EURÓPSKY DVOR AUDÍTOROV

SK

2019

Prekážky účinnej politiky EÚ v oblasti kybernetickej bezpečnosti

Informačný dokument

Marec 2019

O dokumente:

Cieľom tohto informačného dokumentu, ktorý nie je audítorskou správou, je poskytnúť prehľad zložitej situácie EÚ v oblasti politiky kybernetickej bezpečnosti a určiť hlavné prekážky pre jej účinnú realizáciu. Informačný dokument sa venuje sieťovej a informačnej bezpečnosti, počítačovej kriminalite, kybernetickej obrane a dezinformáciám. Dokument bude v budúcnosti tiež slúžiť ako základ pre audítorskú činnosť v tejto oblasti.

Analýzu sme založili na preskúmaní písomných, verejne dostupných informácií nachádzajúcich sa v úradných dokladoch, pozičných dokumentoch a v štúdiách tretích strán. Práca v teréne prebiehala od apríla do septembra 2018 a zohľadnil sa aj vývoj do decembra 2018. Svoju prácu sme doplnili prieskumom vo vnútroštátnych kontrolných úradoch členských štátov a rozhovormi s hlavnými zainteresovanými stranami spomedzi inštitúcií EÚ a zástupcov súkromného sektora.

Výzvy, ktoré sme identifikovali, sú zoskupené do štyroch všeobecných oblastí: i) politický rámec; ii) financovanie a výdavky; iii) budovanie kybernetickej odolnosti a iv) účinné reagovanie na kybernetické incidenty. Dosiahnutie vyššej úrovne kybernetickej bezpečnosti v EÚ zostáva kategorickým testom. Na konci každej kapitoly preto uvádzame súbor myšlienok na ďalšie zváženie tvorcami politík, zákonodarcami a aplikujúcimi odborníkmi.

Chceme poďakovať za konštruktívnu spätnú väzbu od útvarov Komisie, Európskej služby pre vonkajšiu činnosť, Rady Európskej únie, agentúry ENISA, Europolu, Európskej organizácie kybernetickej bezpečnosti a vnútroštátnych kontrolných úradov členských štátov.

Obsah

	Body
Zhrnutie	I – XIII
Úvod	01 – 24
Čo je kybernetická bezpečnosť?	02 – 06
Aká je závažnosť tohto problému?	07 – 10
Opatrenia EÚ v oblasti kybernetickej bezpečnosti	11 – 24
Politika	13 – 18
Právne predpisy	19 – 24
Vybudovanie politického a legislatívneho rámca	25 – 39
Problém 1: zmysluplné hodnotenie a zodpovednosť	26 – 32
Problém 2: odstraňovanie medzier v práve EÚ a jeho nerovnomerná transpozícia	33 – 39
Financovanie a výdavky	40 – 64
Problém 3: zosúladenie úrovne investícií s cieľmi	41 – 46
Zvyšovanie investícií	41 – 44
Zvýšenie účinku	45 – 46
Problém 4: jasný prehľad rozpočtových výdavkov EÚ	47 – 60
Identifikovateľné výdavky na kybernetickú bezpečnosť	50 – 56
Iné výdavky na kybernetickú bezpečnosť	57 – 58
Pohľad do budúcnosti	59 – 60
Problém 5: primerané zabezpečenie zdrojov pre agentúry EÚ	61 – 64
Budovanie spoločnosti odolnej proti kybernetickým útokom	65 – 100
Problém 6: posilnenie správy a noriem	66 – 81
Správa informačnej bezpečnosti	66 – 75
Posudzovanie hrozieb a rizika	76 – 78

Stimuly 79 – 81

Problém 7: zvyšovanie úrovne zručností a informovanosti 82 – 90

Odborná príprava, zručnosti a budovanie kapacít 84 – 87

Informovanosť 88 – 90

Problém 8: lepšia výmena informácií a koordinácia 91 – 100

Koordinácia medzi inštitúciami EÚ a s členskými štátmi 92 – 96

Spolupráca a výmena informácií so súkromným sektorom 97 – 100

Účinné reagovanie na kybernetické incidenty 101 – 117

Problém 9: účinné odhalenie a reakcia 102 – 111

Odhaľovanie a oznamovanie 102 – 105

Koordinovaná reakcia 106 – 111

Problém 10: ochrana kritickej infraštruktúry a spoločenských funkcií 112 – 117

Ochrana infraštruktúry 112 – 115

Posilnenie autonómie 116 – 117

Záverečné poznámky 118 – 121

Príloha I — Komplexné, mnohovrstevné prostredie s množstvom aktérov

Príloha II — Výdavky EÚ na kybernetickú bezpečnosť od roku 2014

Príloha III — Správy kontrolných úradov členských štátov EÚ

Skratky

Glosár

Tím Európskeho dvora audítorov

Zhrnutie

I Technológie otvárajú celý nový svet možností a nové produkty a služby sa stávajú neoddeliteľnou súčasťou našich každodenných životov. V dôsledku toho sa zvyšuje riziko, že sa staneme obeťou počítačovej kriminality alebo kybernetického útoku, ktorých vplyv na spoločnosť a hospodárstvo naďalej rastie. Zvýšená pozornosť EÚ v nedávnom období po roku 2017 venovaná zintenzívneniu úsilia o posilnenie kybernetickej bezpečnosti a jej digitálnej autonómie teda prichádzajú v rozhodujúcom okamihu.

II Cieľom tohto informačného dokumentu, ktorý nie je audítorskou správou a ktorý je založený na verejne dostupných informáciách, je poskytnutie prehľadu o zložitej a nevyváženej situácii týkajúcej sa politiky a určenie hlavných prekážok pre jej účinnú realizáciu. Rozsah tohto dokumentu sa týka politiky EÚ v oblasti kybernetickej bezpečnosti, ako aj počítačovej kriminality a kybernetickej obrany a takisto zahŕňa úsilie bojovať proti dezinformáciám. Výzvy, ktoré sme identifikovali, sú zoskupené do štyroch všeobecných oblastí: i) politický a legislatívny rámec; ii) financovanie a výdavky; iii) budovanie kybernetickej odolnosti a iv) účinné reagovanie na kybernetické incidenty. Každá kapitola obsahuje určité podnety na zamyslenie o diskutovaných problémoch.

Politický a legislatívny rámec

III Vytvorenie opatrenia, ktoré by bolo v súlade so širokými cieľmi stratégie kybernetickej bezpečnosti EÚ, aby sa z Únie stalo najbezpečnejšie digitálne prostredie na svete, je bez merateľných cieľov a vzácnych, spoľahlivých údajov problematické. Účinky sa zriedkakedy merajú a vyhodnotených bolo iba málo oblastí politiky. Hlavným problémom je teda **zabezpečenie primeranej zodpovednosti a hodnotenia** prostredníctvom prechodu na kultúru výkonnosti, ktorej súčasťou sú hodnotiace postupy.

IV Legislatívny rámec zostáva neúplný. **Medzery v práve EÚ a jeho nedôsledná transpozícia** môžu sťažiť to, aby právne predpisy dosiahli svoj úplný potenciál.

Financovanie a výdavky

V **Zosúladenie úrovne investícií s cieľmi** je náročné: nevyžaduje si len zvýšenie celkových investícií v oblasti kybernetickej bezpečnosti, ktoré sú v EÚ nízke

a rozdrobené, ale aj zvýšenie ich účinku, najmä pokiaľ ide o lepšie využitie výsledkov výdavkov na výskum a zabezpečenie účinného zacielenia a financovania startupov.

VI **Jasný prehľad výdavkov EÚ** je pre EÚ a jej členské štáty nevyhnutný, aby poznali, ktoré nedostatky treba odstrániť v záujme splnenia cieľov, ktoré si stanovili. Keďže neexistuje špecializovaný rozpočet EÚ určený na financovanie stratégie kybernetickej bezpečnosti, neexistuje ani jasná predstava o tom, kam smerujú konkrétne finančné sumy.

VII V čase politických priorít motivovaných zvýšenými obavami o bezpečnosť môžu **obmedzenia týkajúce sa primeraného zabezpečovania zdrojov pre agentúry EÚ zaoberajúce sa oblasťou kybernetiky** zabrániť dosiahnutiu ambícií EÚ. Súčasťou riešenia tohto problému je hľadanie spôsobov, ako prilákať talenty a ako si ich udržať.

Budovanie kybernetickej odolnosti

VIII Nedostatky v riadení kybernetickej bezpečnosti sú časté vo verejnom a súkromnom sektore, a to v celej EÚ aj na medzinárodnej úrovni. Ich hojnosť poškodzuje schopnosť svetového spoločenstva reagovať na kybernetické útoky a zabraňovať im a oslabuje jednotný prístup na úrovni EÚ. Problémom je teda **posilnenie riadenia kybernetickej bezpečnosti**.

IX Vzhľadom na čoraz väčší nedostatok zručností v oblasti kybernetickej bezpečnosti je nevyhnutné **zvyšovanie úrovne zručností a informovanosti** vo všetkých sektoroch a na všetkých úrovniach spoločnosti. V celej EÚ sú v súčasnosti slabé normy týkajúce sa odbornej prípravy, certifikácie alebo posudzovania kybernetických rizík.

X Na posilnenie celkovej kybernetickej odolnosti je nevyhnutné prostredie dôvery. Sama Komisia hodnotením dospela k záveru, že všeobecná koordinácia je stále nedostatočná. Problémom zostáva **zlepšenie výmeny informácií a koordinácie** medzi verejným a súkromným sektorom.

Účinné reagovanie na kybernetické incidenty

XI Digitálne systémy sa stávajú natoľko komplexnými, že je nemožné zabrániť všetkým útokom. Reakciou na tento problém je **rýchle odhalenie a reakcia**. Kybernetická bezpečnosť však ešte stále nie je celkom začlenená do existujúcich mechanizmov koordinácie reakcie na krízu na úrovni EÚ, čo by mohlo znižovať schopnosť EÚ reagovať v prípade rozsiahlych, cezhraničných kybernetických incidentov.

XII Kľúčom je **ochrana kritickej infraštruktúry a spoločenských funkcií**. Závažným problémom je potenciálne zasahovanie do volebných procesov a dezinformačné kampane.

XIII Aktuálne problémy, ktoré predstavujú kybernetické hrozby, ktorým čelí EÚ, a širšie globálne prostredie si vyžadujú nepretržité odhodlanie a neprestajné, vytrvalé dodržiavanie základných hodnôt EÚ.

Úvod

01 Technológie otvárajú celý nový svet možností. Nové produkty a služby sa zároveň so svojím zavádzaním stávajú neoddeliteľnou súčasťou našich každodenných životov. S každým novým vývojom sa však zvyšuje naša technologická závislosť a s ňou rastie aj význam kybernetickej bezpečnosti. Čím viac osobných údajov zverejníme online a čím viac sme prepojení, o to je pravdepodobnejšie, že sa staneme obeťou niektorej formy počítačovej kriminality alebo kybernetického útoku.

Čo je kybernetická bezpečnosť?

02 Neexistuje nijaké štandardné, všeobecne uznávané vymedzenie pojmu kybernetická bezpečnosť[1]. Vo všeobecnosti ide o všetky bezpečnostné záruky a opatrenia prijaté na ochranu informačných systémov a ich používateľov proti neoprávnenému prístupu, útoku a poškodeniu, ktorých cieľom je zabezpečenie dôvernosti, integrity a prístupnosti údajov.

03 Kybernetická bezpečnosť zahŕňa kybernetickú prevenciu, odhaľovanie kybernetických útokov, reagovanie na ne a zaistenie nápravy. Incidenty môžu byť úmyselné alebo neúmyselné a ich rozsah je napríklad od náhodného zverejnenia informácií po útoky na podniky a kritickú infraštruktúru, po krádež osobných údajov, ba dokonca po zasahovanie do demokratických procesov a môžu mať rozsiahle škodlivé účinky na jednotlivcov, organizácie a spoločenstvá.

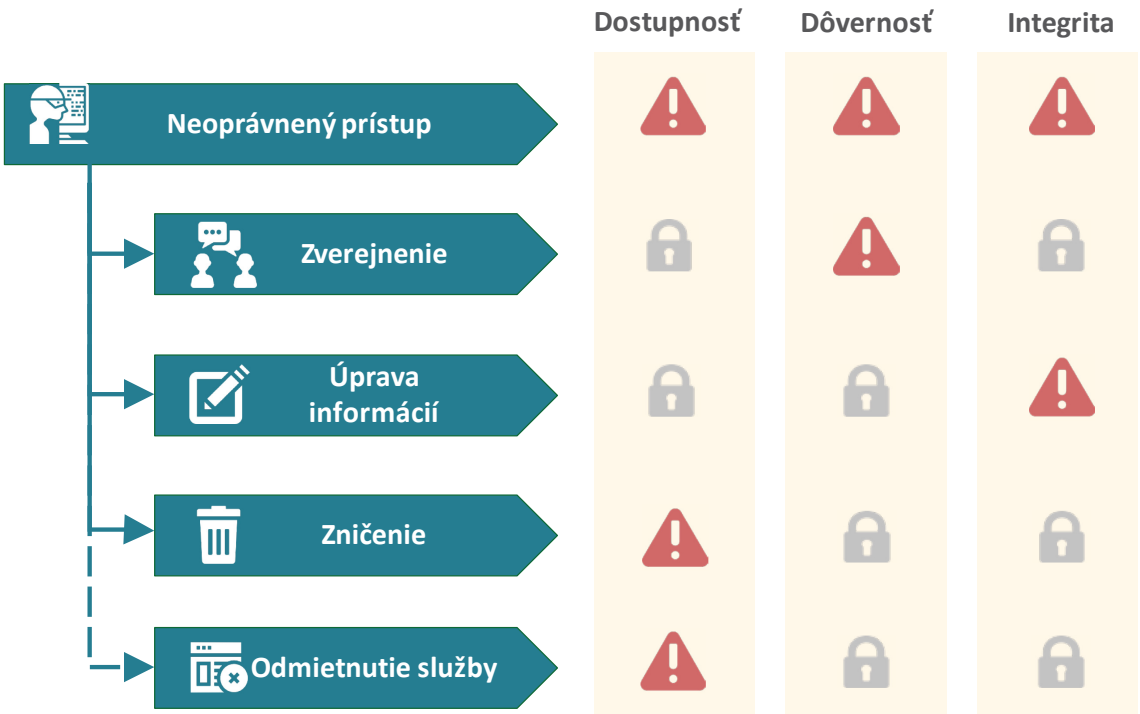
04 Kybernetická bezpečnosť sa ako pojem používaný v politických kruhoch EÚ netýka iba sieťovej a informačnej bezpečnosti. Vzťahuje sa aj na všetky nezákonné činnosti, pri ktorých sa využívajú digitálne technológie v kybernetickom priestore. Tento pojem preto môže zahŕňať počítačovú kriminalitu, ako sú útoky prostredníctvom počítačových vírusov a podvody s bezhotovostnými platobnými prostriedkami, a môže preklenúť priepasť medzi systémami a obsahom, ako pri rozširovaní detskej pornografie na internete. Týka sa aj dezinformačných kampaní, ktorých cieľom je ovplyvňovanie internetových diskusií, a údajných zasahovaní do volebného procesu. Europol okrem toho vidí blízkosť medzi počítačovou kriminalitou a terorizmom[2].

05 Kybernetické incidenty podnecujú rozličné subjekty (vrátane štátov, zločineckých skupín a tzv. hacktivistov) s rozdielnymi pohnútkami. Dôsledky týchto incidentov sa prejavujú na vnútroštátnej, európskej či dokonca celosvetovej úrovni. Nehmotná

a zväčša bezhraničná povaha internetu a používaných nástrojov a taktiky však často sťažujú identifikáciu páchateľa útoku (takzvaný atribučný problém).

06 Mnoho druhov kybernetických hrozieb možno rozdeliť podľa toho, ako nakladajú s údajmi (zverejnenie, úprava, zničenie alebo zamietnutie prístupu), alebo podľa toho, ktoré základné zásady informačnej bezpečnosti porušujú, ako je znázornené ďalej na ***ilustrácii 1***. Niekoľko príkladov útokov sa uvádza v ***rámčeku 1***. Zatiaľ čo sa zvyšuje dômyselnosť útokov na informačné systémy, naše obranné mechanizmy strácajú svoju účinnosť[3].

Ilustrácia 1 – Druhy hrozieb a nimi ohrozené zásady bezpečnosti



Zdroj: Európsky dvor audítorov, úprava podľa štúdie Európskeho parlamentu[4]. Zámka = bezpečnosť nedotknutá, výkričník = bezpečnosť ohrozená.

Rámček 1

Druhy kybernetických útokov

Zakaždým, keď sa nové zariadenie pripojí na internet alebo sa prepojí s inými zariadeniami, zvyšuje sa tým možnosť útokov proti kybernetickej bezpečnosti. Exponenciálny rast internetu vecí, cloudu, veľkých dát (big data) a digitalizácie priemyslu sprevádza zvyšovanie miery vystavenia slabinám systému, ktoré zločinným subjektom umožňujú cieliť na čoraz viac obetí. Rozmanitosť druhov útokov a ich čoraz väčšia dômyselnosť prakticky znemožňujú držať krok s ich vývojom[5].

Malvér (škodlivý softvér) je navrhnutý tak, aby poškodzoval zariadenia alebo siete. Táto kategória zahŕňa vírusy, trójske kone, ransomvér, počítačové červy, advér a spyvér. **Ransomvér** je softvér, ktorý šifruje údaje, čím bráni používateľom v prístupe k ich súborom, kým nezaplatia výkupné, zvyčajne v kryptomene, alebo kým vykonajú istú činnosť. Podľa Europolu prevládajú útoky typu ransomvéru a v niekoľkých posledných rokoch došlo k prudkému nárastu počtu druhov ransomvéru. Pribúdajú útoky **distribuovaného odmietnutia služby** (ďalej len „útoky DDoS“), pri ktorých sa znemožní prístup k službám alebo zdrojom prostredníctvom zaplavenia týchto služieb alebo zdrojov vyšším počtom požiadaviek, než sú schopné zvládnuť, pričom v roku 2017 tento druh útokov postihol jednu tretinu organizácií[6].

Používateľov je možné zmanipulovať tak, aby nevedomky vykonali istú akciu alebo zverejnili dôverné informácie. Tento úskok sa môže použiť pri krádeži údajov alebo kybernetickej špionáži a je známy ako **sociálne inžinierstvo**. Existujú rozličné spôsoby, ako to dosiahnuť, bežnou metódou však je tzv. **phishing**, pri ktorom sa prostredníctvom e-mailových správ, ktoré vyzerajú, akoby pochádzali z dôveryhodných zdrojov, oklamú používatelia, aby prezradili isté informácie alebo klikli na hypertextové odkazy, ktoré nakazia ich zariadenie stiahnutým malvérom. Vyše polovice členských štátov nahlásilo vyšetrovania týkajúce sa útokov na siete[7].

Asi najpodlejším druhom hrozieb sú **pokročilé pretrvávajúce hrozby**. Ide o rafinovaných útočníkov, ktorí dlhodobo sledujú a kradnú údaje, pričom niekedy prechovávajú aj deštruktívne ciele. Cieľom týchto útokov je držať sa čo najdlhšie mimo dosahu radaru bez odhalenia. Pokročilé pretrvávajúce hrozby často bývajú spojené so štátom a bývajú zamerané najmä na citlivé sektory, ako sú technológie, obrana a kritická infraštruktúra. Kybernetická špionáž údajne predstavuje najmenej jednu štvrtinu všetkých kybernetických incidentov a väčšinu nákladov[8].

Aká je závažnosť tohto problému?

07 Opis účinkov slabej prípravy na kybernetický útok je ťažký z dôvodu nedostatku spoľahlivých údajov. Hospodársky vplyv počítačovej kriminality sa medzi rokmi 2013 až 2017 päťnásobne zvýšil[9], pričom táto kriminalita postihla vlády a veľké aj malé

spoločnosti. Tento trend sa odzrkadľuje v odhadovanom raste poistného pre prípad kybernetických útokov z 3 mld. EUR v roku 2018 na 8,9 mld. EUR v roku 2020.

08 Hoci sa finančný vplyv kybernetických útokov naďalej zvyšuje, náklady na spustenie útoku a náklady na predchádzanie, vyšetrovanie a nápravu útoku sú znepokojivo rozdielne. Napríklad náklady na uskutočnenie útoku DDoS môžu byť iba 15 EUR mesačne, ale straty spôsobené podniku, ktorý je terčom útoku, vrátane poškodenia jeho dobrého mena, sú oveľa vyššie[10].

09 Hoci 80 % podnikov v EÚ v roku 2016 zaznamenalo aspoň jeden kybernetický bezpečnostný incident[11], miera uznania rizík je stále znepokojivo nízka. Znalosti o svojom vystavení kybernetickým hrozbám nemá 69 % spoločností v EÚ, alebo má o ňom iba základné znalosti[12], a 60 % nikdy neuskutočnilo odhad možných finančných strát[13]. Navyše podľa globálneho prieskumu by každá tretia organizácia radšej hackerom vyplatila výkupné, než by investovala do informačnej bezpečnosti[14].

10 Celosvetové útoky prostredníctvom ransomvéru *WannaCry* a malvéru na vymazanie údajov *NotPetya* v roku 2017 spoločne postihli viac ako 320 000 obetí približne v 150 krajinách[15]. Tieto incidenty viedli k určitému celosvetovému uvedomeniu si hrozby, ktorú predstavujú kybernetické útoky, a k novému impulzu začleniť kybernetickú bezpečnosť do hlavného prúdu politického myslenia. Okrem toho 86 % občanov EÚ je v súčasnosti presvedčených o zvýšení rizika, že sa stanú obeťou počítačovej kriminality[16].

Opatrenia EÚ v oblasti kybernetickej bezpečnosti

11 Európska únia sa v roku 2001 stala pozorovateľskou organizáciou Výboru pre Dohovor Rady Európy o počítačovej kriminalite[17] (Budapeštiansky dohovor). Odvtedy EÚ používa politiky, právne predpisy a výdavky na zlepšenie svojej kybernetickej odolnosti. Na pozadí čoraz vyššieho počtu významných kybernetických útokov a incidentov sa od roku 2013 vystupňovali aktivity, ako je znázornené na ***ilustrácii 2***. Členské štáty zároveň prijali (a v niektorých prípadoch aj aktualizovali) svoje prvé národné stratégie kybernetickej bezpečnosti.

12 Hlavné subjekty EÚ zodpovedajúce za kybernetickú bezpečnosť sa uvádzajú v ***rámčeku 2*** a ***prílohe I***.

Rámček 2

Kto je zapojený?

Cieľom **Európskej komisie** je zvýšiť spôsobilosti a spoluprácu v oblasti kybernetickej bezpečnosti, posilniť EÚ v úlohe aktéra v tejto oblasti a začleniť kybernetickú bezpečnosť do ostatných politík EÚ. Hlavnými generálnymi riaditeľstvami (GR) zodpovednými za politiku kybernetickej bezpečnosti sú GR **pre komunikačné siete, obsah a technológie (CNECT)** (kybernetická bezpečnosť) a GR **pre migráciu a vnútorné záležitosti (HOME)** (počítačová kriminalita), ktoré zodpovedajú za digitálny jednotný trh (CNECT) a za bezpečnostnú úniu (HOME). Generálne riaditeľstvo **pre informatiku (DIGIT)** je zodpovedné za bezpečnosť informačných technológií vlastných systémov Komisie.

