivé činnosti.

Bezpečnost informací: Soubor postupů a nástrojů chránících fyzické a digitální údaje před neoprávněným přístupem, použitím, zveřejněním, narušením, pozměněním, zaznamenáním nebo zničením.

Bezpečnost sítě: Podskupina kybernetické bezpečnosti chránící údaje předávané prostřednictvím zařízení ve stejné síti s cílem zajistit, že informace nebudou zachyceny ani změněny.

Botnet: Síť počítačů infikovaných škodlivým softwarem a ovládaných na dálku, bez vědomí uživatele, které slouží k rozesílání nevyžádaných e-mailů (spamu), krádežím informací nebo vedení koordinovaných kybernetických útoků.

Cloud computing: Poskytování IT zdrojů na vyžádání – např. ukládání, výpočetní výkon nebo kapacita sdílení údajů – přes internet prostřednictvím hostingu na vzdálených serverech.

Dezinformace: Prokazatelně falešná nebo zavádějící informace, která vzniká, prezentuje se a šíří se za účelem ekonomického prospěchu nebo úmyslného klamání veřejnosti a může přivodit veřejnou újmu.

Digitální obsah: Veškeré údaje – například text, zvuk, obrázky nebo video – uložené v digitálním formátu.

Distribuované odepření služby (DDoS, Distributed Denial of Service): Kybernetický útok zabraňující oprávněným uživatelům v přístupu k on-line službě nebo zdroji tím, že je zahlcuje větším množstvím požadavků, než mohou zvládnout.

Dostupnost: Zajištění včasného a spolehlivého přístupu k informacím a jejich využívání.

Důvěrnost: Ochrana informací, údajů nebo majetku před neoprávněným přístupem nebo zveřejněním.

Hacktivista: Jednotlivci nebo skupiny, které získávají neoprávněný přístup k informačním systémům nebo sítím s cílem prosazovat sociální nebo politické cíle.

Hybridní hrozba: Uskutečňování nepřátelského záměru prováděného protivníky v intenzivní snaze o dosažení svých cílů za smíšeného použití konvenčních i nekonvenčních technik vedení války (tj. vojenských, politických, ekonomických a technologických metod).

Integrita: Ochrana proti nekalému pozměnění nebo zničení informací, za účelem zaručení jejich autenticity.

Internet věcí: Síť každodenních předmětů vybavených elektronikou, softwarem a senzory, aby mohly komunikovat a provádět výměnu údajů přes internet.

Kritická infrastruktura: Fyzické zdroje, služby a zařízení, jejichž nefunkčnost nebo zničení by mělo vážný dopad na fungování hospodářství a společnosti.

Kryptoměna: Digitální aktivum, které je emitováno a vyměňováno za použití šifrovacích technik, nezávisle na centrální bance. Mezi členy virtuální komunity je přijímáno jako platební prostředek.

Kyberkriminalita: Různé trestné činnosti zahrnující počítače a informační systémy jako primární nástroj nebo primární cíl. Mezi tyto činnosti patří: tradiční trestné činy (např. podvody, padělání a krádež totožnosti), trestné činy související s obsahem (např. distribuce dětské pornografie on-line nebo podněcování k rasové nenávisti) a trestné činy specifické pro počítače a informační systémy (např. útoky na informační systémy, útoky odepření služby a malware).

Kybernetická bezpečnost: Veškerá ochranná a bezpečnostní opatření přijatá na obranu informačních systémů a jejich údajů před neoprávněným přístupem, útokem a poškozením za účelem zajištění jejich dostupnosti, důvěrné povahy a integrity.

Kybernetická obrana: Podskupina kybernetické bezpečnosti, jejímž cílem je obrana kyberprostoru pomocí vojenských a jiných vhodných prostředků za účelem dosažení vojensko-strategických cílů.

Kybernetická odolnost: Schopnost kybernetickým útokům a bezpečnostním incidentům zabránit, připravit se na ně, odolat jim a zotavit se z nich.

Kybernetický bezpečnostní incident: Událost, která přímo nebo nepřímo poškozuje nebo ohrožuje odolnost a bezpečnost informačního systému a údajů, které zpracovává, uchovává nebo přenáší.

Kybernetický ekosystém: Komplexní komunita zařízení, údajů, sítí, osob, procesů a organizací v interakci a prostředí procesů a technologií, které tuto interakci ovlivňují a podporují.

Kybernetický útok: Pokus narušit nebo zničit důvěrnou povahu, integritu a dostupnost údajů nebo počítačový systém prostřednictvím kyberprostoru.

Kyberprostor: Nehmotné globální prostředí, v němž dochází k on-line komunikaci mezi lidmi, softwarem a službami prostřednictvím počítačových sítí a technologických zařízení.

Malware: Škodlivý software. Počítačový program určený k poškození počítače, serveru nebo sítě.

Opravná řešení: Zavádění změn v softwaru za účelem jeho aktualizace, opravy nebo vylepšení, včetně řešení nedostatků v jeho bezpečnosti.

Osobní údaje: Informace týkající se identifikovatelné osoby.

Phishing : Zasílání e-mailů navozujících zdání důvěryhodného původu s cílem přimět příjemce, aby na základě klamného dojmu klikli na škodlivé odkazy nebo sdíleli osobní údaje.

Ransomware: Škodlivý software, který oběti odpírá přístup k počítačovému systému nebo činí soubory nečitelné, obvykle prostřednictvím šifrování. Útočník potom obvykle vydírá oběť tím, že odmítne přístup obnovit, dokud nebude vyplaceno výkupné.

Řízení zranitelnosti: Nedílná součást bezpečnosti počítačů a sítí, jejímž účelem je proaktivně zmírňovat zneužívání slabých míst v systému a softwaru nebo mu předcházet, a sice tak, že slabá místa jsou identifikována, klasifikována a odstraňována.

Skimming: Krádež údajů o kreditní nebo debetní kartě, když jsou zadány on-line.

Služby vytvářející důvěru: Služby posilující právní platnost elektronické transakce, jako jsou elektronické podpisy, pečeti, časové razítka, doporučeného doručování a autentizace internetových stránek.

