EURÓPSKA
KOMISIA

VYSOKÁ PREDSTAVITEĽKA
ÚNIE PRE
ZAHRANIČNÉ VECI
A BEZPEČNOSTNÚ POLITIKU

V Bruseli 13. 9. 2017
JOIN(2017) 450 final

SPOLOČNÉ OZNÁMENIE EURÓPSKEMU PARLAMENTU A RADE

Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ

1. ÚVOD

Kybernetická bezpečnosť je nevyhnutná pre našu prosperitu aj bezpečnosť. Keďže naše každodenné životy a naše hospodárstva čoraz viac závisia od digitálnych technológií, sme čím ďalej tým viac vystavení rizikám, ktoré sú s ich využívaním spojené. Kybernetické incidenty sa diverzifikujú tak z hľadiska toho, kto je za ne zodpovedný, ako aj z hľadiska toho, čo je ich cieľom. Kybernetické činnosti so zlým úmyslom nielenže ohrozujú naše hospodárstva a naše snahy smerom k digitálnemu jednotnému trhu, ale aj samotné fungovanie našich demokracií, naše slobody a hodnoty. Naša budúca bezpečnosť závisí od transformácie našej schopnosti chrániť EÚ pred kybernetickými hrozbami: civilné infraštruktúry, ako aj vojenské kapacity závisia od bezpečných digitálnych systémov. Bolo to uznané na zasadnutí Európskej rady v júni 2017[1], ako aj v Globálnej stratégii pre zahraničnú a bezpečnostnú politiku Európskej únie[2].

Riziká narastajú exponenciálne. Štúdie ukazujú, že hospodársky vplyv počítačovej kriminality sa od roku 2013 do roku 2017 päťnásobne zvýšil a do roku 2019 by sa mohol ďalej štvornásobne zvýšiť[3]. Zaznamenal sa značný nárast softvéru ransomware[4], pričom nedávne útoky[5] odzrkadľujú dramatický nárast počítačových kriminálnych činností. Softvér ransomware však ani zďaleka nie je jedinou hrozbou.

Kybernetické hrozby prichádzajú zo strany neštátnych aj štátnych subjektov: často krát majú kriminálnu povahu, sú motivované ziskom, ale môžu mať aj politický alebo strategický charakter. Hrozbu trestnej činnosti zosilňujú nejasné hranice medzi počítačovou kriminalitou a „tradičnou“ trestnou činnosťou, keďže zločinci využívajú internet ako prostriedok na rozširovanie svojich činností a zároveň ako zdroj na nájdenie nových metód a nástrojov na páchanie trestnej činnosti[6]. V prevažnej väčšine prípadov sú však šance na vypátranie zločincov minimálne a šance na trestné stíhanie ešte slabšie.

Zároveň štátne subjekty v čoraz väčšej miere realizujú svoje geopolitické ciele nielen prostredníctvom tradičných nástrojov, ako je vojenská sila, ale takisto pomocou menej transparentných počítačových nástrojov vrátane zasahovania do vnútorných demokratických procesov. Využívanie kybernetického priestoru ako oblasti vedenia vojny, a to buď samostatne, alebo ako súčasť hybridnej taktiky, sa v súčasnosti všeobecne uznáva. Dezinformačné kampane, falošné správy a kybernetické operácie zamerané na kritickú infraštruktúru sú čoraz bežnejšie a vyžadujú si reakciu. Z tohto dôvodu Komisia vo svojom Diskusnom dokumente o budúcnosti európskej obrany[7] zdôraznila význam spolupráce v oblasti kybernetickej obrany.

Pokiaľ výrazne nezlepšíme našu kybernetickú bezpečnosť, riziko sa bude zvyšovať paralelne s digitálnou transformáciou. Očakáva sa, že do roku 2020 sa k „internetu vecí“ pripoja

---

1 http://www.consilium.europa.eu/sk/press/press-releases/2017/06/23-euco-conclusions/.

2 http://europa.eu/globalstrategy/.

3 Pozri napríklad spoločnú štúdiu McAfee & Centrum pre strategické a medzinárodné štúdie: *Net losses: Estimating the Global Cost of Cybercrime* (Čisté straty: odhad globálnych nákladov súvisiacich s počítačovou kriminalitou), 2014.

4 Ransomware je špecifický druh zlomyseľného softvéru, ktorý používateľom systémov znemožňuje alebo obmedzuje prístup k ich systému, a to buď blokovaním zobrazovacieho okna systému alebo blokovaním súborov používateľov, pokiaľ títo nezaplatia výkupné.

5 V máji 2017 útok prostredníctvom ransomvéru pod názvom WannaCry zasiahol viac ako 400 000 počítačov vo viac ako 150 krajinách. O mesiac neskôr útok ransomvérom Peťa zasiahol Ukrajinu a niekoľko spoločností na celom svete.

6 EUROPOL: Hodnotenie hrozieb závažnej a organizovanej trestnej činnosti, 2017.

7 https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_sk.pdf.

desiatky miliárd zariadení, ale pri ich navrhovaní stále nie je prioritou kybernetická bezpečnosť[8]. Nedostatočná ochrana zariadení, ktoré budú riadiť naše elektrické rozvodné siete, vozidlá a dopravné siete, továrne, financie, nemocnice a domovy, by mohla mať ničivé následky a mohla by spôsobiť obrovské škody, pokiaľ ide o dôveru spotrebiteľov v rozvíjajúce sa technológie. Hrozba politicky motivovaných útokov na civilné ciele a nedostatky vo vojenskej kybernetickej obrane toto riziko ešte prehlbujú.

Prístup stanovený v tomto spoločnom oznámení pomôže, aby EÚ bola lepšie pripravená čeliť týmto hrozbám. Tento prístup by pomohol dosiahnuť väčšiu odolnosť a strategickú autonómiu, posilnili by sa ním kapacity v oblasti technológií a zručností a zároveň by pomohol pri budovaní silného jednotného trhu. Vyžaduje si to dostupnosť správnych štruktúr na budovanie silnej kybernetickej bezpečnosti a zabezpečenie reakcie v prípade potreby za plnej účasti všetkých kľúčových aktérov. Tento prístup by takisto umožnil lepšie odrádzať od kybernetických útokov, a to zintenzívnením činnosti zameranej na odhaľovanie, sledovanie a stíhanie osôb, ktoré sú za takéto narušovanie bezpečnosti zodpovedné. Takisto by sa na základe neho uznal globálny rozmer, a to rozvíjaním medzinárodnej spolupráce ako platformy pre vedúce postavenie EÚ v oblasti kybernetickej bezpečnosti. Tieto kroky vychádzajú z prístupov digitálneho jednotného trhu, globálnej stratégie, Európskeho programu v oblasti bezpečnosti[9], Spoločného rámca pre boj proti hybridným hrozbám[10] a oznámenia o zriadení Európskeho obranného fondu[11][12].

EÚ už rieši mnohé z týchto otázok. Teraz je čas vytvoriť spoločné platformy pre rôzne pracovné línie. EÚ v roku 2013 vytýčila stratégiu kybernetickej bezpečnosti, v rámci ktorej sa zaviedlo niekoľko kľúčových pracovných línií na zvýšenie kybernetickej odolnosti[13]. Jej hlavné ciele a zásady posilňovať spoľahlivý, bezpečný a otvorený kybernetický ekosystém zostávajú v platnosti. Prostredie s neustále sa vyvíjajúcou a prehlbujúcou štruktúrou hrozieb si však vyžaduje ďalšie opatrenia na odolávanie a zabránenie útokom v budúcnosti[14].

EÚ má dobré predpoklady na riešenie kybernetickej bezpečnosti vzhľadom na rozsah svojich politík a nástrojov, štruktúr a kapacít, ktoré má k dispozícii. Zatiaľ čo členské štáty zostávajú zodpovedné za národnú bezpečnosť, rozsah a cezhraničná povaha hrozby oprávňujú EÚ konať, a to poskytovaním stimulov a podpory pre členské štáty, aby rozvíjali a udržiavali väčšie a lepšie vnútroštátne kapacity v oblasti kybernetickej bezpečnosti, ako aj budovaním kapacít na úrovni EÚ. Tento prístup je zameraný na podnietenie všetkých aktérov – EÚ, členských štátov, odvetvia a jednotlivcov – aby kybernetickej bezpečnosti prisudzovali náležité prioritné postavenie na budovanie odolnosti a zabezpečenie lepšej reakcie EÚ na kybernetické útoky. Prinesie konkrétne kroky s cieľom pomôcť odhaľovať a vyšetrovať všetky formy kybernetických incidentov voči EÚ a jej členským štátom a primerane na ne reagovať, a to aj prostredníctvom trestného stíhania zločincov. Umožní, aby sa v rámci

---

8 IDC a TXT Solutions (2014), SMART 2013/0037 *Cloud and IoT combination* (Kombinácia cloudu a internetu vecí), štúdia pre Komisiu.

9 COM(2015) 185 final.

10 JOIN(2016) 18 final.

11 COM(2017) 295.

12 Tento prístup je takisto podložený nezávislým vedeckým poradenstvom, ktoré Komisii poskytuje Skupina vedeckých poradcov na vysokej úrovni v rámci mechanizmu vedeckého poradenstva (pozri ďalej uvedené odkazy).

13 JOIN(2013) 1 final. Hodnotenie tejto stratégie je k dispozícii v pracovnom dokumente útvarov Komisie SWD(2017) 295.

14 Pokiaľ nie je uvedené inak, návrhy v tomto oznámení sú rozpočtovo neutrálne. Všetky iniciatívy, ktoré majú vplyv na rozpočet, sa budú náležite riadiť ročnými rozpočtovými postupmi a nemôžu mať vplyv na budúci viacročný finančný rámec po roku 2020.

vonkajšej činnosti EÚ účinne podporovala kybernetická bezpečnosť na globálnej úrovni. Výsledkom bude posun EÚ od reaktívneho k proaktívnemu prístupu k ochrane európskej prosperity, spoločnosti a európskych hodnôt, ako aj základných práv a slobôd reagovaním na súčasné i budúce hrozby.

2. BUDOVANIE ODOLNOSTI EÚ PROTI KYBERNETICKÝM ÚTOKOM

Vysoká kybernetická odolnosť si vyžaduje kolektívny a prístup so širokým záberom. To si vyžaduje pevnejšie a účinnejšie štruktúry na podporu kybernetickej bezpečnosti a reagovanie na kybernetické útoky v členských štátoch, ale aj v samotných inštitúciách, agentúrach a orgánoch EÚ. Takisto si to vyžaduje komplexnejší prístup naprieč politikami pri budovaní kybernetickej odolnosti a strategickej autonómie so silným jednotným trhom, významným pokrokom v technologických kapacitách EÚ a omnoho väčším počtom kvalifikovaných odborníkov. Ústredným prvkom tejto stratégie je všeobecné uznanie toho, že kybernetická bezpečnosť je spoločnou spoločenskou výzvou, takže by do jej zaisťovania mali byť zapojené viaceré vrstvy verejnej správy, hospodárstva a spoločnosti.

2.1 Posilnenie Agentúry Európskej únie pre sieťovú a informačnú bezpečnosť

Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA) má zohrávať kľúčovú úlohu pri posilňovaní kybernetickej odolnosti a reakcie EÚ, je však obmedzená svojím súčasným mandátom. Komisia preto predkladá ambiciózny návrh reformy vrátane **trvalého mandátu pre agentúru**[15]. Tým sa zabezpečí, že agentúra ENISA bude môcť poskytovať podporu členským štátom, inštitúciám EÚ a podnikom v EÚ v kľúčových oblastiach vrátane vykonávania smernice o bezpečnosti sietí a informačných systémov (ďalej len „smernica NIS“)[16] a navrhovaného rámca certifikácie kybernetickej bezpečnosti.