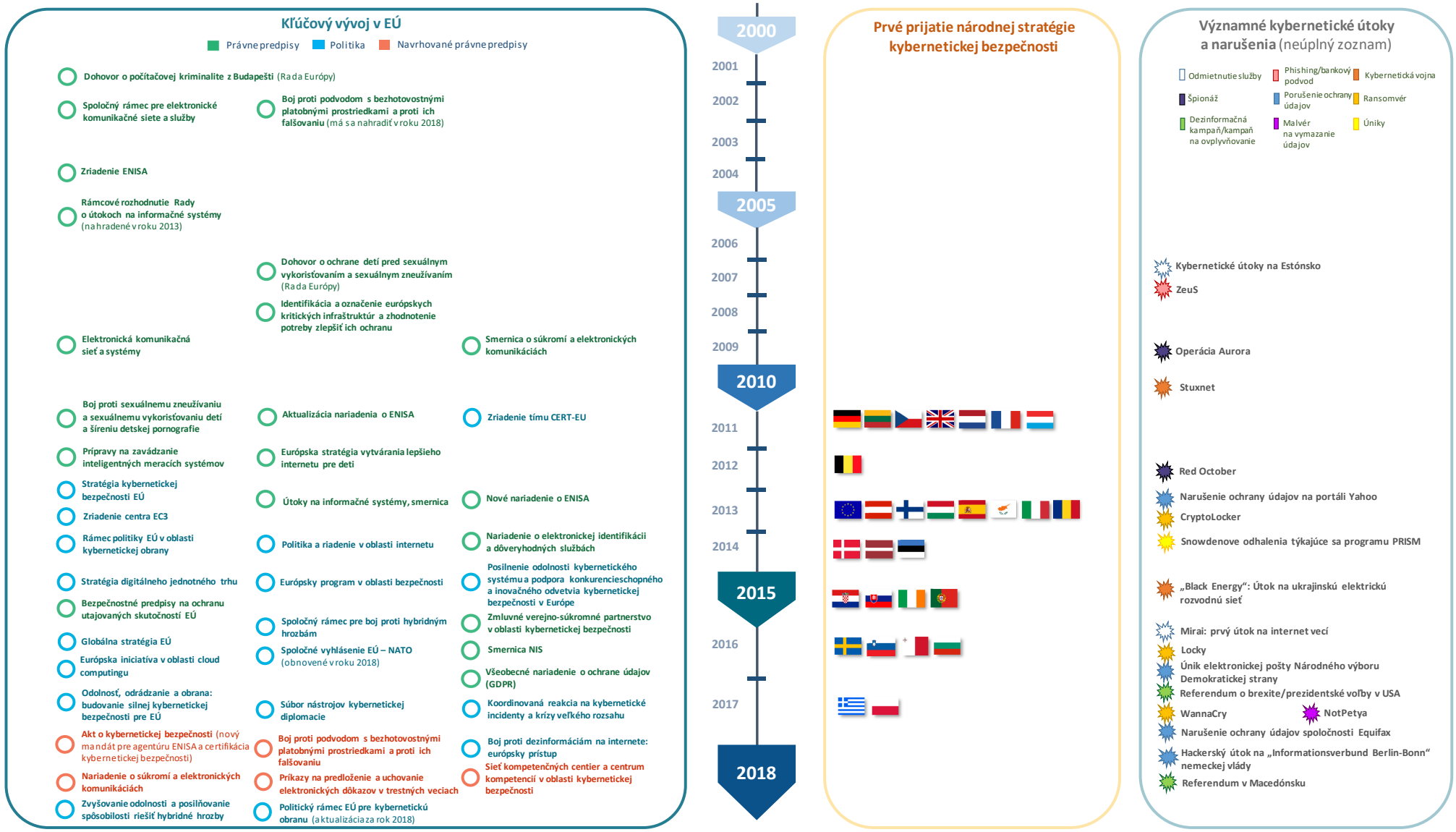
Podporu Komisii poskytuje množstvo agentúr EÚ, najmä agentúra **ENISA** (Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť), Agentúra Európskej únie pre kybernetickú bezpečnosť – hlavný poradný orgán, ktorý pomáha s tvorbou politík, budovaním kapacít a zvyšovaním informovanosti. Európske centrum boja proti počítačovej kriminalite (**EC3**) v rámci Europolu bolo zriadené s cieľom posilniť reakciu orgánov presadzovania práva EÚ na počítačovú kriminalitu. Tím reakcie na núdzové počítačové situácie (**CERT-EU**) podporujúci všetky inštitúcie, orgány a agentúry Únie zabezpečuje Komisia.

Európska služba pre vonkajšiu činnosť (ESVČ) má vedúcu úlohu v oblasti kybernetickej obrany, kybernetickej diplomacie a strategickej komunikácie a zabezpečuje spravodajské a analytické centrá. Cieľom **Európskej obrannej agentúry** (EDA) je rozvoj spôsobilostí v oblasti kybernetickej obrany.

Členské štáty v prvom rade zodpovedajú za svoju vlastnú kybernetickú bezpečnosť a na úrovni EÚ konajú prostredníctvom **Rady**, ktorá má množstvo orgánov na koordináciu a výmenu informácií (patrí medzi ne horizontálna pracovná skupina pre kybernetické otázky). **Európsky parlament** pôsobí ako spoluzákonodarca.

Organizácie súkromného sektora vrátane odvetvia, orgánov na správu internetu a akademickej obce sú partnermi a prispievateľmi k rozvoju a vykonávaniu politiky, a to aj prostredníctvom zmluvných verejno-súkromných partnerstiev (**cPPP**).

Ilustrácia 2 – Zrýchlenie v oblasti tvorby politík a právnych predpisov (do 31. decembra 2018)



Zdroj: Európsky dvor audítorov.

Politika

13 Ekosystém kybernetickej bezpečnosti v EÚ je komplexný a mnohovrstevný, dotýka sa množstva oblastí vnútornej politiky, ako sú politiky v oblasti spravodlivosti a vnútorných vecí, digitálneho jednotného trhu a výskumu. V prípade vonkajšej politiky zohráva kybernetická bezpečnosť úlohu v diplomacii a čoraz viac sa stáva súčasťou vznikajúcej obrannej politiky EÚ.

14 Základným kameňom politiky EÚ je **stratégia kybernetickej bezpečnosti z roku 2013**[18], ktorej cieľom je dosiahnuť, aby digitálne prostredie EÚ bolo najbezpečnejším prostredím na svete, a zároveň ochraňovať základné hodnoty a slobody. Stratégia má päť hlavných cieľov: i) zvýšenie kybernetickej odolnosti; ii) zníženie počítačovej kriminality; iii) rozvoj politiky a spôsobilostí kybernetickej obrany; iv) rozvoj priemyselných a technologických zdrojov pre kybernetickú bezpečnosť a v) vytvorenie medzinárodnej politiky kybernetického priestoru v súlade s kľúčovými hodnotami EÚ.

15 Stratégia kybernetickej bezpečnosti je vzájomne prepojená s tromi neskôr prijatými stratégiami:

— Cieľom **Európskeho programu v oblasti bezpečnosti** (2015) je zlepšiť presadzovanie práva a reakciu justičného systému na počítačovú kriminalitu, a to najmä prostredníctvom obnovenia aktualizácií existujúcich politík a právnych predpisov[19]. Program má takisto určiť prekážky pre vyšetrovanie počítačovej kriminality a posilniť budovanie kapacít v oblasti kybernetickej bezpečnosti.

— Cieľom **stratégie digitálneho jednotného trhu**[20] (2015) je poskytovanie lepšieho prístupu k digitálnemu tovaru a službám vytvorením správnych podmienok, v ktorých sa má maximalizovať rastový potenciál digitálneho hospodárstva. Na tento účel je nevyhnutné posilniť online bezpečnosť, dôveru a inklúziu.

— **Globálna stratégia**[21] z roku 2016 je zameraná na posilnenie úlohy EÚ vo svete. Kybernetická bezpečnosť tvorí základný pilier prostredníctvom obnoveného záväzku voči otázkam kybernetickej bezpečnosti, spolupráce s kľúčovými partnermi a odhodlania riešiť otázky kybernetickej bezpečnosti vo všetkých oblastiach politiky vrátane vyvracania dezinformácií prostredníctvom strategickej komunikácie.

16 V posledných rokoch sa kybernetický priestor s postupnou militarizáciou[22] a prispôsobovaním na použitie vo vojne[23] začal chápať ako piata oblasť vedenia vojny[24]. Kybernetická obrana chráni systémy kybernetického priestoru, siete a kritickú

infraštruktúru pred útokmi vojenskými a inými prostriedkami. **Politický rámec pre kybernetickú obranu** bol prijatý v roku 2014 a v roku 2018 bol aktualizovaný[25]. V rámci aktualizácie z roku 2018 sa určilo šesť priorít vrátane budovania spôsobilostí v oblasti kybernetickej obrany, ako aj ochrany komunikačných a informačných sietí spoločnej bezpečnostnej a obrannej politiky EÚ. Kybernetická obrana je takisto súčasťou rámca stálej štruktúrovanej spolupráce (PESCO) a spolupráce medzi EÚ a NATO.

17 **Spoločný rámec EÚ pre boj proti hybridným hrozbám** (2016) sa zaoberá riešením kybernetických hrozieb pre kritickú infraštruktúru aj pre súkromných používateľov, pričom sa v ňom zdôrazňuje, že kybernetické útoky sa môžu uskutočniť prostredníctvom dezinformačných kampaní v sociálnych médiách[26]. Takisto sa v ňom poukazuje na to, že treba zvýšiť informovanosť a posilniť spoluprácu medzi EÚ a NATO, čo sa potvrdilo v spoločných vyhláseniach EÚ – NATO z rokov 2016 a 2018[27].

18 V roku 2017 Komisia predstavila nový balík opatrení v oblasti kybernetickej bezpečnosti, v ktorom sa odzrkadľuje čoraz väčšia naliehavosť digitálnej ochrany. Súčasťou balíka je nové oznámenie Komisie, ktorým sa aktualizuje stratégia kybernetickej bezpečnosti z roku 2013[28], koncepcia rýchlej a koordinovanej reakcie na veľký útok a pohotové vykonanie smernice o kybernetickej bezpečnosti (smernica NIS)[29]. Balík okrem toho obsahoval niekoľko legislatívnych návrhov (pozri bod ***22***).

Právne predpisy

19 Od roku 2002 sa prijímajú právne predpisy, ktoré sa v rôznej miere týkali kybernetickej bezpečnosti.

20 Hlavným pilierom stratégie kybernetickej bezpečnosti z roku 2013 a ústredným právnym predpisom je **smernica o kybernetickej bezpečnosti (smernica NIS)**[30] z roku 2016, ktorá je prvým celoeurópskym právnym predpisom o kybernetickej bezpečnosti. Cieľom smernice, ktorá mala byť transponovaná do mája 2018, je dosiahnutie minimálnej úrovne harmonizovaných kapacít tým, že členským štátom ukladá povinnosť prijať národné stratégie pre sieťovú a informačnú bezpečnosť a zriadiť jednotné kontaktné miesta a jednotky pre riešenie počítačových bezpečnostných incidentov (jednotky CSIRT)[31]. Stanovujú sa v nej aj bezpečnostné a oznamovacie požiadavky pre prevádzkovateľov základných služieb v kľúčových odvetviach a pre poskytovateľov digitálnych služieb.

21 Súbežne s touto smernicou v roku 2016 nadobudlo účinnosť **všeobecné nariadenie o ochrane údajov**[32] (GDPR), ktoré sa uplatňuje od mája 2018. Jeho cieľom je ochrana osobných údajov občanov Európskej únie tým, že stanovuje pravidlá týkajúce sa ich spracovania a šírenia. Nariadenie dotknutým osobám priznáva isté práva a ukladá povinnosti prevádzkovateľom údajov (poskytovateľom digitálnych služieb), pokiaľ ide o používanie a prenos informácií. Takisto sa ním ukladá oznamovacia povinnosť v prípade narušenia a v určitých prípadoch možnosť vyberať pokuty. Na ***ilustrácii 3*** je znázornené, ako sa smernica NIS a všeobecné nariadenie o ochrane údajov navzájom dopĺňajú z hľadiska svojich cieľov posilnenia kybernetickej bezpečnosti a zabezpečenia ochrany osobných údajov.

22 V súčasnosti sa prerokúvajú návrhy právnych predpisov, medzi ktoré patrí návrh aktu o kybernetickej bezpečnosti na posilnenie agentúry ENISA a vytvorenie celoeurópskeho certifikačného mechanizmu[33], návrh nariadenia o príkaze na predloženie a uchovanie elektronických dôkazov[34] a návrh smernice o elektronických dôkazoch[35]. Návrh na zriadenie Európskeho centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a siete národných koordinačných centier (ďalej len „sieť kompetenčných centier kybernetickej bezpečnosti“ a “centrum výskumných kompetencií“) z roku 2018 je súčasťou balíka opatrení v oblasti kybernetickej bezpečnosti z roku 2017[36].

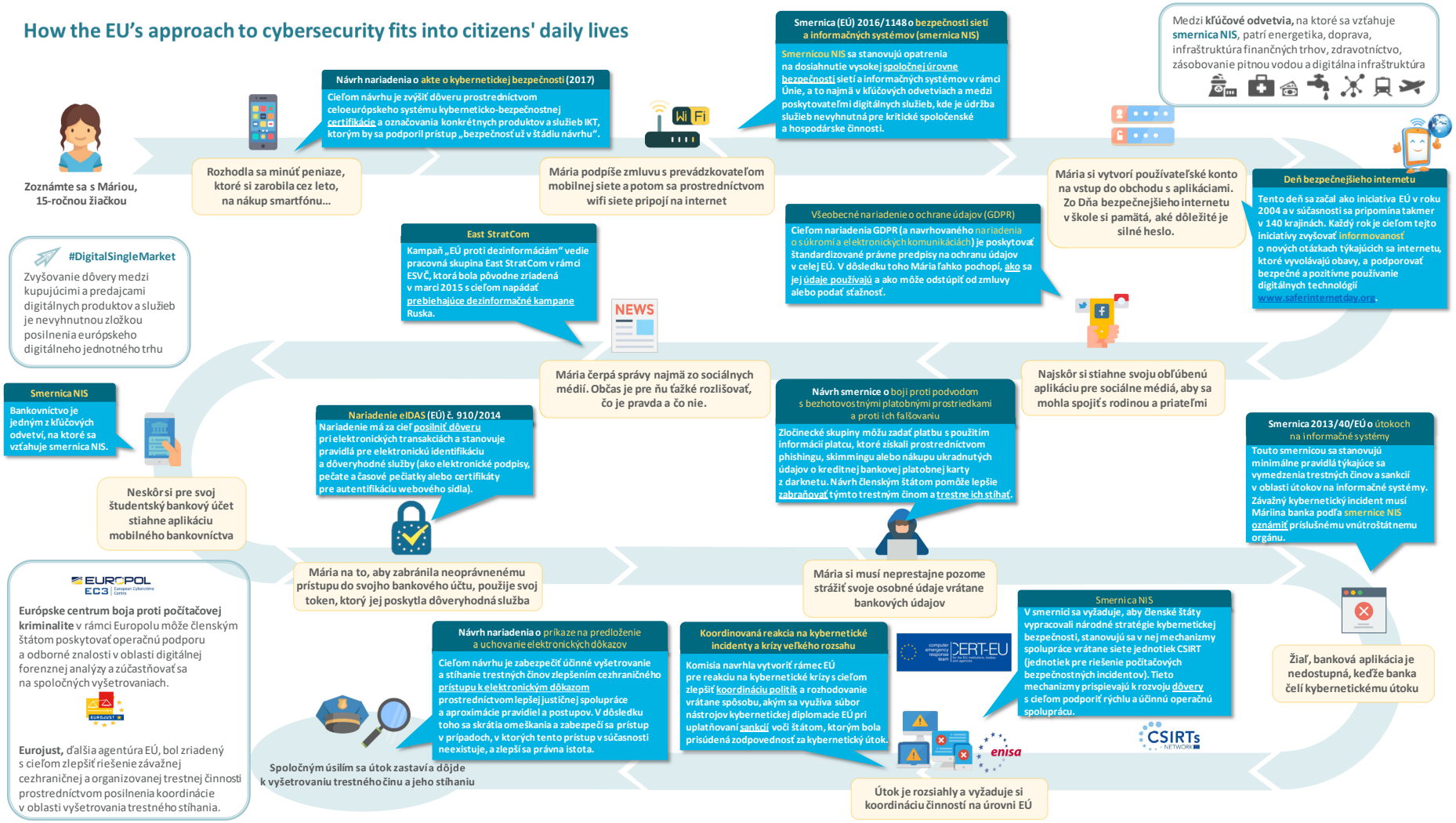
23 Môže byť ťažké porozumieť rozsahu politického a legislatívneho rámca, ktorý sa týka kybernetickej bezpečnosti, a spôsobu, akým ovplyvňuje naše každodenné životy.

24 ***Ilustrácia 4*** predstavuje pokus zmapovať prieniky jednotlivých legislatívnych aktov a ostatných činností v živote fiktívneho občana Európskej únie.

Ilustrácia 3 – Ako sa navzájom dopĺňajú všeobecné nariadenie o ochrane údajov a smernica NIS

Zdroj: Európsky dvor audítorov.

Ilustrácia 4 – Ako sa prístup EÚ ku kybernetickej bezpečnosti prejavuje v každodennom živote občanov



Zdroj: Európsky dvor audítorov.

Vybudovanie politického a legislatívneho rámca

25 Ekosystém kybernetickej bezpečnosti v EÚ je komplexný a mnohovrstevný a týka sa veľkého množstva zainteresovaných strán (pozri ***prílohu I***). Spojiť všetky jeho nesúrodé časti je značne náročné. Od roku 2013 sa vyvíja sústredené úsilie o to, aby sa do oblasti kybernetickej bezpečnosti v EÚ vniesla súdržnosť[37].

Problém 1: zmysluplné hodnotenie a zodpovednosť

26 Preukázanie kauzálneho vzťahu medzi stratégiou z roku 2013 a akýmikoľvek pozorovanými zmenami je náročné, ako konštatovala Komisia. Ciele stratégie z roku 2013 boli formulované veľmi všeobecne, takže „vyjadrovali skôr víziu než merateľný cieľ“[38]. Vytvorenie opatrenia, ktoré by bolo v súlade s týmito širokými cieľmi, je bez merateľných cieľov problematické. Aktualizovaný politický rámec pre kybernetickú obranu (2018) bude zameraný na vytvorenie cieľov, ktorými sa stanoví minimálna úroveň kybernetickej bezpečnosti a dôvery, ktorá sa má dosiahnuť. Tieto ciele sa však budú týkať iba kybernetickej obrany. Ciele vymedzujúce požadovanú úroveň odolnosti pre EÚ ako celok ešte neboli stanovené.

27 Účinky sa zriedkakedy merajú a vyhodnotených bolo iba málo oblastí politiky[39]. Je to čiastočne spôsobené nedávnym vykonaním množstva opatrení, legislatívnych alebo iných, čo zabránilo plnému vyhodnoteniu ich vplyvu. Problémom je stanoviť zmysluplné kritériá posudzovania, ktoré môžu pomôcť pri meraní vplyvu. Okrem toho dôkladné hodnotenie sa v oblasti kybernetickej bezpečnosti vo všeobecnosti zatiaľ nestalo normou. Je preto potrebný prechod ku kultúre výkonnosti, ktorej súčasťou sú hodnotiace postupy a štandardizované vykazovanie. Súčasný mandát agentúry ENISA sa nedotýka hodnotenia a monitorovania stavu kybernetickej bezpečnosti EÚ a pripravenosti.

28 Tvorba politík založená na dôkazoch závisí od dostupnosti dostatočného množstva spoľahlivých údajov a štatistiky na pomoc pri monitorovaní a analýze trendov a potrieb. Bez povinného a spoločného monitorovacieho systém sú spoľahlivé údaje vzácne. Ukazovatele často nie sú ľahko k dispozícii a je ťažké ich stanoviť[40]. V určitých oblastiach, ako je cyklus politík EÚ, však boli vypracované osobitné ukazovatele, ktoré sa používajú na boj proti závažnej a organizovanej trestnej činnosti.

29 Niekoľko členských štátov pravidelne zhromažďuje oficiálne údaje o záležitostiach súvisiacich s kybernetickou oblasťou, čo bráni porovnateľnosti. Európska únia doteraz poskytla len málo informácií o potrebe konsolidácie štatistických údajov na európskej úrovni[41]. K dispozícii je takisto veľmi málo nezávislých celoeurópskych analýz kľúčových tém, ako napríklad[42]: hospodárske aspekty kybernetickej bezpečnosti vrátane behaviorálnych aspektov (rozdielne nastavenie stimulov, informačná asymetria); porozumenie vplyvu zlyhaní kybernetickej bezpečnosti a počítačovej kriminality; makroštatistické údaje o trendoch v kybernetickej oblasti a predpokladaných problémoch a najlepšie riešenia na odstránenie hrozieb.

30 Vzhľadom na to, že neexistujú špecifické ciele a spoľahlivé údaje a riadne vymedzené ukazovatele sú vzácne, posúdenie úspechov stratégie bolo doteraz zväčša kvalitatívne. V správach o pokroku sa často opisujú vykonané činnosti alebo dosiahnuté čiastkové ciele, ale bez dôkladného vyhodnotenia výsledkov. Okrem toho zatiaľ neboli stanovené východiská pre posudzovanie odolnosti systémov. Navyše pre nedostatok kodifikovaného vymedzenia pojmu počítačová kriminalita je takmer nemožné nájsť vhodné európske ukazovatele, ktoré by boli užitočné pri monitorovaní a hodnotení.

31 Nezávislý dohľad nad vykonávaním politiky kybernetickej bezpečnosti sa medzi členskými štátmi líši. Spravili sme prieskum vo vnútroštátnych kontrolných úradoch o skúsenostiach s kontrolami v tejto oblasti. Polovica všetkých respondentov[43] audit v tejto oblasti nikdy nevykonala. Pokiaľ ide o tých, ktorí audit uskutočnili, ich kontroly sa zamerali najmä na: správu údajov; ochranu kritickej infraštruktúry; výmenu informácií a koordináciu medzi hlavnými zainteresovanými stranami; pripravenosť na incidenty, ich oznamovanie a reakciu na ne. Menej častým predmetom auditov boli opatrenia na zvyšovanie informovanosti a nedostatočná úroveň digitálnych zručností. Výsledky týchto auditov alebo hodnotení neboli vždy zverejnené z dôvodov národnej bezpečnosti. Zoznam uverejnených audítorských správ vnútroštátnych kontrolných úradov sa nachádza v ***prílohe III***.

32 Respondenti vnímali obmedzenia týkajúce sa zručností v oblasti kybernetickej bezpečnosti (pozri tiež body ***82 až 90***) a ťažkosti pri vyhodnocovaní pokroku v oblasti kybernetickej bezpečnosti ako hlavné prekážky pre audit vládnych opatrení v tejto oblasti.

Problém 2: odstraňovanie medzier v práve EÚ a jeho nerovnomerná transpozícia

33 Rýchlosť, akou vznikajú nové technológie a hrozby, značne predstihuje navrhovanie a vykonávanie právnych predpisov EÚ. Postupy Únie neboli navrhnuté so zreteľom na digitálny vek: zásadnou prioritou je vypracovanie inovatívnych a pružných postupov, ktorými sa zabezpečí, že politický a legislatívny rámec, ktorý plní svoj účel[44], bude lepšie pripravený na budúcnosť a bude ju utvárať[45].

34 Legislatívny rámec pre kybernetickú bezpečnosť napriek úsiliu o väčšiu mieru súdržnosti zostáva neúplný (niekoľko príkladov sa nachádza v ***tabuľke 1***). Rozdrobenosť a medzery bránia dosiahnutiu celkových cieľov politiky a spôsobujú neefektívnosť. Medzery, ktoré zistila Komisia pri posudzovaní stratégie, sa týkali internetu vecí, vyváženia povinností medzi používateľmi a poskytovateľmi digitálnych produktov a určitých aspektov, ktoré boli v smernici NIS vynechané. Navrhovaný akt o kybernetickej bezpečnosti predstavuje snahu o riešenie týchto medzier čiastočne presadzovaním bezpečnosti už v štádiu návrhu prostredníctvom celoeurópskeho systému certifikácie. Niektoré zainteresované strany sa domnievajú, že stále zjavne chýba jasne vymedzená politika kybernetického odvetvia a spoločný prístup ku kybernetickej špionáži[46].

Tabuľka 1 – Medzery v legislatívnom rámci a nerovnomerná transpozícia v ňom (neúplné)

Oblasť politiky	Príklady
Digitálny jednotný trh	o Súčasná smernica o predaji spotrebného tovaru sa nezaoberá kybernetickou bezpečnosťou. Riešenie tejto medzery je cieľom navrhovaných smerníc o digitálnom obsahu[47] a o online predaji[48]. o Členské štáty majú obmedzené a rozmanité právne rámce týkajúce sa povinností náležitej starostlivosti, z čoho vyplýva právna neistota a ťažkosti pri vymáhaní právnych prostriedkov nápravy[49]. o Členské štáty vypracúvajú svoje politiky súvisiace so zverejňovaním informácií o zraniteľnosti softvéru rozličným tempom a chýba im spoločný právny rámec na úrovni EÚ, ktorý by umožnil koordinovaný prístup[50].
Posilnenie sieťovej a informačnej bezpečnosti	o Členské štáty môžu slobodne začleňovať sektory, ktoré boli zo smernice NIS vynechané[51]. Odvetvia poskytovania pohostinských služieb, ktoré nepatria do rozsahu pôsobnosti smernice, sa môžu stať bránou pre iné trestné činy vrátane obchodovania s ľuďmi a drogami a nelegálneho prisťahovalectva[52].
Boj proti počítačovej kriminalite	o Veľa členských štátov nemá vo svojich vnútroštátnych právnych predpisoch vymedzený pojem „elektronické dôkazy“[53] (pozri aj bod 22). o Súčasné rámcové rozhodnutie o podvodoch s bezhotovostnými platobnými prostriedkami sa výslovne nevzťahuje na nehmotné platobné nástroje, ako sú virtuálne meny, elektronické peniaze a mobilné peniaze, ani do jeho rozsahu nepatria činy, ako sú phishing, skimming a držba a zverejnenie informácií o platiteľovi[54]. o Smernica o útokoch na informačné systémy sa nezákonným získavaním údajov zvnútra (napr. kybernetická špionáž) nezaoberá priamo, čo sťažuje presadzovanie práva[55]. o Rozdiely medzi členskými štátmi v tom, ako uplatňujú právny rámec v dôsledku rozsudku Súdneho dvora Európskej únie o uchovávaní údajov[56], bránia orgánom presadzovania práva v činnosti, čo by mohlo viesť k strate stôp pre vyšetrovanie a poškodiť účinné stíhanie online trestnej činnosti[57].