Sociální inženýrství: V oblasti bezpečnosti informací psychologická manipulace usilující přimět člověka, aby na základě klamného dojmu provedl určitý úkon nebo prozradil důvěrnou informaci.

Starší systém: Neaktuální nebo zastaralý počítačový systém, aplikace nebo programovací jazyk, který je stále používán, ale pro který už nemusí být k dispozici aktualizace a podpora prodejců, včetně podpory zabezpečení.

Šifrování: Přeměna čitelných informací na nečitelný kód za účelem jejich ochrany. Aby uživatel mohl informace přečíst, musí mít přístup k tajnému klíči nebo heslu.

Trestná činnost prováděná kybernetickými prostředky: Tradiční trestná činnost páchaná ve větším měřítku za použití informačně technologických systémů.

Trestná činnost závisející na kybernetických prostředcích: Trestná činnost, která může být spáchána pouze za použití informačně technologických zařízení.

Údaje o přístupu: Informace o přihlašování uživatele pro přístup ke službě a o jeho odhlašování, např. čas, datum a IP adresa.

Vektorizace textu: Proces konverze slov, vět nebo celých dokumentů do numerických vektorů, aby je mohly používat algoritmy pro strojové učení.

Volební infrastruktura: Zahrnuje informační systémy a databáze kampaní, citlivé informace o kandidátech, systémy registrace voličů a řízení.

Wiper: Druh malwaru, jehož záměrem je nevratně smazat pevný disk počítače, který infikuje.

Zločin jako služba (crime-as-a-service , CaaS): Zločinný podnikatelský model, který je hnací silou šedé digitální ekonomiky a poskytuje širokou škálu komerčních služeb a nástrojů umožňujících nezkušeným, začátečnickým pachatelům dopouštět se kybernetické kriminality.

[1] V návrhu aktu EU o kybernetické bezpečnosti byla definována jako „veškeré činnosti nezbytné k ochraně sítí a informačních systémů, jejich uživatelů a osob dotčených kybernetickými hrozbami“. Očekává se, že akt bude přijat Evropským parlamentem a Radou na počátku roku 2019.

[2] Europol, *Internet Organised Crime Threat Assessment 2017* (Posouzení hrozeb organizované trestné činnosti na internetu za rok 2017).

[3] Evropská organizace pro kybernetickou bezpečnost (ECSO), *European Cybersecurity Industry Proposal for a contractual Public-Private Partnership* (Návrh evropského odvětví kybernetické bezpečnosti na smluvní partnerství veřejného a soukromého sektoru), červen 2016.

[4] Evropský parlament, *Kybernetická bezpečnost v Evropské unii a ve světě: zkoumání hrozeb a jejich řešení*, Studie pro výbor LIBE, září 2015.

[5] ENISA, *ENISA Threat Landscape Report 2017* (ENISA, Situační zpráva o hrozbách), 18. ledna 2018.

[6] Europol, *Internet Organised Crime Threat Assessment 2018* (Posouzení hrozeb organizované trestné činnosti na internetu za rok 2018).

[7] Europol, tamtéž, 2018.

[8] Evropské středisko pro politickou ekonomii, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?* (O krok napřed: dovolíme kybernetické špionáži zbrzdit Evropu v globálním soupeření o průmyslovou konkurenceschopnost?), příležitostný dokument č. 2/18, únor 2018.

[9] Předseda Evropské komise Projev o stavu Unie 2017.

[10] Europol, *World’s Biggest Marketplace selling internet paralysing DDoS attacks taken down* (Uzavření největší světové služby prodávající paralyzující útoky DDoS), tisková zpráva, 25. dubna 2018.

[11] Europol, *Internet Organised Crime Threat Assessment 2017* (Posouzení hrozeb organizované trestné činnosti na internetu za rok 2017).

[12] Přehled Evropské komise v oblasti kybernetické bezpečnosti, září 2017.

[13] Náklady by mohly zahrnovat: ztrátu příjmů, náklady na opravu poškozených systémů, případné závazky za ukradená aktiva nebo informace, pobídky k udržení zákazníků, vyšší pojistné, zvýšené náklady na ochranu (nové systémy, zaměstnanci, odborná příprava), případné vypořádání nákladů na soulad nebo soudní spory.

[14] NTT Security, *Risk: Value 2018 Report* (Riziko: Hodnotová zpráva za rok 2018).

[15] Ransomware *Wannacry* využíval zranitelná místa v protokolu Microsoft Windows umožňující vzdálené převzetí jakéhokoli počítače. Společnost Microsoft přinesla opravný prostředek poté, co objevila zranitelná místa. Stovky tisíc počítačů však ještě nebyly aktualizovány a mnoho z nich bylo následně infikováno. Zdroj: A. Greenberg, *Hold North*

Korea Accountable For Wannacry—and the NSA, too (Za Wannacry by se měla zpovídat Severní Korea — a také NSA), WIRED, 19. prosince 2017.

[16] Evropská komise, *Postoj evropských občanů ke kybernetické bezpečnosti*, Zvláštní Eurobarometr 464a, září 2017. Předpokládáme, že následný průzkum bude vydán počátkem roku 2019.

[17] Tato Budapešťská úmluva je závazným mezinárodním vodítkem pro země, které připravují právní předpisy proti kyberkriminalitě. Představuje rámec pro mezinárodní spolupráci mezi jednotlivými státy. Komise, Rada Evropské unie, Europol, ENISA a Eurojust v současnosti zastupují EU.

[18] Evropská komise, *Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor*, JOIN (2013) 1 final, 7. února 2013.

[19] Evropská komise, *Evropský program pro bezpečnost*, COM(2015) 185 final, 28. dubna 2015.

[20] Evropská komise, *Strategie pro jednotný digitální trh v Evropě*, COM(2015) 192 final, 6. května 2015.

[21] *Sdílená vize* EEAS*, Společný postup: Silnější Evropa. Globální strategie zahraniční a bezpečnostní politiky EU*, červen 2016.