Zreformovaná agentúra ENISA bude mať silnú poradnú úlohu, pokiaľ ide o vypracúvanie a vykonávanie politiky, a to vrátane podpory súdržnosti medzi sektorovými iniciatívami a smernicou NIS a pomoci pri zriaďovaní stredísk na výmenu a analýzu informácií v kritických odvetviach. Vďaka agentúre ENISA sa „zdvihne latka“ a posilní sa európska pripravenosť, a to organizovaním každoročných celoeurópskych cvičení v oblasti kybernetickej bezpečnosti, v rámci ktorých sa spojí reakcia na rôznych úrovniach. Bude tiež podporovať vypracovanie politiky EÚ v oblasti certifikácie kybernetickej bezpečnosti v informačných a komunikačných technológiách (IKT) a zohrávať dôležitú úlohu pri zintenzívňovaní operatívnej spolupráce a krízového riadenia v celej EÚ. Agentúra bude zároveň slúžiť ako kontaktné miesto pre informácie a vedomosti v komunite kybernetickej bezpečnosti.

Rýchle a spoločné pochopenie hrozieb a prebiehajúcich incidentov je nevyhnutným predpokladom pre rozhodovanie o tom, či sú potrebné spoločné opatrenia na ich zmiernenie alebo riešenie podporované EÚ. Takáto výmena informácií si vyžaduje zapojenie všetkých príslušných aktérov – orgánov a agentúr EÚ, ako aj členských štátov – na technickej, operačnej a strategickej úrovni. Agentúra ENISA v spolupráci s príslušnými orgánmi na úrovni členských štátov a na úrovni EÚ, najmä so sieťou jednotiek pre riešenie

[15] COM(2017) 477.

[16] 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.

počítačových bezpečnostných incidentov[17], tímom CERT-EU, Europolom a Centrom EÚ pre analýzu spravodajských informácií (INTCEN), bude takisto prispievať k situačnému povedomiu na úrovni EÚ. Toto možno využiť pri získavaní spravodajských informácií o hrozbách a pri tvorbe politiky v kontexte pravidelného monitorovania štruktúry hrozieb a efektívnej operačnej spolupráce, ako aj pri reakcii na veľké cezhraničné incidenty.

2.2 Smerom k jednotnému trhu kybernetickej bezpečnosti

Rast trhu kybernetickej bezpečnosti v EÚ – z hľadiska produktov, služieb a procesov – je spomalený v mnohých ohľadoch. Kľúčovým aspektom je nedostatok systémov kybernetickobezpečnostnej certifikácie uznávaných v celej EÚ na vytvorenie vyšších štandardov odolnosti produktov a na posilnenie celoeurópskej dôvery v trh. Komisia preto predkladá návrh na vytvorenie **európskeho rámca kybernetickobezpečnostnej certifikácie**[18]. Týmto rámcom by sa stanovil postup na vytvorenie celoúnijných systémov kybernetickobezpečnostnej certifikácie zahŕňajúci produkty, služby a/alebo systémy, ktoré prispôsobujú úroveň spoľahlivosti príslušnému používaniu (či už ide o kritickú infraštruktúru alebo spotrebiteľské zariadenia)[19]. Prinieslo by to jasné výhody pre podniky tým, že nemuseli prejsť pri cezhraničnom obchodovaní cez niekoľko certifikačných postupov, a tým by sa obmedzili administratívne a finančné náklady. Používanie systémov vytvorených podľa tohto rámca by tiež pomohlo vybudovať dôveru spotrebiteľov, keďže osvedčenie o zhode bude kupujúcich a používateľov informovať a ubezpečovať o bezpečnostných vlastnostiach produktov a služieb, ktoré si kupujú a používajú. Prísne kybernetickobezpečnostné normy by tak sa stali zdrojom konkurenčnej výhody. Výsledkom by bola zvýšená odolnosť, pretože produkty a služby IKT by sa formálne vyhodnocovali podľa vymedzeného súboru kybernetickobezpečnostných noriem, ktoré by sa mohli vypracovať v úzkom spojení so širšou prebiehajúcou prácou na tvorbe noriem IKT[20].

Systémy tohto rámca by boli dobrovoľné a nevytvárali by žiadne okamžité regulačné povinnosti pre predajcov alebo poskytovateľov služieb. Systémy by neboli v rozpore so žiadnymi uplatniteľnými právnymi požiadavkami, ako sú napr. právne predpisy EÚ o ochrane údajov.

Po vytvorení tohto rámca Komisia vyzve príslušné zainteresované strany, aby sa zamerali na tri prioritné oblasti:

- Bezpečnosť v kritických alebo vysokorizikových aplikáciách[21]: systémy, na ktorých sme závislí pri našich každodenných činnostiach – od našich áut po strojné zariadenia v továrňach, od najväčších systémov, ako sú napríklad lietadlá alebo elektrárne, po najmenšie, ako sú napríklad zdravotnícke pomôcky – sa stávajú čoraz viac digitalizovanými a navzájom prepojenými. Preto by si základné zložky IKT v takýchto produktoch a systémoch vyžadovali prísne posúdenie bezpečnosti.

- Kybernetická bezpečnosť v najrozšírenejších digitálnych produktoch, sieťach, systémoch a službách, ktoré používa súkromný, ako aj verejný sektor na obranu pred útokmi

[17] Ako sa stanovuje v článku 9 smernice NIS.
[18] COM(2017) 477.
[19] Úroveň spoľahlivosti označuje stupeň prísnosti posúdenia bezpečnosti a zvyčajne zodpovedá úrovni rizika spojeného s týmito oblasťami použitia alebo funkciami (t. j. vyššia úroveň spoľahlivosti požadovaná pre produkty alebo služby IKT používané vo vysoko rizikových oblastiach použitia alebo funkciách).
[20] COM(2016) 176.
[21] Výnimkou by boli prípady, keď by sa povinná alebo dobrovoľná certifikácia upravovala inými aktmi Únie.

a na uplatňovanie regulačných povinností[22] – ako napríklad kódovanie e-mailov, firewally a virtuálne súkromné siete; je nevyhnutné, aby rozšírené používanie týchto nástrojov neviedlo k vzniku nových zdrojov rizík alebo nových zraniteľných miest.

- Používanie metód „bezpečnosti už v štádiu návrhu“ v nízko nákladových, digitálnych a navzájom prepojených zariadeniach hromadnej spotreby, ktoré tvoria internet vecí: systémy vytvorené podľa tohto rámca by sa mohli používať na signalizáciu toho, že pri konštrukcii produktov sa používajú najmodernejšie bezpečné vývojárske metódy, že prešli príslušnými bezpečnostnými testami a že predajcovia sa zaviazali aktualizovať softvér produktov v prípade novozistených zraniteľných miest alebo hrozieb.

Tieto priority by mali osobitne zohľadňovať neustále sa vyvíjajúcu štruktúru kybernetickobezpečnostných hrozieb, ako aj význam základných služieb, ako sú ako doprava, energetika, zdravotná starostlivosť, bankovníctvo, infraštruktúry finančných trhov, pitná voda alebo digitálna infraštruktúra[23].

Keďže žiadny produkt, systém ani žiadna služba IKT nemôžu byť zaručene „100 %-ne“ bezpečné, existuje niekoľko známych a dobre zdokumentovaných nedostatkov pri navrhovaní produktov IKT, ktoré možno využiť na útoky. Pomocou prístupu založeného na „bezpečnosti už v štádiu návrhu“, ktorý by zaviedli výrobcovia prepojených zariadení, softvéru a vybavenia IT, by sa zabezpečilo, že kybernetická bezpečnosť sa bude riešiť ešte pred uvedením nových produktov na trh. Toto by mohlo byť súčasťou zásady „povinnosti náležitej starostlivosti“, ktorá by sa mala ďalej rozvíjať spolu s príslušným odvetvím, čím by sa mohol znížiť počet zraniteľných miest produktov/softvéru, a to použitím celého radu metód od návrhu po testovanie a overovanie vrátane prípadného formálneho overovania, dlhodobej údržby a používania bezpečných procesov životného cyklu vývoja, ako aj vývoja aktualizácií a softvérových záplat zameraných na riešenie dovtedy nezistených zraniteľných miest a rýchlej aktualizácie a opravy[24]. Zároveň by sa tak zvýšila dôvera spotrebiteľov v digitálne produkty.

Okrem toho treba uznať dôležitú úlohu výskumných pracovníkov tretích strán v oblasti bezpečnosti pri zisťovaní zraniteľnosti existujúcich produktov a služieb a vytvoriť podmienky umožňujúce koordinované zverejňovanie informácií o zraniteľnosti[25] vo všetkých členských štátoch na základe osvedčených postupov[26] a príslušných noriem[27].

---

[22] Napríklad smernica (EÚ) 2016/1148, nariadenie (EÚ) 2016/679, smernica (EÚ) 2015/2366 a iné navrhované právne predpisy, ako napríklad Európsky kódex elektronickej komunikácie; v každom z týchto predpisov sa vyžaduje, aby organizácie zaviedli primerané bezpečnostné opatrenia na riešenie príslušných kybernetickobezpečnostných rizík.

[23] Oblasti patriace do rozsahu pôsobnosti smernice 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.

[24] *Cybersecurity in the European Digital Single Market* (Kybernetická bezpečnosť na európskom digitálnom jednotnom trhu), skupina vedeckých poradcov na vysokej úrovni, marec 2017.

[25] Koordinované zverejňovanie informácií o zraniteľnosti je formou spolupráce, ktorá výskumným pracovníkom v oblasti bezpečnosti umožňuje a uľahčuje oznamovanie miest zraniteľnosti vlastníkovi alebo predajcovi informačného systému, a dáva tak organizácii príležitosť diagnostikovať zraniteľné miesto a zabezpečiť nápravu správne a včas pred zverejnením podrobných informácií o zraniteľnosti tretím stranám alebo verejnosti.

[26] Napríklad *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations* (Príručka osvedčených postupov pri zverejňovaní informácií o zraniteľných miestach. Od výziev k odporúčaniam), ENISA, 2016.

[27] ISO/IEC 29147:2014 Informačné technológie – Bezpečnostné techniky – Zverejňovanie informácií o zraniteľnosti.

Zároveň **konkrétne odvetvia** čelia osobitným problémom a mali by sa podporovať, aby vyvíjali svoj vlastný prístup. Týmto spôsobom by sa všeobecné kyberneticko-bezpečnostné stratégie doplnili o odvetvové kyberneticko-bezpečnostné stratégie v oblastiach, ako sú finančné služby[28], energetika, doprava a zdravotníctvo[29].

Komisia už zdôraznila osobitné otázky týkajúce sa **zodpovednosti**, ktoré so sebou prinášajú nové digitálne technológie[30] a práve prebieha analýza dôsledkov, pričom ďalšie kroky sa uzavrú do júna 2018. Kybernetická bezpečnosť nastoľuje otázky v súvislosti s pripísaním zodpovednosti za škody, ktoré vznikli podnikateľským subjektom a dodávateľským reťazcom, a neschopnosť riešiť tieto otázky bude brzdiť rozvoj silného jednotného trhu s kyberneticko-bezpečnostnými produktmi a službami.