Zdroj: Európsky dvor audítorov.

35 Uplatňovanie určitých prvkov právnych predpisov je pre vnútroštátne orgány aj pre súkromných prevádzkovateľov naďalej dobrovoľné. Napríklad v rámci skupiny pre spoluprácu je dobrovoľné hodnotenie národných stratégií v oblasti bezpečnosti sietí a informačných systémov a účinnosti jednotiek CSIRT. V rámci systémov certifikácie navrhovaných v akte o kybernetickej bezpečnosti bude dobrovoľná aj certifikácia produktov a služieb informačných a komunikačných technológií.

36 V EÚ je kybernetická bezpečnosť výsadou členských štátov. Napriek tomu EÚ zohráva rozhodujúcu úlohu pri tvorbe podmienok na zvyšovanie kapacít jej členských štátov a na to, aby členské štáty pracovali spoločne a aby vytvoril prostredie dôvery. Vzhľadom na značné rozdiely medzi členskými štátmi z hľadiska ich kapacity a účasti[58] však poskytovanie citlivých informácií (týkajúcich sa národnej bezpečnosti) ostane dobrovoľné.

37 Nedôsledná transpozícia práva EÚ v členských štátoch môže viesť k právnemu a operačnému nesúladu a môže zabrániť tomu, aby právne predpisy dosiahli svoj plný potenciál. Napríklad členské štáty majú odlišné výklady spôsobu, ako by sa mala uplatňovať kontrola vývozu položiek s dvojakým použitím[59], a výsledkom je, že niektoré spoločnosti so sídlom v EÚ môžu vyvážať technológie a služby, ktoré sa môžu použiť na kybernetický dohľad a porušovanie ľudských práv prostredníctvom cenzúry alebo odpočúvania. Európsky parlament v tejto veci vyjadril znepokojenie[60].

38 Ochrana súkromia a sloboda prejavu si navyše vyžadujú špecializovanú legislatívnu odpoveď, a to s cieľom dosiahnuť potrebnú rovnováhu medzi ochranou základných hodnôt a plnením naliehavých požiadaviek EÚ na bezpečnosť. Napríklad, ako sa má zabezpečiť šifrovanie medzi koncovými zariadeniami a zároveň nájsť najlepší spôsob, ako podporiť presadzovanie práva? Prípadne, ako by sme mohli splniť ciele všeobecného nariadenia o ochrane údajov a zároveň chápať dôsledky, ktoré z neho vyplývajú pre verejne dostupné informácie o žiadateľoch o registráciu názvu domény a držiteľoch blokov IP adries? A napokon, ako by to mohlo nepriaznivo ovplyvniť vyšetrovania orgánov presadzovania práva[61]?

39 Samotné právne predpisy nie sú zárukou odolnosti. Hoci cieľom smernice NIS je dosiahnuť vysokú úroveň bezpečnosti v celej EÚ, otvorene sa zameriava na dosiahnutie minimálnej, a nie maximálnej harmonizácie[62]. S vývojom kybernetického prostredia sa budú ďalej objavovať nové medzery.

Podnety na zamyslenie – Politický rámec

- **Aké kľúčové kroky sú potrebné na vyvolanie toho, aby tvorcovia politík, ako aj zákonodarcovia prešli k silnejšej kultúre výkonnosti v oblasti kybernetickej bezpečnosti, a na vymedzenie celkovej odolnosti?**
- **Akým spôsobom môže výskum lepšie prispieť k získaniu potrebných údajov a štatistických informácií, ktoré umožnia zmysluplné hodnotenie?**
- **Ako by sa mohli upraviť legislatívne procesy EÚ, aby boli pružnejšie a viac zohľadňovali rýchlosť vývoja v oblasti technológií a hrozieb?**
- **Ako by sa mohli upraviť, rozšíriť a zopakovať postupy vytvorenia nástrojov merania (ukazovatele, ciele) v cykle politík EÚ pre oblasť kybernetickej bezpečnosti ako celku?**
- **Čo sa môžu dozvedieť vnútroštátne kontrolné úrady z prístupov ostatných kontrolných úradov k auditom politík a opatrení v oblasti kybernetickej bezpečnosti?**
- **Ktoré nezrovnalosti pri transpozícií a vykonávaní právneho rámca EÚ oslabujú účinnejšiu reakciu na medzery v kybernetickej bezpečnosti a na počítačovú kriminalitu a ako by členské štáty a inštitúcie EÚ mohli čo najlepšie vyriešiť tieto nezrovnalosti?**
- **Aké účinné sú kontroly vývozu kybernetického tovaru a služieb z EÚ pri predchádzaní porušovaniu ľudských práv za hranicami EÚ?**

Financovanie a výdavky

40 Európska únia sa zamerala na to, aby sa z nej stalo najbezpečnejšie online prostredie na svete. Dosiahnutie tejto ambície si vyžaduje značné úsilie všetkých zainteresovaných strán vrátane zdravého a dobre riadeného finančného základu.

Problém 3: zosúladenie úrovne investícií s cieľmi

Zvyšovanie investícií

41 Celkové výdavky na globálnu kybernetickú bezpečnosť ako percentuálny podiel HDP sa odhadujú približne na 0,1 %. V Spojených štátoch amerických[63] táto hodnota dosahuje približne 0,35 % (a zahŕňa aj súkromný sektor). Výdavky federálnej vlády USA ako percentuálny podiel HDP sú približne 0,1 % alebo 21 mld. USD vyčlenených v rozpočte na rok 2019[64].

42 Naproti tomu boli výdavky v EÚ nízke, roztrieštené a často boli bez podpory koordinovaných vládnych programov. Číselné údaje sa ťažko získavajú, ale verejné výdavky EÚ na kybernetickú bezpečnosť sa odhadom pohybujú v rozpätí od 1 do 2 mld. EUR ročne[65]. Výdavky niektorých členských štátov ako percentuálny podiel HDP sa rovnajú jednej desatine úrovne v USA alebo sú ešte nižšie[66]. Európska únia a členské štáty musia vedieť, koľko prostriedkov spoločne investujú, aby zistili, ktoré nedostatky treba odstrániť.

43 Bez jasných údajov je ťažké vytvoriť ucelený prehľad z dôvodu prierezového charakteru kybernetickej bezpečnosti a preto, lebo výdavky na kybernetickú bezpečnosť a na všeobecné informačné technológie sú často nerozoznateľné[67]. Naším prieskumom sa potvrdilo, že je náročné získať spoľahlivé štatistické údaje o výdavkoch vo verejnom aj v súkromnom sektore. Tri štvrtiny vnútroštátnych kontrolných úradov oznámili, že nemajú nijaký centralizovaný prehľad o verejných výdavkoch na oblasť kybernetickej bezpečnosti, a ani jeden členský štát neuložil verejným subjektom povinnosť osobitne vykazovať výdavky na kybernetickú bezpečnosť v ich finančných plánoch.

44 Osobitným problémom je zvýšenie verejno-súkromných investícií do európskych podnikov zaoberajúcich sa kybernetickou bezpečnosťou. Verejný kapitál je často k dispozícii pre počiatočné fázy, no už zriedkavejšie v štádiách rastu a rozširovania[68]. Existuje veľa finančných iniciatív EÚ, nevyužívajú sa však, a to prevažne z dôvodu

byrokracie[69]. Z celkového hľadiska podniky z EÚ pôsobiace v oblasti kybernetickej bezpečnosti nedosahujú rovnakú výkonnosť v porovnaní s ich medzinárodnými partnermi: je ich menej, priemerná výška finančných prostriedkov, ktoré zhromaždia, je oveľa nižšia[70]. Zabezpečenie účinného zamerania sa na startupy a ich financovania je preto kľúčové na dosiahnutie cieľov digitálnej politiky EÚ.

Zvýšenie účinku

45 Odstránenie nedostatku investícií v kybernetickej oblasti musí priniesť užitočné výsledky. Napríklad napriek sile sektora výskumu a inovácií EÚ sa výsledky dostatočne nechránia patentmi, nevyužívajú komerčne ani nerozširujú v záujme posilnenia odolnosti, konkurencieschopnosti a digitálnej autonómie[71]. Platí to predovšetkým pri porovnaní so svetovými konkurentmi EÚ. Nedostatok riadne využívaných výsledkov vyplýva z množstva faktorov[72] vrátane:

- chýbajúcej konzistentnej nadnárodnej stratégie na rozšírenie prístupu tak, aby vyhovoval širšej digitálnej potrebe EÚ v oblasti konkurencieschopnosti a väčšej autonómie,
- dĺžky cyklu hodnotového reťazca, čo znamená, že nástroje čoskoro zastarajú,
- nedostatočnej udržateľnosti, keďže projekty sa obvykle končia rozpustením projektového tímu a zastavením podpory vrátane aktualizácií a opráv.

46 Návrh Komisie na zriadenie siete kompetenčných centier kybernetickej bezpečnosti a centra výskumných kompetencií je pokusom na prekonanie roztrieštenosti v oblasti výskumu pre kybernetickú bezpečnosť a na podnietenie väčších investícií[73]. Spolu je v EÚ približne 665 centier odborných znalostí.

Problém 4: jasný prehľad rozpočtových výdavkov EÚ

47 Centralizovaný prehľad výdavkov je dôležitý pre transparentnosť a lepšiu koordináciu. Bez neho je pre tvorcov politík ťažké pochopiť, ako sú výdavky v súlade s potrebami, aby mohli splniť prioritné ciele.

48 Neexistuje špecializovaný rozpočet určený na financovanie stratégie kybernetickej bezpečnosti. Prostriedky na výdavky na kybernetickú bezpečnosť na úrovni EÚ namiesto toho pochádzajú zo všeobecného rozpočtu EÚ a zo spolufinancovania členských štátov. Analýzou sa odhalila komplexná štruktúra

najmenej desiatich rôznych nástrojov v rámci všeobecného rozpočtu EÚ, neukázala však jasný prehľad o tom, kam smerujú konkrétne finančné sumy (pozri ***prílohu II***).

49 Vypracovanie jasného prehľadu o výdavkoch v rámci témy, ktorá sa prelína mnohými oblasťami politiky, je preto značne náročné. Výdavkové programy spravujú rôzne časti Komisie, pričom každý má vlastné ciele, pravidlá a harmonogram. Prehľad sa ešte viac komplikuje, keď sa započíta spolufinancovanie členskými štátmi, ako napríklad v rámci Fondu pre vnútornú bezpečnosť – polícia[74].

Identifikovateľné výdavky na kybernetickú bezpečnosť

50 V rokoch 2014 – 2018 Komisia vynaložila minimálne 1,4 mld. EUR na vykonávanie stratégie[75], pričom najväčšia časť tejto sumy sa pridelila na program Horizont 2020[76]. Finančné prostriedky programu Horizont 2020 sa poskytujú najmä prostredníctvom programu Bezpečná spoločnosť a v projektoch Vedúce postavenie v rámci podporných a priemyselných technológií[77]. Zistili sme 279 zmlúv na projekty v oblasti kybernetickej bezpečnosti uzatvorených do septembra 2018 s celkovou hodnotou financovania z EÚ vo výške 786 mil. EUR[78]. Na ***ilustrácii 5*** je znázornený prehľad typov týchto projektov vychádzajúci z tejto analýzy.

Ilustrácia 5 – Zmluvne uzatvorené výskumné projekty v oblasti kybernetickej bezpečnosti v rámci projektu Horizont 2020 (v mil. EUR)

Zdroj: Európsky dvor audítorov.

51 V roku 2016 bolo vytvorené zmluvné verejno-súkromné partnerstvo (cPPP) na povzbudenie európskeho odvetvia kybernetickej bezpečnosti. Cieľom bolo nasmerovať 450 mil. EUR z programu Horizont 2020 do zmluvného verejno-súkromného partnerstva a do roku 2020 prilákať ďalších 1,8 mld. EUR zo súkromného sektora. Za 18 mesiacov do 31. decembra 2017 bolo do zmluvného verejno-súkromného partnerstva prevedených 67,5 mil. EUR z programu Horizont 2020 a súkromný sektor investoval 1 mld. EUR[79].

52 Boj proti počítačovej kriminalite podporuje aj časť Fondu pre vnútornú bezpečnosť týkajúca sa polície (ISF-P). Časť Fondu pre vnútornú bezpečnosť týkajúca sa polície podporuje štúdie, stretnutia expertov a komunikačné aktivity a táto podpora v rokoch 2014 – 2017 dosiahla takmer 62 mil. EUR. Členské štáty navyše môžu prijímať granty na vybavenie, odbornú prípravu, výskum a zber údajov v rámci zdieľaného riadenia. Granty v hodnote 42 mil. EUR prijalo deväťnásť členských štátov.

53 Výška finančných prostriedkov na podporu justičnej spolupráce a na fungovanie zmlúv o vzájomnej právnej pomoci s osobitným zameraním na výmenu elektronických

údajov a finančných informácií dosiahla v rámci programu Spravodlivosť, spravovaného GR pre spravodlivosť a spotrebiteľov (GR JUST), 9 mil. EUR.

54 V smernici NIS sa jasne uvádza, že jednotky CSIRT musia mať primerané zdroje na účinné plnenie svojich úloh[80]. V rokoch 2016 – 2018 bolo ročne k dispozícii 13 mil. EUR z Nástroja na prepájanie Európy, na ktorý sa členské štáty mohli obrátiť so žiadosťou o pomoc pri vykonávaní požiadaviek smernice. Neexistuje nijaká štúdia, v ktorej by sa určili skutočné finančné potreby, aby sieť jednotiek CSIRT a skupina pre spoluprácu mohli byť účinné.

55 Prevádzkové náklady niekoľkých agentúr sú osobitne určené na kybernetickú bezpečnosť alebo činnosti spojené s počítačovou kriminalitou. Z dostupných verejných informácií je však ťažké získať akékoľvek konkrétne čísla.

56 Budapeštiansky dohovor (pozri bod ***11***) tvorí hlavnú oporu vonkajších výdavkov EÚ na kybernetickú bezpečnosť. Európska únia v rokoch 2014 – 2018 vynaložila približne 50 mil. EUR na posilnenie kybernetickej bezpečnosti za svojimi hranicami. Takmer polovica tejto sumy sa financovala z nástroja na podporu stability a mieru s jedným hlavným projektom (projekt GLACY+ v hodnote 13,5 mil. EUR), ktorého cieľom je posilnenie celosvetových kapacít na tvorbu a vykonávanie právnych predpisov v oblasti boja proti počítačovej kriminalite a na zvýšenie medzinárodnej spolupráce[81]. V iných prípadoch bol ťažiskom výdavkov ďalších finančných nástrojov EÚ prevažne región západného Balkánu[82], ako aj krajiny európskeho susedstva, napríklad projekt Cybercrime@EaP s krajinami Východného partnerstva je zameraný na zlepšenie medzinárodnej spolupráce v oblasti počítačovej kriminality a elektronických dôkazov.

Iné výdavky na kybernetickú bezpečnosť

57 Nie vždy je v programoch EÚ možné určiť konkrétne výdavky na kybernetickú bezpečnosť:

- Finančné prostriedky programu Horizont 2020 sa poskytujú aj prostredníctvom spoločného podniku na vykonávanie spoločnej technologickej iniciatívy Elektronické komponenty a systémy pre vedúce postavenie Európy (ECSEL) pre kyberneticko-fyzikálne systémy. Nemohli sme však určiť, ktoré výdavky spomedzi 27 projektov v rokoch 2015 – 2016 v celkovej hodnote 437 mil. EUR konkrétne súviseli s kybernetickou bezpečnosťou.

- V rámci európskych štrukturálnych a investičných fondov je na výdavky na kybernetickú bezpečnosť a dôveryhodné služby k dispozícii až 400 mil. EUR. Táto suma je určená na investície do bezpečnosti a ochrany údajov na posilnenie interoperability a vzájomné prepojenie digitálnej infraštruktúry, elektronickej identifikácie a služieb na ochranu súkromia a dôveryhodných služieb.

58 Vo svojom operačnom pláne na rok 2018 Európska investičná banka oznámila svoj zámer zvýšiť financovanie technológií dvojakého použitia, kybernetickej bezpečnosti a civilnej bezpečnosti až do výšky 6 mld. EUR počas troch rokov[83].

Pohľad do budúcnosti

59 Suma 2 mld. EUR zložky navrhovaného nového programu Digitálna Európa[84] na obdobie 2021 – 2027 týkajúcej sa kybernetickej bezpečnosti je určená na posilnenie odvetvia kybernetickej bezpečnosti a celkovej ochrany spoločnosti, a to aj prostredníctvom pomoci pri vykonávaní smernice NIS. Navrhovaná sieť kompetenčných centier kybernetickej bezpečnosti a centrum výskumných kompetencií, ktorého cieľom je vznik efektívnejšieho prístupu, majú vytvoriť hlavný implementačný mechanizmus pre výdavky EÚ v rámci programu Digitálna Európa.

60 Výdavky na obranu z rozpočtu EÚ sa prednedávnom prostredníctvom Programu rozvoja európskeho obranného priemyslu zvýšili, pričom sa na roky 2019 a 2020 vyčlenia prostriedky vo výške 500 mil. EUR[85]. Tým sa prostriedky zamerajú na zlepšenie koordinácie a efektívnosti výdavkov členských štátov na obranu prostredníctvom stimulov na spoločný vývoj. Jeho cieľom je vytvorenie investícií do obrannej spôsobilosti po roku 2020 vo výške 13 mld. EUR, a to prostredníctvom Európskeho obranného fondu, ktorých časť sa týka kybernetickej obrany[86].

Problém 5: primerané zabezpečenie zdrojov pre agentúry EÚ

61 Tri hlavné orgány, ktoré tvoria jadro politiky EÚ v oblasti kybernetickej bezpečnosti – ENISA, Európske centrum boja proti počítačovej kriminalite (EC3) pri Europole a CERT-EU (pozri ***rámček 2***) – majú v čase zvýšených politických priorít súvisiacich s bezpečnosťou problémy so zabezpečením zdrojov. Aktuálne pridelenie ľudských a finančných zdrojov v agentúrach EÚ ostáva pre ne prekážkou na splnenie očakávaní[87].

62 Žiadosti agentúr o dodatočné prostriedky na splnenie zvyšujúcich sa nárokov neboli plne uspokojené, čo by mohlo ohroziť (včasné) splnenie cieľov politiky. Napríklad:

- Nízky objem prostriedkov zohral svoju úlohu pri tom, že agentúra ENISA nemohla v roku 2017 dosiahnuť svoje ciele v plnej miere[88]. V balíku opatrení z roku 2017 boli na splnenie nového mandátu agentúry ENISA navrhnuté dodatočné prostriedky.

- Ponuka analytikov a investície do kapacít IKT v centre EC3 pri Europole zaostávajú za dopytom[89]. Navyše, v spoločnej pracovnej skupine pre počítačovú kriminalitu (J-CAT), ktorá pôsobí v rámci centra EC3 pri Europole, sú zamestnaní odborníci z členských štátov a tretích krajín, ktorí podporujú vyšetrovania založené na zhromaždených informáciách. Náklady však zväčša nesú vysielajúce štáty, čo ich odrádza od toho, aby vysielali vyšší počet expertov. Navrhnuté bolo dočasné vysielanie pracovníkov v jednotlivých prípadoch s určitou finančnou podporou Europolu alebo cyklu politík EÚ, čím by sa umožnila účasť viacerých krajín.

63 Určité obmedzenia si spôsobujú samotné agentúry. Veľa zamestnancov v CERT-EU a agentúre ENISA sú zmluvní zamestnanci, ktorých postupy prijímania bývajú zvyčajne pomalé. Ďalšie obmedzenia, ktoré sa týkajú napríklad prilákania talentov a ich udržania, vyplývajú z neschopnosti agentúr konkurovať platom v súkromnom sektore alebo sú spôsobené slabými vyhliadkami na kariérny postup. Agentúra ENISA preto veľkú časť svojej práce v rokoch 2014 – 2016 zabezpečovala externe[90].

64 Nedostatok zamestnancov a potrebných nástrojov môže mať za následok závažné riziká, najmä pokiaľ ide o zhromažďovanie spravodajských informácií o hrozbách. Objem údajov z otvorených a neverejných zdrojov sa naďalej zväčšuje a hrozí, že prekoná schopnosti analytikov vykonávať riadnu analýzu hrozieb. Tieto údaje sa bez správnych spôsobilostí a nástrojov na ich úspešné zjednotenie a vzájomné prepojenie účinne nepremenia na použiteľné spravodajské informácie o hrozbách, ktoré si krajiny v EÚ môžu navzájom vymieňať a analyzovať[91].

Podnety na zamyslenie – Financovanie a výdavky

- **Akými spôsobmi môže Komisia a zákonodarcovia zefektívniť výdavky EÚ na kybernetickú bezpečnosť a zreteľnejšie ich zosúladiť s jasne stanovenými cieľmi?**
- **Ako by sa nedostatky pri zabezpečovaní zdrojov pre agentúry EÚ mohli riešiť všeobecným spôsobom s ohľadom na potreby a ciele Únie?**
- **Aké opatrenia boli určené na úrovni EÚ a členských štátov na odstránenie prekážok pre MSP, ktoré prijímajú investičný kapitál na rozšírenie svojich činností?**
- **Aké konkrétne a trvalé výsledky prinášajú finančné prostriedky programu Horizont 2020, aby vznikli riešenia v oblasti kybernetickej bezpečnosti?**
- **Ako budovanie kapacít EÚ posilňuje kapacity za jej hranicami v súlade s hodnotami EÚ?**

Budovanie spoločnosti odolnej proti kybernetickým útokom

65 Riadenie kybernetickej bezpečnosti sa zaoberá riadením hrozieb a rizík, posilnením kapacít a informovanosti a koordináciou a výmenou informácií založených na dôvere.

Problém 6: posilnenie správy a noriem

Správa informačnej bezpečnosti

66 V správe informačnej bezpečnosti ide o zavádzanie štruktúr a politík v záujme zabezpečenia dôverného charakteru údajov, ich integrity a dostupnosti. Nejde len o technický problém, správa si vyžaduje efektívne vedenie, spoľahlivé procesy a stratégie v súlade s organizačnými cieľmi[92]. Ich podmnožinou je riadenie kybernetickej bezpečnosti, ktoré sa zaoberá všetkými druhmi hrozieb súvisiacich s kybernetickou bezpečnosťou vrátane cielených, dômyselných útokov, narušení alebo incidentov, ktoré je ťažké odhaľovať alebo prekonať.

67 Členské štáty majú rôzne modely kybernetickej bezpečnosti a zodpovednosť za kybernetickú bezpečnosť v nich často býva rozdelená medzi množstvo subjektov. Tieto rozdiely by mohli prekážať spolupráci potrebnej na reakciu na rozsiahle, cezhraničné incidenty a na výmenu spravodajských informácií o hrozbách na vnútroštátnej úrovni, nehovoriac už o úrovni EÚ. Z nášho prieskumu vnútroštátnych

kontrolných úradov vyplynulo, že nedostatky v mechanizmoch správy a v riadení rizika orgánov verejnej moci boli vnímané ako najvyššie riziko.

68 Hoci dôsledky pre organizácie súkromného sektora môžu byť závažné, oblasť správy kybernetickej bezpečnosti oplýva nedostatkami. Takmer deväť z desiatich organizácií uvádza, že ich funkcia kybernetickej bezpečnosti nespĺňa celkom ich potreby[93], a pracovníkov pre kybernetickú bezpečnosť od predstavenstva často oddeľujú aspoň dve úrovne[94].

69 V práve EÚ týkajúcom sa obchodných spoločností sa nestanovujú osobitné požiadavky na zverejňovanie kybernetických rizík. Americká Komisia pre burzu a cenné papiere prednedávnom vydala nezáväzné usmernenie, ktoré má verejným spoločnostiam pomôcť pri príprave zverejňovania kybernetických bezpečnostných rizík a incidentov[95]. Spoločný výbor európskych orgánov dohľadu[96] (ESA) varoval pred zvyšovaním kybernetických rizík, povzbudil finančné inštitúcie, aby posilnili svoje krehké systémy IT a preskúmali inherentné riziká pre informačnú bezpečnosť, pripojiteľnosť a externé zabezpečovanie činností[97].

70 Obzvlášť náročné je posilnenie správy informačnej bezpečnosti MSP, keďže často nastáva situácia, keď nie sú schopné zaviesť vhodné systémy. Malým a stredným podnikom chýbajú vhodné usmernenia pre uplatňovanie informačnej bezpečnosti a požiadaviek na ochranu súkromia a zmierňovanie technologických rizík[98]. K hlavným úlohám teda patrí lepšie porozumieť ich potrebám a poskytnúť potrebné stimuly a podporu.