[22] Centrum pro evropská politická studia, *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force* (Posílení kybernetické obrany EU – zpráva pracovní skupiny CEPS), listopad 2018.

[23] Malware za útokem ransomware Wannacry, který byl Spojenými státy, Spojeným královstvím a Austrálií připisován Severní Koreji, byl původně vyvinut a držen Agenturou pro národní bezpečnost USA za účelem využití zranitelných míst ve Windows. Zdroj: A. Greenberg, tamtéž, WIRED, 19. prosince 2017. Ihned po útocích Microsoft odsoudil hromadění zranitelných míst softwaru ze strany států a opakovala svůj požadavek na digitální Ženevskou úmluvu.

[24] Kromě země, moře, ovzduší a vesmíru.

[25] Politický rámec EU pro kybernetickou obranu (aktualizace z roku 2018), 14413/18, 19. listopadu 2018.

[26] Evropská komise/Evropská služba pro vnější činnost, *Společný rámec pro boj proti hybridním hrozbám: Reakce Evropské unie*, JOIN(2016) 18 final, 6. dubna 2016.

[27] Společné prohlášení předsedy Evropské rady, předsedy Evropské komise a generálního tajemníka Severoatlantické aliance, 8. července 2016 a 10. července 2018.

[28] Evropská komise/Evropská služba pro vnější činnost, *Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU*, JOIN(2017) 450 final, 13. září 2017.

[29] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016, s. 1).

[30] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

[31] Jsou integrovány do kooperačních struktur stanovených směrnicí, do sítě CSIRTS (síť složená z CSIRT stanovených členskými státy EU a CERT-EU, ENISA je hostitelem sekretariátu) a skupiny pro spolupráci (podporuje a usnadňuje strategickou spolupráci a výměnu informací mezi členskými státy, jejíž sekretariát hostí Komise).

[32] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

[33] Evropská komise, *Návrh nařízení Evropského parlamentu a Rady o agentuře ENISA, Agentuře EU pro kybernetickou bezpečnost, a zrušení nařízení (EU) č. 526/2013 a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií („akt o kybernetické bezpečnosti“)*, COM(2017) 477 final, 13. září 2017.

[34] Evropská komise, *Návrh nařízení Evropského parlamentu a Rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech,* COM(2018) 225 final*,* 17. dubna 2018*.*

[35] Evropská komise, *Návrh směrnice Evropského parlamentu a Rady, kterou se stanoví harmonizovaná pravidla pro jmenování právních zástupců za účelem shromažďování důkazů v trestním řízení*. COM(2018) 226 final, 17. dubna 2018.

[36] Evropská komise, *Návrh nařízení Evropského parlamentu a Rady, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center,* COM(2018) 630 final, 12. září 2018.

[37] H. Carrapico a A. Barrinha, *The EU as a Coherent (Cyber)Security Actor?* (EU jako jednotný hráč v oblasti (kybernetické) bezpečnosti?), Journal of Common Market Studies, sv. 55, č. 6, 2017.

[38] Evropská komise, tamtéž, SWD(2017) 295 final, 13. září 2017.

[39] Výzkumná služba Evropského parlamentu, *Transatlantic cyber-insecurity and cybercrime* (Transatlantická kybernetická bezpečnost a kybernetický zločin). *Economic impact and future prospects*, PE 603.948, prosinec 2017.

[40] ENISA, *An evaluation framework for Cyber Security Strategies* (Hodnotící rámec pro strategie kybernetické bezpečnosti), 27. listopadu 2014.

[41] Výjimkou je článek 14 („Sledování a statistika“) směrnice 2013/40/EU Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVVA.

[42] Evropský hospodářský a sociální výbor, *Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks* (Kybernetická bezpečnost: zajištění informovanosti a odolnosti soukromého sektoru v Evropě tvář v tvář rostoucím

kybernetickým rizikům), březen 2018. Skupina CEPS-ECRI, Cybersecurity in Finance: Getting the policy mix right!, červen 2018.

[43] Na náš průzkum odpovědělo 24 z 28 vnitrostátních kontrolních úřadů.

[44] To znamená, že jsou založeny na zásadách a co nejvíce technologicky neutrální.

[45] Odborný poradní mechanismus Evropské komise Odborné stanovisko č. 2/2017, 24. března 2017.

[46] L. Rebuffi, *EU Digital Autonomy: A possible approach* (Digitální autonomie EU: možný přístup), Digma Zeitschrift für Datenrecht und Informationssicherheit, září 2018. Evropské středisko pro politickou ekonomii, tamtéž, příležitostný dokument č. 2/18, únor 2018.

[47] Evropská komise, *Návrh směrnice Evropského parlamentu a Rady o některých aspektech smluv o poskytování digitálního obsahu*, COM(2015) 634 final, 9. prosince 2015.

[48] Evropská komise, *Návrh směrnice Evropského parlamentu a Rady o některých aspektech smluv o prodeji zboží online a jinými prostředky na dálku*, COM(2017) 635 final, 9. prosince 2015.

[49] Nizozemský výbor pro kybernetickou bezpečnost, *Evropské setkání k dalšímu vývoji v oblasti kybernetické bezpečnosti 2016: Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care* (Odborná doporučení Evropské komisi týkající se internetu věcí a harmonizace povinnosti řádné péče), 2016.

[50] Centrum pro evropská politická studia, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges – Report of a CEPS Task Force* (Zveřejnění informací o zranitelnosti softwaru v Evropě: technologické, odborné a právní otázky – zpráva pracovní skupiny CEPS), červen 2018.

[51] Evropská komise, *Maximální využití směrnice o bezpečnosti sítí a informací – účinné provedení směrnice (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii*, COM(2017) 476 final/2, 4. října 2017.

[52] Europol, tamtéž,, 2017.

[53] Rada Evropské unie, *Závěrečná zpráva o sedmém kole vzájemných hodnocení týkající se „Praktického provádění a fungování evropských politik v oblasti předcházení kyberkriminalitě a boje proti ní“*, 12711/1/17 REV 1, 9. října 2017.