Napokon, rozvoj jednotného trhu EÚ závisí aj od zohľadnenia kybernetickej bezpečnosti v obchodnej a investičnej politike. Vplyv zahraničných akvizícií na kritické technológie – ktorých významným príkladom je kybernetická bezpečnosť – je kľúčovým aspektom v rámci **preverovania priamych zahraničných investícií v Európskej únii**[31], ktorého cieľom je umožniť preverenie investícií z tretích krajín z dôvodu bezpečnosti a verejného poriadku. Rovnako, kyberneticko-bezpečnostné požiadavky už vytvorili obchodné bariéry pre tovar a služby EÚ v dôležitých odvetviach vo viacerých hospodárstvach tretích krajín. Rámcom EÚ pre kyberneticko-bezpečnostnú certifikáciu sa ďalej posilní medzinárodná pozícia Európy a malo by ho dopĺňať pokračujúce úsilie o prijatie globálnych noriem pre vysokú bezpečnosť a dohôd o vzájomnom uznávaní.

2.3 Úplné vykonávanie smernice o bezpečnosti sietí a informačných systémov

Keďže hlavné nástroje boja za kybernetickú bezpečnosť sa v súčasnosti využívajú na vnútroštátnej úrovni, EÚ uznala potrebu presadzovať prísnejšie normy. V dôsledku čoraz globalizovanejšej, digitálnejšej a prepojenejšej povahy kľúčových odvetví, ako sú bankovníctvo, energetika alebo doprava, sa rozsiahle kybernetické incidenty zriedka týkajú len jedného členského štátu.

Smernica o bezpečnosti sietí a informačných systémov („smernica NIS“) je prvým celoeurópskym právnym predpisom o kybernetickej bezpečnosti[32]. Jej cieľom je budovať odolnosť zlepšením vnútroštátnych spôsobilostí v oblasti kybernetickej bezpečnosti, podporuje sa ňou lepšia spolupráca medzi členskými štátmi a vyžaduje sa v nej, aby podniky vo významných hospodárskych odvetviach prijímali účinné postupy riadenia rizík a aby vnútroštátnym orgánom oznamovali vážne incidenty. Tieto povinnosti sa vzťahujú aj na tri druhy poskytovateľov kľúčových internetových služieb: cloud computingu, internetových vyhľadávačov a elektronických trhov. Jej cieľom je dôslednejší a systematickejší prístup a lepší tok informácií.

Úplné vykonanie smernice vo všetkých členských štátoch do mája 2018 je pre kybernetickú odolnosť EÚ nevyhnutné. Tento proces sa podporuje kolektívnou prácou členských štátov,

[28] Komisia sa vo svojej nadchádzajúcej činnosti v odvetví finančných technológií bude zaoberať kybernetickou bezpečnosťou pre finančný sektor.

[29] Napríklad v energetickom odvetví je možné kombinovať veľmi staré informačné technológie s najmodernejšími informačnými technológiami, predovšetkým s ohľadom na požiadavky elektrickej siete v reálnom čase.

[30] COM(2017) 228.

[31] COM(2017) 478.

[32] 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.

ktorej výsledkom (do jesene 2017) budú usmernenia na podporu harmonizovanejšieho vykonávania, najmä pokiaľ ide o prevádzkovateľov základných služieb. Komisia okrem toho vydáva oznámenie[33] ako súčasť tohto balíka kybernetickej bezpečnosti s cieľom podporiť ich úsilie poskytovaním osvedčených postupov členských štátov, ktoré sa týkajú vykonávania smernice, a usmernení o tom, ako by mala smernica fungovať v praxi.

Oblasť, v ktorej bude potrebné doplniť smernicu, je tok informácií. Smernica napríklad pokrýva iba kľúčové strategické odvetvia – logicky by však bol potrebný podobný prístup všetkých zainteresovaných strán postihnutých počítačovými útokmi, aby bolo možné systematicky posudzovať zraniteľné miesta a vstupné body pre počítačových útočníkov. Okrem toho spolupráca a výmena informácií medzi verejným a súkromným sektorom čelí mnohým prekážkam. Vlády a verejné orgány nie sú ochotné deliť sa o informácie dôležité z hľadiska kybernetickej bezpečnosti, pretože sa obávajú ohrozenia národnej bezpečnosti alebo konkurencieschopnosti. Súkromné podniky sa zdráhajú poskytovať informácie o svojich kybernetických zraniteľných miestach a následných stratách, pretože majú strach z ohrozenia citlivých obchodných informácií, ohrozenia svojho dobrého mena alebo rizika porušenia pravidiel ochrany údajov[34]. Treba posilniť dôveru v partnerstvá medzi verejným a súkromným sektorom s cieľom podporiť širšiu spoluprácu a výmenu informácií vo väčšom počte odvetví. Úloha stredísk pre výmenu a analýzu informácií je osobitne dôležitá pri budovaní dôvery potrebnej na výmenu informácií medzi súkromným a verejným sektorom. Prijali sa prvé kroky v súvislosti s konkrétnymi kritickými odvetviami, ako je napr. letectvo, vytvorením Európskeho centra pre kybernetickú bezpečnosť v letectve[35], a energetika, prostredníctvom rozvoja stredísk pre výmenu a analýzu informácií[36]. Komisia bude v plnej miere prispievať k tomuto prístupu s podporou agentúry ENISA, so zrýchlenými opatreniami, ktoré sú potrebné najmä so zreteľom na odvetvia, ktoré poskytujú základné služby tak, ako sú vymedzené v smernici NIS.

2.4 Odolnosť prostredníctvom rýchlej reakcie na núdzové situácie

Keď dôjde ku kybernetickému útoku, rýchla a účinná reakcia môže zmierniť jeho dôsledky. To tiež dokazuje, že verejné orgány nie sú bezmocné voči kybernetickým útokom, a prispieva to k budovaniu dôvery. Pokiaľ ide o vlastnú reakciu inštitúcií EÚ, v prvom rade by sa kybernetické aspekty mali začleniť do existujúcich mechanizmov EÚ na krízové riadenie: integrovanej politickej reakcie EÚ na krízu koordinovanej predsedníctvom Rady[37] a všeobecných systémov včasného varovania[38]. Potreba reagovať na obzvlášť závažný

---

[33] COM(2017) 476.

[34] *Cybersecurity in the European Digital Single Market* (Kybernetická bezpečnosť na európskom digitálnom jednotnom trhu), skupina vedeckých poradcov na vysokej úrovni, marec 2017. Osobitný problém sa týka obchodného tajomstva, pričom už v júli 2016 Komisia vo svojom oznámení Posilnenie európskeho systému kybernetickej odolnosti spomenula zdržanlivosť pri ohlasovaní kybernetických krádeží obchodných tajomstiev a význam dôveryhodných oznamovacích kanálov zaručujúcich dôvernosť.

[35] https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa.

[36] Ide o neziskové členské organizácie založené súkromnými a verejnými subjektmi s cieľom vymieňať si informácie o kybernetických hrozbách, rizikách, prevencii, zmierňovaní a reakciách. Pozri napr. Európske strediská pre výmenu a analýzu informácií v oblasti energetiky (http://www.ee-isac.eu).

[37] Umožňuje koordináciu reakcií na najvyššej politickej úrovni na najdôležitejšie krízy zasahujúce viaceré odvetvia.

[38] Umožňujú spoločné využívanie interných informácií a koordináciu reakcie v prípade vznikajúcich viacodvetvových krízových situácií alebo predvídateľných, či bezprostredných hrozieb, ktoré si vyžadujú opatrenia na úrovni EÚ.

kybernetický incident alebo útok by pre členský štát mohla predstavovať dostatočný dôvod na uplatnenie doložky EÚ o solidarite[39].

Možnosť rýchlej a účinnej reakcie závisí aj od mechanizmu rýchlej výmeny informácií medzi všetkými kľúčovými aktérmi na vnútroštátnej úrovni a na úrovni EÚ, čo si na druhej strane vyžaduje prehľadnosť, pokiaľ ide o ich príslušné úlohy a právomoci. Komisia uskutočnila konzultácie s inštitúciami a členskými štátmi o „koncepcii“ s cieľom zabezpečiť účinný postup operačnej reakcie na úrovni Únie a členských štátov na rozsiahly kybernetický incident. V **koncepcii** prezentovanej v odporúčaní[40], ktoré je súčasťou tohto balíka, sa vysvetľuje, ako sa kybernetická bezpečnosť začleňuje do existujúcich mechanizmov krízového riadenia na úrovni EÚ, a stanovujú sa v nej ciele a spôsoby spolupráce medzi členskými štátmi, ako aj medzi členskými štátmi a príslušnými inštitúciami, útvarmi, agentúrami a orgánmi EÚ[41] pri reakcii na rozsiahle kybernetické incidenty a krízy. V odporúčaní sa takisto od členských štátov a inštitúcií EÚ požaduje vytvorenie rámca EÚ pre reakciu na kybernetické krízy, aby sa koncepcia mohla uviesť do praxe. Koncepcia sa bude pravidelne testovať formou cvičení zameraných na riadenie kybernetických a iných kríz[42] a bude sa podľa potreby aktualizovať.

Vzhľadom na to, že kybernetické incidenty by mohli významne ovplyvniť fungovanie hospodárstiev a každodenný život ľudí, jednou z možností by bolo zriadenie **núdzového fondu kybernetickej bezpečnostnej reakcie** podľa vzoru takýchto krízových mechanizmov v iných oblastiach politiky EÚ. V Počas mimoriadneho incidentu alebo po ňom by to členským štátom umožnilo vyhľadať pomoc na úrovni EÚ pod podmienkou, že členský štát pred incidentom zaviedol obozretný systém kybernetickej bezpečnosti vrátane úplného vykonania smernice NIS, vyspelého riadenia rizík a rámcov dohľadu na vnútroštátnej úrovni. V rámci takéhoto fondu, ktorý by dopĺňal existujúce mechanizmy krízového riadenia na úrovni EÚ, by sa v záujme solidarity mohla rozvinúť spôsobilosť rýchlej reakcie a mohli by sa financovať osobitné opatrenia na riešenie núdzových situácií, akými sú napr. nahradenie napadnutých zariadení alebo nasadenie nástrojov na zmiernenie škôd alebo na reakciu na hrozby a útoky, pričom by sa vychádzalo z odborných znalostí na vnútroštátnej úrovni získaných vďaka mechanizmu Únie v oblasti civilnej ochrany.

2.5 Kompetenčná sieť kybernetickej bezpečnosti s Európskym strediskom výskumu a kompetencií pre kybernetickú bezpečnosť

Technologické nástroje kybernetickej bezpečnosti sú strategickým majetkom a zároveň sú kľúčovými technológiami rastu v budúcnosti. Je strategickým záujmom EÚ zabezpečiť, aby si zachovala a rozvíjala základné kapacity na zabezpečenie svojho digitálneho hospodárstva, spoločnosti a demokracie, na ochranu kritického hardvéru a softvéru a na poskytovanie kľúčových služieb v oblasti kybernetickej bezpečnosti.

Verejno-súkromné partnerstvo v oblasti kybernetickej bezpečnosti[43] vytvorené v roku 2016 predstavovalo významný prvý krok, ktorý vyvolal investície vo výške 1,8 miliardy EUR

[39] V súlade s článkom 222 Zmluvy o fungovaní Európskej únie.
[40] C(2017) 6100.
[41] Vrátane Europolu, agentúry ENISA, tímu reakcie na núdzové počítačové situácie v inštitúciách, orgánoch a agentúrach EÚ (CERT-EU) a Centra EÚ pre analýzu spravodajských informácií (INTCEN).
[42] Napríklad tých, ktoré uskutočňuje agentúra ENISA: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.
[43] C(2016) 4400 final.

do roku 2020. Rozsah investícií v iných častiach sveta[44] však naznačuje, že EÚ musí urobiť viac z hľadiska investícií a že musí prekonať fragmentáciu kapacít v celej EÚ.

