Rada
Evropské unie

Brusel 14. září 2017
(OR. en)

12211/17

CYBER 132
RELEX 767
JAI 790
ENFOPOL 413
TELECOM 212
MI 633
RECH 308

PRŮVODNÍ POZNÁMKA

Odesílatel:	Jordi AYET PUIGARNAU, ředitel, za generálního tajemníka Evropské komise
Datum přijetí:	13. září 2017
Příjemce:	Jeppe TRANHOLM-MIKKELSEN, generální tajemník Rady Evropské unie
Č. dok. Komise:	JOIN(2017) 450 final
Předmět:	SPOLEČNÉ SDĚLENÍ EVROPSKÉMU PARLAMENTU A RADĚ Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU

Delegace naleznou v příloze dokument JOIN(2017) 450 final.

Příloha: JOIN(2017) 450 final

EVROPSKÁ
KOMISE

VYSOKÁ PŘEDSTAVITELKA
UNIE PRO ZAHRANIČNÍ
VĚCI A BEZPEČNOSTNÍ
POLITIKU

V Bruselu dne 13.9.2017
JOIN(2017) 450 final

SPOLEČNÉ SDĚLENÍ EVROPSKÉMU PARLAMENTU A RADĚ

Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU

1. ÚVOD

Kybernetická bezpečnost je kriticky důležitá pro naši prosperitu i bezpečnost. Jak se naše každodenní životy a ekonomiky stávají závislejší na digitálních technologiích, jsme kybernetickým hrozbám vystaveni čím dál tím víc. Kybernetické bezpečnostní incidenty se stále více různí, a to jak z hlediska toho, kdo je za ně odpovědný, tak i toho, čeho se snaží dosáhnout. Nekalé činnosti v kyberprostoru ohrožují nejenom naše ekonomiky a prosazování jednotného digitálního trhu, ale také samotné fungování našich demokracií, naši svobodu a naše hodnoty. Naše budoucí bezpečnost závisí na transformaci našich schopností chránit EU před kybernetickými hrozbami: civilní infrastruktura i vojenská kapacita se opírají o bezpečné digitální systémy. Bylo to uznáno Evropskou radou v červnu 2017[1] a také v Globální strategii zahraniční a bezpečnostní politiky Evropské unie[2].

Rizika rostou exponenciálně. Studie ukazují, že hospodářský dopad kyberkriminality se od roku 2013 do roku 2017 zvýšil pětinásobně a do roku 2019 by se mohl dále zčtyřnásobit[3]. Roste zejména dopad ransomwaru[4] a poslední útoky[5] odrážejí značný nárůst kybernetické trestné činnosti. Ransomware však zdaleka není jedinou hrozbou.

Kybernetické hrozby pocházejí jak od nestátních, tak i od státních subjektů: často jde o trestnou činnost motivovanou ziskem, pohnutky mohou však být i politické a strategické. Hrozbu trestné činnosti stupňuje stírání hranic mezi kyberkriminalitou a „tradičními“ trestnými činy, protože zločinci používají internet jednak jako cestu, jak svou činnost rozšířit, jednak jako zdroj pro hledání nových metod a nástrojů pro páchání trestných činů[6]. V převážné většině případů jsou však šance na vysledování zločinců minimální a šance na jejich stíhání ještě menší.

Současně s tím státní subjekty dosahují ve stále větší míře svých geopolitických cílů nejenom prostřednictvím tradičních nástrojů, jako jsou vojenské síly, ale také pomocí méně nápadných kybernetických nástrojů, včetně zasahování do vnitřních demokratických procesů. V současné době se všeobecně přiznává využívání kybernetického prostoru jako oblasti vedení války, a to buď samostatně, nebo v rámci hybridního přístupu. Dezinformační kampaně, falešné zprávy a kybernetické operace namířené na kritickou infrastrukturu jsou čím dál tím běžnější a vyžadují si reakci. Proto Komise ve svém diskusním dokumentu o budoucnosti evropské obrany[7] zdůraznila význam spolupráce v oblasti kybernetické obrany.

Pokud svou kybernetickou bezpečnost podstatně nezlepšíme, bude se riziko souběžně s digitální transformací zvyšovat. Očekává se, že do roku 2020 budou na internet připojeny desítky miliard zařízení „internetu věcí“, ale kybernetická bezpečnost zatím nemá při jejich konstruování prioritu[8]. Když se nebudou chránit zařízení, která budou řídit naše energetické sítě, vozidla a dopravní sítě, podniky, finance, nemocnice a domovy, mohlo by to mít

---

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

2 http://europa.eu/globalstrategy/

3 Viz například „Net losses: Estimating the Global Cost of Cybercrime“ (Čisté ztráty: Odhad globálních nákladů způsobených kyberkriminalitou), McAfee & Centre for Strategic and International Studies, 2014.