71 Chýbajúci súdržný rámec medzinárodnej správy kybernetickej bezpečnosti oslabuje schopnosť medzinárodného spoločenstva reagovať na kybernetické útoky a obmedzovať ich. Je preto dôležité vytvoriť konsenzus o takom rámci správy, ktorý bude čo najviac odzrkadľovať záujmy a hodnoty EÚ[99]. Pokusy stanoviť záväzné medzinárodné normy pre kybernetický priestor sú čoraz viac náročnejšie, čo sa prejavilo tým, že skupina vládnych expertov OSN v roku 2017 nedosiahla konsenzus o spôsobe, akým by sa medzinárodné právo malo uplatňovať na reakcie štátu na incidenty.

72 V záujme posilnenia svojho programu riadenia kybernetického priestoru EÚ takisto oficiálne schválila šesť partnerstiev v kybernetickej oblasti, aby začala pravidelné dialógy o politike s cieľom posilniť dôveru a vybudovať spoločné oblasti spolupráce[100]. Výsledky sú zmiešané, vo všeobecnosti sa však EÚ na medzinárodnej

úrovni ešte nemôže považovať za „významného aktéra v oblasti kybernetickej bezpečnosti“, hoci si zlepšila svoj profil[101].

Informačná bezpečnosť v inštitúciách EÚ

73 Každá inštitúcia EÚ má svoje vlastné pravidlá správy informačnej bezpečnosti. V medziinštitucionálnej dohode je zaistená pomoc Komisie iným inštitúciám a agentúram v oblasti informačnej bezpečnosti. Inštitúcie a orgány EÚ uznali potrebu jednotne rozvíjať svoje kybernetické kapacity a prístupy riadenia rizika. Komisia, Rada a ESVČ majú v roku 2020 predložiť horizontálnej pracovnej skupine pre kybernetické otázky správu o riadení a pokroku dosiahnutom pri objasňovaní a harmonizovaní riadenia kybernetickej bezpečnosti v inštitúciách a agentúrach EÚ[102].

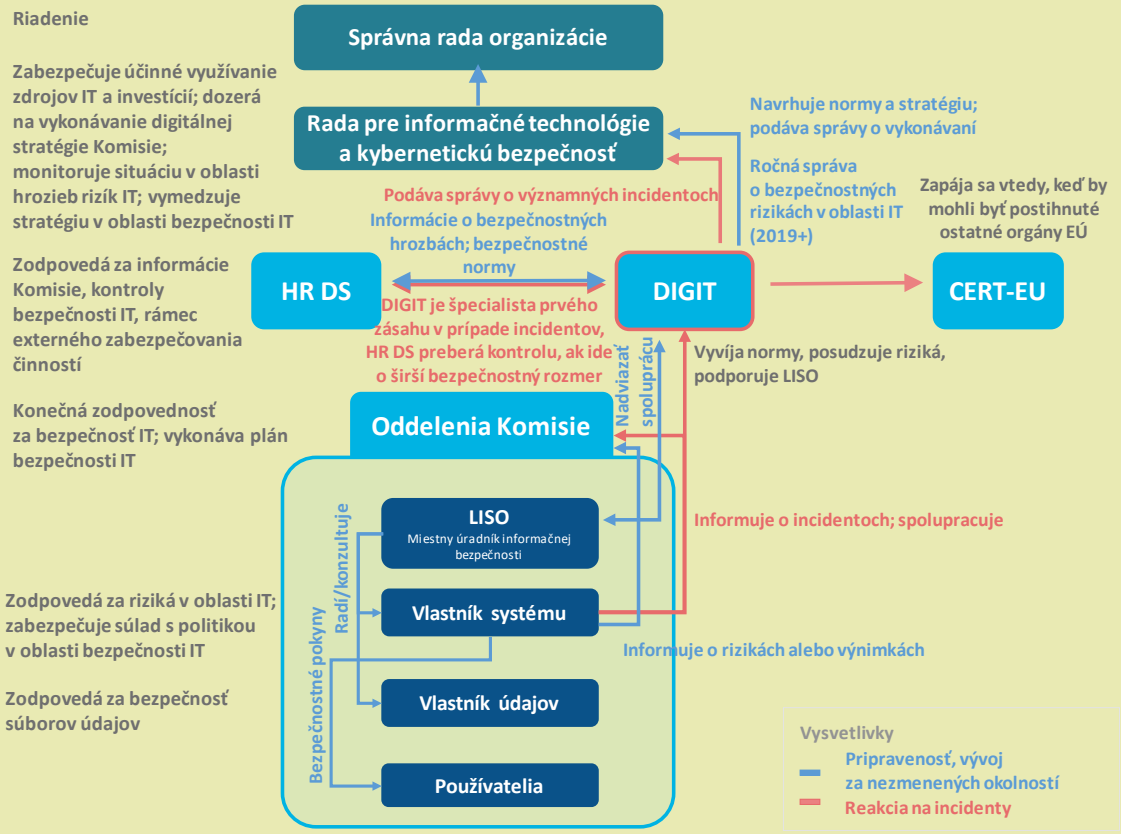
74 V rámci Komisie za bezpečnosť infraštruktúry a služieb IT nesie zodpovednosť Generálne riaditeľstvo pre informatiku (DIGIT) (pozri ***rámček 3***). Hlavnými cieľmi v oblasti bezpečnosti informačných technológií digitálnej stratégie Komisie sú začlenenie bezpečnosti informačných technológií do procesov riadenia, zabezpečenie (nákladovo) efektívnej infraštruktúry a odolnosti, rozšírenie rozsahu odhaľovania incidentov a reakcií na ne a zjednotenie riadenia informačných technológií a bezpečnosti[103]. Komisia podľa svojej zmluvy s poskytovateľmi zabezpečuje, že takmer všetok softvér sa bude aktívne udržiavať a že sa bude používať iba softvér podporovaný predajcom[104].

75 Význam ochrany inštitúcií sa vzťahuje aj na misie a štruktúry spoločnej bezpečnostnej a obrannej politiky (SBOP) EÚ na celom svete. Jednou z priorít politického rámca EÚ pre kybernetickú obranu (aktualizácia za rok 2018) je zlepšiť ochranu komunikačných a informačných systémov SBOP využívaných subjektmi z EÚ. V súčasnosti funguje interný výbor ESVČ pre správu kybernetických záležitostí a prvýkrát sa stretol v júni 2017[105].

Rámček 3

Ochrana informačných systémov Komisie

Približne 1 300 systémov a 50 000 zariadení Komisie je neprestajne cieľom kybernetických útokov. Zodpovednosť za informačné technológie je decentralizovaná, ako je znázornené na ilustrácii ďalej. Informačná bezpečnosť a bezpečnosť informačných technológií sú založené na spoločnom pláne bezpečnosti informačných technológií, ktorý pripravilo GR pre informatiku. Rada pre informačné technológie a kybernetickú bezpečnosť pôsobí ako faktický hlavný úradník Komisie pre informačnú bezpečnosť a spája prevádzkovú časť bezpečnosti informačných technológií s vrcholovým manažmentom Komisie, ktorý zastupuje správna rada organizácie.



Zdroj: Európsky dvor audítorov na základe rozhodnutí Komisie[106].

Hlavnou úlohou GR pre ľudské zdroje a bezpečnosť (GR HR DS) je ochraňovať zamestnancov, informácie a majetok Komisie. Okrem toho vykonávať bezpečnostné vyšetrovania incidentov, ktoré majú širší bezpečnostný rozmer než iba informačné technológie, čím získava informácie pre kontrarozviedkovú činnosť a pre boj proti terorizmu.

Generálne riaditeľstvo pre informatiku zodpovedá za bezpečnosť informačných technológií a zabezpečuje CERT-EU (tím reakcie na núdzové počítačové situácie). Tím CERT-EU, zriadený v roku 2011, funguje s ročným rozpočtom približne 2,5 mil. EUR ročne a má zhruba 30 zamestnancov. Ide o špecialistu prvého zásahu pri akomkoľvek incidente

v oblasti bezpečnosti informačných technológií, ktorý sa zaoberá niekoľkými inštitúciami, zatiaľ však nefunguje nepretržite, a ktorý zabezpečuje platformu na výmenu informácií. V roku 2018 CERT-EU podpísal nezáväzné memorandum o porozumení s agentúrou ENISA, centrom EC3 a Európskou obrannou agentúrou v záujme posilnenia spolupráce a koordinácie. Tím takisto uzatvoril technickú dohodu s tímom pre spôsobilosť reakcie na počítačové incidenty NATO (NCIRC).

Posudzovanie hrozieb a rizika

76 Podložené a neprerušované posudzovania hrozieb a rizík sú dôležitými nástrojmi pre verejné aj súkromné organizácie. Neexistuje však nijaký štandardný prístup ku klasifikácii a k mapovaniu kybernetických hrozieb alebo k posudzovaniu rizík, čo znamená, že obsah posúdení je značne premenlivý, čo zas sťažuje súdržný celoeurópsky prístup ku kybernetickej bezpečnosti[107]. Posúdenia sa navyše často opierajú o tie isté zdroje či dokonca o iné posúdenia hrozieb a výsledkom je ozvena, v ktorej sa opakujú tie isté zistenia[108], a hrozí, že ďalším hrozbám nebude venovaná dostatočná pozornosť. Situáciu zhoršuje neprestajná neochota vymieňať si informácie a nedostatočné nahlasovanie incidentov.

77 Bolo zriadené stredisko EÚ pre hybridné hrozby[109], ktoré je súčasťou ESVČ, a jeho cieľom je zlepšiť situačné povedomie a poskytovať podporu pre rozhodovanie prostredníctvom výmeny analýz, musí však rozšíriť svoje odborné znalosti, a to aj v oblasti kybernetickej bezpečnosti. Tím CERT-EU zároveň inštitúciám, orgánom a agentúram EÚ poskytuje správy a stručné správy týkajúce sa kybernetických hrozieb, ktoré na ne cielia.

78 Agentúra ENISA v minulosti poukázala na to, že veľa členských štátov chápe hrozby kvalitatívne a že je potrebné viac modelovania kybernetických hrozieb[110]. Monitorovacia kapacita pre strategickú analýzu posilní celkové porozumenie. Posúdenia hrozieb by sa však okrem technologických hrozieb mohli týkať aj sociálno-politických a hospodárskych hrozieb, aby sa získal komplexnejší prehľad, ako aj príčin hrozieb a motívov aktérov.

Stimuly

79 Organizácie majú stále príliš málo právnych a hospodárskych stimulov na oznamovanie a výmenu informácií o incidentoch. Veľa organizácií zo strachu z poškodenia dobrého mena ešte stále uprednostňuje diskrétne riešenie kybernetických útokov alebo vyplatenie páchateľov. Treba si počkať, akou účinnou sa ukáže smernica NIS pri zvyšovaní úrovne oznámení. Komisia očakáva, že sa zlepšenia

prejavia predovšetkým na vnútroštátnej úrovni, v dôsledku aktu o kybernetickej bezpečnosti sa však pohľad rozšíri na celú EÚ[111].

80 V dôsledku začlenenia určitých štandardov do svojich postupov verejného obstarávania majú orgány verejnej moci nad dodávateľmi značný vplyv ako nákupcovia digitálnych produktov a služieb prostredníctvom verejného obstarávania a financovania výskumu a programov (napríklad v dôsledku požiadavky na prijatie určitých technických noriem, ako je internetový protokol IPv6, s cieľom pomôcť v boji proti počítačovej kriminalite). V súčasnosti však neexistuje rámec spoločného obstarávania pre infraštruktúru kybernetickej bezpečnosti[112]. V tejto súvislosti môže Komisia spraviť ešte veľa práce. Cieľom programu Digitálna Európa navrhovaného pre ďalší viacročný finančný rámec je riešiť až doteraz obmedzené investície verejného sektora do nákupu najnovších technológií kybernetickej bezpečnosti.

81 Komisia môže prostredníctvom svojej regulačnej kapacity zabezpečiť vypracovanie tých správnych štandardov na široké prijatie v záujme zvýšenia bezpečnosti. Komisia a Europol spolupracujú s orgánmi správy internetu, napríklad s organizáciou ICANN (pozri bod ***38***) a s RIPE-NCC[113], čo je nevyhnutné na zavádzanie správnej architektúry na boj proti počítačovej kriminalite v záujme podpory orgánov presadzovania práva a justičných orgánov.

Problém 7: zvyšovanie úrovne zručností a informovanosti

82 Agentúra ENISA poukázala na to, že používatelia zohrávajú v boji proti kybernetickým útokom rozhodujúcu úlohu a že posilnenie úrovne ich zručností, vzdelania a informovanosti je kľúčom k vybudovaniu spoločnosti odolnej proti kybernetickým útokom[114]. Osoby v pracovnom alebo domácom prostredí, ktoré majú skúsenosti s rozpoznávaním varovných signálov a sú vybavené správnymi zručnosťami, môžu útoky spomaliť alebo im zabrániť.

83 Osobitný význam má čoraz väčšia asymetria medzi odbornými znalosťami potrebnými na páchanie počítačovej kriminality alebo na uskutočnenie kybernetického útoku a zručnosťami potrebnými na obranu proti nim. V dôsledku modelu „zločin ako služba“ sa znížili prekážky pre vstup na trh s počítačovou kriminalitou: jednotlivci bez technických znalostí si teraz môžu prenajať botnety, súpravy exploitov alebo balíky s ransomvérom.

Odborná príprava, zručnosti a budovanie kapacít

84 Svet trápi čoraz väčší nedostatok zručností v oblasti kybernetickej bezpečnosti; rozdiel medzi požadovanou a dostupnou pracovnou silou sa od roku 2015 zväčšil o 20 %[115]. Tradičné spôsoby prijímania zamestnancov neuspokojujú dopyt, a to ani dopyt po zamestnancoch na vedúce a medziodborové pozície[116]. Takmer 90 % zamestnancov v oblasti kybernetickej bezpečnosti na svete sú muži a trvalý nedostatok rodovej rozmanitosti ešte viac obmedzuje zásoby talentov[117]. Navyše na univerzitách nemajú predmety spojené s kybernetickou bezpečnosťou v netechnických študijných programoch dostatočné zastúpenie.

85 Odborná príprava a vzdelávanie sú potrebné celoplošne, medzi zamestnancami verejnej správy, príslušníkmi orgánov presadzovania práva, v justičných orgánoch, ozbrojených silách a medzi pedagógmi. Napríklad súdy musia byť schopné riešiť rýchlo sa meniace technické osobitosti počítačovej kriminality a jej obetí[118]. V súčasnosti neexistujú nijaké celoeurópske normy týkajúce sa odbornej prípravy a certifikácie[119]. V inštitúciách EÚ je dôležité získanie správnej kombinácie zručností. Bez správnej kombinácie zručností by inštitúcie nemuseli byť schopné vhodne vymedziť rozsah, určiť správnych partnerov a potreby v oblasti bezpečnosti alebo by im mohla chýbať kapacita na riadenie programov. Dôsledkom môže byť oslabenie účinnosti tvorby programov a politík EÚ.

86 Hoci členské štáty zodpovedajú za politiky vzdelávania na úrovni EÚ, množstvo činností súvisiacich s odbornou prípravou (pozri ***tabuľku 2***) a cvičenia (pozri ***rámček 4***) sa už uskutočňuje. Európska únia môže pomôcť zapracovať celoeurópske normy do učebných plánov vo všetkých relevantných disciplínach[120]. Napríklad v oblasti digitálnej forenznej analýzy spoločné štandardy odbornej prípravy musia uľahčiť zaisťovanie prípustnosti dôkazov v členských štátoch. Z dôvodu cezhraničnej povahy počítačovej kriminality sa do riešenia môže zapojiť viacero jurisdikcií, čo si vyžaduje odbornú prípravu na úrovni EÚ. A predsa, agentúra CEPOL, agentúra EÚ pre odbornú prípravu v oblasti presadzovania práva, upozornila na to, že dve tretiny členských štátov neposkytujú príslušníkom orgánov presadzovania práva pravidelnú odbornú prípravu v kybernetickej oblasti[121]. Európska únia môže takisto teoreticky určiť spôsoby na vytvorenie synergie medzi civilnou a vojenskou sférou v oblasti vzdelávania a odbornej prípravy[122]. Vzhľadom na to agentúra ENISA zistila, že kým súčasné možnosti odbornej prípravy v kľúčových odvetviach sú rozsiahle, nie sú dostatočne zacielené na odolnosť kritickej infraštruktúry[123].

Tabuľka 2 – Niektoré z iniciatív odbornej prípravy EÚ v oblasti kybernetickej bezpečnosti

Projekty Európskej obrannej agentúry, napr. podpora pri výcviku zo strany súkromného sektora a projekt Cyber Ranges	Sieť Európskej akadémie bezpečnosti a obrany (poskytovanie civilno-vojenskej prípravy) vrátane platformy pre vzdelávanie, odbornú prípravu, výcvik a hodnotenie v kybernetickej oblasti	Odborná príprava agentúry ENISA s ponukou programov školení v prípadoch, keď tieto programy komerčný trh nie je schopný zabezpečiť
Programy odbornej prípravy Europolu, agentúry CEPOL, skupiny ECTEG [124] vrátane modelu riadenia odbornej prípravy a rámca kompetencií v oblasti odbornej prípravy (vrátane certifikácie)	Sieť kompetenčných centier a centrum výskumných kompetencií (navrhované)	Opatrenia týkajúce sa šifrovania navrhnuté v 11. správe o pokroku dosiahnutom pri budovaní bezpečnostnej únie
Spolupráca medzi EÚ a NATO v oblasti odbornej prípravy a vzdelávania súvisiacich s kybernetickou obranou	Program vojenský Erasmus	Európska sieť odbornej justičnej prípravy

Zdroj: Európsky dvor audítorov.

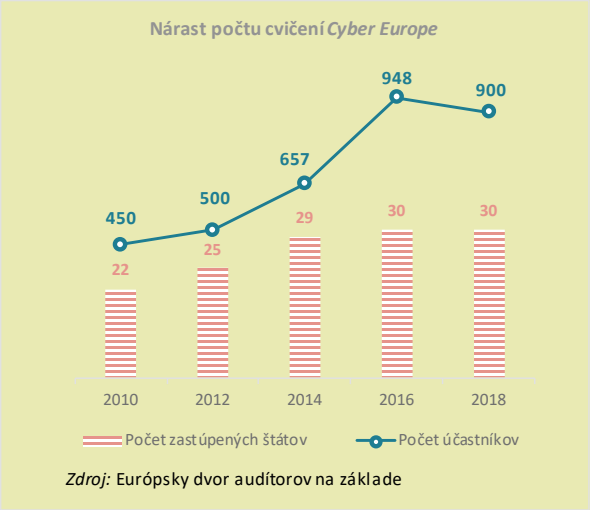
87 Európska únia vyslala odborníkov na boj proti terorizmu a bezpečnosť do 17 delegácií s cieľom posilniť spojenie medzi vnútornou a vonkajšou bezpečnosťou EÚ[125]. Napriek obmedzeným zdrojom by väčšie odborné znalosti v kybernetickej oblasti mohli pomôcť pri zavádzaní správnych projektov, ako aj pri určovaní synergií s ďalšími programami alebo zdrojmi financovania[126]. V dôsledku toho by sa mohol zlepšiť aj profil kybernetickej bezpečnosti v politickom dialógu, hoci bude musieť súperiť s mnohými ďalšími prioritami, ako sú migrácia, organizovaná trestná činnosť alebo vracajúci sa zahraniční bojovníci.

Rámček 4

Cvičenia

Cvičenia sú dôležitým prvkom vzdelávania a odbornej prípravy v kybernetickej oblasti, ktoré ponúkajú najlepšiu príležitosť na zvýšenie pripravenosti prostredníctvom skúšania spôsobilosti, ponuky reakcií na skutočné situácie a budovania sietí pracovných vzťahov. Od roku 2010 sa ich frekvencia výrazne zvýšila.

Účastníci sa zapájajú na mieste alebo na diaľku. Uskutočňujú sa posúdenia po cvičeniach s cieľom určiť získané poznatky, hoci tieto poznatky sa ešte nemusia šíriť v plnej miere medzi strategickou/politickou, prevádzkovou a technickou vrstvou[127].



Zdroj: Európsky dvor audítorov na základe

V dôsledku hlavných cvičení EÚ a NATO – cvičenie Cyber Europe (operačné), ktoré sa koná každé dva roky, a každoročné cvičenie Locked Shields (technické) – sa zhromaždilo vyše 1 000 účastníkov približne z 30 zúčastnených štátov. Obidve cvičenia sú zamerané na ochranu a zachovanie kritickej infraštruktúry v scenároch simulovaného útoku. Cvičenia sa značne prehĺbili a obidve v súčasnosti obsahujú mediálne a právne prvky a prvky finančnej politiky na zlepšenie situačného povedomia aplikujúcich odborníkov. Súbežné a koordinované cvičenia PACE (strategické) skúšajú vzájomnú komunikáciu medzi EÚ a NATO v scenári hybridnej krízy.

Nejde o jediné medzinárodné cvičenia. Agentúra ENISA organizuje každoročnú súťaž, v ktorej tímy súťažia v riešení problémov spojených s bezpečnosťou, ako je webová a mobilná bezpečnosť, kryptografické hádanky, reverzné inžinierstvo, etika a forenzná analýza. Prvé cvičenie na úrovni ministerstiev, EU CYBRID, sa uskutočnilo v septembri 2017 a bolo zamerané na strategické rozhodovanie. V roku 2018 sa uskutočnilo cvičenie Crossed Swords spojené s organizáciou NATO, ktorého cieľom bolo zlepšiť ofenzívne prvky jeho cvičenia Locked Shields. Organizácia NATO organizuje aj cvičenia Cyber Coalition.

Hlavným problémom je zabezpečiť aktívnu účasť všetkých dôležitých zainteresovaných strán a koordináciu všetkých cvičení, aby sa zabránilo duplicite a zabezpečila sa efektívna výmena získaných poznatkov.

Informovanosť

88 Občania často bývajú vektormi útokov a šírenia dezinformácií, keďže môžu byť nevedomky vystavení chybám v lacných a veľmi rozšírených zariadeniach a softvéri alebo sa môžu stať obeťou sociálneho inžinierstva. Zvyšovanie informovanosti je preto nevyhnutné na vybudovanie účinnej kybernetickej odolnosti, v nijakom prípade však nejde o jednoduchú úlohu, keďže pre neodborníkov je ťažké porozumieť zložitosti kybernetickej bezpečnosti a súvisiacim rizikám.

89 Príkladom na zvyšovanie informovanosti je každoročná organizácia Európskeho mesiaca kybernetickej bezpečnosti (ECSM) a Deň bezpečnejšieho internetu. K Európskemu mesiacu kybernetickej bezpečnosti sa teraz pripojilo sedem krajín mimo EÚ[128]. Kampaň Europolu *Say No!* je zameraná na zníženie rizika, že sa deti stanú obeťou sexuálneho nátlaku a vydierania na internete. Zníženie rizika je dôležité, pretože v súčasnosti len málo obetí útoku tieto zločiny oznamuje polícii[129]. Komisia uznáva, že stratégia kybernetickej bezpečnosti je len „čiastočne účinná“ pri zvyšovaní informovanosti občanov a podnikov[130]. Príčinou je rozsah úlohy, obmedzené zdroje, nerovnomerné zapojenie členských štátov a nedostatok vedeckých dôkazov týkajúcich sa najlepšieho spôsobu zvyšovania a merania informovanosti.

90 Výzvou pre Komisiu a príslušné agentúry je zabezpečenie, aby opatrenia na zvýšenie informovanosti: boli správne zacielené a propagované; boli inkluzívne; aby sa riadili štruktúrou hrozieb; aby sa vyhýbali nezamýšľaným účinkom, ako je „únava z bezpečnosti“[131] a aby sa vypracovali hodnotiace metódy a ukazovatele na posúdenie účinnosti opatrení. Toto by malo v rovnakej miere platiť aj v rámci samotných inštitúcií EÚ, v ktorých je potrebné zlepšiť kultúru informovanosti[132].

Problém 8: lepšia výmena informácií a koordinácia

91 Kybernetická bezpečnosť si vyžaduje spoluprácu medzi verejným a súkromným sektorom, najmä pokiaľ ide o výmenu informácií a najlepších postupov. Na všetkých úrovniach je dôležitá dôvera, aby sa vytvorilo správne prostredie na výmenu citlivých informácií medzi krajinami. Slabá koordinácia má za následok roztrieštenosť, duplicitu úsilia a rozptýlenie odborných znalostí. Účinná koordinácia môže viesť ku skutočným úspechom, ako je uzavretie trhovísk temného webu[133]. Napriek pokroku, ktorý sa v posledných rokoch dosiahol, úroveň dôvery na úrovni EÚ a v niektorých členských štátoch[134] je stále „nedostatočná“[135].