Zložitosť technológie kybernetickej bezpečnosti, nevyhnutnosť rozsiahlych investícií a potreba riešení, ktoré by fungovali na celom území EÚ, si vyžadujú osobitné opatrenia na úrovni EÚ. V nadväznosti na prácu členských štátov a verejno-súkromného partnerstva by ďalším krokom bolo posilnenie spôsobilosti EÚ v oblasti kybernetickej bezpečnosti prostredníctvom **siete kompetenčných centier kybernetickej bezpečnosti**[45] s **Európskym strediskom výskumu a kompetencií pre kybernetickú bezpečnosť** ako ústredným aktérom. Táto sieť a jej centrum by stimulovali vývoj a zavádzanie technológií v oblasti kybernetickej bezpečnosti a dopĺňali by úsilie pri budovaní kapacít v tejto oblasti na európskej a vnútroštátnej úrovni. Komisia uskutoční posúdenie vplyvu, aby preskúmala dostupné možnosti – vrátane zriadenia spoločného podniku – s cieľom vytvoriť túto štruktúru v roku 2018.

Ako prvý krok a s cieľom poskytnúť informácie pre budúce uvažovanie Komisia navrhne, aby sa pilotná fáza začala v rámci programu Horizont 2020 s cieľom spoločne zapojiť národné strediská do siete, a vytvoriť tak nový impulz pre rozvoj kompetencií a technológií v oblasti kybernetickej bezpečnosti. Plánuje navrhnúť na tento účel krátkodobý finančný príspevok vo výške 50 miliónov EUR. Táto činnosť bude dopĺňať prebiehajúce vykonávanie verejno-súkromného partnerstva v oblasti kybernetickej bezpečnosti.

Spájanie a formovanie výskumného úsilia by bolo ústrednou úlohou siete a počiatočným zameraním strediska. Na podporu rozvoja priemyselných kapacít by stredisko mohlo pôsobiť ako projektový manažér pre spôsobilosti schopný zvládnuť nadnárodné projekty. Rovnako by to prinieslo ďalší impulz pre inovácie a konkurencieschopnosť priemyslu EÚ na globálnej scéne pri vývoji digitálnych technológií novej generácie vrátane umelej inteligencie, kvantovej výpočtovej techniky, technológií blockchain a bezpečných digitálnych identít, ako aj pri zabezpečovaní prístupu k hromadným údajom pre spoločnosti so sídlom v EÚ – všetky tieto prvky sú kľúčové pre kybernetickú bezpečnosť v budúcnosti. Stredisko by tiež čerpalo z práce EÚ na rozšírení infraštruktúry vysokovýkonnej výpočtovej techniky: je to základným predpokladom pre analýzu veľkého množstva údajov, rýchle šifrovanie a dešifrovanie údajov, overovanie totožnosti, simuláciu kybernetických útokov a analýzu videomateriálov[46].

Sieť kompetenčných centier by mohla mať aj kapacity na podporu priemyslu prostredníctvom testovania a simulácie v záujme podpory kyberneticko-bezpečnostnej certifikácie opísanej v oddiele 2.2. Jej zapojenie do celej škály aktivít EÚ v oblasti kybernetickej bezpečnosti by zabezpečilo neustálu aktualizáciu jej zamerania v súlade s potrebami. Cieľom strediska by bolo presadzovať prísne normy kybernetickej bezpečnosti nielen v technologických systémoch a systémoch kybernetickej bezpečnosti, ale aj pri rozvoji vysokošpecializovaných zručností odborníkov, a to poskytovaním riešení a modelov, pokiaľ ide o úsilie členských štátov zavádzať digitálne zručnosti. V tejto súvislosti by takisto prispievalo k zlepšeniu kyberneticko-bezpečnostných spôsobilostí na úrovni EÚ a ťažilo by zo synergií, najmä s agentúrou ENISA, tímom CERT-EU, Europolom, možným budúcim núdzovým fondom kybernetickej bezpečnostnej reakcie a vnútroštátnymi jednotkami CSIRT.

---

[44] USA budú v roku 2017 investovať do kybernetickej bezpečnosti 19 miliárd dolárov, čo v porovnaní s rokom 2016 predstavuje nárast o 35 %. Biely dom, kancelária tlačového hovorcu: *Fact Sheet: Cybersecurity National Action Plan* (Informačný list: Národný akčný plán v oblasti kybernetickej bezpečnosti), 9. február 2016.

[45] Táto sieť by zahrnula existujúce a budúce strediská kybernetickej bezpečnosti zriadené v členských štátoch, ktorých členovia by boli štandardne verejné výskumné organizácie a laboratóriá.

[46] COM(2012) 45 final a COM(2016) 178 final.

Kompetenčná sieť sa musí v rámci svojich aktivít osobitne zamerať na nedostatok európskych kapacít na hodnotenie **šifrovania** produktov a služieb, ktoré využívajú občania, podniky a vlády v rámci digitálneho jednotného trhu. Silné šifrovanie je základom bezpečných elektronických identifikačných systémov, ktoré zohrávajú kľúčovú úlohu pri účinnom zaisťovaní kybernetickej bezpečnosti[47]. Takisto chráni duševné vlastníctvo osôb a umožňuje ochraňovať základné práva, ako sú sloboda prejavu a ochrana osobných údajov, a zabezpečuje bezpečné online obchodovanie[48].

Keďže trhy EÚ v oblasti civilnej a obrannej kybernetickej bezpečnosti musia riešiť spoločné výzvy[49] a používajú rovnaké technológie dvojakého použitia, ktoré si vyžadujú úzku spoluprácu v kritických oblastiach, mohla by sa ďalej rozvíjať druhá fáza siete a jej strediska s kybernetickým obranným rozmerom pri plnom rešpektovaní ustanovení zmluvy týkajúcich sa spoločnej bezpečnostnej a obrannej politiky. Okrem technologického zamerania by obranný rozmer mohol prispievať k spolupráci členských štátov v oblasti kybernetickej obrany vrátane spoločného využívania informácií, situačného povedomia, budovania odborných znalostí a koordinovaných reakcií a podpory rozvoja spoločných kapacít členskými štátmi. Sieť by mohla tiež slúžiť ako platforma, ktorá členským štátom umožňuje určovať priority kybernetickej obrany EÚ, skúmať spoločné riešenia, prispievať k rozvoju spoločných stratégií, uľahčovať spoločnú odbornú prípravu v oblasti kybernetickej obrany, cvičenia a testovanie na európskej úrovni a ktorá bude podporovať prácu na taxonómii a normách pre kybernetickú obranu, pričom stredisko bude mať podpornú a poradenskú úlohu. Aby stredisko mohlo pokračovať v týchto aktivitách, bude musieť úzko a ako plnohodnotný partner spolupracovať s Európskou obrannou agentúrou v oblasti kybernetickej obrany, ako aj s agentúrou ENISA v oblasti kybernetickej odolnosti. V rámci tohto obranného rozmeru by sa zohľadňoval proces, ktorý sa spustil na základe diskusného dokumentu o budúcnosti európskej obrany.

Vysoká miera odolnosti, ktorá je potrebná na kybernetickú obranu, si vyžaduje osobitné zameranie úsilia v oblasti výskumu a technológií. Projekty alebo technológie v oblasti kybernetickej obrany, ktoré vyvinuli podniky, by mohli využívať financovanie z Európskeho obranného fondu, pokiaľ ide o fázu výskumu aj fázu vývoja[50]. Špecifické oblasti, ako sú napríklad šifrovacie systémy založené na kvantových technológiách, kybernetické situačné povedomie, biometrické systémy kontroly prístupu, detekcia pokročilých pretrvávajúcich hrozieb alebo hĺbková analýza údajov, by mohli byť v tejto súvislosti mimoriadne dôležité. Vysoká predstaviteľka/vysoký predstaviteľ, Európska obranná agentúra a Komisia budú členské štáty podporovať pri určovaní oblastí, v ktorých by sa mohlo zvážiť financovanie spoločných projektov v oblasti kybernetickej bezpečnosti prostredníctvom Európskeho obranného fondu.

2.6 Vybudovanie silnej základne EÚ pre kybernetické zručnosti

Silným rozmerom kybernetickej bezpečnosti je vzdelávanie. Účinná kybernetická bezpečnosť závisí vo veľkej miere od zručností dotknutých osôb. Predpokladá sa však, že v súkromnom

[47] Komisia už v rámci programu Horizont 2020 otvorí novú súťaž Cena Horizon, ktorej víťaz dostane 4 milióny EUR za najlepšie inovatívne riešenie pre bezproblémové metódy elektronickej autentifikácie.

[48] *Cybersecurity in the European Digital Single Market* (Kybernetická bezpečnosť na európskom digitálnom jednotnom trhu), skupina vedeckých poradcov na vysokej úrovni, marec 2017.

[49] *Study on synergies between the civilian and the defence cybersecurity markets* (Štúdia o súčinnosti medzi civilným a obranným segmentom trhu s kybernetickou bezpečnosťou) (Optimity; SMART 2014-0059).

[50] V rámci programu rozvoja európskeho obranného priemyslu sa už teraz budú uprednostňovať projekty v oblasti kybernetickej obrany a kybernetická obrana bude jednou z tém výzvy na predkladanie návrhov, ktorá sa uverejní v roku 2018.

sektore v Európe bude do roku 2022 chýbať 350 000 odborníkov so zručnosťami v oblasti kybernetickej bezpečnosti[51]. Vzdelávanie v oblasti kybernetickej bezpečnosti by sa malo rozvíjať na všetkých úrovniach, počnúc pravidelnou odbornou prípravou pracovnej sily pracujúcej v oblasti kybernetickej bezpečnosti cez dodatočnú odbornú prípravu všetkých odborníkov v oblasti IKT zameranú na kybernetickú bezpečnosť až po nové osobitné učebné plány v oblasti kybernetickej bezpečnosti. Mali by sa zriadiť výkonné akademické kompetenčné centrá s cieľom splniť požiadavky na urýchlené vzdelávanie a odbornú prípravu, ktoré by mohli vychádzať z usmernení Európskeho strediska výskumu a kompetencií pre kybernetickú bezpečnosť a agentúry ENISA. Cieľom by malo byť, aby sa pri navrhovaní IKT produktov a systémov od samého začiatku prirodzene zohľadňovali zásady bezpečnosti. Vzdelávanie v oblasti kybernetickej bezpečnosti by sa nemalo obmedzovať len na odborníkov v oblasti IT, ale malo by sa začleniť do učebných osnov aj v iných oblastiach, ako je napr. inžinierstvo, riadenie podnikov alebo právo, ako aj do odvetvovo špecifických vzdelávacích programov. Napokon, učitelia a žiaci v primárnom a sekundárnom vzdelávaní by sa mali oboznamovať s problematikou počítačovej kriminality a kybernetickej bezpečnosti v rámci nadobúdania digitálnych kompetencií na školách.

EÚ spolu s členskými štátmi by mala tiež prispieť k tejto práci tým, že bude vychádzať z činnosti koalície pre digitálne zručnosti a pracovné miesta[52] a napríklad pre malé a stredné podniky zavedie systémy učňovského vzdelávania v oblasti kybernetickej bezpečnosti.