4 Ransomware je typ škodlivého softwaru, který zabraňuje uživatelům v přístupu k jejich systému, nebo ho omezuje, a to buď blokováním obrazovky systému, nebo blokováním uživatelských souborů, pokud se nezaplatí výkupné.

5 V květnu 2017 útok ransomwaru WannaCry postihl přes 400 000 počítačů ve více než 150 zemích. O měsíc později útok ransomwaru „Petya“ zasáhl Ukrajinu a několik společností na celém světě.

6 Posouzení hrozeb závažné organizované trestné činnosti, Europol, 2017.

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

8 IDC a TXT Solutions (2014), SMART 2013/0037. Propojení cloud computingu a internetu věcí, studie vypracovaná pro Evropskou komisi.

zničující následky a nesmírně poškodit důvěru spotřebitelů ve vznikající technologie. Nebezpečí politicky motivovaných útoků na civilní cíle a nedostatky ve vojenské kybernetické obraně toto riziko ještě více prohlubují.

Přístup stanovený v tomto společném sdělení poskytne EU lepší pozici, aby mohla těmto hrozbám čelit. Zabezpečil by větší odolnost a strategickou autonomii, zvýšil by schopnosti z hlediska technologie a dovedností, a také by pomohl vytvořit silný jednotný trh. K tomu je třeba zavést správné struktury, aby byla zajištěna robustní kybernetická bezpečnost a reakce v případě potřeby, a to s plnou účastí všech klíčových subjektů. Tento přístup by také lépe odrazoval od kybernetických útoků, neboť by zintenzivnil práci na tom, aby jejich pachatelé byli odhaleni, vysledováni a pohnáni k odpovědnosti. Rozvojem mezinárodní spolupráce jako platformy pro vedoucí postavení EU v oblasti kybernetické bezpečnosti by rovněž zohlednil mezinárodní rozměr. Tyto kroky jsou založeny na přístupech jednotného digitálního trhu, globální strategii, Evropském programu pro bezpečnost[9], společném rámci pro boj proti hybridním hrozbám[10] a sdělení o vzniku Evropského obranného fondu[11] [12].

EU už na mnohých těchto otázkách pracuje: teď nastal čas spojit různé směry, kterými se práce ubírá. V roce 2013 EU vytyčila strategii kybernetické bezpečnosti, která zahájila řadu klíčových činností ke zvýšení kybernetické odolnosti[13]. Její hlavní cíle a zásady, a to podpora spolehlivého, bezpečného a otevřeného kybernetického ekosystému, zůstávají platné. Situace v oblasti hrozeb, která se neustále vyvíjí a prohlubuje, si však vyžaduje více opatření, abychom odolali a útokům a odradili jejich pachatele i v budoucnosti[14].

Vzhledem k oblasti působnosti svých politik a díky nástrojům, strukturám a schopnostem, které jsou jí k dispozici, má EU dobrou pozici k tomu, aby se kybernetickou bezpečností zabývala. I když za národní bezpečnost nadále odpovídají členské státy, rozsah a přeshraniční charakter hrozby je pádným důvodem pro opatření EU, která členským státům poskytnou pobídky a podporu, aby rozvíjely a udržovaly větší a lepší vnitrostátní schopnosti kybernetické bezpečnosti, a současně vybudují kapacity na úrovni EU. Tento přístup má motivovat všechny subjekty – EU, členské státy, průmysl i jednotlivé osoby – k tomu, aby kybernetické bezpečnosti daly prioritu, která je potřebná k zajištění odolnosti a lepší reakce EU na kybernetické útoky. Přinese konkrétní kroky s cílem pomoci odhalit a vyšetřit jakoukoli formu kybernetických incidentů proti EU a jejím členským státům a příslušně reagovat, včetně stíhání pachatelů trestných činů. Umožní, aby vnější činnost EU účinně podporovala kybernetickou bezpečnost v celosvětovém měřítku. Výsledkem bude, že se EU posune od reaktivního k proaktivnímu přístupu, pokud jde o ochranu evropské prosperity, společnosti a hodnot, jakož i základních práv a svobod, a bude reagovat na existující i budoucí hrozby.