[54] Evropská komise, Posouzení dopadů doprovázející dokument Návrh směrnice o boji proti podvodům a padělání bezhotovostních platebních prostředků, SWD/2017/0298 final, 13. září 2017. Politické dohody o novém právním předpisu byla dosažena v prosinci 2018 a očekává se, že předpis bude přijat počátkem roku 2019.

[55] Europol, tamtéž,, 2017.

[56] C-362/14: Maximillian Schrems v. komisař pro ochranu údajů (Irsko), 6. října 2015.

[57] Europol/Eurojust, *Common challenges in combating cybercrime* (Společné výzvy v boji proti kybernetickému zločinu), 7021/17, 13. března 2017.

[58] Evropská komise, *Posouzení strategie EU v oblasti kybernetické bezpečnosti za rok 2013*, SWD (2017) 295 final, 13. září 2017.

[59] Výzkumná služba Evropského parlamentu, *Briefing: EU Legislation in Progress – Review of dual-use export controls*, *PE589.832* (Briefing: vývoj právních předpisů EU – přezkoumání kontrol vývozu zboží dvojího užití).

[60] Usnesení Evropského parlamentu, *Lidská práva a technologie: dopad systémů narušování a sledování na lidská práva ve třetích zemích*, (2014/2232(INI)), 8. září 2015. Zboží a služby dvojího použití, které zahrnují software a technologii, mohou mít civilní a vojenské uplatnění.

[61] Veřejně dostupné informace jsou uloženy v databázi WHOIS, kterou spravuje ICANN (Internet Corporation for Assigned Names and Numbers). ICANN spravuje systém doménových jmen. Zneužívání doménových jmen usnadňuje kyberkriminalitu.

[62] Článek 3, směrnice o bezpečnosti sítí a informací, tamtéž

[63] Atlantická rada, *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures* (Podlehnout kybernetickým rizikům? Ekonomické výhody a náklady alternativní kybernetické budoucnosti), 10. září 2015.

[64] Bílý dům, *Cybersecurity spending fiscal year 2019* (Výdaje na kybernetickou bezpečnost za fiskální rok 2019).

[65] Evropská komise, *Pracovní dokument útvarů Komise: Hodnocení dopadu jako doložka k dokumentu „Návrh nařízení Evropského parlamentu a Rady, kterým se zavádí program Digitální Evropa na období 2021–2027“*, SWD(2018) 305 final, 6. června 2018.

[66] Haagské středisko pro strategické studie, *Dutch investments in ICT and cybersecurity: putting it in perspective* (Nizozemské investice do IKT a kybernetické bezpečnosti: souvislosti), prosinec 2016.

[67] Evropská komise, tamtéž, COM(2018) 630 final, 12. září 2018.

[68] Výzkumná služba Evropského parlamentu, oddělení odborného plánování, *Achieving a sovereign and trustworthy ICT industry in the EU* (Vytvoření suverénního a důvěryhodného sektoru IKT v EU), prosinec 2017.

[69] Evropské sdružení digitálních malých a středních podniků, *Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem* (Stanovisko k evropské strategii kybernetické bezpečnosti: podpora ekosystému malých a středních podniků), 31. července 2017.

[70] Výzkumná služba Evropského parlamentu, oddělení odborného plánování, tamtéž, prosinec 2017.

[71] tamtéž.

[72] Evropská komise, *Hodnocení dopadu navrhovaného výzkumného centra kompetencí a sítě národních koordinačních center*, SWD(2018) 403 final (část 1/4), 12. září 2018.

[73] Evropská komise, tamtéž, COM(2018) 630 final, 12. září 2018.

[74] EÚD, zvláštní zpráva č. 13/2018: „Boj proti radikalizaci vedoucí k terorismu“.

[75] Údaje uvedené v tomto oddíle pocházejí z veřejně dostupných dokumentů Komise, s výjimkou 42 milionů EUR v bodě ***51***, které nám Komise přímo sdělila.

[76] Program Horizont 2020 je výzkumným a inovačním programem EU ve výši 80 miliard EUR, který podporuje Unii inovací, jež je zaměřena na zajištění globální konkurenceschopnosti EU.

[77] Společenská výzva č. 7 programu Horizont 2020 „Zabezpečené a inovativní společnosti: ochrana svobody a bezpečnosti Evropy a jejích občanů“.

[78] Analyzovali jsme projekty H2020 z datového souboru CORDIS. V popisu každého projektu jsme provedli vektorizaci textu s použitím taxonomie kybernetické bezpečnosti JRC (viz ***rámeček 5*** v další kapitole) s cílem identifikovat projekty, které by měly souviset s kybernetickou bezpečností. Poté jsme ručně zkontrolovali a analyzovali výsledky.

[79] Evropská organizace pro kybernetickou bezpečnost, *ECS cPPP Progress Monitoring Report 2016-2017* (Zpráva ECS o monitorování pokroku cPPP), 29 . října 2018.

[80] Čl. 9 odst. 2, směrnice o bezpečnosti sítí a informací, tamtéž

[81] GLACY+ (Globální akce v oblasti kyberkriminality+) je společným projektem s Radou Evropy. Podporuje dvanáct zemí v Africe, v asijsko-tichomořském a latinskoamerickém a karibském regionu, které mohou na oplátku sloužit jako centra pro sdílení svých zkušeností v rámci svých regionů.

[82] Evropské středisko pro politickou strategii (EPSC), think-tank Komise, vyjádřilo své připomínky k riziku vzniku „digitálního slepého místa“, jestliže se rozdíly mezi EU a jejími sousedy v oblasti západního Balkánu nadále rozšiřují. Země jako Čína a Rusko do regionu investují značné částky, což hrozí marginalizací EU jako kybernetického činitele v regionu. Zdroj: EPSC, *Engaging with the Western Balkans: an investment in Europe’s security* (Spolupráce na západním Balkáně: investice do bezpečnosti Evropy), 17. května 2018.

[83] Evropská investiční banka, *The EIB Group Operating Framework and Operational Plan 2018* (Operační rámec a operační plán skupiny EIB v roce 2018), 12. prosince 2017. V době přípravy nebyly dostupné žádné další informace.