2.7 Presadzovanie počítačovej hygieny a informovanosti

Keďže približne 95 % incidentov bolo spôsobených „určitým druhom ľudskej chyby – úmyselnej alebo nie“[53], určitú úlohu v tomto smere zohráva silný ľudský faktor. Kybernetická bezpečnosť je preto zodpovednosťou každého jednotlivca. Znamená to, že sa musí zmeniť správanie jednotlivcov, podnikov a verejnej správy, aby sa zabezpečilo, že každý chápe hrozbu, a aby bol každý vybavený nástrojmi a zručnosťami potrebnými na rýchle odhalenie útokov a aktívnu ochranu pred nimi. Jednotlivci si musia osvojovať návyky v oblasti počítačovej hygieny a podniky a organizácie musia prijímať primerané programy v oblasti kybernetickej bezpečnosti založené na rizikách a musia ich pravidelne aktualizovať, aby odrážali vyvíjajúcu sa štruktúru rizík.

V smernici NIS sa stanovujú nielen povinnosti členských štátov, pokiaľ ide o výmenu informácií o kybernetických útokoch na úrovni EÚ, ale aj ich povinnosti, pokiaľ ide o zavedenie vyspelých národných stratégií v oblasti kybernetickej bezpečnosti a rámcov v oblasti bezpečnosti sietí a informačných systémov. Orgány verejnej správy na úrovni EÚ a na vnútroštátnej úrovni by mali zohrávať vedúcu úlohu pri podpore tohto úsilia.

Po prvé, členské štáty by mali maximalizovať dostupnosť nástrojov v oblasti kybernetickej bezpečnosti pre podniky a jednotlivcov. Predovšetkým by sa malo zaviesť viac opatrení s cieľom predchádzať a zmierňovať vplyv počítačovej kriminality na koncových používateľov. Príklad už existuje – v rámci práce Europolu s kampaňou *NoMoreRansom*[54], ktorá bola vytvorená prostredníctvom úzkej spolupráce medzi orgánmi presadzovania práva a spoločnosťami pôsobiacimi v oblasti kybernetickej bezpečnosti s cieľom pomôcť používateľom predchádzať infekciám spôsobeným softvérom ransomware a dešifrovať údaje,

[51] *Global Information Security Workforce Study* (Štúdia o celosvetovej pracovnej sile v odvetví bezpečnosti informácií), 2017. Deficit na celom svete predstavuje 1,8 milióna pracovníkov.

[52] https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.

[53] IBM, The Cybersecurity Intelligence Index 2014, na ktorý sa odkazuje v Securitymagazine.com, 19. jún 2014.

[54] https://www.nomoreransom.org/.

ak sa stanú obeťami útoku. Takéto systémy by sa mali spustiť aj pre iné druhy zlomyseľného softvéru, v iných oblastiach a EÚ by mala vytvoriť **jeden portál s cieľom spojiť všetky takéto nástroje do jednotného kontaktného miesta**, ktoré bude používateľom poskytovať poradenstvo týkajúce sa prevencie a odhaľovania zlomyseľného softvéru, ako aj odkazy na mechanizmy podávania správ.

Po druhé, členské štáty by mali urýchliť **využívanie väčšieho počtu nástrojov na zabezpečenie kybernetickej bezpečnosti pri rozvoji svojej elektronickej verejnej správy** a zároveň by mali v plnej miere využívať kompetenčnú sieť. Malo by sa podporovať prijímanie bezpečných prostriedkov identifikácie, pričom by sa malo vychádzať z rámca EÚ pre elektronickú identifikáciu a dôveryhodné služby pre elektronické transakcie na vnútornom trhu, ktorý je v platnosti od roku 2016 a ktorým sa zabezpečuje predvídateľné regulačné prostredie v záujme umožňovania bezpečnej a bezproblémovej elektronickej interakcie medzi podnikmi, jednotlivcami a orgánmi verejnej moci[55]. Okrem toho verejné inštitúcie, predovšetkým tie, ktoré poskytujú základné služby, by mali zabezpečiť, aby bol ich personál vyškolený v oblastiach týkajúcich sa kybernetickej bezpečnosti.

Po tretie, členské štáty by mali kybernetickú informovanosť umiestniť na popredné miesto v rámci svojich **kampaní na zvyšovanie informovanosti** vrátane tých, ktoré sa zameriavajú na školy, univerzity, podnikateľské kruhy a výskumné inštitúcie. Mesiac kybernetickej bezpečnosti, ktorý sa koná každý rok v októbri a ktorý koordinuje agentúra ENISA, sa väčšmi zviditeľní, aby sa tak docielil jeho väčší dosah v rámci spoločného komunikačného úsilia na úrovni EÚ a na vnútroštátnej úrovni. Zvyšovanie informovanosti vo vzťahu k online **dezinformačným kampaniam a falošným správam** v sociálnych médiách, ktoré sú konkrétne zamerané na oslabenie demokratických procesov a európskych hodnôt, je rovnako dôležité. Kým hlavná zodpovednosť zostáva na vnútroštátnej úrovni – a to aj v prípade volieb do Európskeho parlamentu – zhromažďovanie odborných znalostí a výmena skúseností na európskej úrovni sa ukázali byť pridanou hodnotou pri cielenom zavádzaní opatrení[56].

Významnú úlohu v tomto smere zohráva aj **priemysel** vo všeobecnosti, ale osobitný význam majú poskytovatelia digitálnych služieb a výrobcovia. Priemysel musí podporovať používateľov (jednotlivcov, podniky a verejné správy) pomocou nástrojov, ktoré im umožnia prevziať zodpovednosť za ich vlastné činnosti online, pričom treba jasne zdôrazniť, že zachovanie počítačovej hygieny je neodmysliteľnou súčasťou ponuky pre spotrebiteľov[57]. Priemysel by sa mal v záujme zisťovania a odstraňovania zraniteľných miest usilovať o fungujúce vnútorné procesy, ktoré sa zaoberajú vyšetrovaním, klasifikáciou a riešením prípadov zraniteľnosti, bez ohľadu na to, či je zdroj potenciálnej zraniteľnosti v príslušnej spoločnosti vonkajší alebo vnútorný.

Kľúčové opatrenia

[55] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (nariadenie eIDAS), prijaté 23. júla 2014. Okrem toho Európska komisia poskytuje stavebné kamene a nástroje pre interoperabilitu elektronickej identifikácie a elektronického podpisu (napr. prehliadače dôveryhodných zoznamov – Trusted Lists Browsers) prostredníctvom programu Nástroja na prepájanie Európy.

[56] Príkladom je pracovná skupina East StratCom zriadená v roku 2015 členskými štátmi a vysokou predstaviteľkou, ktorá sa zaoberá pokračujúcimi dezinformačnými kampaňami Ruska. Tím sa podieľa na tvorbe komunikačných produktov a kampaní zameraných na objasňovanie politík EÚ v regióne Východného partnerstva.

[57] Niektorí výrobcovia sú už na tento koncept zvyknutí, keďže v niektorých európskych právnych predpisoch týkajúcich sa výrobkov (napríklad v smernici 2006/42/ES o strojových zariadeniach) sa stanovujú zásady pre „bezpečnosť už v štádiu návrhu“.

- Úplné vykonávanie smernice o bezpečnosti sietí a informačných systémov,
- rýchle prijatie nariadenia, ktorým sa stanovuje nový mandát pre agentúru ENISA a európsky rámec pre certifikáciu[58], Európskym parlamentom a Radou,
- spoločná iniciatíva Komisie a priemyslu zameraná na vymedzenie zásady „povinnosti náležitej starostlivosti“ na zníženie zraniteľnosti produktov/softvéru a podporu „bezpečnosti už v štádiu návrhu“,
- urýchlené vykonávanie plánu pre cezhraničné reakcie na závažné incidenty,
- začať posúdenie vplyvu s cieľom preštudovať možnosť návrhu Komisie v roku 2018 na vytvorenie siete kompetenčných centier pre kybernetickú bezpečnosť a európskeho výskumného a kompetenčného centra pre kybernetickú bezpečnosť v nadväznosti na okamžitú pilotnú fázu,
- podporovať členské štáty pri určovaní oblastí, v ktorých by sa mohlo uvažovať o spoločných projektoch v oblasti kybernetickej bezpečnosti, ktoré by sa mohli podporovať z Európskeho obranného fondu,
- celoeurópske jednotné kontaktné miesto, ktoré by obetiam kybernetických útokov poskytovalo pomoc, informácie o najnovších hrozbách a ktoré by zhromažďovalo praktické rady a nástroje v oblasti kybernetickej bezpečnosti,
- opatrenia členských štátov na začlenenie kybernetickej bezpečnosti do programov rozvoja zručností, elektronickej verejnej správy a informačných kampaní,
- opatrenia priemyslu na zintenzívnenie odbornej prípravy jeho zamestnancov v oblastiach súvisiacich s kybernetickou bezpečnosťou a na prijatie prístupu „bezpečnosť už v štádiu návrhu“ pre jeho výrobky, služby a procesy.

3. VYTVORENIE ÚČINNÉHO ODRÁDZANIA OD POČÍTAČOVEJ KRIMINALITY NA ÚROVNI EÚ

Účinným odradením sa myslí zavedenie rámca opatrení, ktoré sú dôveryhodné a zároveň odrádzajúce potenciálnych páchateľov počítačovej kriminality a kybernetických útokov. Pokiaľ sa páchatelia kybernetických útokov – neštátni, ako aj štátni – nemusia ničoho báť okrem ich prípadného zlyhania, nebudú mať veľkú motiváciu prestať sa o ne pokúšať. Pri budovaní účinných mechanizmov odrádzania je zásadná účinnejšia reakcia orgánov presadzovania práva zameraná na odhaľovanie, sledovanie a stíhanie páchateľov počítačovej kriminality. K tomu sa pripája potreba EÚ podporovať členské štáty pri rozvoji spôsobilostí s dvojakým použitím v oblasti kybernetickej bezpečnosti. Existujúcu situáciu, pokiaľ ide o kybernetické útoky, začneme meniť až vtedy, keď zvýšime šance na odhalenie takýchto zločincov a ich potrestanie. Kybernetické útoky by sa mali urýchlene vyšetriť a páchatelia sa musia predviesť pred súd, alebo sa musia prijať opatrenia s cieľom umožniť primeranú politickú alebo diplomatickú reakciu. V prípade vážnej krízy s významným medzinárodným a obranným rozmerom by vysoký predstaviteľ/vysoká predstaviteľka mohol/mohla predstaviť Rade možnosti na vhodnú reakciu.

Jeden krok smerom k zlepšeniu trestnoprávnej reakcie na kybernetické útoky sa už vykonal, a to v roku 2013 prijatím smernice o útokoch na informačné systémy[59]. Stanovili sa v nej minimálne pravidlá týkajúce sa vymedzenia trestných činov a sankcií v oblasti útokov na informačné systémy a aj operačné opatrenia na zlepšenie spolupráce medzi orgánmi. Smernica viedla k podstatnému pokroku v oblasti zosúladenia stupňa kriminalizácie kybernetických útokov medzi členskými štátmi, čo uľahčuje cezhraničnú spoluprácu orgánov

[58] COM(2017) 477.

[59] Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy.

presadzovania práva, ktoré vyšetrujú tieto druhy trestných činov. Stále však existuje priestor na využitie plného potenciálu smernice, ak by členské štáty v plnej miere vykonávali všetky jej ustanovenia[60]. Komisia bude aj naďalej poskytovať podporu členským štátom pri vykonávaní smernice a v súčasnosti zastáva názor, že nie je potrebné navrhovať zmeny tejto smernice.