Koordinácia medzi inštitúciami EÚ a s členskými štátmi

92 Jedným z cieľov stratégie kybernetickej bezpečnosti a štruktúr spolupráce zavedených smernicou NIS je posilnenie dôvery medzi zainteresovanými stranami. V posúdení stratégie sa uznalo, že boli položené základy pre strategickú a operačnú spoluprácu na úrovni EÚ[136]. Napriek tomu je koordinácia vo všeobecnosti „nedostatočná“[137]. Problémom je zabezpečiť, aby výmena informácií nebola iba zmysluplná, ale aby umožňovala aj úplný pohľad na celkový obraz. V tejto súvislosti je dôležitým faktorom dosiahnutie spoločnej dohody založenej na uznávanej terminológii (pozri ***rámček 5***).

93 Agentúra ENISA však vo svojom hodnotení upozornila na to, že prístup EÚ ku kybernetickej bezpečnosti nebol dostatočne koordinovaný, čo malo za následok absenciu synergií medzi činnosťami agentúry ENISA a činnosťami iných zainteresovaných strán. Mechanizmy spolupráce sú stále pomerne nevyspelé[138]. Zámerom aktu o kybernetickej bezpečnosti je riešenie tejto situácie posilnením koordinačnej úlohy agentúry ENISA. Želanie posilniť spoluprácu bolo základom pre memorandum o porozumení, ktoré v roku 2018 podpísali agentúry ENISA a EDA, centrum EC3 pri Europole a tím CERT-EU[139]. Prioritou Komisie v nasledujúcich rokoch bude zabezpečenie náležitého zladenia medzi politickými iniciatívami, potrebami a investičnými programami s cieľom prekonať roztrieštenosť a vytvoriť synergie[140].

94 Koordinačné funkcie sú zakotvené v rozličných inštitucionálnych orgánoch. Bola zriadená osobitná skupina pre bezpečnostnú úniu, ktorej úlohou je zohrávať hlavnú rolu pri koordinácii jednotlivých generálnych riaditeľstiev Komisie s cieľom podporovať program bezpečnostnej únie[141]. GR pre komunikačné siete, obsah a technológie predsedá pracovnej podskupine osobitnej skupiny pre kybernetickú bezpečnosť.

95 V Rade sa kybernetickou bezpečnosťou zaoberá horizontálna pracovná skupina pre kybernetické otázky, ktorá koordinuje strategické a horizontálne kybernetické otázky a pomáha pri príprave cvičení a hodnotení ich výsledkov. Pracovná skupina úzko spolupracuje s Politickým a bezpečnostným výborom, ktorý má ústrednú úlohu pri rozhodovaní v súvislosti s akýmikoľvek diplomatickými opatreniami v kybernetickej oblasti (pozri ***rámček 6*** v ďalšej kapitole). Keďže kybernetická bezpečnosť je prierezový predmet, koordinácia všetkých relevantných záujmov nie je priamočiara: kybernetickými otázkami sa nedávno zaoberalo najmenej 24 pracovných skupín a prípravných orgánov[142].

96 Na riešenie roztrieštenosti a duplicity úsilia sú špeciálne určené dva najnovšie legislatívne návrhy týkajúce sa posilnenia agentúry ENISA (2017) a zriadenia siete

kompetenčných centier kybernetickej bezpečnosti a centra výskumných kompetencií (2018). Podnetom pre sieť kompetenčných centier kybernetickej bezpečnosti a centrum výskumných kompetencií bola potreba vyplniť medzeru, ktorú štruktúry spolupráce podľa smernice NIS nevyplnili, lebo neboli navrhnuté na podporu vypracúvania najmodernejších riešení.

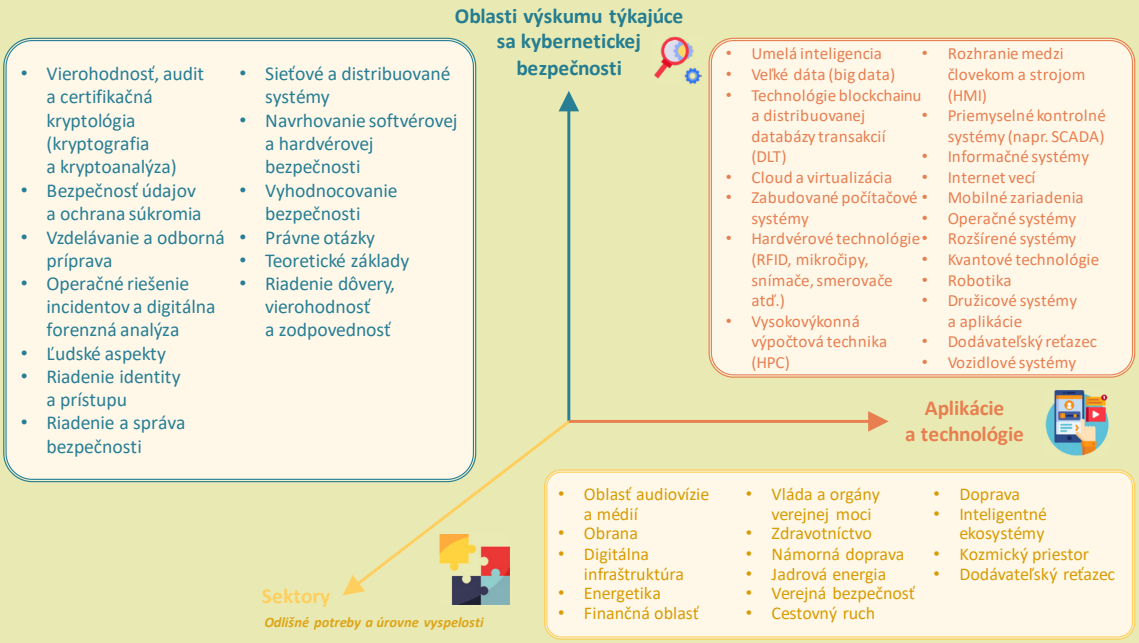
Rámček 5

Snaha dorozumieť sa tým istým kybernetickým jazykom: *technologická súdržnosť*

Zrozumiteľná terminológia zvyšuje situačné povedomie a koordináciu[143] a pomáha presne stanoviť to, čo tvorí hrozbu a riziko.

Spoločné výskumné centrum Komisie (JRC) prednedávnom vypracovalo revidovanú taxonómiu pre výskum, ktorá čerpá z rôznych medzinárodných noriem[144]. Táto taxonómia sa má stať referenčným bodom, ktorý majú používať výskumné subjekty z celej Európy ako register.

Taxonómia pre kybernetickú bezpečnosť



Zdroj: Európsky dvor audítorov, upravené podľa údajov Európskej komisie.

Až donedávna nemali inštitúcie a agentúry EÚ nijaké spoločné vymedzenia. To sa teraz mení. V rámci svojej koncepcie skupina pre spoluprácu navrhla taxonómiu pre incidenty s cieľom uľahčiť účinnú cezhraničnú spoluprácu.

Spolupráca a výmena informácií so súkromným sektorom

97 Spolupráca medzi orgánmi verejnej moci a súkromným sektorom je dôležitá na posilnenie celkovej úrovne kybernetickej bezpečnosti. Napriek tomu Komisia vo svojom posúdení stratégie kybernetickej bezpečnosti z roku 2017 zistila, že výmena informácií medzi súkromnými zainteresovanými stranami a medzi verejným a súkromným sektorom „nebola zatiaľ optimálna“ z dôvodu „nedostatku dôveryhodných mechanizmov podávania správ a stimulov na výmenu informácií“[145], čo bránilo dosiahnutiu strategických cieľov. Komisia takisto poukázala na to, že neexistujú účinné mechanizmy spolupráce, podľa ktorých členské štáty spolupracujú na strategickom posilnení trvanlivých, rozsiahlych priemyselných kapacít[146].

98 Strediská pre výmenu a analýzu informácií (ISAC) sú organizácie zriadené na to, aby poskytovali platformy a zdroje na uľahčenie výmeny informácií medzi verejným a súkromným sektorom, ako aj na zhromažďovanie informácií o kybernetických hrozbách. Ich cieľom je vybudovanie dôvery prostredníctvom výmeny skúseností, znalostí a analýz, týkajúcich sa najmä hlavných príčin, incidentov a hrozieb. V mnohých členských štátoch už existujú vnútroštátne a sektorové strediská pre výmenu a analýzu informácií, na európskej úrovni sú však stále pomerne vzácne[147]. Spájajú sa však s viacerými problémami (obmedzenia týkajúce sa zabezpečenia zdrojov, ťažkosti pri vyhodnocovaní ich úspešnosti, zabezpečenie správnych štruktúr na zapojenie verejného aj súkromného sektora, zapojenie orgánov presadzovania práva), ktoré sa musia prekonať, pokiaľ majú prispieť k vykonávaniu smernice NIS a k vybudovaniu spôsobilostí v oblasti bezpečnosti na celoeurópskej úrovni[148].

99 Úzka spolupráca so súkromným sektorom je mimoriadne dôležitá na boj proti komplexnej počítačovej kriminalite, jej efektívnosť však v členských štátoch nie je rovnaká a závisí od úrovne dôvery[149]. Centrum EC3 pri Europole však vytvorilo niekoľko poradných skupín s prevádzkovateľmi zo súkromného sektora, s inštitúciami a agentúrami EÚ a s ďalšími medzinárodnými organizáciami, aby sa zlepšila spolupráca prostredníctvom tvorby sietí, výmeny strategických spravodajských informácií a spolupráce. Pracujú podľa plánov, ktoré sú v súlade s cieľmi cyklu politík EÚ[150]. Trestné zneužívanie šifrovania je ďalšou oblasťou s veľkým počtom problémov, ktoré si vyžadujú viac spolupráce so súkromným sektorom. Centrum EC3 pri Europole v súčasnosti skúma možnosti zabezpečenia osobitných krátkodobých doplnkov k spoločnej pracovnej skupine pre počítačovú kriminalitu (pozri bod ***62***) pre odborníkov zo súkromného sektora a akademickej obce.

100 Neexistencia účinných mechanizmov spolupráce postihuje civilné a obranné komunity, verejné aj súkromné. Medzi oblasti, ktoré predstavujú spoločné problémy,

patrí kryptografia, zabezpečené zabudované systémy, odhaľovanie škodlivého softvéru, metódy simulácie, ochrana sietí a komunikačných systémov a autentifikačné technológie. Presadzovanie civilno-vojenskej spolupráce a podpora výskumu a technológií (najmä prostredníctvom podpory pre MSP) sú dve z priorít aktualizovaného politického rámca pre kybernetickú obranu (aktualizácia za rok 2018).

Podnety na zamyslenie – Budovanie odolnosti

- **Ako možno na úrovni EÚ dosiahnuť vhodnú rovnováhu medzi potrebou začlenenia politiky v oblasti kybernetickej bezpečnosti a zabezpečením účinnej koordinácie medzi rôznymi subjektmi a rozptýlením povinností?**
- **Ako dobre sú inštitúcie a agentúry EÚ pripravené na ďalší veľký útok zameraný priamo proti nim?**
- **Ako sa môžu agentúry EÚ zaoberajúce sa oblasťou kybernetiky stať príťažlivejšími pre talenty?**
- **Aké ďalšie kroky sú potrebné na zabezpečenie primeranej kapacity v inštitúciách a agentúrach EÚ s cieľom umožniť vznik súdržného rámca na posudzovanie rizík a hrozieb?**
- **Akými spôsobmi európske orgány dohľadu (Európsky orgán pre bankovníctvo, Európsky orgán pre cenné papiere a trhy a Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov) riešia kybernetické zraniteľnosti späté s finančným sektorom a aké poznatky z toho môžu čerpať ďalšie sektory?**
- **Ako možno vzhľadom na celkový nedostatok odborných znalostí využiť technickú pomoc EÚ pre orgány verejnej moci čo najlepšie tak, aby mala maximálny celkový vplyv na zvýšenie kybernetickej odolnosti?**
- **Ako môžu EÚ a členské štáty zabezpečiť zmysluplnú účasť na medzinárodných diskusiách s cieľom formovať riadenie kybernetického priestoru a normy a presadzovať hodnoty EÚ?**
- **Ktoré opatrenia na zvyšovanie informovanosti na úrovni EÚ a členských štátov (vrátane preventívneho úsilia) majú skutočný vplyv a čo môže EÚ spraviť na ich rozšírenie?**
- **Akú úlohu by mohla EÚ zaujať, aby sa do oblasti kybernetickej bezpečnosti vniesla rodová rozmanitosť?**
- **Ako môžu EÚ a členské štáty posilniť synergie medzi civilnými a obrannými komunitami v súlade s politickým rámcom pre kybernetickú obranu (aktualizácia za rok 2018)?**

Účinné reagovanie na kybernetické incidenty

101 Navrhnutie účinnej reakcie na kybernetické útoky je zásadné na ich úplné zastavenie v čo najskoršej fáze. Obzvlášť je dôležité, aby kľúčové odvetvia, členské štáty a inštitúcie EÚ boli schopné pohotovo reagovať koordinovaným spôsobom. Na to je dôležité včasné odhalenie útoku.

Problém 9: účinné odhalenie a reakcia

Odhaľovanie a oznamovanie

102 Bežné nástroje odhaľovania každý deň pomáhajú zvíťaziť nad veľkou väčšinou útokov[151]. Digitálne systémy sa však stávajú natoľko komplexnými, že je nemožné zabrániť úplne každému útoku. Ich komplikovanosť znamená, že útoky často dlhý čas unikajú odhaleniu. Odborníci teda tvrdia, že pozornosť by sa mala venovať rýchlemu odhaľovaniu a obrane[152]. Niektoré nástroje odhaľovania (ako je automatizácia, strojové učenie a behaviorálna analýza, ktoré sa zaoberajú znižovaním rizík a analýzou a odvodením poučení zo systémového správania) trpia nízkou mierou prijímania medzi podnikmi[153]. Príčinou je sčasti vytvorenie falošne pozitívnych nálezov, v dôsledku ktorých sa neškodné činnosti chybne považujú za škodlivé.

103 Po odhalení a analýze narušenia musí nasledovať okamžité oznámenie a ohlásenie, aby ostatné verejné a súkromné subjekty mohli prijať preventívne opatrenia a aby príslušné orgány mohli pomôcť postihnutým subjektom. Veľa organizácií váha s potvrdením kybernetických incidentov a s ich ohlasovaním[154]. Dôležité je aj včasné zapojenie orgánov presadzovania práva do prvej reakcie na podozrivé počítačové trestné činy a iniciatívna výmena informácií s jednotkami CSIRT.

104 Predchádzajúci nedostatok spoločných požiadaviek EÚ týkajúcich sa oznamovania incidentov predstavoval riziko omeškania komunikácie o narušeniach a zbrzdenia reakcie, ktoré sa malo odstrániť zavedením smernice NIS (pozri bod ***20***). Po útokoch malvéru WannaCry v roku 2017 Komisia dospela k záveru, že sieťový systém jednotiek CSIRT „ešte nebol plne funkčný“[155]. Kým sa pokračuje vo vykonávaní smernice, treba si počkať, či usmernenia vypracované skupinou pre spoluprácu prispejú k účinnému prekonaniu neochoty ohlasovať incidenty[156].

105 Prevádzkovatelia základných služieb v istých sektoroch majú podľa existujúcich právnych predpisoch EÚ viacero oznamovacích povinností (vrátane povinnosti voči spotrebiteľom), čo môže oslabovať účinnosť procesu. Napríklad na prevádzkovateľov vo finančnom a bankovom sektore sa vzťahujú odlišné kritériá, normy, stropy a časové rámce týkajúce sa notifikačnej povinnosti podľa všeobecného nariadenia o ochrane údajov, smernice NIS, smernice o platobných službách, ECB/SSM, systému TARGET2 a nariadenia eIDAS[157]. Je preto dôležité tieto povinnosti zjednodušiť, keďže okrem toho, že predstavujú zbytočné administratívne zaťaženie, táto rôznorodosť by mohla viesť k roztrieštenosti podávaných správ.

Koordinovaná reakcia

106 Rozvoj európskeho rámca spolupráce v prípade kybernetickej bezpečnostnej krízy stále prebieha. Predstavená preto bola súvisiaca koncepcia[158] (pozri bod ***18***), aby sa do mechanizmu integrovanej politickej reakcie na krízu (IPCR) vnieslo hľadisko kybernetickej bezpečnosti, zlepšilo situačné povedomie a zabezpečila lepšia integrácia s inými mechanizmami krízového riadenia EÚ[159]. Koncepcia sa týka inštitúcií, agentúr a členských štátov EÚ. Konzistentná integrácia všetkých týchto mechanizmov reakcií na krízu je náročná[160]. Vážnym nedostatkom je aj to, že v súčasnosti európskym inštitúciám chýba spoločná bezpečná komunikačná sieť[161].

107 Schopnosť EÚ reagovať na kybernetické útoky na operačnej a politickej úrovni v prípade rozsiahleho cezhraničného incidentu sa označuje ako „obmedzená“, čo je čiastočne spôsobené tým, že kybernetická bezpečnosť ešte nie je začlenená do existujúcich mechanizmov koordinácie reakcie na krízu na úrovni EÚ[162]. Tento nedostatok sa v smernici NIS nerieši.

108 Nedávno navrhovanú reformu agentúry ENISA, v ktorej sa počítalo s väčšou operačnou úlohou pri riešení rozsiahlych kybernetických bezpečnostných incidentov, nepodporili členské štáty, ktoré dávajú prednosť tomu, že úlohou agentúry by mala byť podpora a dopĺňanie ich vlastných operačných opatrení[163]. Na úrovni členských štátov už existuje veľa tímov CERT-EU/jednotiek CSIRT, ich kapacity sa však značne líšia. To je prekážkou účinnej cezhraničnej spolupráce potrebnej pre reakcie na rozsiahle incidenty[164].

109 Pokúsili sme sa zmapovať rôzne úlohy pridelené rozličným subjektom určeným v koncepcii, boli v nej však medzery, ktoré sa budú musieť odstrániť v rámci napredovania vykonávania. Jednou, pôvodne nedostatočne riešenou oblasťou, bolo

presadzovanie práva, hoci protokol reakcie na núdzové situácie v oblasti presadzovania práva EÚ nadobudol účinnosť v decembri 2018[165]. Zabezpečiť to, že koncepcia je praktická a že všetky strany poznajú svoje úlohy, je kľúčom jeho úspechu. Toto tvrdenie sa v nasledujúcich rokoch bude musieť dôkladne preveriť.

110 Účinná reakcia je viac než zmiernenie škôd; kľúčové je aj určenie zodpovednosti za útoky. Sledovanie a identifikácia páchateľov, predovšetkým v prípade hybridného útoku, môžu byť veľmi ťažké z dôvodu čoraz vyššej miery využívania anonymizačných nástrojov, kryptomien a šifrovania. Tento problém je známy ako atribučný problém. Jeho náprava nie je len technickou otázkou, ale aj problémom trestnej justície. Právne a procesné rozdiely medzi krajinami môžu brániť vyšetrovaniam a trestnému stíhaniu podozrivých osôb. Na riešenie atribučného problému bude potrebná formálnejšia operačná výmena informácií prostredníctvom jasnejších postupov napríklad s Europolom alebo s Európskou justičnou sieťou na boj proti počítačovej kriminalite Eurojustu.

111 Na politickej úrovni bol vypracovaný súbor nástrojov kybernetickej diplomacie (pozri ***rámček 6***) s cieľom podporiť mierové riešenie medzinárodných sporov v kybernetickom priestore. Vytvorenie tímov rýchlej kybernetickej reakcie a vznik iniciatívy pre vzájomnú pomoc v oblasti kybernetickej bezpečnosti sú dva projekty podporujúce rozvoj lepšej výmeny informácií, na ktorých sa pracuje v rámci stálej štruktúrovanej spolupráce[166].

Rámček 6

Súbor nástrojov kybernetickej diplomacie

Spoločná diplomatická reakcia EÚ na škodlivé kybernetické činnosti[167], alebo súbor nástrojov kybernetickej diplomacie, vyrástla na základoch záverov Rady z roku 2015 o kybernetickej diplomacii[168]. Cieľom kybernetickej diplomacie je rozvoj a vykonávanie spoločného a komplexného prístupu ku kybernetickému priestoru založeného na hodnotách EÚ, na zásadách právneho štátu, na budovaní kapacít a partnerstiev, na podpore modelu správy internetu, ktorý je založený na viacerých zainteresovaných stranách, a na zmierňovaní kybernetických hrozieb a väčšej stabilite v medzinárodných vzťahoch.

Tento súbor nástrojov umožňuje EÚ a jej členským štátom zorganizovať spoločnú diplomatickú reakciu na škodlivé kybernetické činnosti, pri ktorej budú v plnej miere využívať opatrenia v rámci spoločnej zahraničnej a bezpečnostnej politiky. Môže ísť o preventívne opatrenia (napr. zvyšovanie informovanosti, budovanie kapacít), opatrenia na podporu spolupráce, stability a reštriktívne opatrenia (napr. zákaz cestovania, embargá na vývoz zbraní, zmrazenie finančných prostriedkov) alebo o podporu reakciám členských štátov[169]. Hlavnou myšlienkou je to, že ďalšia

spolupráca s cieľom zmierniť hrozby a jasne naznačiť možné následky spoločnej reakcie môžu zabrániť (potenciálne) agresívnemu správaniu.

Reakcia EÚ na škodlivé kybernetické činnosti bude úmerná rozsahu, miere, trvaniu, intenzite, komplexnosti, sofistikovanosti a vplyvu kybernetickej činnosti.

Pre úspech súboru nástrojov bude zásadné to, do akej miery je prepletený s koncepciou a mechanizmom integrovanej politickej reakcie na krízu (pozri bod ***106***), do akej miery sa prostredníctvom rýchlej a nepretržitej výmeny informácií (vrátane informácií o prvkoch priraďovania)[170] vytvorilo situačné povedomie, a napokon preň bude dôležitá účinná spolupráca. Kľúčom pre úspešné využitie súboru nástrojov je aj účinná a koordinovaná komunikácia. Súbor nástrojov sa doteraz použil dvakrát: na začatie dialógu so Spojenými štátmi americkými po útoku *WannaCry*[171] a na vypracovanie záverov Rady odsudzujúcich škodlivé používanie informačných a komunikačných technológií[172]. Prebieha operačné využívanie súboru nástrojov a treba si počkať, aký účinný tento súbor bude pri plnení svojich cieľov.

Problém 10: ochrana kritickej infraštruktúry a spoločenských funkcií

Ochrana infraštruktúry

112 Veľká časť kritickej infraštruktúry EÚ sa riadi prostredníctvom priemyselných kontrolných systémov (ICS)[173]. Mnohé z nich boli navrhnuté ako samostatné systémy s obmedzeným prepojením s vonkajším svetom. Keď sa zložky priemyselných kontrolných systémov pripojili na internet, stali sa zraniteľnejšie voči rušeniu zvonka. Údržba a opravovanie existujúcich systémov už nemusia byť možné, ich inovácia však nie je rýchla ani lacná. Snahy o zvýšenie bezpečnosti kritickej infraštruktúry teda musia zahŕňať inováciu priemyselných kontrolných systémov.

113 Kým priemysel pokračuje v digitalizácii (všeobecne známy ako „Priemysel 4.0“), vplyv rozsiahleho incidentu v jednom priemyselnom sektore môže mať dominový efekt v inom sektore. Agentúra ENISA upozornila na význam mapovania vplyvu vzájomných prepojení kľúčových odvetví[174], ktoré je nevyhnutné na porozumenie možného šírenia incidentu a ktoré je základom dobre koordinovaných reakcií.

114 Cieľom smernice NIS je posilnenie pripravenosti v kľúčových sektoroch zodpovedajúcich za kritickú infraštruktúru. Nevzťahuje sa však na všetky sektory (pozri ***tabuľku 1***)[175], čo „znižuje účinnosť stratégie“[176]: zvláštnu pozornosť si v tejto súvislosti

zasluhuje ochrana integrity demokratických volieb pred zasahovaním do volebnej infraštruktúry a dezinformáciami (pozri ***rámček 7***). Hlavným problémom okrem revízie existujúcich právnych predpisov bude teda pochopenie toho, ako zapojiť tieto sektory do účinných reakcií na rozsiahle incidenty.

115 Zraniteľné miesta v kritickej infraštruktúre nekončia na hraniciach Európy. Osobitnou výzvou pre Komisiu je povzbudenie kandidátskych krajín, aby prijali tie isté normy ako členské štáty, napríklad v takých oblastiach, ako sú právne predpisy súvisiace s kybernetickou bezpečnosťou alebo ochrana kritickej infraštruktúry.

Rámček 7

Ochrana kritických spoločenských funkcií: *boj proti zasahovaniu do volieb*

V máji 2019 pôjde k voľbám do Európskeho parlamentu takmer 400 miliónov voličov. Pôjde o prvé voľby, ktoré sa budú konať podľa všeobecného nariadenia o ochrane údajov. Tieto voľby prichádzajú tesne po škandáloch týkajúcich sa zneužívania osobných údajov na politické mikrozacielenie a bezprecedentných koordinovaných dezinformačných (tzv. falošné správy) kampaní. Komisia varovala pred možným kybernetickým zasahovaním do týchto volieb[177]. Boj proti nemu si vyžiada nadrezortný a celospoločenský prístup.