[84] Evropská komise, *Návrh nařízení Evropského parlamentu a Rady, kterým se zavádí program Digitální Evropa na období 2021–2027*, COM(2018) 434 final, 6. června 2018.

[85] Evropská komise, *Nařízení Evropského parlamentu a Rady (EU) 2018/1092 ze dne 18. července 2018, kterým se zřizuje Evropský program rozvoje obranného průmyslu s cílem podpořit konkurenceschopnost a inovační kapacitu obranného průmyslu Unie* (Úř. věst. L 200, 7.8.2018, s. 30) Kromě toho byly v roce 2017 zahájeny přípravné kroky na obranný výzkum v celkové výši 90 milionů EUR na období 2017–2019 a financované z H2020. Není jasné, zda se jedná o výdaje spojené s kybernetickou bezpečností.

[86] V roce 2019 by měl být zveřejněn informační dokument EÚD o obraně EU.

[87] Europol EC3, ENISA, ESVČ, Evropská obranná agentura a CERT-EU mají dohromady 159 pracovníků. Toto celkové množství nezahrnuje pracovníky v oblasti kybernetické

bezpečnosti v Evropské komisi nebo v členských státech. Zdroj: Centrum pro evropská politická studia, tamtéž, listopad 2018.

[88] *Hodnocení ENISA*, 2017.

[89] Europol požadoval ve svém víceletém plánu na období 2018–2020 roční nárůst počtu zaměstnanců o 70 dočasných zaměstnanců, avšak pro rok 2018 byl schválen nárůst pouze o 26 pracovníků. V dalším návrhu víceletého plánu na období 2019–2021 Europol žádal mírný nárůst a „předpokládal, že větší poptávka po zdrojích nebude uspokojena“. Zdroj: Konzultace o návrhu víceletého programu na období 2019–2021 předložené skupině pro společnou parlamentní kontrolu A 000834 dne 1. února 2018.

[90] *Hodnocení ENISA*, 2017. V letech 2014–2016 bylo přibližně 80 % rozpočtu agentury ENISA použito na zadávání studií.

[91] ENISA, *Exploring the opportunities and limitations of current Threat Intelligence Platforms* (Možnosti a omezení současných platforem týkajících se kybernetických hrozeb), prosinec 2017.

[92] ISACA (dříve známá jako Asociace auditu a kontroly informačních systémů), *Information Security Governance: Guidance for Boards of Directors and Executive Management* (Řízení informační bezpečnosti: pokyny pro správní rady a nejvyšší vedení), 2. vydání, 2006.

[93] EY, *Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017* (Návrat ke kybernetické bezpečnosti: příprava na boj kybernetickými útoky. Dvacátý průzkum celosvětové informační bezpečnosti, 2017), s. 16.

[94] McKinsey (J. Choi, J. Kaplan, C. Krishnamurthy a H. Lung), *Hit or myth? Understanding the true costs and impact of cybersecurity programs* (Zásah nebo mýtus: pochopení skutečných nákladů a dopadu programů kybernetické bezpečnosti), červenec 2017.

[95] Komise pro cenné papíry, *Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures* (Pokyny k vykazování informační o kybernetické bezpečnosti veřejných společností), 21. února 2018.

[96] Fórum pro spolupráci mezi Evropským orgánem pro bankovnictví, Evropským orgánem pro cenné papíry a trhy a Evropským orgánem pro pojišťovnictví a zaměstnanecké penzijní pojištění.

[97] Evropský orgán pro cenné papíry a trhy, *Joint Committee report on risks and vulnerabilities in the EU financial system* (Zpráva společného výboru o rizicích a zranitelných místech finančního systému EU), duben 2018.

[98] ENISA, *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in SMEs* (Standardy v oblasti bezpečnosti a zachovávání důvěrnosti informací pro malé a střední podniky: doporučení ke zlepšení), prosinec 2015.

[99] Pokud jde o členské státy EU, mechanismus vědeckého poradenství Komise zaznamenal „podstatnou a jedinečnou úroveň dohody o základních zásadách a hodnotách, jakož i sdílený strategický zájem, který může být jádrem účinného řízení kybernetické bezpečnosti v EU“. Zdroj: Odborné stanovisko č. 2/2017, 24. března 2017.

[100] USA, Čína, Japonsko, Jižní Korea, Indie a Brazílie.

[101] European Security and Defence College (T. Renard a A. Barrinha), *Handbook on cyber security, chapter 3.4 The EU as a partner in cyber diplomacy and defence* (Příručka o kybernetické bezpečnosti, kapitola 3.4 EU jako partner v kybernetické diplomacii a obraně), 23. listopadu 2018.

[102] Rada Evropské unie, *Akční plán pro účely provádění závěrů Rady o společném sdělení Evropskému parlamentu a Radě: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU*, 15748/17, 12. prosince 2017.

[103] Evropská komise, *Digitální strategie Evropské komise: Komise zaměřená na digitální transformaci, uživatele a údaje*, C(2018) 7118 final, 21. listopadu 2018.

[104] Odpověď komisaře Gabriela na otázku Parlamentu k písemnému zodpovězení (E-004294-17), 28. června 2017.

[105] Rada Evropské unie, *Výroční zpráva o provádění rámce politiky pro kybernetickou obranu*, 15870/17, 19. prosince 2017.

[106] Bezpečnost komunikačních a informačních systému Komise se řídí rozhodnutími 2015/443, 2015/444 a 2017/46. Rozhodnutím Komise C (2018) 7706 ze dne 21. listopadu 2018 se zřizuje Rada pro informační technologie a kybernetickou bezpečnost, která sdružuje předchozí Řídící radu pro IT a Radu pro bezpečnost informačních systémů.

[107] Evropský hospodářský a sociální výbor, tamtéž, březen 2018.

[108] Evropský parlament, tamtéž, září 2015.

[109] Středisko pro hybridní hrozby bylo založeno v roce 2016 v rámci Střediska EU pro analýzu zpravodajských informací ESVČ. Získává a analyzuje klasifikované informace a informace z otevřených zdrojů od různých zúčastněných stran ohledně hybridních hrozeb.