3.1 Identifikácia škodlivých aktérov

Aby sme zvýšili naše šance na predvedenie páchateľov pred súd, musíme urýchlene zlepšiť našu schopnosť identifikovať osoby, ktoré sú zodpovedné za kybernetické útoky. Hľadanie užitočných informácií na účely vyšetrovania počítačovej kriminality, najmä vo forme digitálnych stôp, predstavuje veľkú výzvu pre orgány presadzovania práva. Je preto potrebné, aby sme zvýšili svoju technologickú spôsobilosť na vedenie účinných vyšetrovaní, okrem iného aj posilnením jednotky Europolu na boj proti počítačovej kriminalite o odborníkov na kybernetiku. Europol sa stal kľúčovým aktérom pri podpore vyšetrovaní vo viacerých členských štátoch. Mal by sa stať centrom expertízy pre orgány presadzovania práva v členských štátoch, pokiaľ ide o online vyšetrovania a počítačovú forenznú analýzu.

Bežné postupy priradenia viacerých používateľov – niekedy sú ich tisícky – k jednej IP adrese z technického hľadiska významne obmedzuje úspešné vyšetrovanie škodlivého online správania. Niekedy je z tohto dôvodu takisto potrebné, napr. v prípade závažných zločinov, ako je sexuálne zneužívanie detí, prešetriť veľký počet používateľov s cieľom identifikovať jedného škodlivého aktéra. EÚ bude preto podporovať rozšírenie nového protokolu (IPv6), keďže umožňuje pridelenie jediného používateľa k jednej IP adrese, čím má jasné výhody v oblasti presadzovania práva a vyšetrovania týkajúceho sa kybernetickej bezpečnosti. Ako prvý krok na podporu takéhoto prechodu bude Komisia začleňovať požiadavku na prechod na IPv6 v rámci svojich politík vrátane požiadaviek v oblasti obstarávania, financovania projektov a výskumu, ako aj podpory nevyhnutných vzdelávacích materiálov. Členské štáty by okrem toho mali zvážiť dobrovoľné dohody s poskytovateľmi internetových služieb s cieľom stimulovať zavádzanie IPv6.

Belgicko má vedúce postavenie vo svete[61], pokiaľ ide o mieru zavádzania IPv6, a to aj vďaka spolupráci medzi verejným a súkromným sektorom: príslušné zainteresované strany zvážili obmedzenie používania jednej IP adresy na maximálne 16 používateľov ako súčasť dobrovoľného samoregulačného opatrenia, ktorým sa stimuloval prechod na IPv6[62].

Všeobecnejšie by sa mala ďalej podporovať online zodpovednosť. Znamená to podporovať opatrenia na predchádzanie zneužívania názvov domén na distribúciu nevyžiadaných správ alebo na phishingové útoky. Na tento účel bude Komisia vyvíjať činnosti s cieľom zlepšiť

[60] COM(2017) 474.

[61] https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption.

[62] http://bipt.be/public/files/nl/22027/Raadpleging_ipv6.pdf.

fungovanie systémov názvov domén a IP WHOIS[63], ako aj dostupnosť a presnosť informácií v týchto systémoch v súlade s úsilím Internetovej korporácie pre prideľovanie mien a čísel[64].

3.2 Zintenzívnenie reakcie na strane presadzovania práva

Kľúčovým odstrašujúcim prostriedkom pre kybernetické útoky je účinné **vyšetrovanie** a **trestné stíhanie** trestnej činnosti páchanej za pomoci kybernetického priestoru. Existujúci procesný rámec však treba lepšie prispôsobiť internetovému veku[65]. Naše postupy nemusia byť schopné držať krok s rýchlosťou kybernetických útokov, ktorá môže vyvolať konkrétnu potrebu rýchlej cezhraničnej spolupráce. Komisia na tento účel, ako bolo oznámené v Európskom programe v oblasti bezpečnosti, začiatkom roku 2018 predloží návrhy na **uľahčenie cezhraničného prístupu k elektronickým dôkazom**. Súčasne Komisia vykonáva praktické opatrenia na zlepšenie cezhraničného prístupu k elektronickým dôkazom pri vyšetrovaní trestných činov vrátane financovania odbornej prípravy v oblasti cezhraničnej spolupráce, rozvoja elektronickej platformy na výmenu informácií v rámci EÚ a štandardizácie formulárov používaných na justičnú spoluprácu medzi členskými štátmi.
Ďalšou prekážkou účinného trestného stíhania sú rozličné forenzné postupy na získavanie elektronických dôkazov v súvislosti s vyšetrovaniami počítačovej kriminality v členských štátoch. Túto prekážku by bolo možné zmierniť postupným zavedením spoločných noriem vo forenznej oblasti. Okrem toho na podporu vysledovateľnosti a prisudzovania zodpovednosti treba posilniť forenzné kapacity. Jedným krokom by bolo ďalej rozvíjať forenzné kapacity v Europole prispôsobením existujúcich rozpočtových a ľudských zdrojov Európskeho centra boja proti počítačovej kriminalite, ktoré pôsobí v rámci Europolu, s cieľom uspokojiť rastúce potreby týkajúce sa operačnej podpory pri cezhraničných vyšetrovaniach počítačovej kriminality. V ďalšom kroku by sa vyššie uvedená požiadavka technologického zamerania v prípade šifrovania mohla odraziť v skúmaní toho, ako jeho zneužívanie zločincami vytvára veľké výzvy v boji proti závažnej trestnej činnosti vrátane terorizmu a počítačovej kriminality. Komisia predloží výsledky súčasných úvah o **úlohe šifrovania pri vyšetrovaní trestných činov**[66] do októbra 2017[67].

Vzhľadom na bezhraničnú povahu internetu rámec medzinárodnej spolupráce **Budapeštianskeho dohovoru Rady Európy o počítačovej kriminalite**[68] poskytuje rozmanitej skupine krajín príležitosť využívať optimálnu právnu normu v prípade rôznych vnútroštátnych právnych predpisov týkajúcich sa počítačovej kriminality. V súčasnosti sa skúma možnosť pridania protokolu k dohovoru[69], čo by takisto poskytlo užitočnú príležitosť

---

[63] Protokol dopytu a odozvy, ktorý sa často používa na prehľadávanie databáz, ktoré obsahujú údaje o registrovaných používateľoch alebo pridelených prostriedkoch internetových zdrojov.

[64] Internetová korporácia pre prideľovanie mien a čísel (ICANN) je nezisková organizácia, ktorá je zodpovedná za koordináciu údržby a postupov v rámci niekoľkých databáz týkajúcich sa internetových priestorov názvov (namespaces).

[65] Ako jeden z príkladov uvádzame (virtuálny) server ústredného velenia a riadenia botnetu Avalanche, ktorý presúval fyzické servery a domény každých päť minút.

[66] Predsedníctvo Rady, Výsledky zasadnutia Rady pre spravodlivosť a vnútorné veci z 8. – 9. decembra 2016, č. 15391/16.

[67] Ôsma správa o pokroku smerom k dosiahnutiu účinnej a skutočnej bezpečnostnej Únie, 29. júna 2017, COM(2017) 354 final.

[68] Tento dohovor je prvou medzinárodnou dohodou v oblasti trestnej činnosti páchanej prostredníctvom internetu a iných počítačových sietí, ktorá sa osobitne zaoberá porušovaním autorských práv, počítačovými podvodmi, detskou pornografiou a porušovaním bezpečnosti sietí. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 V roku 2017 ratifikovalo Dohovor Rady Európy o počítačovej kriminalite alebo k nemu pristúpilo 55 vlád.

[69] Mandát na prípravu návrhu 2. dodatkového protokolu k Budapeštianskemu dohovoru o počítačovej kriminalite, T-CY (2017)3.

na riešenie otázky cezhraničného prístupu k elektronickým dôkazom v medzinárodnom kontexte. Namiesto vytvárania nových medzinárodných právnych nástrojov pre otázky počítačovej kriminality EÚ vyzýva všetky krajiny, aby vypracovali vhodné vnútroštátne právne predpisy a ďalej rozvíjali spoluprácu v rámci existujúceho medzinárodného rámca.

Rozšírená dostupnosť anonymizačných nástrojov umožňuje páchateľom schovávať sa. **„Darknet“**[70] otvoril pre páchateľov nové možnosti prístupu k detskej pornografii, drogám alebo strelným zbraniam, často s nízkym rizikom odhalenia[71]. Takisto je teraz kľúčovým zdrojom nástrojov používaných pri počítačovej trestnej činnosti, ako sú napríklad škodlivé softvéry a hackovacie nástroje. Komisia bude spolu s príslušnými zainteresovanými stranami analyzovať vnútroštátne prístupy s cieľom nájsť nové riešenia. Europol by mal uľahčovať a podporovať vyšetrovania súvisiace s darknetom, mal by posudzovať hrozby a pomáhať pri určovaní právomoci a stanovovaní priority pre vysoko rizikové prípady a EÚ môže zohrávať vedúcu úlohu pri koordinácii medzinárodnej akcie[72].
Jednou z čoraz častejších oblastí počítačovej trestnej činnosti je podvodné používanie údajov z kreditných kariet alebo iných elektronických platobných prostriedkov. Platobné údaje získané prostredníctvom kybernetických útokov proti online maloobchodným predajcom alebo iným legitímnym podnikom sa potom predávajú online a páchatelia ich môžu používať na páchanie podvodov[73]. Komisia predkladá návrh na posilnenie odrádzajúceho účinku prostredníctvom **o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich falšovaniu**[74]. Cieľom návrhu je aktualizovať existujúce pravidlá v tejto oblasti a posilniť schopnosť orgánov presadzovania práva bojovať proti tejto forme trestnej činnosti.
Okrem toho treba posilniť kapacity na vyšetrovanie počítačovej kriminality, ktoré majú k dispozícii orgány presadzovania práva v členských štátoch, ako aj zlepšiť chápanie trestnej činnosti páchanej za pomoci kybernetického priestoru a možnosti dokazovania zo strany prokurátorov a sudcov. Eurojust a Europol prispievajú k tomuto cieľu a k posilnenej koordinácii v úzkej spolupráci so špecializovanými poradnými skupinami pôsobiacimi v rámci centra boja proti počítačovej kriminalite Europolu a so sieťami veliteľov jednotiek boja proti počítačovej kriminalite a prokurátorov, ktorí sa špecializujú na počítačovú kriminalitu. Komisia vyčlení 10,5 milióna EUR na boj proti počítačovej kriminalite, a to najmä v rámci **policajného programu Fondu pre vnútornú bezpečnosť**. Odborná príprava je dôležitým prvkom a Európska skupina pre vzdelávanie a odbornú prípravu v oblasti boja proti počítačovej kriminalite vypracovala niekoľko užitočných materiálov. Tie by sa teraz s podporou Agentúry Európskej únie pre odbornú prípravu v oblasti presadzovania práva (CEPOL) mali všeobecne prezentovať profesionálom v oblasti presadzovania práva.

3.3 Spolupráca verejného a súkromného sektora v boji proti počítačovej kriminalite

[70] Darknet pozostáva z obsahu v prekrývajúcich sa sieťach, ktoré využívajú internet, ale na prístup si vyžadujú špecifický softvér, konfigurácie alebo povolenie. Darknet tvorí malú časť deep webu, časť webu, ktorá sa neindexuje prostredníctvom vyhľadávačov.

[71] Pozoruhodnou výnimkou je nedávne odstránenie dvoch z najväčších zločineckých dark web trhov AlphaBay a Hansa: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

[72] Europol už v tejto oblasti zohráva významnú úlohu. Pozri nedávny príklad: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

[73] Výnosy z podvodov sú dôležitým zdrojom príjmov pre organizovaný zločin, a preto predstavujú faktor, ktorý umožňuje ďalšiu trestnú činnosť, ako napríklad terorizmus, obchodovanie s drogami a obchodovanie s ľuďmi.