Volebná infraštruktúra

Organizácia volieb je zložitá a za zabezpečenie ich ochrany a integrity zodpovedajú členské štáty. Zasahovanie do volieb a volebnej infraštruktúry môže mať za cieľ ovplyvnenie preferencií voličov, ich účasti na voľbách alebo volebného procesu vrátane samotného hlasovania a sčítavania hlasov a oznámenia výsledkov. Vo voľbách do Európskeho parlamentu je obzvlášť problematická ochrana posledného článku v reťazci (oznámenia výsledkov z hlavných miest členských štátov do Bruselu) vzhľadom na to, že neexistuje spoločný bezpečnostný prístup a ani nijaký podobný prístup nebol v tejto súvislosti vyskúšaný[178].

Nedávny balík opatrení Komisie týkajúcich sa volieb obsahoval opatrenia na posilnenie kybernetickej bezpečnosti volieb, ako je zriadenie vnútroštátnych kontaktných miest na koordináciu činností a výmenu informácií na začiatku volieb. Mimoriadny význam má výmena najlepších postupov a získaných poznatkov[179].

Volebné systémy sa nepovažujú za súčasť kritickej infraštruktúry[180], ani sa na ne nevzťahuje smernica NIS. Skupina pre spoluprácu napriek tomu vypracovala praktické usmernenia o bezpečnosti volebných technológií na pomoc orgánom verejnej moci. Zverejnenie nadväzujúceho prieskumu sa očakáva začiatkom roku 2019[181]. Členským štátom sa takisto odporúča, aby vykonali posúdenia rizík kybernetických hrozieb pre ich volebné procesy.

Dezinformácie

Dezinformácie sa stávajú čoraz významnejším prvkom hybridných útokov, medzi ktoré patria kybernetické útoky a hackovanie sietí. Použiť sa môžu na rozdelenie spoločností, zasiatie nedôvery a oslabenie dôvery v demokratické procesy alebo na iné problémy (napríklad odpor proti očkovaniu alebo zmena klímy). Ich miera, rýchlosť šírenia a rozpätie sa zvyšujú a dezinformácie predstavujú skutočnú bezpečnostnú hrozbu pre EÚ.

Európska únia prijala niekoľko opatrení na boj proti dezinformáciám. V roku 2015 bola v rámci ESVČ vytvorená pracovná skupina East StratCom, ktorej cieľom je napádať ruské dezinformačné kampane[182]. Odborníci chvália úsilie skupiny pri presadzovaní politík EÚ, podpore nezávislých médií v susedských krajinách a predvídaní dezinformácií, ich sledovaní a boji proti nim[183]. Jednako len sú zdroje pracovnej skupiny obmedzené v pomere k miere a zložitosti dezinformačných kampaní[184]. Potrebná je systematickejšia interakcia s existujúcimi štruktúrami EÚ a lepšia spolupráca v oblasti strategickej komunikácie[185]. Európska rada v decembri 2018 schválila nový akčný plán[186].

Najnovšie Komisia na základe svojho oznámenia z apríla 2018 o boji proti dezinformáciám na internete[187] vypracovala dobrovoľný, samoregulačný kód*ex post*upov[188], ktorý vychádza z existujúcich nástrojov politiky a ktorý sa online platformy a reklamný priemysel zaviazali dodržiavať[189]. Súčasťou opatrení je pomoc pri zvyšovaní dôveryhodnosti obsahu a podpora úsilia o zvýšenie mediálnej a spravodajskej gramotnosti. Pôsobiť začala aj nezávislá európska sieť overovateľov faktov.

Komisia uviedla, že v prípade nedodržiavania kódexu postupov môžu nasledovať ďalšie regulačné opatrenia. Ako kľúčové sa ukáže určovanie účinnosti opatrení, a to najmä rozhodovanie o spôsobe vyhodnocovania zlepšení dôvery, transparentnosti a zodpovednosti.

Ďalším problémom bude hľadanie spôsobov na zlepšenie zisťovania, analýzy a odhaľovania dezinformácií[190]. Potrebné je aj aktívne a strategické monitorovanie a analýza zdrojov otvorených údajov[191]. Pokusy o získanie lepšieho porozumenia prostrediu hrozieb by mali zahŕňať aj nové tendencie, ako sú tzv. deepfake (falošné videá vyrobené pomocou umelej inteligencie a hĺbkového strojového učenia), ako aj nástroje potrebné na ich odhaľovanie.

Posilnenie autonómie

116 Európska únia je čistým dovozcom produktov a služieb v oblasti kybernetickej bezpečnosti, čo zvyšuje riziko technologickej závislosti od mimoeurópskych prevádzkovateľov a zraniteľnosti voči nim[192]. Táto skutočnosť konkrétne oslabuje bezpečnosť kritickej infraštruktúry EÚ, čo napomáhajú aj komplexné globálne dodávateľské reťazce. Riziko je ešte vyššie v prípade, keď mimoeurópski prevádzkovatelia nadobúdajú európske podniky zaoberajúce sa kybernetickou bezpečnosťou. Členské štáty zodpovedajú za preverovanie priamych zahraničných investícií (PZI) a v súčasnosti neexistuje nijaký celoeurópsky mechanizmus preverovania[193].

117 Väčšia strategická autonómia je cieľ stanovený v globálnej stratégii EÚ a v oznámení *Odolnosť, odrádzanie a obrana*[194] z roku 2017. Riešenie myriád problémov uvedených v tejto správe pomôže posilniť túto požadovanú autonómiu. Žiadne opatrenie tento cieľ nedosiahne samostatne.

Podnety na zamyslenie – Účinná reakcia

- **Ako sa v dôsledku smernice NIS zlepšilo oznamovanie kybernetických incidentov v kľúčových odvetviach a mimo nich?**
- **Do akej miery inštitúcie EÚ prijali za vlastnú koordináciu reakcie na krízu v prípade rozsiahlych kybernetických incidentov?**
- **Ako by kybernetická diplomacia mohla zohrávať významnejšiu úlohu vo vonkajších činnostiach EÚ?**
- **Sú súčasné štruktúry a opatrenia EÚ na boj proti dezinformáciám primerané miere a zložitosti problému?**

Záverečné poznámky

118 V posledných rokoch EÚ a jej členské štáty posunuli kybernetickú bezpečnosť na vyššie miesto programu s cieľom zlepšiť celkovú kybernetickú odolnosť. Dosiahnutie vyššej úrovne kybernetickej bezpečnosti v Únii však stále zostáva obrovským záväzkom. V tomto informačnom dokumente sme sa snažili poukázať na niektoré z hlavných problémov pre cieľ EÚ stať sa najbezpečnejším digitálnym prostredím na svete.

119 Z nášho prehľadu vyplýva, že na zabezpečenie **primeranej zodpovednosti a hodnotenia** je potrebný prechod na kultúru výkonnosti, ktorej súčasťou sú hodnotiace postupy. **Pretrvávajú isté medzery v práve a členské štáty netransponovali existujúce právne predpisy dôsledne**. Táto skutočnosť môže sťažiť to, aby právne predpisy dosiahli svoj plný potenciál. Ďalší zistený problém sa týka **zosúladenia úrovne investícií so strategickými cieľmi**, čo si vyžaduje zvýšiť úrovne investícií a ich vplyv. To je náročnejšie v prípade, keď EÚ a jej členské štáty nemajú **jasný prehľad o výdavkoch EÚ** v oblasti kybernetickej bezpečnosti**.** Nahlásené boli aj **obmedzenia týkajúce sa primeraného zabezpečovania zdrojov pre agentúry EÚ zaoberajúce sa oblasťou kybernetiky**, ako aj ťažkosti pri lákaní talentov a ich udržaní.

120 Záverom dostupných štúdií je, že **riadenie kybernetickej bezpečnosti je možné posilniť** s cieľom zvýšiť schopnosť celosvetového spoločenstva reagovať na kybernetické útoky a incidenty. Zároveň je nemožné zabrániť všetkým útokom. **Rýchle odhalenie a reakcia** a **ochrana kritickej infraštruktúry a spoločenských funkcií** preto spoločne s lepšou **výmenou informácií a koordináciou** medzi verejným a súkromným sektorom predstavujú hlavné problémy, ktoré treba riešiť. A napokon, čoraz väčší nedostatok zručností v oblasti kybernetickej bezpečnosti znamená, že životne dôležitým problémom je aj **zvyšovanie úrovne zručností a informovanosti** vo všetkých sektoroch a na všetkých úrovniach spoločnosti.

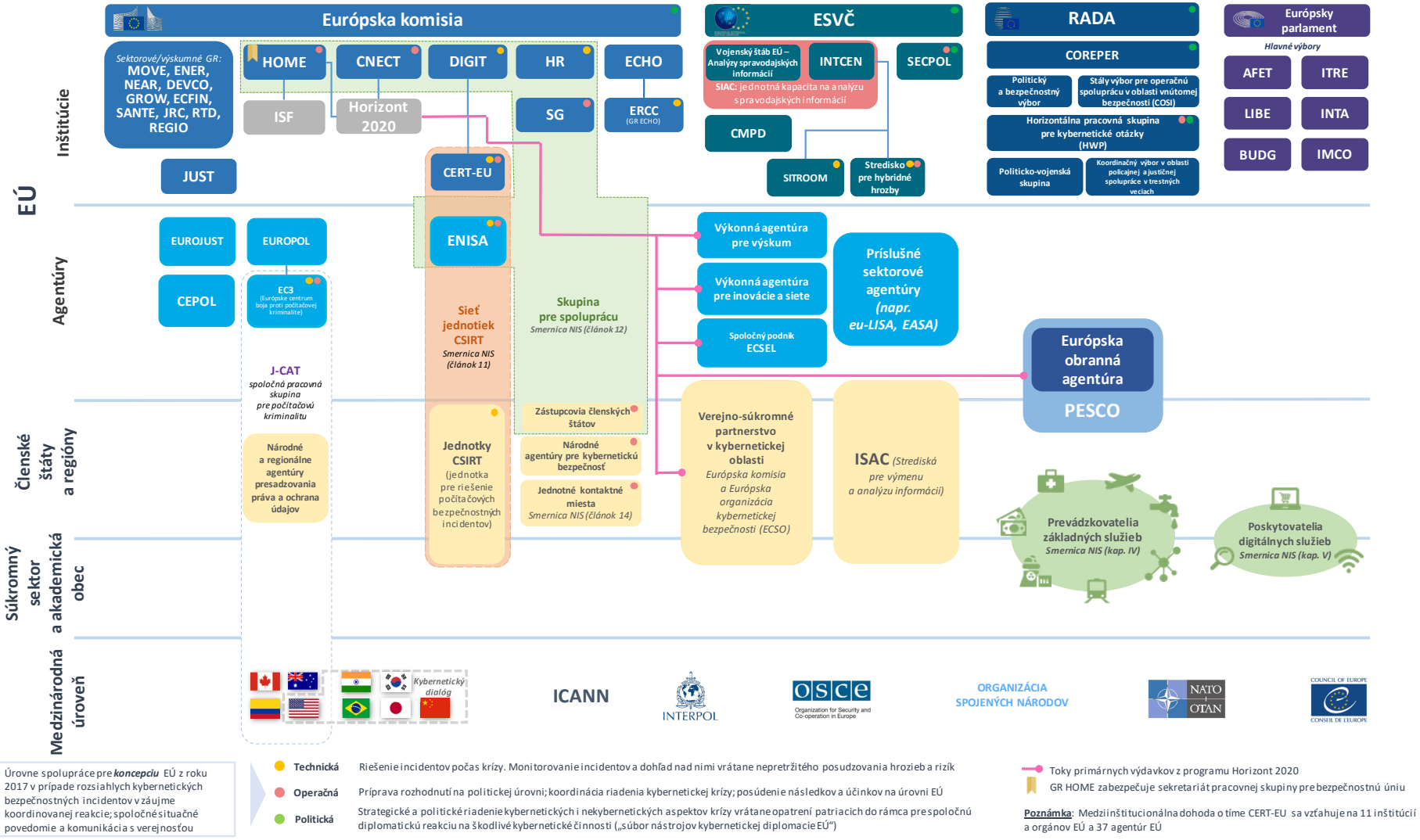
121 Tieto problémy, ktoré predstavujú kybernetické hrozby, ktorým čelí EÚ, a širšie globálne prostredie si vyžadujú nepretržité odhodlanie a neprestajné, vytrvalé dodržiavanie hodnôt EÚ.

Tento informačný dokument prijala komora III na svojom zasadnutí dňa 14. februára 2019.

Za Dvor audítorov

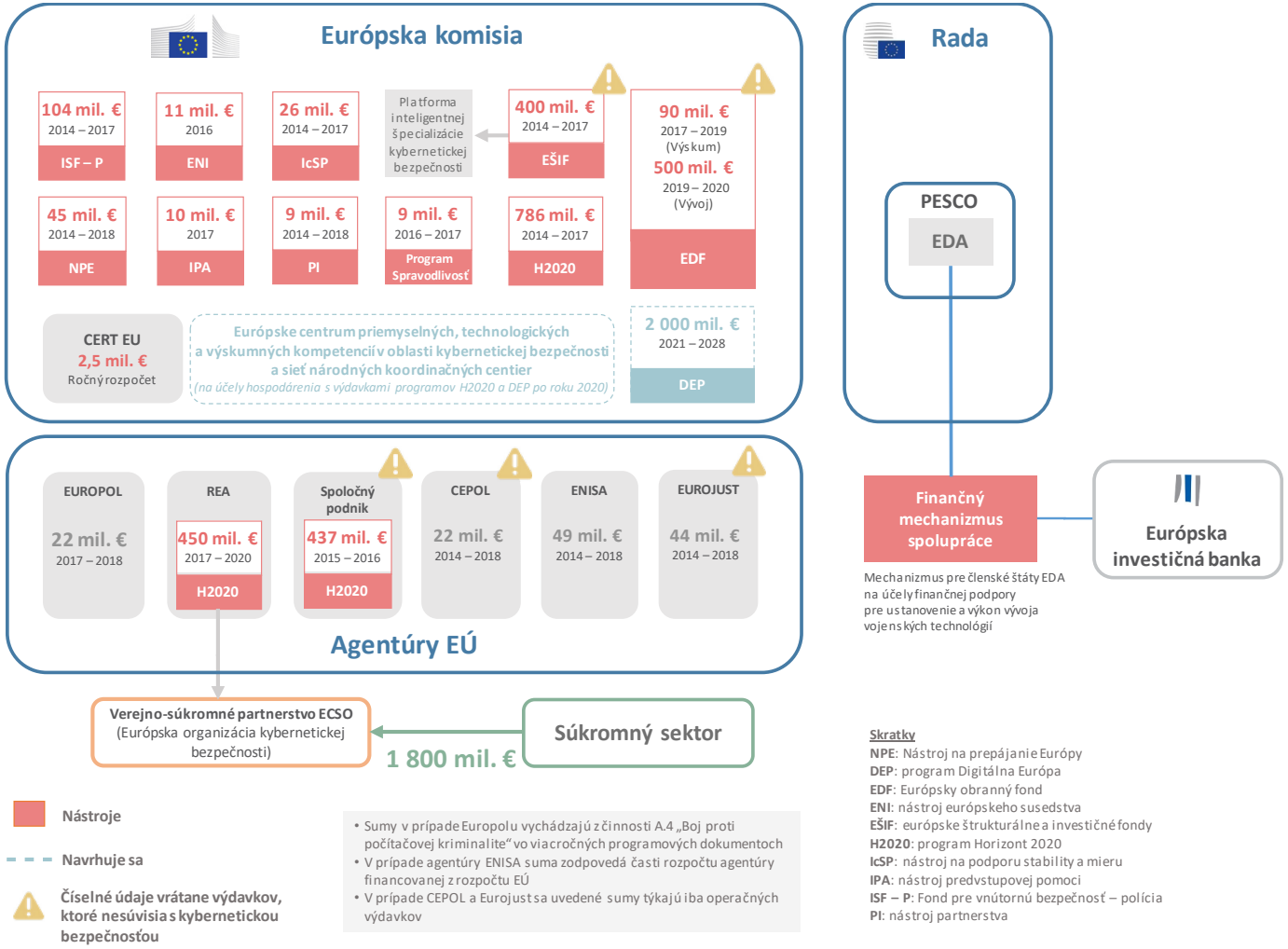
Klaus-Heiner Lehne
predseda

Príloha I — Komplexné, mnohovrstevné prostredie s množstvom aktérov



Zdroj: Európsky dvor audítorov.

Príloha II — Výdavky EÚ na kybernetickú bezpečnosť od roku 2014



Zdroj: Európsky dvor audítorov podľa dokumentov Európskej komisie a agentúr EÚ.

Príloha III — Správy kontrolných úradov členských štátov EÚ

Typ	Názov (s hypertextovým odkazom)	Rok	Členský štát
Audity zhody	Poznámka k hodnoteniu vnútornej kontroly	2014	FR
	Správa o osvedčení účtov všeobecného systému sociálneho zabezpečenia (obrana, zahraničné veci)	2016	FR
	Osvedčenie štátnej účtovnej závierky	2016	FR
	Zaistenie bezpečnosti a ochrany estónskych vnútroštátnych databáz kľúčového významu	Dokončené 2018/ zatiaľ neuverejnené	EE
	Účinnosť vnútorných kontrol pri ochrane osobných údajov vo vnútroštátnych databázach	2008	EE
Audity výkonnosti/audity optimálneho využívania finančných prostriedkov	Správa o zmierňovaní kybernetických útokov	2013	DK
	RiR 2014:23 Informačná bezpečnosť v civilnej verejnej správe	2014	SE
	Správa o spracúvaní dôverných údajov osôb a spoločností zo strany vlády	2014	DK
	Národný program kybernetickej bezpečnosti	2014	UK
	Správa rozpočtovému výboru nemeckého spolkového parlamentu v súlade s § 88 ods. 2 spolkového rozpočtového zákonníka (BHO) – Konsolidácia informačných technológií, spolková vláda	2015	DE
	Správa o prístupe do systémov IT, ktoré podporujú poskytovanie základných služieb dánskej spoločnosti	2015	DK
	Orgán pre verejné plánovanie Plaine de France	2015	FR
	„Prostredie kybernetickej bezpečnosti v Litve“ litovské znenie zhrnutie preložené do angličtiny	2015	LT
	Výkonnosť úloh verejných subjektov v oblasti kybernetickej bezpečnosti v Poľsku (v PL)	2015	PL
	RiR 2015:21 Počítačová kriminalita – polícia a prokuratúry by mohli byť efektívnejšie	2015	SE
	Nedostatočná úroveň digitálnych zručností vo vláde (prieskum)	2015	UK
	Správa federálnemu parlamentu: Federálne financie: výber dedičskej dane	2016	BE
	Správa o riadení bezpečnosti informačných technológií v systémoch zverených externým dodávateľom	2016	DK
	Audítorská správa o úverovej činnosti Inštitútu verejných úverov za rok 2016	2016	ES
	Usmerňovanie vládnej bezpečnostnej siete	2016	FI
	Zaistenie bezpečnosti systémov informačných technológií používaných na verejné úlohy	2016	PL
	Predchádzanie kybernetickému šikanovaniu medzi deťmi a mladými ľuďmi a boj proti nemu	2016	PL

Typ	Názov (s hypertextovým odkazom)	Rok	Členský štát
	Činnosti v oblasti informačnej bezpečnosti v deviatich agentúrach – Ďalší audit informačnej bezpečnosti v štáte. RiR 2016:8	2016	SE
	Ochrana informácií vo vláde	2016	UK
	Správa o ochrane systémov informačných technológií a zdravotných údajov v troch dánskych regiónoch	2017	DK
	Poznámka o výsledkoch medzinárodného paralelného auditu „Účinnosť vnútorných kontrol pri ochrane osobných údajov vo vnútroštátnych databázach“	2017	EE
	Mechanizmy kybernetickej ochrany	2017	FI
	Usmerňovanie prevádzkovej spoľahlivosti elektronických služieb	2017	FI
	Sieť poľnohospodárskych komôr (syntéza)	2017	FR
	Obchodná a priemyselná komora departmánu Vaucluse (regionálna audítorská komora regiónu Provence-Alpes-Côte-d'Azur)	2017	FR
	Zaistenie bezpečnosti a ochrany estónskych vnútroštátnych databáz kľúčového významu	Dokončené 2018/ zatiaľ neuverejnené	EE
	„Rozvoj vnútroštátnej infraštruktúry elektronických komunikácií“ litovské znenie zhrnutie preložené do angličtiny	2017	LT
	Audit informačných technológií: Kybernetická bezpečnosť v štátnych subjektoch	2017	MT
	Systém národných registrov: bezpečnosť, výkonnosť a použiteľnosť	2017	PL
	Incident WannaCry	2017	UK
	Online podvod	2017	UK
	Správa o ochrane proti útokom ransomvéru	2018	DK
	Nemocnica v meste Arpajon (regionálna komora regiónu Île-de-France)	2018	FR
	„Riadenie zdrojov kritických štátnych informácií“	2018	LT
	„Elektronické trestné činy“	2019	LT
	Informačná bezpečnosť v Poľsku	2019	PL
Iné	Databáza verejných subjektov	neuvedené	BE
	Dotazník o politike bezpečnosti a analýze rizík (prebiehajúci)	neuvedené	BE

Skratky

CERT -EU: tím reakcie na núdzové počítačové situácie

cPPP: zmluvné verejno-súkromné partnerstvo

CSIRT: jednotka pre riešenie počítačových bezpečnostných incidentov

DDoS: distribuované odmietnutie služieb

DEP: program Digitálna Európa

DIGIT: Generálne riaditeľstvo pre informatiku

EC3: Európske centrum boja proti počítačovej kriminalite pri Europole

ECSEL: Elektronické komponenty a systémy pre vedúce postavenie Európy

ECSM: Európsky mesiac informovanosti o kybernetickej bezpečnosti

ECSO: Európska organizácia kybernetickej bezpečnosti

EDA: Európska obranná agentúra

EDA: Európsky dvor audítorov

ENISA: Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť

ESA: európsky orgán dohľadu

ESVČ: Európska služba pre vonkajšiu činnosť

EŠIF: európske štrukturálne a investičné fondy

EÚ: Európska únia

GDPR: všeobecné nariadenie o ochrane údajov

GR CONNECT: Generálne riaditeľstvo pre komunikačné siete, obsah a technológie

GR HOME: Generálne riaditeľstvo pre migráciu a vnútorné záležitosti

GR JUST: Generálne riaditeľstvo pre spravodlivosť a spotrebiteľov

HWPCI: horizontálna pracovná skupina pre kybernetické otázky

ICS: priemyselné kontrolné systémy

ISF – P: Fond pre vnútornú bezpečnosť – polícia

ISSB: riadiaci výbor pre informačnú bezpečnosť

JRC: Spoločné výskumné centrum

LISO: miestny úradník bezpečnosti informácií

MSP: malý a stredný podnik

NCIRC: tím pre spôsobilosť reakcie na počítačové incidenty NATO

PESCO: rámec stálej štruktúrovanej spolupráce

PZI: priame zahraničné investície

SBOP: spoločná bezpečnostná a obranná politika

smernica NIS: smernica o kybernetickej bezpečnosti

VKÚ: vnútroštátny kontrolný úrad

Glosár

Advér škodlivý softvér, ktorý zobrazuje reklamné nápisy alebo automaticky otvárané okná, ktorý obsahuje kód na sledovanie správania obetí na internete.

Bezpečnosť siete: podmnožina údajov na ochranu kybernetickej bezpečnosti odoslaných zo zariadení na tej istej sieti, ktorých cieľom je zabezpečiť, že nedôjde k zachyteniu alebo zmene informácií.

Botnet: sieť počítačov nakazených škodlivým softvérom a ovládaných na diaľku bez vedomia používateľov, ktorá sa používa na posielanie nevyžiadanej elektronickej pošty, krádež informácií alebo spustenie koordinovaných kybernetických útokov.

Cloud computing: poskytovanie zdrojov výpočtovej techniky na požiadanie, ako sú napríklad úložiská, výpočtové kapacity alebo kapacity na výmenu údajov, cez internet prostredníctvom poskytovania hostiteľských služieb na vzdialených serveroch.

Dezinformácia: overiteľne nepravdivá alebo zavádzajúca informácia, ktorá je vytvorená, prezentovaná a šírená na účely hospodárskeho zisku alebo zámerného zavádzania verejnosti a ktorá môže poškodiť verejný záujem.

Digitálny obsah: všetky údaje – ako je text, zvuk, obrázky alebo video – uložené v digitálnom formáte.

Distribuované odmietnutie služieb (útok DDoS): kybernetický útok, ktorý bráni oprávneným používateľom v prístupe k službe alebo zdrojom online tým, že túto službu či zdroj zaplaví takým množstvom požiadaviek, ktoré prevyšuje jej kapacity.

Dôvernosť: ochrana informácií, údajov alebo aktív pred neoprávneným prístupom alebo zverejnením.

Dôveryhodné služby: služby, ktoré zvyšujú platnosť elektronickej transakcie, ako sú elektronické podpisy, pečate, časové pečiatky, doručovacie služby pre registrované zásielky a autentifikácia webových sídiel.