2. BUDOVÁNÍ ODOLNOSTI EU VŮČI KYBERNETICKÝM ÚTOKŮM

Silná kybernetická odolnost vyžaduje kolektivní a široký přístup. K tomu jsou zapotřebí robustnější a efektivnější struktury na podporu kybernetické bezpečnosti a reakci na

[9] COM(2015) 185 final.
[10] JOIN(2016) 18 final.
[11] COM(2017) 295.
[12] Tento přístup je rovněž podložen nezávislým vědeckým poradenstvím poskytovaným skupinou vědeckých poradců Evropské komise na vysoké úrovni v rámci mechanismu vědeckého poradenství (viz odkazy níže).
[13] JOIN(2013) 1 final. Posouzení této strategie je k dispozici v SWD(2017) 295.
[14] Není-li stanoveno jinak, návrhy v tomto sdělení jsou rozpočtově neutrální. Každá iniciativa, která má dopad na rozpočet, bude podléhat řádnému rozpočtovému procesu a nemůže předjímat příští víceletý finanční rámec po roce 2020.

kybernetické útoky v členských státech, ale také v orgánech, agenturách a institucích EU. Také je k tomu zapotřebí komplexnější a průřezový přístup k vytváření kybernetické odolnosti a strategické autonomie se silným jednotným trhem, velkým pokrokem v technologických schopnostech EU a mnohem většími počty kvalifikovaných odborníků. Ústředním prvkem je širší shoda na tom, že kybernetická bezpečnost je společnou společenskou výzvou, takže by se mělo zapojit více úrovní vlády, ekonomiky a společnosti.

2.1 Posílení Agentury Evropské unie pro bezpečnost sítí a informací

Agentura Evropské unie pro bezpečnost sítí a informací (ENISA) má hrát klíčovou roli v posílení kybernetické odolnosti a reakce EU, je však omezená svým současným mandátem. Komise proto předkládá ambiciózní návrh reformy, včetně **stálého mandátu agentury**[15]. Tím se zabezpečí, že ENISA bude moci poskytovat podporu členským státům, orgánům EU a podnikům v klíčových oblastech, včetně provádění směrnice o bezpečnosti sítí a informačních systémů[16] (dále jen „směrnice o bezpečnosti sítí a informací“) a navrženého rámce pro certifikaci kybernetické bezpečnosti.

Reformovaná ENISA bude mít silnou poradní úlohu v rozvoji a provádění politik, včetně podpory soudržnosti mezi odvětvovými iniciativami a směrnicí o bezpečnosti sítí a informací a pomoci při zřizování odvětvových středisek pro sdílení a analýzu informací v kritických odvětvích. ENISA zvýší úroveň evropské připravenosti každoročním pořádáním celoevropských cvičení v kybernetické bezpečnosti, která spojí odezvu napříč různými úrovněmi. Podpoří také rozvoj politiky EU v oblasti certifikace kybernetické bezpečnosti informačních a komunikačních technologií (IKT) a bude hrát významnou roli v prohlubování operativní spolupráce a krizového řízení v celé EU. Agentura bude rovněž sloužit jako kontaktní místo pro informace a znalosti v kruzích zabývajících se kybernetickou bezpečností

Nezbytným předpokladem k rozhodnutí, zda jsou potřebná společná zmírňující opatření nebo jiná reakce podporovaná EU, je rychlé a společné pochopení hrozeb a incidentů, když se odehrávají. Tato výměna informací vyžaduje zapojení všech příslušných subjektů – institucí a agentur EU a také členských států – na technických, operativních a strategických úrovních. ENISA ve spolupráci s příslušnými orgány na úrovni členských států a EU, zejména se sítí bezpečnostních týmů CSIRT[17], CERT-EU, Europolem a Střediskem EU pro analýzu zpravodajských informací (INTCEN), přispěje také k informovanosti o situaci na úrovni EU. To se může využít při zpracování zpravodajských informací o hrozbách a tvorbě politik jak v souvislosti s pravidelným monitorováním situace v oblasti hrozeb a efektivní operativní spoluprací, tak i v reakci na rozsáhlé přeshraniční incidenty.