[74] COM(2017) 489.

Účinnosť tradičných mechanizmov presadzovania práva je spochybnená prvkami digitálneho sveta, ktorý tvoria prevažne infraštruktúry v súkromnom vlastníctve a mnoho rôznych aktérov v rôznych jurisdikciách. V dôsledku toho má spolupráca so súkromným sektorom vrátane priemyslu a občianskej spoločnosti zásadný význam pre orgány verejnej moci, aby mohli účinne bojovať proti trestnej činnosti. V tejto súvislosti má kľúčovú úlohu aj finančný sektor a spolupráca s ním by sa mala zintenzívniť. Napríklad mala by sa posilniť úloha finančných spravodajských jednotiek[75] v súvislosti s počítačovou kriminalitou.

Niektoré členské štáty už prijali kľúčové opatrenia. V Holandsku finančné inštitúcie a orgány presadzovania práva spolupracujú na riešení online podvodov a počítačovej kriminality formou pracovnej skupiny pre elektronickú kriminalitu. Nemecké kompetenčné centrum boja proti počítačovej kriminalite poskytuje operačnú platformu pre svojich členov na výmenu informácií v úzkej spolupráci so Spolkovým vyšetrovacím úradom a rozvoj opatrení zameraných na zabezpečenie ochrany proti počítačovej kriminalite. 16 členských štátov[76] vytvorilo centrá excelentnosti v oblasti boja proti počítačovej kriminalite s cieľom uľahčiť spoluprácu medzi orgánmi presadzovania práva, akademickou obcou a súkromnými partnermi pri rozvoji a výmene najlepších postupov, odbornej príprave a budovaní kapacít.
Komisia podporuje vytváranie verejno-súkromných partnerstiev a mechanizmov spolupráce prostredníctvom osobitných projektov, ako napríklad kybernetické centrum a sieť expertov na boj proti online podvodom[77], zavádzanie modelu a normy na spoločné využívanie informácií s cieľom analyzovať a zmierňovať riziká elektronických trestných činov a online podvodov.

V kontexte počítačovej kriminality musia mať súkromné podniky možnosť vymieňať si s orgánmi presadzovania práva informácie o konkrétnych incidentoch – vrátane osobných údajov – pri plnom dodržiavaní pravidiel ochrany údajov. V rámci reformy ochrany údajov v EÚ, ktorá sa začne uplatňovať v máji 2018, sa stanovuje spoločný súbor pravidiel, v ktorých sa určujú podmienky, za akých môžu spolupracovať orgány presadzovania práva a súkromné subjekty. Európska komisia bude spolupracovať s Európskym výborom pre ochranu údajov a príslušnými zainteresovanými stranami s cieľom určiť najlepšie postupy v tejto oblasti a v prípade potreby bude poskytovať usmernenia.

3.4 Zintenzívnenie politickej reakcie

V nedávno prijatom **rámci pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti**[78] („balík nástrojov pre diplomaciu v oblasti kybernetiky“) sa stanovujú opatrenia v rámci spoločnej zahraničnej a bezpečnostnej politiky vrátane reštriktívnych opatrení, ktoré sa môžu použiť na posilnenie reakcie EÚ na činnosti, ktoré poškodzujú jej politické, bezpečnostné a hospodárske záujmy. Rámec predstavuje dôležitý krok v rozvoji signalizačných a reaktívnych kapacít na úrovni EÚ a na úrovni členských štátov. Zvýši našu schopnosť pripisovať zodpovednosť za škodlivé kybernetické činnosti s cieľom ovplyvniť správanie potenciálnych agresorov, pričom sa bude prihliadať na potrebu zabezpečiť

[75] Finančné spravodajské jednotky slúžia ako národné centrá pre prijímanie a analyzovanie správ o podozrivých transakciách a iných informácií relevantných z hľadiska prania špinavých peňazí, súvisiacich predikatívnych trestných činov a financovania terorizmu, ako aj pre šírenie výsledkov takýchto analýz.

[76] Belgicko, Bulharsko, Cyprus, Česká republika, Estónsko, Francúzsko, Grécko, Írsko, Litva, Nemecko, Poľsko, Rakúsko, Rumunsko, Slovinsko, Spojené kráľovstvo a Španielsko.

[77] Cieľom iniciatívy EÚ-OF2CEN je umožniť systematickú, celoeurópsku výmenu informácií o internetových podvodoch medzi bankami a orgánmi presadzovania práva s cieľom zamedziť platby podvodníkom a bielym koňom a na účely vyšetrovania a trestného stíhania páchateľov. Iniciatívu spolufinancuje EÚ (policajný program Fondu pre vnútornú bezpečnosť).

[78] http://www.consilium.europa.eu/sk/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.

primeranú reakciu. Pripísanie zodpovednosti štátnemu alebo neštátnemu subjektu zostáva suverénnym politickým rozhodnutím založeným na spravodajských informáciách vychádzajúcich zo všetkých zdrojov. V súčasnosti v členských štátoch prebiehajú činnosti zamerané na vykonávanie rámca, ktoré budú pokračovať v úzkej koordinácii s plánom spolupráce s cieľom reagovať na rozsiahle kybernetické incidenty[79]. Centrum INTCEN[80] by malo v úzkej spolupráci s členskými štátmi a inštitúciami EÚ zhromažďovať, analyzovať a šíriť situačné povedomie potrebné na využívanie opatrení tohto rámca.

3.5 Vytváranie odrádzajúceho účinku na zvýšenie kybernetickej bezpečnosti prostredníctvom obrannej spôsobilosti členských štátov

Členské štáty už rozvíjajú spôsobilosti v oblasti kybernetickej obrany. Okrem toho vzhľadom na stieranie hraníc medzi kybernetickou obranou a kybernetickou bezpečnosťou a dvojaké použitie počítačových nástrojov a technológií, ako aj na veľké rozdiely medzi prístupmi členských štátov má EÚ dobrú pozíciu na to, aby podporovala synergie medzi vojenskými a civilnými úsiliami[81].

Členské štáty s vyspelejšími spôsobilosťami v oblasti kybernetickej bezpečnosti, ktoré by sa chceli združiť, by mohli uvažovať s podporou vysokého predstaviteľa/vysokej predstaviteľky, Komisie a Európskej obrannej agentúry o zahrnutí kybernetickej obrany do rámca „stálej štruktúrovanej spolupráce“ (PESCO). Takáto spolupráca by sa mohla podporovať vyššie uvedenými činnosťami na podporu priemyselných kapacít a strategickej autonómie EÚ. EÚ môže takisto podporovať interoperabilitu, a to aj podporou rozvoja spôsobilostí, koordinácie odbornej prípravy a vzdelávania a úsilia o normalizáciu v oblasti dvojakého použitia.

Rovnako by sa mal v plnej miere využívať spoločný rámec s cieľom reagovať na hybridné hrozby, ktoré často zahŕňajú kybernetické útoky, najmä prostredníctvom strediska EÚ pre hybridné hrozby a nedávno zriadeného Európskeho centra pre boj proti hybridným hrozbám v Helsinkách, ktorých úlohou je podporovať strategický dialóg, viesť výskum a uskutočňovať analýzy.

EÚ obnoví dôraz na politický rámec EÚ pre kybernetickú obranu z roku 2014[82] ako nástroj na ďalšie začleňovanie kybernetickej bezpečnosti a kybernetickej obrany do spoločnej bezpečnostnej a obrannej politiky (SBOP). Kybernetická odolnosť misií a operácií v rámci SBOP je nevyhnutná: vypracujú sa štandardizované postupy a technické spôsobilosti, ktoré by mohli slúžiť na podporu nasadenia civilných aj vojenských misií a operácií, ako aj na podporu ich príslušných štruktúr plánovania a vedenia a poskytovateľov služieb v oblasti informačných technológií pre Európsku službu pre vonkajšiu činnosť (ESVČ). S cieľom zintenzívniť spoluprácu členských štátov a lepšie usmerňovať úsilie EÚ v tejto oblasti Európska obranná agentúra a ESVČ v spolupráci s útvarmi Komisie uľahčia účasť na strategickej úrovni medzi tvorcami politík v oblasti kybernetickej obrany v členských štátoch. EÚ bude takisto podporovať rozvoj európskych riešení kybernetickej bezpečnosti ako súčasť svojho úsilia v prospech európskej obrannej technologickej a priemyselnej základne. Patrí sem aj podpora regionálnych zoskupení excelentnosti pre kybernetickú bezpečnosť a obranu.

---

79 C(2017) 6100.

80 JOIN(2016) 018 final.

81 EÚ považuje kybernetický priestor za podobnú oblasť operácií, ako sú pozemný, vzdušný a námorný priestor. Úsilie v oblasti kybernetickej obrany zahŕňa aj ochranu a odolnosť kozmických zariadení a súvisiacej pozemnej infraštruktúry.

82 www.consilium.europa.eu/sk/workarea/downloadasset.aspx?id=40802190515.

Útvary Komisie v úzkej spolupráci s ESVČ, členskými štátmi a ďalšími príslušnými orgánmi EÚ zavedú do roku 2018 **platformu odbornej prípravy a vzdelávania v oblasti kybernetickej obrany**, ktorá bude slúžiť na riešenie existujúceho nedostatku zručností v oblasti kybernetickej obrany. Tieto činnosti budú dopĺňať prácu Európskej obrannej agentúry v tejto oblasti a pomáhať pri riešení súčasného nedostatku zručností v oblasti kybernetickej bezpečnosti a kybernetickej obrany.

Kľúčové opatrenia

- Iniciatíva Komisie pre cezhraničný prístup k elektronickým dôkazom (začiatkom roka 2018),
- rýchle prijatie navrhovanej smernice o boji proti podvodom a falšovaniu bezhotovostných platobných prostriedkov Európskym parlamentom a Radou,
- zavedenie požiadaviek na IPv6 pri obstarávaní, výskume a financovaní projektov EÚ, dobrovoľné dohody medzi členskými štátmi a poskytovateľmi internetových služieb s cieľom stimulovať prechod na IPv6,
- obnovené/rozšírené zameranie Europolu na počítačovú forenznú analýzu a monitorovanie darknetu,
- vykonávanie rámca pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti,
- zvýšená finančná podpora pre vnútroštátne a nadnárodné projekty zamerané na zlepšenie trestného súdnictva v oblasti kybernetického priestoru,
- vytvorenie vzdelávacej platformy pre kybernetickú bezpečnosť v roku 2018 s cieľom riešiť existujúci nedostatok zručností v oblasti kybernetickej bezpečnosti a kybernetickej obrany.

4. POSILNENIE MEDZINÁRODNEJ SPOLUPRÁCE V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

Vychádzajúc zo základných hodnôt EÚ a zo základných práv, ako je sloboda prejavu a právo na súkromie a ochranu osobných údajov, a v záujme podpory otvoreného, slobodného a bezpečného kybernetického priestoru je medzinárodná politika EÚ v oblasti kybernetickej bezpečnosti navrhovaná s cieľom reagovať na neustále sa meniacu výzvu podporovať globálnu kybernetickú stabilitu, ako aj prispievať k strategickej autonómii Európy v kybernetickom priestore.

4.1 Kybernetická bezpečnosť a vonkajšie vzťahy

Dôkazy nasvedčujú tomu, že ľudia z celého sveta považujú kybernetické útoky z iných krajín za popredné hrozby pre národnú bezpečnosť[83]. Vzhľadom na globálnu povahu hrozby je budovanie a udržiavanie spoľahlivých spojenectiev a partnerstiev s tretími krajinami základom prevencie kybernetických útokov a odrádzania od nich, keďže čoraz viac ohrozujú medzinárodnú stabilitu a bezpečnosť. EÚ sa vo svojich záväzkoch – či už dvoj- a viacstranných, alebo tých voči regionálnym subjektom a viacerým zainteresovaným stranám – bude prioritne zameriavať na vytvorenie strategického rámca na predchádzanie konfliktom a pre stabilitu v kybernetickom priestore.