Ekosystém kybernetickej bezpečnosti: komplexná komunita navzájom prepojených a komunikujúcich zariadení, údajov, sietí, osôb, procesov a organizácií a prostredie procesov a technológií, ktoré ovplyvňujú a podporujú túto vzájomnú prepojenosť a komunikáciu.

Hacktivista: jednotlivci alebo skupiny, ktoré získavajú neoprávnený prístup do informačných systémov alebo sietí s cieľom presadzovať sociálne alebo politické ciele.

Hybridná hrozba: prejav nepriateľského zámeru uskutočňovaný nepriateľmi s použitím kombinácie konvenčných a nekonvenčných metód boja (t. j. vojenských, politických, hospodárskych a technologických metód) v mocnom úsilí o dosiahnutie svojich cieľov.

Informačná bezpečnosť: skupina procesov a nástrojov, ktoré chránia fyzické a digitálne údaje pred neoprávneným prístupom, použitím, zverejnením, narušením, úpravou, zaznamenaním alebo zničením.

Integrita: ochrana proti nezákonnej úprave alebo zničeniu informácií a zaručenie ich pravosti.

Internet vecí: sieť každodenných predmetov vybavených elektronikou, softvérom a snímačmi, prostredníctvom ktorých môžu komunikovať a uskutočňovať výmenu údajov cez internet.

Kritická infraštruktúra: fyzické zdroje, služby a zariadenia, ktorých narušenie alebo zničenie budú mať závažný vplyv na fungovanie hospodárstva a spoločnosti.

Kryptomena: digitálny prostriedok, ktorý sa vydáva a vymieňa s použitím šifrovacích techník a nezávisle od centrálnej banky. Členovia virtuálneho spoločenstva ho prijímajú ako platobný prostriedok.

Kybernetická bezpečnosť: všetky bezpečnostné záruky a opatrenia prijaté na ochranu systémov IT a ich údajov proti neoprávnenému prístupu, útoku a poškodeniu, ktorých cieľom je zabezpečenie prístupnosti, dôvernosti a integrity údajov.

Kybernetická obrana: podmnožina kybernetickej bezpečnosti zameraná na obranu kybernetického priestoru vojenskými a inými primeranými prostriedkami s cieľom dosiahnuť vojensko-strategické ciele.

Kybernetická odolnosť: schopnosť zabrániť kybernetickým útokom a incidentom, pripraviť sa na ne, odolať im a zotaviť sa po nich.

Kybernetický incident: udalosť, ktorá priamo alebo nepriamo poškodzuje alebo ohrozuje odolnosť a bezpečnosť systému IT a údajov, ktoré sa v tomto systéme spracúvajú, ukladajú alebo prenášajú.

Kybernetický priestor: nehmotné globálne prostredie, v ktorom dochádza k online komunikácii medzi ľuďmi, softvérom a službami prostredníctvom počítačových sietí a technologických zariadení.

Kybernetický útok: pokus o oslabenie alebo zničenie dôvernosti, integrity a prístupnosti údajov alebo počítačového systému prostredníctvom kybernetického priestoru.

Malvér na vymazanie údajov: trieda malvéru, ktorého účelom je vymazanie pevného disku nakazeného počítača.

Malvér: škodlivý softvér. Počítačový program navrhnutý tak, aby poškodzoval počítače, servery alebo siete.

Model „zločin ako služba“: zločinný obchodný model, ktorý je motorom digitálneho tieňového hospodárstva a ktorý poskytuje široký okruh obchodných služieb a nástrojov umožňujúcich neodborným, začínajúcim páchateľom dopúšťať sa počítačovej kriminality.

Opravy: poskytnutie súboru zmien v softvéri alebo na jeho aktualizáciu, opravu alebo zlepšenie vrátane odstránenia bezpečnostných chýb.

Osobné údaje: informácie týkajúce sa identifikovateľnej osoby.

Phishing: metóda posielania elektronickej pošty, ktorá vyvoláva zdanie, že pochádza z dôveryhodného zdroja, s cieľom podvodom prinútiť prijímateľov k tomu, aby klikli na škodlivý hypertextový odkaz alebo poskytli svoje osobné údaje.

Počítačová kriminalita: rôzne trestné činnosti, pri ktorých sa počítače a systémy informačných technológií buď používajú ako primárne nástroje, alebo slúžia ako primárne ciele. Medzi tieto činnosti patria: tradičné trestné činy (napr. podvod, falšovanie a krádež totožnosti), trestné činy súvisiace s obsahom (napr. online distribúcia detskej pornografie alebo podnecovanie k rasovej nenávisti) a trestné činy špecifické pre počítače a informačné systémy (napr. útok na informačné systémy, odmietnutie služby a škodlivý softvér).

Pôvodný systém: zastaraný alebo nemoderný počítačový systém, aplikácia alebo programovací jazyk, ktorý sa stále používa, ku ktorému však už nemusia byť k dispozícii aktualizácie a podpora predajcu vrátane bezpečnostnej podpory.

Prístupnosť: zabezpečenie včasného a spoľahlivého prístupu k informáciám a ich používania.

Ransomvér: škodlivý softvér, ktorý obetiam bráni v prístupe do počítačového systému alebo znemožňuje čitateľnosť súborov, obvykle prostredníctvom šifrovania. Útočník následne zvyčajne obeť vydiera tým, že jej odmietne obnoviť prístup do chvíle, kým obeť nezaplatí výkupné.

Riadenie zraniteľnosti: neoddeliteľná súčasť počítačovej a sieťovej bezpečnosti na iniciatívne zmiernenie zneužitia chýb v systéme a softvéri alebo na zabránenie ich zneužitia prostredníctvom ich identifikácie, klasifikácie a nápravy.

Skimming: krádež údajov z kreditnej alebo debetnej bankovej platobnej karty pri ich zadávaní prostredníctvom internetu.

Sociálne inžinierstvo: v oblasti informačnej bezpečnosti ide o spôsob psychologickej manipulácie, ktorej cieľom je podvodom prinútiť ľudí k tomu, aby vykonali požadovanú akciu alebo prezradili informácie dôvernej povahy.

Súprava exploitov: druh súboru nástrojov, ktoré páchatelia počítačovej kriminality používajú na útok proti chybám v sieti a informačných systémoch, aby mohli rozširovať malvér alebo vykonávať iné škodlivé činnosti.

Šifrovanie: prevedenie čitateľných informácií na nečitateľný kód v záujme ochrany šifrovaných informácií. Na prečítanie informácií musí mať používateľ prístup k súkromnému kľúču alebo heslu.

Trestná činnosť umožnená počítačom: tradičná trestná činnosť spáchaná vo väčšom rozsahu s použitím systémov informačných technológií.

Trestná činnosť závislá od počítača: trestná činnosť, ktorú možno spáchať iba s použitím zariadení informačných technológií.

Údaje o prístupe: informácie o prihlásení sa používateľa do služby a odhlásení sa z nej, ako je čas, dátum a IP adresa.

Vektorizácia textu: proces premeny slov, viet alebo celých dokumentov na číselné vektory tak, aby ich mohli využiť algoritmy strojového učenia.

Volebná infraštruktúra: patria sem informačné systémy a databázy kampaní, citlivé informácie o kandidátoch, systémy na registráciu voličov a systémy riadenia.

[1] V návrhu aktu EÚ o kybernetickej bezpečnosti bol tento pojem vymedzený ako „všetky činnosti potrebné na ochranu sietí a informačných systémov, ich používateľov a dotknutých osôb pred kybernetickými hrozbami“. Prijatie aktu Európskym parlamentom a Radou sa očakáva začiatkom roku 2019.

[2] Europol, *Hodnotenie hrozieb internetovej organizovanej trestnej činnosti za rok 2017*.

[3] Európska organizácia kybernetickej bezpečnosti (ECSO), *European Cybersecurity Industry Proposal for a contractual Public-Private Partnership* (Návrh európskeho odvetvia kybernetickej bezpečnosti na vytvorenie zmluvného verejno-súkromného partnerstva), jún 2016.

[4] Európsky parlament, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses* (Kybernetická bezpečnosť v Európskej únii a za jej hranicami: preskúmanie hrozieb a politických reakcií), štúdia pre výbor LIBE, september 2015.

[5] ENISA, *ENISA Threat Landscape Report 2017* (Správa ENISA o štruktúre hrozieb za rok 2017), 18. januára 2018.

[6] Europol, *Hodnotenie hrozieb internetovej organizovanej trestnej činnosti za rok 2018*.

[7] Europol, *tamže*, 2018.

[8] European Centre for Political Economy, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?* (Európske centrum pre politickú ekonómiu: „Krádež nápadov: povolí sa kybernetická špionáž na spomalenie Európy v globálnych pretekoch o konkurencieschopnosť priemyslu?“), Occasional Paper č. 2/18, február 2018.

[9] Európska komisia, Správa predsedu Komisie o stave Únie za rok 2017.

[10] Europol, *World’s Biggest Marketplace selling internet paralysing DDoS attacks taken down* (Zrušenie najväčšieho svetového trhu predávajúceho útoky DDoS, ktoré paralyzujú internet), tlačová správa, 25. apríla 2018.

[11] Europol, *Hodnotenie hrozieb internetovej organizovanej trestnej činnosti za rok 2017*.

[12] Prehľad Európskej komisie v oblasti kybernetickej bezpečnosti, september 2017.

[13] Medzi tieto náklady patrí: strata príjmu, náklady na opravu poškodených systémov, možné dlhy vyplývajúce z ukradnutého majetku alebo informácií, stimuly na udržanie zákazníkov, vyššie poistné, vyššie náklady na ochranu (nové systémy, zamestnanci, odborná príprava), možné vyrovnanie nákladov na dodržiavanie predpisov alebo súdny spor.

[14] NTT Security, *Risk:Value 2018 Report*.

[15] Ransomvér *WannaCry* využíval chyby v protokole operačného systému Microsoft Windows, ktoré umožňovali prevziať na diaľku kontrolu nad akýmkoľvek počítačom. Spoločnosť Microsoft po odhalení chyby vydala opravu. Doteraz však neboli aktualizované stovky tisícok počítačov a mnoho z nich bolo neskôr infikovaných. Zdroj: A. Greenberg, *Hold North*

Korea Accountable For WannaCry — and the NSA, too (Za WannaCry sa musí zodpovedať Severná Kórea – ale aj NSA), WIRED, 19. decembra 2017.

[16] Európska komisia, *Europeans' attitudes towards cybersecurity* (Postoje Európanov ku kybernetickej bezpečnosti), Špeciálny Eurobarometer 464a, september 2017. Zverejnenie nadväzujúceho prieskumu sa očakáva začiatkom roku 2019.

[17] Budapeštiansky dohovor je záväzné medzinárodné usmernenie pre krajiny, ktoré vypracúvajú právne predpisy na boj proti počítačovej kriminalite. Dohovor poskytuje rámec medzinárodnej spolupráce medzi zmluvnými štátmi. Európsku úniu v súčasnosti zastupuje Komisia, Rada Európskej únie, Europol, ENISA a Eurojust.

[18] Európska komisia, *Stratégia kybernetickej bezpečnosti Európskej únie: Otvorený, bezpečný a chránený kybernetický priestor*, JOIN(2013) 1 final, 7. februára 2013.

[19] Európska komisia, *Európsky program v oblasti bezpečnosti*, COM(2015) 185 final, 28. apríla 2015.

[20] Európska komisia, *Stratégia pre jednotný digitálny trh v Európe*, COM(2015) 192 final, 6. mája 2015.

[21] ESVČ, *Spoločná vízia, spoločný postup: silnejšia Európa. Globálna stratégia pre zahraničnú a bezpečnostnú politiku Európskej únie*, jún 2016.

[22] Centrum pre európske politické štúdie, *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force* (Posilnenie spôsobilostí EÚ v oblasti kybernetickej obrany – Správa osobitnej skupiny CEPS), november 2018.

[23] Malvér, ktorý bol zdrojom útokov prostredníctvom ransomvéru WannaCry, za ktorých pôvodcu Spojené štáty, Spojené kráľovstvo a Austrália označili Severnú Kóreu, pôvodne vyvinula americká Národná bezpečnostná agentúra, ktorá zhromažďovala údaje o chybách v operačnom systéme Windows s cieľom využiť tieto nedostatky. Zdroj: A. Greenberg, Hold North Korea Accountable For WannaCry — and the NSA, too, WIRED, 19. decembra 2017. Hneď po útokoch Microsoft odsúdil zhromažďovanie chýb v softvéri zo strany vlád a zopakoval svoju výzvu na prijatie digitálneho ženevského dohovoru.

[24] Popri zemi, mori, vzduchu a vesmíre.

[25] Politický rámec EÚ pre kybernetickú obranu (aktualizácia za rok 2018), 14413/18, 19. novembra 2018.

[26] Európska komisia/Európska služba pre vonkajšiu činnosť, *Spoločný rámec pre boj proti hybridným hrozbám: reakcia Európskej únie*, JOIN(2016) 18 final, 6. apríla 2016.

[27] Spoločné vyhlásenie predsedu Európskej rady, predsedu Európskej komisie a generálneho tajomníka Organizácie Severoatlantickej zmluvy, 8. júla 2016 a 10. júla 2018.

[28] Európska komisia/Európska služba pre vonkajšiu činnosť, *Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ*, JOIN(2017) 450 final, 13. septembra 2017.

[29] Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016, s. 1).

[30] Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.

[31] Tieto tímy sú začlenené do štruktúr spolupráce zriadených na základe smernice, do siete jednotiek CSIRT (sieť tvorená určenými jednotkami CSIRT členských štátov EÚ a tímom CERT-EU; sekretariát zabezpečuje agentúra ENISA) a do skupiny pre spoluprácu (ktorá podporuje a uľahčuje strategickú spoluprácu a výmenu informácií medzi členskými štátmi a ktorej sekretariát zabezpečuje Komisia).

[32] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

[33] Európska komisia, *Návrh nariadenia Európskeho parlamentu a Rady o Agentúre EÚ pre kybernetickú bezpečnosť (ENISA), o zrušení nariadenia (EÚ) č. 526/2013 a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií („akt o kybernetickej bezpečnosti“)*, COM(2017) 477 final, 13. septembra 2017.

[34] Európska komisia, *Návrh nariadenia Európskeho parlamentu a Rady o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach*, COM(2018) 225 final, 17. apríla 2018.

[35] Európska komisia, *Návrh smernice Európskeho parlamentu a Rady, ktorou sa stanovujú harmonizované pravidlá určovania právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní*. COM(2018) 226 final, 17. apríla 2018.

[36] Európska komisia, *Návrh nariadenia Európskeho parlamentu a Rady, ktorým sa zriaďuje Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier,* COM(2018) 630 final, 12. septembra 2018.

[37] H. Carrapico a A. Barrinha, *The EU as a Coherent (Cyber)Security Actor?* [EÚ ako súdržný aktér v oblasti (kybernetickej) bezpečnosti], Journal of Common Market Studies, zv. 55, č. 6, 2017.

[38] Európska komisia, tamže, SWD(2017) 295 final, 13. septembra 2017.

[39] Výskumná služba Európskeho parlamentu, *Transatlantic cyber-insecurity and cybercrime. Economic impact and future prospects* (Nedostatočná kybernetická bezpečnosť a počítačová kriminalita v transatlantických vzťahoch. Vplyv na hospodárstvo a vyhliadky do budúcnosti), PE 603.948, december 2017.

[40] ENISA, *An evaluation framework for Cyber Security Strategies* (Rámec pre hodnotenie stratégií kybernetickej bezpečnosti), 27. novembra 2014.

[41] Výnimkou je článok 14 („Monitorovanie a štatistika“) smernice Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV.

[42] Európsky hospodársky a sociálny výbor, *Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks* (Kybernetická bezpečnosť: zabezpečenie informovanosti a odolnosti súkromného sektora v celej Európe zoči-voči zvyšujúcim sa kybernetickým rizikám), marec 2018. Osobitná skupina CEPS-ECRI, Cybersecurity in Finance: Getting the policy mix right! (Kybernetická bezpečnosť v oblasti finančníctva: správne nastavenie súboru politík), jún 2018.

[43] Odpovede na otázky prieskumu poslalo 24 z 28 vnútroštátnych kontrolných úradov.

[44] To znamená, že je založený na zásadách a z technologického hľadiska čo najviac neutrálny.

[45] Mechanizmus vedeckého poradenstva Európskej komisie, Vedecké stanovisko č. 2/2017, 24. marca 2017.

[46] L. Rebuffi, *EU Digital Autonomy: A possible approach* (Digitálna autonómia EÚ: možný prístup), Digma Zeitschrift für Datenrecht und Informationssicherheit, september 2018. European Centre for Political Economy, tamže, Occasional Paper č. 2/18, február 2018.

[47] Európska komisia, *Návrh smernice Európskeho parlamentu a Rady o určitých aspektoch týkajúcich sa zmlúv o dodávaní digitálneho obsahu*, COM(2015) 634 final, 9. decembra 2015.

[48] Európska komisia, *Návrh smernice Európskeho parlamentu a Rady o určitých aspektoch týkajúcich sa zmlúv o online a iných predajoch tovaru na diaľku*, COM(2015) 635 final, 9. decembra 2015.

[49] Holandská Rada pre kybernetickú bezpečnosť, *European Foresight Cyber Security Meeting 2016: Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care* (Európske stretnutie pre obozretnosť v oblasti kybernetickej bezpečnosti 2016: Verejno-súkromné teoretické odporúčania Európskej komisii týkajúce sa internetu vecí a harmonizácie povinností náležitej starostlivosti), 2016.

[50] Centrum pre európske politické štúdie, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges – Report of a CEPS Task Force* (Zverejňovanie informácií o zraniteľnosti softvéru v Európe: technologické, politické a právne problémy – Správa osobitnej skupiny CEPS), jún 2018.

[51] Európska komisia, *Čo najlepšie využívanie sietí a informačných systémov – smerom k účinnej implementácii smernice 2016/1148/EÚ, pokiaľ ide o opatrenia na dosiahnutie vysokej všeobecnej úrovne bezpečnosti sietí a informačných systémov v EÚ*, COM(2017) 476 final/2, 4. októbra 2017.

[52] Europol, tamže, 2017.

[53] Rada Európskej únie, *Záverečná správa o 7. kole vzájomných hodnotení s názvom „Praktické vykonávanie a uplatňovanie európskych politík v oblasti predchádzania počítačovej kriminalite a boja proti nej“*, 12711/1/17 REV 1, 9. októbra 2017.

[54] Európska komisia, Posúdenie vplyvu, sprievodný dokument k návrhu smernice o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich falšovaniu, SWD(2017) 298 final, 13. septembra 2017. Politickú dohodu o novom právnom predpise sa podarilo dosiahnuť v decembri 2018 a jeho prijatie sa očakáva začiatkom roku 2019.

[55] Europol, tamže, 2017.

[56] C-362/14: Maximillian Schrems proti Data Protection Commissioner (Írsko), 6. októbra 2015.

[57] Europol/Eurojust, *Common challenges in combating cybercrime* (Spoločné prekážky boja proti počítačovej kriminalite), 7021/17, 13. marca 2017.

[58] Európska komisia, *Posúdenie stratégie kybernetickej bezpečnosti EÚ z roku 2013*, SWD(2017) 295 final, 13. septembra 2017.

[59] Výskumná služba Európskeho parlamentu, *Briefing: EU Legislation in Progress – Review of dual-use export controls* (Informačný dokument: Pokrok v oblasti právnych predpisov EÚ – Preskúmanie kontrol vývozu položiek s dvojakým použitím), *PE589.832*.

[60] Uznesenie Európskeho parlamentu *Ľudské práva a technológie: vplyv systémov neoprávneného vniknutia a sledovania na ľudské práva v tretích krajinách*, [2014/2232(INI)], 8. septembra 2015. Položky a služby s dvojakým použitím, medzi ktoré patrí softvér a technológie, môžu mať civilné a vojenské použitie.

[61] Verejne dostupné informácie sa uchovávajú v databáze WHOIS, ktorú spravuje organizácia ICANN (Internetová korporácia pre prideľovanie mien a čísel). Táto organizácia spravuje systém názvov domén. Nesprávne používanie názvov domén uľahčuje počítačovú kriminalitu.

[62] Článok 3 smernice NIS.

[63] Atlantic Council, *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures* (Riziko – súvislosti: Zdolaní kybernetickými rizikami? Hospodárske úžitky a náklady alternatívnych možností kybernetickej budúcnosti), 10. septembra 2015.

[64] Biely dom, *Cybersecurity spending fiscal year 2019* (Výdavky na kybernetickú bezpečnosť vo finančnom roku 2019).

[65] Európska komisia, *Pracovný dokument útvarov Komisie: Posúdenie vplyvu, sprievodný dokument k „návrhu nariadenia Európskeho parlamentu a Rady, ktorým sa stanovuje program Digitálna Európa na obdobie 2021 – 2027“*, SWD(2018) 305 final, 6. júna 2018.

[66] The Hague Centre for Strategic Studies, *Dutch investments in ICT and cybersecurity: putting it in perspective* (Holandské investície do IKT a kybernetickej bezpečnosti: uvedenie do súvislostí), december 2016.

[67] Európska komisia, tamže, COM(2018) 630 final, 12. septembra 2018.

[68] Oddelenie vedeckej predikcie výskumnej služby Európskeho parlamentu, *Achieving a sovereign and trustworthy ICT industry in the EU* (Dosiahnutie nezávislého a dôveryhodného odvetvia IKT v EÚ), december 2017.

[69] European Digital SME Alliance, *Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem* (Pozičný dokument o európskej stratégii kybernetickej bezpečnosti: podpora rozvoja ekosystému MSP), 31. júla 2017.

[70] Oddelenie vedeckej predikcie výskumnej služby Európskeho parlamentu, Achieving a sovereign and trustworthy ICT industry in the EU, december 2017.

[71] Tamže.

[72] Európska komisia, *Posúdenie vplyvu týkajúce sa navrhovaného centra výskumných kompetencií a siete národných koordinačných centier*, SWD(2018) 403 final (časť 1/4), 12. septembra 2018.

[73] Európska komisia, tamže, COM(2018) 630 final, 12. septembra 2018.

[74] Osobitná správa Európskeho dvora audítorov č. 13/2018: „Riešenie radikalizácie, ktorá vedie k terorizmu".

[75] Hodnoty uvádzané v tomto oddiele pochádzajú z verejne dostupných dokumentov Komisie s výnimkou údaja 42 mil. EUR v bode ***51***, ktorý nám Komisia poskytla priamo.

[76] Program Horizont 2020 je program EÚ pre výskum a inovácie s rozpočtom 80 mld. EUR, prostredníctvom ktorého sa podporuje iniciatíva Inovácia v Únii zameraná na zaistenie konkurencieschopnosti EÚ vo svete.

[77] Spoločenská výzva 7 programu Horizont 2020 „Bezpečné a inovatívne spoločnosti – ochrana slobody a bezpečnosti Európy a jej občanov".

[78] Analyzovali sme projekty Horizont 2020 zo súboru údajov CORDIS. Pri každom opise projektu sme vykonali vektorizáciu textu s použitím taxonómie pre kybernetickú bezpečnosť Spoločného výskumného centra (JRC) (pozri ***rámček 5*** v ďalšej kapitole), aby sme určili projekty, ktoré by mohli súvisieť s kybernetickou bezpečnosťou. Výsledky sme potom ručne overili a analyzovali.

[79] Európska organizácia kybernetickej bezpečnosti, *ECS cPPP Progress Monitoring Report 2016-2017* (Správa o monitorovaní pokroku zmluvného verejno-súkromného partnerstva v rámci európskej stratégie kybernetickej bezpečnosti), 29. októbra 2018.

[80] Článok 9 ods. 2 smernice NIS, tamže.

[81] GLACY+ (Globálny boj proti počítačovej kriminalite+) je spoločný projekt s Radou Európy. Projekt podporuje dvanásť krajín v Afrike, Ázii a Tichomorí a v Latinskej Amerike a Karibskej oblasti, ktoré zas môžu slúžiť ako centrá na sprostredkovanie svojich skúseností vo svojich príslušných regiónoch.

[82] Európske centrum politickej stratégie (EPSC), expertná skupina Komisie, vznieslo pripomienku týkajúcu sa rizika „digitálnej slepej škvrny", ktorá vznikne, ak sa rozdiel medzi EÚ a jej susedmi zo západného Balkánu bude naďalej zväčšovať. Krajiny ako Čína a Rusko investujú v regióne značné sumy, čo hrozí marginalizáciou EÚ ako aktéra v kybernetickej oblasti v regióne. Zdroj: EPSC, *Engaging with the Western Balkans: an investment in Europe's security* (Spolupráca s krajinami západného Balkánu: investícia do bezpečnosti Európy), 17. mája 2018.

[83] Európska investičná banka, *The EIB Group Operating Framework and Operational Plan 2018* (Operačný rámec a operačný plán skupiny EIB na rok 2018), 12. decembra 2017. V čase vzniku tohto dokumentu neboli k dispozícii žiadne ďalšie informácie.