[110] ENISA, *National-level Risk Assessments: An Analysis Report* (Posouzení rizik na národní úrovni: analýza), listopad 2013.

[111] Evropská komise, *Posouzení dopadů na Agenturu EU pro kybernetickou bezpečnost a akt o kybernetické bezpečnosti* , SWD(2017) 500 final (část 1/6), 13. září 2017.

[112] Evropská komise, tamtéž, SWD(2018) 403 final, 12. září 2018.

[113] Koordinační centrum sítě Résaux IP Européens, regionální internetový registr pro Evropu, který dohlíží na přidělování a registraci zdrojů internetového čísla.

[114] ENISA, *EISAS Large-Scale Pilot Collaborative Awareness Raising for EU Citizens & SMEs* (Rozsáhlá společná pilotní informační kampaň EISAS pro občany EU a malé a střední podniky), listopad 2012.

[115] The Centre for Cyber Safety and Education, ve spolupráci s Booz Allen Hamilton, Alta Associates and Frost & Sullivan, *2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk* (Studie celosvětové pracovní síly v oblasti informační bezpečnosti – porovnání kapacit a reakce na kybernetická rizika).

[116] Evropský hospodářský a sociální výbor, tamtéž, březen 2018.

[117] Sněmovna lordů, Dolní sněmovna *Joint Committee on the National Security Strategy, Cyber Security Skills and the UK's Critical National Infrastructure, Second Report of Session 2017–19* (Společný výbor pro národní bezpečnostní strategii, znalosti v oblasti kybernetické bezpečnosti a kritická národní infrastruktura Spojeného království, druhá zpráva ze zasedání za období 2017–2019), 16. července 2018.

[118] Europol/Eurojust, *Common challenges in combating cybercrime* (Společné výzvy v boji proti kybernetickému zločinu), 7021/17, 13. března 2017.

[119] Europol/Eurojust, tamtéž, 7021/17, 13. března 2017.

[120] Evropská komise, tamtéž, SWD(2018) 403 final, 12. září 2018.

[121] CEPOL, *Rozhodnutí správní rady 33/2018/MB o jednotném programovém dokumentu CEPOL na období 2020–2022*, 20. listopadu 2018.

[122] Například spolupráce mezi ESVČ, členskými státy, agenturami a subjekty, jako je CEPOL, ECTEG nebo EDSC.

[123] ENISA, *Rozsah potřebných školení v oblasti informační bezpečnosti v kriticky důležitých odvětvích*, prosinec 2017.

[124] Evropská skupina pro vzdělávání a odbornou přípravu v oblasti kyberkriminality.

[125] Evropská komise, třináctá zpráva o pokroku směrem k účinné a skutečné unii bezpečnosti, COM (2018) 46 final, 24. ledna 2018.

[126] Na základě zjištění ve zvláštní zprávě č. 14/2018, tamtéž

[127] Usnesení Evropského parlamentu ze dne 13. června 2018 o kybernetické obraně (2018/2004(INI)). Rada Evropské unie, tamtéž, 15870/17, 19. prosince 2017.

[128] Švýcarsko, Bývalá jugoslávská republika Makedonie, Ukrajina, Bosna a Hercegovina, Kosovo (tímto označením nejsou dotčeny postoje týkající se statutu a je v souladu s rezolucí Rady bezpečnosti OSN č. 1244/1999 a stanoviskem Mezinárodního soudního dvora k prohlášení o nezávislosti Kosova), Turecko a USA.

[129] Europol, *Internet Organised Crime Threat Assessment 2018* (Posouzení hrozeb organizované trestné činnosti na internetu za rok 2018).

[130] Evropská komise, tamtéž, SWD(2017) 295 final, 13. září 2017.

[131] B. Stanton, M. F. Theofanos, S. S. Prettyman a S. Furman, *Security Fatigue* (Únava z tématu bezpečnosti), „IT Professional", sv. 18, č. 5, 2016, s. 26–32. Viz též NIST.

[132] Evropská komise/Evropská služba pro vnější činnost, *Zvýšení odolnosti a posílení kapacit pro řešení hybridních hrozeb*, JOIN(2018) 16 final, 13. června 2018.

[133] Například uzavření AlphaBay a Hansa v rámci společných operací pod vedením FBI a nizozemské státní policie s podporou Europolu. Jednalo se o dva z největších trhů pro obchodování s nedovoleným zbožím, jako jsou drogy, zbraně a nástroje pro kyberkriminalitu, jako je malware. Zdroj: Europol, *Crime on the Dark Web: Law Enforcement coordination is the only cure* (Kriminalita na darknetu: koordinace donucovacích orgánů je jediným řešením), tisková zpráva, 29. května 2018.

[134] Rada Evropské unie, tamtéž, 12711/1/17 REV 1, 9. října 2017.

[135] Evropská komise, tamtéž, SWD(2018) 403 final, 12. září 2018.

[136] Evropská komise, tamtéž, SWD(2017) 295 final, 13. září 2017.

[137] Evropská komise/Evropská služba pro vnější činnost, tamtéž, JOIN(2018) 16, 13. června 2018.

[138] Evropská komise, SWD(2017) 500 final, 13. září 2017.

[139] *Memorandum o porozumění – ENISA, EDA, Europol EC3 a CERT-EU*; 23. května 2018.

[140] Evropská komise, výzva k podávání nabídek: *Zřízení a provoz pilotního projektu sítě kompetencí pro kybernetickou bezpečnost s cílem vytvořit a zavést společný plán výzkumu a inovací v oblasti kybernetické bezpečnosti*, 27. října 2017.

[141] Jean-Claude Juncker, Pověřovací dopis komisaři pro bezpečnostní unii, 2. srpna 2016. Obrana nespadá do náplně práce pracovní skupiny.

[142] Rada Evropské unie, *Plán pro kybernetickou bezpečnost EU*, 8901/17, 11. května 2017.