EÚ dôrazne podporuje stanovisko, že medzinárodné právo, najmä Charta OSN, sa uplatňuje v kybernetickom priestore. Ako doplnok k záväznému medzinárodnému právu EÚ potvrdzuje dobrovoľné nezáväzné normy, pravidlá a zásady zodpovedného správania sa štátov, ktoré

[83] *Spring 2017 Global Attitudes Survey* (Prieskum globálnych postojov z jari 2017), Pew Research Centre.

sformulovala skupina vládnych expertov OSN[84]; EÚ takisto podporuje rozvoj a vykonávanie opatrení na budovanie dôvery na regionálnej úrovni, tak v rámci Organizácie pre bezpečnosť a spoluprácu v Európe, ako aj v iných regiónoch.

Na bilaterálnej úrovni budú pokračovať dialógy o kybernetickej bezpečnosti[85], ktoré bude ďalej rozvíjať a dopĺňať úsilie zamerané na uľahčenie spolupráce s tretími krajinami s cieľom posilniť zásady náležitej starostlivosti a zodpovednosti štátu v otázkach týkajúcich sa kybernetického priestoru. Európska únia sa prioritne zameria na otázky medzinárodnej bezpečnosti v kybernetickom priestore v rámci svojich medzinárodných záväzkov a zároveň zabezpečí, aby sa kybernetická bezpečnosť nestala zámienkou na ochranu trhu a obmedzenie základných práv a slobôd vrátane slobody prejavu a prístupu k informáciám. Komplexný prístup ku kybernetickej bezpečnosti si vyžaduje dodržiavanie ľudských práv a EÚ bude naďalej presadzovať svoje základné hodnoty na celom svete, pričom bude vychádzať z usmernení EÚ v oblasti ľudských práv týkajúcich sa slobody prejavu online[86]. EÚ v tejto súvislosti zdôrazňuje význam zapojenia všetkých zainteresovaných strán do riadenia internetu.

Komisia takisto predložila návrh[87] na modernizáciu kontrol vývozu EÚ vrátane zavedenia kontrol vývozu kritických technológií kybernetického dohľadu, ktoré by mohli spôsobovať porušovanie ľudských práv alebo by sa mohli zneužiť na ohrozenie bezpečnosti samotnej EÚ, a zintenzívni dialógy s tretími krajinami s cieľom podporovať celosvetové zbližovanie a zodpovedné správanie v tejto oblasti.

4.2 Budovanie kyberneticko-bezpečnostných kapacít

Globálna kybernetická stabilita závisí od schopnosti miestnych a celoštátnych aktérov všetkých krajín predchádzať kybernetickým incidentom a reagovať na ne, ako aj vyšetrovať a stíhať prípady počítačovej kriminality. Podpora úsilia o budovanie odolnosti tretích krajín zvýši úroveň kybernetickej bezpečnosti na celom svete, čo bude mať pozitívne dôsledky aj pre EÚ. Boj proti rýchlo sa vyvíjajúcim kybernetickým hrozbám si vyžaduje odbornú prípravu, úsilie o tvorbu politiky a právnych predpisov, ako aj efektívne fungujúce tímy reakcie na núdzové počítačové situácie a jednotky boja proti počítačovej kriminalite vo všetkých krajinách na celom svete.

EÚ je od roku 2013 na čele medzinárodného budovania kapacít kybernetickej bezpečnosti a systematicky toto úsilie prepája so svojou rozvojovou spoluprácou. EÚ bude naďalej podporovať model budovania kapacít založený na právach v súlade s prístupom Digital4Development[88]. Prioritami pre EÚ, pokiaľ ide o budovanie kapacít, budú krajiny európskeho susedstva a rozvojové krajiny, v ktorých sa rýchlo rozmáha pripojiteľnosť a rýchlo narastajú kybernetické hrozby. Úsilie EÚ bude dopĺňať rozvojovú agendu EÚ vzhľadom na program trvalo udržateľného rozvoja do roku 2030 a celkové úsilie zamerané na budovanie inštitucionálnych kapacít.

S cieľom zlepšiť schopnosť EÚ mobilizovať svoje kolektívne odborné znalosti na podporu tohto budovania kapacít by sa mala vytvoriť špecializovaná sieť zameraná na budovanie kybernetických kapacít EÚ, ktorá by združovala ESVČ, orgány členských štátov zodpovedné

---

[84] A/68/98 a A/70/174.

[85] V septembri 2017 sa uskutočnili dialógy o kybernetickej bezpečnosti medzi EÚ a USA, Čínou, Japonskom, Kórejskou republikou a Indiou.

[86] Usmernenia EÚ v oblasti ľudských práv týkajúce sa slobody prejavu online a offline.

[87] COM(2016) 616.

[88] SWD(2017) 157.

za otázky kybernetiky, agentúry EÚ, útvary Komisie, akademickú obec a občiansku spoločnosť. V záujme kvalitnejšieho politického vedenia a ľahšieho stanovovania priorít v úsilí EÚ o pomoc tretím krajinám budú vypracované usmernenia EÚ o budovaní kybernetických kapacít.

EÚ bude navyše spolupracovať s ostatnými darcami v tejto oblasti, aby zabránila duplicitnej práci a umožnila cielenejšie budovanie kapacít v rôznych regiónoch.

4.3 Spolupráca medzi EÚ a NATO

EÚ v nadväznosti na doposiaľ dosiahnutý podstatný pokrok posilní spoluprácu s organizáciou NATO v oblasti kybernetickej bezpečnosti, hybridných hrozieb a obrany, ako sa uvádza v spoločnom vyhlásení z 8. júla 2016[89]. Medzi priority patrí podpora interoperability prostredníctvom zosúladených požiadaviek a noriem kybernetickej obrany, posilnenie spolupráce v oblasti odbornej prípravy a cvičení a harmonizácia požiadaviek na odbornú prípravu.

EÚ a NATO budú takisto podporovať spoluprácu v oblasti výskumu a inovácie v rámci kybernetickej obrany a budú sa opierať o súčasné technické opatrenia v oblasti výmeny informácií týkajúcich sa kybernetickej bezpečnosti medzi svojimi príslušnými kybernetickobezpečnostnými orgánmi[90]. Nedávne spoločné úsilie v oblasti boja proti hybridným hrozbám, najmä spolupráca medzi strediskom EÚ pre hybridné hrozby a zložkou NATO pre hybridné analýzy by mala ďalej posilniť odolnosť voči kybernetickým krízam a reakciu na ne. Ďalšia spolupráca medzi EÚ a NATO sa bude posilňovať prostredníctvom cvičení v oblasti kybernetickej obrany za účasti ESVČ a iných subjektov EÚ a príslušných partnerov NATO vrátane Centra excelentnosti NATO pre spoluprácu v oblasti kybernetickej obrany v Tallinne. NATO a EÚ budú po prvýkrát uskutočňovať paralelné a koordinované cvičenia v reakcii na hybridný scenár, pričom NATO bude mať vedúcu pozíciu v roku 2017, ktorú v roku 2018 podobným spôsobom prevezme EÚ. Ďalšia správa o spolupráci medzi EÚ a NATO, ktorá sa má predložiť príslušným radám v decembri 2017, bude príležitosťou, aby sa zvážili možnosti na ďalšie rozšírenie spolupráce, najmä zabezpečením spoločných, bezpečných a spoľahlivých komunikačných prostriedkov medzi všetkými príslušnými inštitúciami a orgánmi vrátane agentúry ENISA.

Kľúčové opatrenia

- Pokročiť v strategickom rámci na predchádzanie konfliktom a stabilitu v kybernetickom priestore,
- vytvoriť novú sieť na budovanie kapacít na podporu schopnosti tretích krajín reagovať na kybernetické hrozby a vypracovať usmernenia EÚ o budovaní kybernetickobezpečnostných kapacít zamerané na lepšie stanovenie priorít v rámci úsilia EÚ,
- ďalšia spolupráca medzi EÚ a NATO vrátane účasti na paralelných a koordinovaných cvičeniach a posilnenej interoperability kyberneticko-bezpečnostných noriem.

5. ZÁVER

[89] http://www.consilium.europa.eu/sk/press/press-releases/2016/07/08-eu-nato-joint-declaration/.

[90] CERT-EU a NATO Computer Incident Response Capability (NCIRC, jednotka NATO na riešenie počítačových incidentov).

Kybernetická pripravenosť EÚ je ústredným prvkom digitálneho jednotného trhu aj našej bezpečnostnej a obrannej únie. Posilnenie európskej kybernetickej bezpečnosti a riešenie hrozieb pre civilné aj vojenské ciele je nevyhnutnou požiadavkou.

Nadchádzajúci digitálny samit, ktorý organizuje estónske predsedníctvo 29. septembra 2017, poskytuje príležitosť preukázať spoločné odhodlanie prisúdiť kybernetickej bezpečnosti ústredné postavenie v EÚ ako digitálnej spoločnosti. Ako súčasť tohto spoločného záväzku Komisia vyzýva členské štáty, aby sa zaviazali, akým spôsobom chcú konať v oblastiach, v ktorých majú primárnu zodpovednosť. Tento záväzok by mal zahŕňať posilnenie kybernetickej bezpečnosti na základe týchto opatrení:

- zabezpečenie úplného a účinného vykonávania smernice NIS do 9. mája 2018, ako aj zdrojov potrebných pre verejné orgány zodpovedné za kybernetickú bezpečnosť, aby mohli účinne vykonávať svoje úlohy,
- uplatňovanie rovnakých pravidiel v rámci verejných správ vzhľadom na úlohu, ktorú zohrávajú v spoločnosti a hospodárstve ako celku,
- poskytovanie odbornej prípravy zameranej na kybernetickú bezpečnosť pre pracovníkov verejných správ,
- umiestňovanie kybernetického povedomia do popredia v rámci informačných kampaní a zahrnutie kybernetickej bezpečnosti do učebných plánov akademického a odborného vzdelávania,
- využívanie iniciatív v rámci „stálej štruktúrovanej spolupráce“ (PESCO) a Európskeho obranného fondu na podporu vývoja projektov v oblasti kybernetickej obrany.

V tomto spoločnom oznámení sa stanovil rozsah problému a škála opatrení, ktoré môže EÚ prijať. Potrebujeme Európu, ktorá je odolná, ktorá dokáže účinne chrániť svojich občanov tým, že bude predvídať možné kybernetické incidenty, budovaním silnej ochrany vo svojich štruktúrach a správaní, rýchlou nápravou škôd spôsobených kybernetickými útokmi a odrádzaním osôb zodpovedných za kybernetické hrozby a útoky. V tomto oznámení sa predkladajú cielené opatrenia, ktorými sa budú ďalej posilňovať štruktúry a spôsobilosti EÚ v oblasti kybernetickej bezpečnosti koordinovaným spôsobom za plnej spolupráce členských štátov a rôznych zapojených štruktúr EÚ a pri rešpektovaní ich právomocí a zodpovedností. Jeho vykonávanie poskytne jasný dôkaz toho, že EÚ a členské štáty budú pracovať spoločne, aby zaviedli normy kybernetickej bezpečnosti, ktoré budú zodpovedať neustále rastúcim výzvam, ktorým Európa v súčasnosti čelí.