[84] Európska komisia, *Návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovuje program Digitálna Európa na obdobie 2021 – 2027*, COM(2018) 434 final, 6. júna 2018.

[85] Európska komisia, *Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1092 z 18. júla 2018, ktorým sa zriaďuje Program rozvoja európskeho obranného priemyslu zameraný na podporu konkurencieschopnosti a inovačnej kapacity obranného priemyslu Únie* (Ú. v. EÚ L 200, 7.8.2018, s. 30). Okrem toho v roku 2017 bola vytvorená prípravná akcia pre výskum v oblasti obrany v celkovej hodnote 90 mil. EUR na roky 2017 – 2019, ktorá je financovaná z programu Horizont 2020. Nie je jasné, či táto suma zahŕňa výdavky spojené s kybernetickou bezpečnosťou.

[86] Na rok 2019 je naplánované zverejnenie samostatného informačného dokumentu Európskeho dvora audítorov o obrane EÚ.

[87] Centrum EC3 pri Europole, agentúra ENISA, ESVČ, Európska obranná agentúra a CERT-EU majú spoločne 159 zamestnancov. Tento súčet neobsahuje zamestnancov zaoberajúcich sa oblasťou kybernetickej bezpečnosti v Európskej komisii alebo v členských štátoch. Zdroj: Centrum pre európske politické štúdie, tamže, november 2018.

[88] *Hodnotenie agentúry ENISA*, 2017.

[89] Europol vo svojom viacročnom pláne na roky 2018 – 2020 požiadal o ročné zvýšenie počtu zamestnancov o 70 dočasných zamestnancov, na rok 2018 však bolo schválené zvýšenie iba o 26 pracovníkov. V ďalšom návrhu viacročného plánu na roky 2019 – 2021 Europol počíta s miernym zvýšením „a predpokladá, že vyššej požiadavke zdrojov by sa nevyhovelo“. Zdroj: Konzultácie o návrhu viacročného plánovania na roky 2019 – 2021, predloženého spoločnej parlamentnej kontrolnej skupine, A 000834, 1. februára 2018.

[90] *Hodnotenie agentúry ENISA*, 2017. V rokoch 2014 – 2016 sa približne 80 % prevádzkového rozpočtu agentúry ENISA použilo na obstarávanie štúdií.

[91] ENISA, *Exploring the opportunities and limitations of current Threat Intelligence Platforms* (Preskúmanie možností a obmedzení súčasných platforiem pre spravodajské informácie o hrozbách), december 2017.

[92] ISACA (predtým známa ako Asociácia auditu a kontroly informačných systémov), *Information Security Governance: Guidance for Boards of Directors and Executive Management* (Správa informačnej bezpečnosti: usmernenie pre predstavenstvá a výkonný manažment), 2. vyd., 2006.

[93] EY, *Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017* (Znovu získaná kybernetická bezpečnosť: príprava na boj proti kybernetickým útokom. 20. globálny prieskum informačnej 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 či mýtus? Pochopenie skutočných nákladov a dosahu programov kybernetickej bezpečnosti), júl 2017.

[95] Komisia pre burzu a cenné papiere, *Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures* (Výklad a vysvetľujúce usmernenie o zverejňovaní informácií spojených kybernetickou bezpečnosťou verejnými spoločnosťami), 21. februára 2018.

[96] Fórum pre spoluprácu medzi Európskym orgánom pre bankovníctvo, Európskym orgánom pre cenné papiere a trhy a Európskym orgánom pre poisťovníctvo a dôchodkové poistenie zamestnancov.

[97] Európsky orgán pre cenné papiere a trhy, *Joint Committee report on risks and vulnerabilities in the EU financial system* (Správa spoločného výboru o rizikách a zraniteľných miestach vo finančnom systéme EÚ), apríl 2018.

[98] ENISA, *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in SMEs* (Štandardy informačnej bezpečnosti a ochrany súkromia pre MSP: odporúčania na zvýšenie prijatia štandardov informačnej bezpečnosti a ochrany súkromia v MSP), december 2015.

[99] Mechanizmus vedeckého poradenstva Komisie so zreteľom na členské štáty EÚ upozornil na „značnú a jedinečnú mieru zhody, pokiaľ ide o základné zásady a hodnoty, ako aj na spoločný strategický záujem, ktorý môže tvoriť základ účinného riadenia kybernetickej bezpečnosti EÚ“. Zdroj: Vedecké stanovisko č. 2/2017, 24. marca 2017.

[100] Spojené štáty americké, Čína, Japonsko, Južná Kórea, India a Brazília.

[101] Európska akadémia bezpečnosti a obrany (T. Renard a A. Barrinha), *Handbook on cyber security, chapter 3.4 The EU as a partner in cyber diplomacy and defence* (Príručka kybernetickej bezpečnosti, kapitola 3.4 EÚ ako partner v oblasti kybernetickej diplomacie a obrany), 23. novembra 2018.

[102] Rada Európskej únie, *Akčný plán, ktorým sa vykonávajú závery Rady o spoločnom oznámení Európskemu parlamentu a Rade: Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ*, 15748/17, 12. decembra 2017.

[103] Európska komisia, *Digitálna stratégia Európskej komisie: Komisia po digitálnej transformácii, zameraná na používateľov a orientovaná na údaje*, C(2018) 7118 final, 21. novembra 2018.

[104] Odpoveď komisárky Gabrielovej na písomnú parlamentnú otázku (E-004294-17), 28. júna 2017.

[105] Rada Európskej únie, *Výročná správa o vykonávaní politického rámca pre kybernetickú obranu*, 15870/17, 19. decembra 2017.

[106] Bezpečnosť komunikačných a informačných systémov Komisie sa riadi rozhodnutiami (EÚ, Euratom) 2015/443, (EÚ, Euratom) 2015/444 a (EÚ, Euratom) 2017/46. Rozhodnutím Komisie C(2018) 7706 z 21. novembra 2018 sa zriaďuje rada pre informačné technológie a kybernetickú bezpečnosť, ktorá vznikla spojením bývalej rady pre informačné technológie a riadiaceho výboru pre informačnú bezpečnosť.

[107] Európsky hospodársky a sociálny výbor, tamže, marec 2018.

[108] Európsky parlament, tamže, september 2015.

[109] Stredisko EÚ pre hybridné hrozby bolo zriadené v roku 2016 v rámci Spravodajského a situačného centra EÚ Európskej služby pre vonkajšiu činnosť. Stredisko prijíma a analyzuje utajované informácie a informácie z otvorených zdrojov od rôznych zainteresovaných strán týkajúce sa hybridných hrozieb.

[110] ENISA, *National-level Risk Assessments: An Analysis Report* (Posúdenie rizika na vnútroštátnej úrovni: analytická správa), november 2013.

[111] Európska komisia, *Posúdenie vplyvu Agentúry EÚ pre kybernetickú bezpečnosť a aktu o kybernetickej bezpečnosti*, SWD(2017) 500 final (časť 1/6), 13. septembra 2017.

[112] Európska komisia, tamže, SWD(2018) 403 final, 12. septembra 2018.

[113] Résaux IP Européens Network Coordination Centre, regionálny internetový register pre Európu, ktorý dohliada na prideľovanie a registráciu zdrojov internetových čísel.

[114] ENISA, *EISAS Large-Scale Pilot Collaborative Awareness Raising for EU Citizens & SMEs* (Rozsiahle pilotné zvyšovanie informovanosti občanov EÚ a MSP v rámci systému EISAS založené na spolupráci), november 2012.

[115] The Centre for Cyber Safety and Education v spolupráci s Booz Allen Hamilton, Alta Associates a Frost & Sullivan, *2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk* (Štúdia o celosvetovej pracovnej sile v odvetví bezpečnosti informácií z roku 2017 – Referenčné porovnávanie spôsobilosti a reakcií pracovníkov na kybernetické riziká).

[116] Európsky hospodársky a sociálny výbor, tamže, marec 2018.

[117] Snemovňa lordov, Dolná snemovňa, *Spoločný výbor pre národnú bezpečnostnú stratégiu, Zručnosti v oblasti kybernetickej bezpečnosti a národná kritická infraštruktúra Spojeného kráľovstva, Druhá správa za obdobie 2017 – 2019*, 16. júla 2018.

[118] Europol/Eurojust, *Common challenges in combating cybercrime* (Spoločné prekážky boja proti počítačovej kriminalite), 7021/17, 13. marca 2017.

[119] Europol/Eurojust, tamže, 7021/17, 13. marca 2017.

[120] Európska komisia, tamže, SWD(2018) 403 final, 12. septembra 2018.

[121] CEPOL, *Decision of the Management Board 33/2018/MB on the CEPOL Single Programming Document 2020-2022* (Rozhodnutie správnej rady 33/2018/MB o jednotnom programovom dokumente na roky 2020 – 2022), 20. novembra 2018.

[122] Napríklad spolupráca medzi ESVČ, členskými štátmi, agentúrami a orgánmi, ako sú CEPOL, ECTEG alebo EABO.

[123] ENISA, *Stock-taking of information security training needs in critical sectors* (Hodnotenie potrieb odbornej prípravy v oblasti informačnej bezpečnosti v kľúčových odvetviach), december 2017.

[124] Európska skupina pre vzdelávanie a odbornú prípravu v oblasti boja proti počítačovej kriminalite.

[125] Európska komisia, Trinásta správa o pokroku dosiahnutom pri budovaní účinnej a skutočnej bezpečnostnej únie, COM(2018) 46 final, 24. januára 2018.

[126] Na základe pripomienok v osobitnej správe č. 14/2018, tamže.

[127] Uznesenie Európskeho parlamentu z 13. júna 2018 o kybernetickej obrane [2018/2004(INI)]. Rada Európskej únie, tamže, 15870/17, 19. decembra 2017.

[128] Švajčiarsko, bývalá Juhoslovanská republika Macedónsko, Ukrajina, Bosna a Hercegovina, Kosovo (týmto označením nie sú dotknuté pozície k štatútu a označenie je v súlade s rezolúciou Bezpečnostnej rady OSN č. 1244/1999 a so stanoviskom Medzinárodného súdneho dvora k vyhláseniu nezávislosti Kosova), Turecko a Spojené štáty americké.

[129] Europol, *Hodnotenie hrozieb internetovej organizovanej trestnej činnosti za rok 2018*.

[130] Európska komisia, tamže, SWD(2017) 295 final, 13. septembra 2017.

[131] B. Stanton, M. F. Theofanos, S. S. Prettyman a S. Furman, *Security Fatigue* (Únava z bezpečnosti), IT Professional, ročník 18, č. 5, 2016, s. 26 – 32. Pozri aj NIST.

[132] Európska komisia/Európska služba pre vonkajšiu činnosť, *Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby*, JOIN(2018) 16 final, 13. júna 2018.

[133] Napríklad uzavretie trhov AlphaBay a Hansa pri spoločnej operácii, ktorú viedla FBI a holandská štátna polícia s podporou Europolu. Išlo o dva najväčšie trhy na obchodovanie s nezákonným tovarom, ako sú drogy, strelné zbrane a nástroje na počítačovú kriminalitu, ako je malvér. Zdroj: Europol, *Crime on the Dark Web: Law Enforcement coordination is the only cure* (Zločin na temnom webe: koordinácia činností orgánov presadzovania práva je jediný liek), tlačová správa, 29. mája 2018.

[134] Rada Európskej únie, tamže, 12711/1/17 REV 1, 9. októbra 2017.

[135] Európska komisia, tamže, SWD(2018) 403 final, 12. septembra 2018.

[136] Európska komisia, tamže, SWD(2017) 295 final, 13. septembra 2017.

[137] Európska komisia/Európska služba pre vonkajšiu činnosť, tamže, JOIN(2018) 16, 13. júna 2018.

[138] Európska komisia, SWD (2017) 500 final, 13. septembra 2017.

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

[140] Európska komisia, Výzva na predloženie ponuky: *Zriadenie a prevádzka skúšobnej siete kompetenčných centier kybernetickej bezpečnosti s cieľom vypracovať a realizovať spoločný plán výskumu a inovácií v oblasti kybernetickej bezpečnosti*, 27. októbra 2017.

[141] Jean-Claude Juncker, Poverovací list komisárovi pre bezpečnostnú úniu, 2. augusta 2016. Obrana nepatrí do právomoci osobitnej skupiny.

[142] Rada Európskej únie, *Plán stratégie kybernetickej bezpečnosti EÚ*, 8901/17, 11. mája 2017.

[143] Friends of Europe, *Debating Security Plus: Crowdsourcing solutions to the world's security issues (Debating Security Plus: Crowdsourcingové riešenia problémov svetovej bezpečnosti), 5. vyd.*, november 2017.

[144] Technické správy Spoločného výskumného centra, Mapa európskych centier odborných znalostí v oblasti kybernetickej bezpečnosti: *Vymedzenie pojmov a taxonómia.*

Posúdenie vplyvu týkajúce sa navrhovaného centra výskumných kompetencií a siete národných koordinačných centier, SWD(2018) 403 final, 12. septembra 2018.

[145] Európska komisia, tamže, SWD(2017) 295 final, 13. septembra 2017.

[146] Európska komisia, tamže, SWD(2018) 403 final, 12. septembra 2018.

[147] Napríklad stredisko pre výmenu a analýzu informácií európskych finančných inštitúcií zahŕňa zástupcov finančného sektora, vnútroštátnych tímov CERT, agentúr presadzovania práva, agentúry ENISA, Europolu, Európskej centrálnej banky, Európskej platobnej rady a Európskej komisie.

[148] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models* [Strediská pre výmenu a analýzu informácií (ISAC) – Modely spolupráce], 14. februára 2018.

[149] Rada Európskej únie, tamže, 12711/1/17 REV 1, 9. októbra 2017.

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

[151] Zo štúdie spoločnosti Accenture z roku 2018 vykonanej v 15 krajinách vyplynulo, že sa zabránilo 87 % zameraných kybernetických útokov: *2018 State of Cyber Resilience* (Stav kybernetickej odolnosti za rok 2018), 10. apríla 2018.

[152] P. Timmers, *Cybersecurity is Forcing a Rethink of Strategic Autonomy* (Kybernetická bezpečnosť núti prehodnotiť strategickú autonómiu), Oxford University Politics Blog, 14. septembra 2018.

[153] Caroline Preece, *Three reasons why cyber threat detection is still ineffective* (Tri dôvody, prečo je odhaľovanie kybernetických hrozieb stále neúčinné), IT Pro, 14. júla 2017.

[154] Európsky hospodársky a sociálny výbor, *tamže*, marec 2018.

[155] Európska komisia, *Ôsma správa o pokroku na ceste k účinnej a skutočnej bezpečnostnej únii*, COM(2017) 354 final, 29. júna 2017.

[156] Pozri rozličné publikácie skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti.

[157] Druhá smernica o platobných službách: smernica (EÚ) 2015/2366 o platobných službách na vnútornom trhu; ECB/SSM: Európska centrálna banka/jednotný mechanizmus dohľadu; TARGET2: Transeurópsky automatizovaný expresný systém hrubého zúčtovania platieb v reálnom čase (2. generácia), nariadenie (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu. Zdroj: Osobitná skupina CEPS-ECRI, tamže, jún 2018.

[158] Európska komisia, *Odporúčanie o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu*, C(2017) 6100 final, 13. septembra 2017.

[159] Európska komisia, tamže, SWD(2017) 295 final, 13. septembra 2017. Existuje niekoľko mechanizmov krízového riadenia, ako sú mechanizmus integrovanej politickej reakcie na krízu (IPCR), Argus (mechanizmus Komisie pre reakciu na krízu), krízový reakčný

mechanizmus ESVČ, mechanizmus Únie v oblasti civilnej ochrany a protokol reakcie na núdzové situácie v oblasti presadzovania práva EÚ.

[160] Navyše by to mohlo dať podnet aj na aktiváciu článku 42 ods. 7 Zmluvy o Európskej únii (doložka o vzájomnej pomoci) alebo článku 222 Zmluvy o fungovaní Európskej únie (doložka o solidarite).

[161] Európska komisia/Európska služba pre vonkajšiu činnosť, tamže, JOIN(2018) 16, 13. júna 2018. V decembri 2018 sa v médiách objavila správa o údajnom napadnutí diplomatickej komunikačnej siete ESVČ – COREU – [zdroj: *New York Times, Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran* (Ukradnuté diplomatické depeše odhaľujú svet plný úzkosti z Trumpa, Ruska a Iránu); 18. decembra 2018]. Incident sa stále vyšetruje.

[162] Ďalší rozvoj potrebuje aj spolupráca v oblasti včasných varovaní a vzájomnej pomoci: *Závery Rady o koordinovanej reakcii EÚ na kybernetické bezpečnostné incidenty a krízy veľkého rozsahu*, 10085/18, 26. júna 2018.

[163] Výskumná služba Európskeho parlamentu, *Briefing EU Legislation in Progress: ENISA and a new cybersecurity act* (Informačný dokument: Pokrok v oblasti právnych predpisov: Agentúra ENISA a nový akt o kybernetickej bezpečnosti), PE 614.643, september 2018.

[164] Európsky hospodársky a sociálny výbor, tamže, marec 2018.

[165] Rada Európskej únie, *Protokol reakcie na núdzové situácie v oblasti presadzovania práva EÚ (LE ERP) pre rozsiahle cezhraničné kybernetické útoky*, 14893/18, december 2018.

[166] Tímy rýchlej kybernetickej reakcie a vzájomná pomoc v oblasti kybernetickej bezpečnosti; platforma na výmenu informácií v oblasti reakcie na kybernetické hrozby a incidenty. Zdroj: Rada Európskej únie, *Stála štruktúrovaná spolupráca (PESCO), aktualizovaný zoznam projektov PESCO – Prehľad*, 19. novembra 2018.

[167] Rada Európskej únie, Závery o rámci pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti, 9916/17, 7. júna 2017.

[168] Rada Európskej únie, *Závery Rady o kybernetickej diplomacii*, 6122/55, 11. februára 2015.

[169] Rada Európskej únie, *Návrh vykonávacích usmernení pre rámec pre spoločnú diplomatickú reakciu na škodlivé kybernetické činnosti*, 13007/17.

[170] Pridelenie zodpovednosti za incident zostáva zvrchovaným politickým rozhodnutím členských štátov a nie všetky opatrenia súboru nástrojov si vyžadujú jej pridelenie.

[171] Použitie súboru nástrojov neviedlo k jednotnej akcii, jednotlivé členské štáty prijali pozíciu Spojených štátov amerických.

[172] Rada Európskej únie, *Závery o škodlivých kybernetických činnostiach*, 7925/18, 16. apríla 2018.

[173] Počítačové systémy používané na kontrolu procesov v rozmanitých priemyselných odvetviach, ako sú verejné služby, chemická a priemyselná výroba, potravinárstvo, dopravné systémy a uzly a logistické služby.

[174] ENISA, tamže, december 2017.

[175] Napríklad verejná správa, chemický a jadrový priemysel, spracovateľský priemysel, potravinárstvo, cestovný ruch, logistika a civilná ochrana.

[176] Európska komisia, tamže, SWD(2017) 295 final, 13. septembra 2017.

[177] Prejav komisárky Jourovej na plenárnej schôdzi Európskeho parlamentu na tému *Zvyšovanie odolnosti EÚ proti vplyvu zahraničných aktérov na nadchádzajúcu volebnú kampaň do EP*, 14. novembra 2018.

[178] Carnegieho nadácia pre medzinárodný mier, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks* (Zasahovanie Ruska do volieb: boj Európy proti falošným správam a kybernetickým útokom), 23. mája 2018.

[179] Európske centrum politickej stratégie (L. Past), Cybersecurity of Election Technology: Inevitable Attacks and Variety of Responses (Kybernetická bezpečnosť volebných technológií: nevyhnutné útoky a rozmanitosť reakcií), in: „Election Interference in the Digital Age – Building Resilience to Cyber-Enabled Threats: A collection of think pieces of 35 leading practitioners and experts" (Zasahovanie do volieb v digitálnom veku – Budovanie odolnosti proti hrozbám umožneným počítačom: Zbierka úvah popredných 35 špecialistov a odborníkov), 2018.

[180] Podľa smernice Rady 2008/114/ES o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu.

[181] Európska komisia, Odporúčanie Komisie o sieťach spolupráce pri voľbách, transparentnosti na internete, ochrane pred kybernetickými bezpečnostnými incidentmi a boji proti dezinformačným kampaniam v súvislosti s voľbami do Európskeho parlamentu, C(2018) 5949 final, 12. septembra 2018.

[182] Závery Európskej rady, EUCO 11/15, 20. marca 2015. Odvtedy pribudli dve ďalšie pracovné skupiny, jedna pre krajiny západného Balkánu a jedna pre krajiny južného susedstva.

[183] Atlantic Council vo svojej správe vyzvala EÚ, aby od všetkých členských štátov vyžadovala, aby vyslali národných odborníkov do pracovnej skupiny. Pozri: D. Fried a A. Polyakova, *Democratic Defense Against Disinformation* (Demokratická obrana proti dezinformáciám), 5. marca 2018.

[184] Pracovná skupina pôvodne nemala vlastný rozpočet a v roku 2018 jej Európsky parlament pridelil 1,1 mil. EUR na prípravnú akciu „StratCom Plus".

[185] Carnegieho nadácia pre medzinárodný mier (E. Brattberg, T. Maurer), tamže, 23. mája 2018.

[186] Európska komisia, vysoká predstaviteľka Únie pre zahraničné veci a bezpečnostnú politiku, *Akčný plán proti dezinformáciám*, JOIN(2018) 36 final. Plán sa zameriava: na zlepšenie spôsobilostí inštitúcií EÚ zisťovať, analyzovať a odhaľovať dezinformácie; na posilnenie koordinovaných, spoločných reakcií; na aktivizáciu súkromného sektora a na zvyšovanie informovanosti a zvýšenie odolnosti spoločnosti.

[187] Európska komisia, *Boj proti dezinformáciám na internete: európsky prístup*, COM(2018) 236 final, 26. apríla 2018.

[188] Nesmie sa zamieňať s kódexom správania týkajúcim boja proti nelegálnym nenávistným prejavom na internete.

[189] JRC, *The digital transformation of news media and the rise of disinformation and fake news* (Digitálna transformácia spravodajských médií a vzostup dezinformácií a falošných správ), Technické správy Spoločného výskumného centra, Pracovný dokument Spoločného výskumného centra o digitálnom hospodárstve 2018-02, apríl 2018.

[190] ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News")* [Posilnenie sieťovej a informačnej bezpečnosti a ochrana proti dezinformáciám na internete (tzv. falošné správy)], apríl 2018.

[191] Európske centrum politickej stratégie (C. Frutos López), *A Responsibility to Support Electoral Organisations in Anticipating and Countering Cyber Threats* (Povinnosť podporovať volebné organizácie pri príprave na kybernetické hrozby a v boji proti nim), in: tamže, 2018.

[192] Európska komisia, tamže, SWD(2018) 403 final, 12. septembra 2018.

[193] Návrh nariadenia [COM(2017) 487 final, 13. septembra 2018], ktorým sa stanovuje rámec na preverovanie priamych zahraničných investícií, predložený v septembri 2017, v súčasnosti prechádza legislatívnym procesom. Návrh sa konkrétne vzťahuje na kritické technológie, medzi ktoré patrí umelá inteligencia, kybernetická bezpečnosť a aplikácie dvojakého použitia.

[194] Európska komisia/Európska služba pre vonkajšiu činnosť, tamže, JOIN(2017) 450 final, 13. septembra 2017.

Tím Európskeho dvora audítorov

Tento informačný dokument s názvom *Prekážky účinnej politiky EÚ v oblasti kybernetickej bezpečnosti* prijala komora III Vonkajšie opatrenia, bezpečnosť a spravodlivosť, ktorej predsedá členka Európskeho dvora audítorov Bettina Jakobsen. Úlohu viedol člen Európskeho dvora audítorov Baudilio Tomé Muguruza, podporu mu poskytol vedúci kabinetu Daniel Costa de Magalhaes a atašé kabinetu Ignacio Garcia de Parada, hlavný manažér Alejandro Ballester-Gallardo, vedúci úlohy Michiel Sweerts, audítori Simon Dennett, Aurelia Petliza, Mirko Iaconisi, Michele Scardone, Silvia Monteiro Da Cunha a stážista Johannes Bolkart. Hannah Critoph poskytla jazykovú podporu.

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

EURÓPSKY
DVOR
AUDÍTOROV

Úrad pre publikácie

EURÓPSKY DVOR AUDÍTOROV
12, rue Alcide De Gasperi
1615 Luxemburg
LUXEMBURSKO

Tel. +352 4398-1

Otázky: eca.europa.eu/sk/Pages/ContactForm.aspx
Webová stránka: eca.europa.eu
Twitter: @EUAuditors

© Európska únia, 2019.
V prípade použitia či šírenia fotografií a iných materiálov, na ktoré sa nevzťahujú autorské práva Európskej únie, ako sú napríklad logá v ilustrácii 4 a v prílohách I a II, je potrebné žiadať povolenie priamo od držiteľov autorských práv.
Titulná strana: © Syda Productions / Shutterstock.com