[143] Friends of Europe, *Debating Security Plus: Crowdsourcing solutions to the world's security issues*, 5. Vydání (Debata o bezpečnosti: crowdsourcingová řešení celosvětových bezpečnostních otázek), listopad 2017.

[144] Společné výzkumné středisko, technické zprávy, mapa odborných znalostí středisek evropské kybernetické bezpečnosti: *Definice a taxonomie.* Hodnocení dopadu navrhovaného výzkumného centra kompetencí a sítě národních koordinačních center, SWD(2018) 403 final, 12. září 2018.

[145] Evropská komise, tamtéž, SWD(2017) 295 final, 13. září 2017.

[146] Evropská komise, tamtéž, SWD(2018) 403 final, 12. září 2018.

[147] Například ISAC pro evropské finanční instituce zahrnuje zástupce finančního sektoru, národní agentury CERT, orgánů pro prosazování práva, agentury ENISA, Europolu, Evropské centrální banky, Evropské rady pro platební styk a Evropské komise.

[148] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models* (Modely spolupráce středisek pro sdílení a analýzu informací), 14. února 2018.

[149] Rada Evropské unie, tamtéž, 12711/1/17 REV 1, 9. října 2017.

[150] https://www.europol.europa.eu/empact.

[151] Studie Accenture z roku 2018 provedená v 15 zemích ukázala, že 87 % cílených kybernetických útoků bylo zabráněno: *2018 State of Cyber Resilience* (Stav kybernetické odolnosti, zpráva za rok 2018) 10. dubna 2018.

[152] P. Timmers, *Cybersecurity is Forcing a Rethink of Strategic Autonomy* (Kybernetická bezpečnost nutí k přehodnotit strategickou autonomii), Oxford University Politics Blog, 14. září 2018.

[153] Caroline Preece, *Three reasons why cyber threat detection is still ineffective* (Tři důvody, proč se stále nedaří účinně odhalovat kybernetické hrozby), IT Pro, 14. července 2017.

[154] Evropský hospodářský a sociální výbor, tamtéž, březen 2018.

[155] Evropská komise, *Osmá zpráva o pokroku na cestě k účinné a skutečné bezpečnostní unii*, COM (2017) 354 final, 29. června 2017.

[156] Viz různé publikace skupiny pro spolupráci v oblasti bezpečnosti sítí a informací.

[157] PSD2: Směrnice o platebních službách 2; ECB/SSM: Evropská centrální banka/Jednotný mechanismus dohledu; Cíl 2: Transevropský automatizovaný expresní systém hrubého zúčtování plateb v reálném čase (druhá generace), nařízení 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu Zdroj: Skupina CEPS-ECRI, tamtéž, červen 2018.

[158] Evropská komise, *Doporučení koordinované odezvy na rozsáhlé incidenty a krize v oblasti kybernetické bezpečnosti*, C(2017) 6100 final, 13. září 2017.

[159] Evropská komise, tamtéž, SWD(2017) 295 final, 13. září 2017. Existuje několik mechanismů pro řešení krizí, včetně mechanismu integrovaných opatření pro politickou reakci na krize (IPCR), mechanismu Argus (mechanismus Komise pro reakci na krizové situace), mechanismu reakce na krizi ESVČ, mechanismu civilní ochrany Unie a Protokolu o reakci na mimořádné situace v EU v oblasti vymáhání práva.

[160] Navíc to může vyvolat uplatnění čl. 42 odst. 7 Smlouvy o Evropské unii (doložka o vzájemné pomoci) nebo článku 222 Smlouvy o fungování Evropské unie (doložka o solidaritě).

[161] Evropská komise/Evropská služba pro vnější činnost, tamtéž, JOIN(2018) 16, 13. června 2018. V prosinci roku 2018 byly v médiích hlášeny údajné hackerské útoky na diplomatické komunikační sítě ESVČ, COREU (zdroj: *New York Times, Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran* (Uniklé diplomatické depeše EU odhalují obavy z Trumpa, Ruska a Íránu); 18. prosince 2018). Věc je v současné době předmětem šetření.

[162] Spolupráce v oblasti včasného varování a vzájemné pomoci také vyžaduje další rozvoj: *Závěry Rady o koordinované reakci EU na rozsáhlé kybernetické bezpečnostní incidenty a krize*, 10085/18, 26. června 2018.

[163] Výzkumná služba Evropského parlamentu, *Briefing EU Legislation in Progress: ENISA and a new cybersecurity act* (Informační sdělení o projednávaných právních předpisech EU: ENISA a nový akt o kybernetické bezpečnosti), PE 614.643, září 2018.

[164] Evropský hospodářský a sociální výbor, tamtéž, březen 2018.

[165] Rada Evropské unie, *EU Law Enforcement Emergency Response Protocol (LE ERP) for Major Cross-Border Cyber-Attacks*, 14893/18, prosinec 2018.

[166] Týmy rychlé kybernetické reakce a vzájemná pomoc v oblasti kybernetické bezpečnosti; Platforma pro sdílení informací o kybernetických hrozbách a reakci na incidenty. Zdroj: Rada Evropské unie, *Permanent Structured Cooperation (PESCO) updated list of PESCO projects – Overview* (Aktualizovaný seznam projektů stálé strukturované spolupráce PESCO – přehled), 19. listopadu 2018.

[167] Rada Evropské unie , Závěry Rady o rámci pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru , 9916/17, 7. června 2017.

[168] Rada Evropské unie, *Council Conclusions on Cyber Diplomacy*, 6122/55, 11. února 2015.

[169] Rada Evropské unie, *Návrh prováděcích předpisů k rámci Rady pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru*, 13007/17.

[170] Přisouzení odpovědnosti za incident je i nadále pro členské státy suverénním politickým rozhodnutím, a nikoli všechna opatření v souborech nástrojů vyžadují přidělení.

[171] Soubor nástrojů nevedl ke společnému postupu, jednotlivé členské státy přijaly postoj Spojených států.

[172] Rada Evropské unie, *Závěry Rady o nepřátelské činnosti v kyberprostoru*, 7925/18, 16. dubna 2018.

[173] Počítačové systémy používané k řízení procesů v různých oblastech, jako jsou veřejné služby, chemická a průmyslová výroba, zpracování potravin, dopravní systémy a huby a logistické služby.

[174] ENISA, tamtéž, prosinec 2017.

[175] Například veřejná správa, chemický a jaderný průmysl, výroba, zpracování potravin, cestovní ruch, logistika a civilní ochrana.

[176] Evropská komise, tamtéž, SWD(2017) 295 final, 13. září 2017.

[177] Projev komisařky Jourové na plenárním zasedání Evropského parlamentu *Zvyšování odolnosti EU vůči vlivům zahraničních aktérů v nadcházející volební kampani do EP*, 14. listopadu 2018.

[178] Nadace Carnegie pro mezinárodní mír, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks* (Ruské zásahy do voleb: odpověď Evropy na dezinformační kampaně a kybernetické útoky), 23. května 2018.

[179] Evropské politické a strategické centrum (L. Past), Kybernetická bezpečnost volební technologie: Nevyhnutelné útoky a rozmanitost reakcí v: „Election Interference in the Digital Age – Building Resilience to Cyber-Enabled Threats: A collection of think pieces of 35 leading practitioners and experts" (Ovlivňování voleb v digitální éře – budování odolnosti vůči kybernetickým hrozbám: sborník příspěvků 35 předních odborníků), 2018.

[180] Podle směrnice Rady 2008/114 /ES o určování a označování evropských kritických infrastruktur a posouzení potřeby zlepšit jejich ochranu.

[181] Evropská Komise, Doporučení o sítích pro volební spolupráci, transparentnosti on-line, ochraně před kybernetickými bezpečnostními incidenty a boji proti dezinformačním kampaním v souvislosti s volbami do Evropského parlamentu, C(2018) 5949 final, 12. září 2018.

[182] Závěry Evropské rady, EUCO 11/15, 20. března 2015. Od té doby přibyly dvě další pracovní skupiny pro západní Balkán a jižní sousedství.

[183] Zpráva Atlantické rady vyzvala EU, aby požadovala od všech členských států, aby vyslaly své vlastní odborníky do pracovní skupiny. Viz: D. Fried a A. Polyakova, *Democratic Defense Against Disinformation* (Demokratická obrana proti dezinformacím), 5. března 2018.

[184] Skupina, která původně neměla vlastní rozpočet, získala v roce 2018 od Evropského parlamentu 1,1 milionu EUR na přípravné kroky „StratCom Plus“.

[185] Nadace Carnegie pro mezinárodní mír (E. Brattberg, T. Maurer), tamtéž, 23. května 2018.

[186] Evropská komise, vysoká představitelka Unie pro zahraniční věci a bezpečnostní politiku, *Akční plán proti dezinformacím*, JOIN(2018) 36 final. Plán se zaměřuje na zlepšení schopností orgánů EU odhalovat, analyzovat a zveřejňovat dezinformace, na posílení koordinovaných a společných reakcí, na mobilizaci soukromého sektoru, na zvyšování povědomí a zlepšení odolnosti společnosti.

[187] Evropská komise, *Boj proti dezinformacím na internetu: evropský přístup*, COM(2018) 236 final, 26. dubna 2018.

[188] Nesmí být zaměňováno s kodexem chování pro potírání nezákonných projevů nenávisti na internetu.

[189] Společné výzkumné středisko, *The digital transformation of news media and the rise of disinformation and fake news* (Digitální transformace zpravodajských médií a nárůst dezinformací a falešných zpráv), Technické zprávy SVS, pracovní dokument SVS k digitální ekonomice 2018-02, duben 2018.

[190] ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News")* (Posílení síťové a informační bezpečnosti a ochrana proti dezinformacím šířeným po internetu), duben 2018

[191] Evropské středisko pro politickou strategii (C. Frutos López), *A Responsibility to Support Electoral Organisations in Anticipating and Countering Cyber Threats* (Povinnost podporovat volební organizace v předjímání a řešení kybernetických hrozeb), tamtéž, 2018.

[192] Evropská komise, tamtéž, SWD(2018) 403 final, 12. září 2018.

[193] Návrh nařízení (COM(2017) 487 final, 13. září 2018) pro prověřování přímých zahraničních investic, předložený v září 2017, prochází v současné době legislativním procesem. Týká se zejména kritických technologií, což zahrnuje umělou inteligenci, kybernetickou bezpečnost a aplikace s dvojím použitím.

[194] Evropská komise, tamtéž, SWD(2017) 450 final, 13. září 2017.

Tým EÚD

Tento informační dokument s názvem *Výzvy týkající se účinné politiky EU v oblasti kybernetické bezpečnosti* přijal senát III, který odpovídá za audit oblastí vnější činnost a bezpečnost a právo a jemuž předsedá členka EÚD Bettina Jakobsenová. Úkol vedl člen EÚD Baudilio Tomé Muguruza a podporu mu poskytovali vedoucí kabinetu Daniel Costa de Magalhaes a tajemník kabinetu Ignacio Garcia de Parada, vyšší manažer Alejandro Ballester-Gallardo, vedoucí úkolu Michiel Sweerts, auditoři Simon Dennett, Aurelia Petlizová, Mirko Iaconisi, Michele Scardone, Silvia Monteirová Da Cunha a stážista Johannes Bolkart. Jazykovou podporu zajišťovala Hannah Critophová.

Zleva doprava: Ignacio Garcia de Parada, Silvia Monteirová Da Cunha, Michele Scardone, Michiel Sweerts, Mirko Iaconisi, Baudilio Tomé Muguruza, Simon Dennett, Hannah Critophová, Daniel Costa de Magalhaes.

EVROPSKÝ
ÚČETNÍ DVŮR

Úřad pro publikace

EVROPSKÝ ÚČETNÍ DVŮR
12, rue Alcide De Gasperi
1615 Lucemburk
LUCEMBURSKO

Tel.: +352 4398-1

Dotazy: eca.europa.eu/cs/Pages/ContactForm.aspx
Internetová stránka: eca.europa.eu
Twitter: @EUAuditors