2.2 Na cestě k jednotnému trhu kybernetické bezpečnosti

Rozvoj trhu kybernetické bezpečnosti v EU – pokud jde o produkty, služby a procesy – zaostává v několika ohledech. Klíčovým aspektem je neexistence režimů certifikace kybernetické bezpečnosti uznávaných v celé EU, které by zajišťovaly vyšší standard odolnosti výrobků a podporovaly důvěru v trh v rámci celé EU. Komise proto předkládá návrh na

[15] COM(2017) 477.

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

[17] Jak stanoví článek 9 směrnice o bezpečnosti sítí a informací.

zřízení **rámce EU pro certifikaci kybernetické bezpečnosti**[18]. Rámec by stanovil postup pro vytvoření celounijních režimů certifikace kybernetické bezpečnosti a zahrnoval by produkty, služby a/nebo systémy, u nichž se úroveň zabezpečení přizpůsobuje jejich použití (ať už jde o kritickou infrastrukturu nebo spotřebitelská zařízení)[19]. Měl by zřejmé přínosy pro podniky, neboť by odstranil potřebu podstupovat několik procesů certifikace při obchodování přes hranice, čímž by omezil administrativní a finanční náklady. Používání režimů vyvinutých na základě tohoto rámce by také pomohlo vytvářet důvěru spotřebitelů, jelikož certifikátem shody by kupující a uživatelé byli informování a ujištěni o bezpečnostních vlastnostech produktů a služeb, které nakupují a používají. Vysoké normy kybernetické bezpečnosti by se tak staly zdrojem konkurenční výhody. Ve výsledku by se dosáhlo vyšší odolnosti, neboť produkty a služby IKT by se formálně hodnotily s ohledem na stanovený soubor norem kybernetické bezpečnosti, které by se mohly vypracovat v úzkém spojení se širší prací probíhající na normách IKT[20].

Režimy podle rámce by byly dobrovolné a neukládaly by prodejcům nebo poskytovatelům služeb žádné bezprostřední regulační povinnosti. Režimy by nebyly v rozporu s žádnými použitelnými právními požadavky, například právními předpisy EU o ochraně osobních údajů.

Jakmile se rámec vytvoří, Komise vyzve příslušné zúčastněné strany, aby se zaměřily na tři prioritní oblasti:

- bezpečnost v kritických nebo vysoce rizikových aplikacích[21]: systémy, na které se spoléháme v každodenním životě – od automobilů po strojní zařízení v podnicích, od největších systémů, jako jsou letadla nebo elektrárny, po nejmenší, např. zdravotnické prostředky – jsou ve stále větší míře digitální a vzájemně propojené. Klíčové komponenty IKT v takových produktech a systémech by proto podléhaly důslednému posouzení bezpečnosti,

- kybernetická bezpečnost ve velmi rozšířených digitálních produktech, sítích, systémech a službách používaných v soukromém i veřejném sektoru, pokud jde o obranu proti útokům a uplatňování regulačních povinností[22] – například šifrování elektronické pošty, firewally a virtuální soukromé sítě (VPN); je nezbytně důležité, aby rozmach používání těchto nástrojů nevedl k novým zdrojům rizika nebo novým zranitelnostem,

- používání metody „bezpečnost již od fáze návrhu“ v levných, digitálních a vzájemně propojených zařízeních pro širokou spotřebitelskou veřejnost, která vytvářejí internet věcí: režimy podle rámce by mohly informovat, že výrobky jsou vytvořeny s použitím nejnovějších metod bezpečného vývoje, že byly podrobeny příslušným bezpečnostním testům a že prodejci se zavázali aktualizovat software v případě nově zjištěných zranitelností nebo hrozeb.

Tyto priority by měly náležitě zohledňovat vyvíjející se situaci v oblasti hrozeb kybernetické bezpečnosti, jakož i důležitost základních služeb, například infrastruktur v oblasti dopravy,

---

[18] COM(2017) 477.

[19] Úroveň zabezpečení udává stupeň důslednosti posouzení bezpečnosti a obvykle je úměrná úrovni rizika spojeného s těmito oblastmi používání nebo funkcemi (tj. pro produkty nebo služby IKT používané ve vysoce rizikových oblastech používání nebo funkcích je požadována vyšší úroveň zabezpečení).

[20] COM(2016) 176.

[21] Výjimkou by byly případy, kdy se povinná nebo dobrovolná certifikace řídí jinými akty Unie.

[22] Například směrnice (EU) 2016/1148, nařízení (EU) 2016/679, směrnice (EU) 2015/2366 a další navrhované právní předpisy, jako je evropský kodex pro elektronické komunikace, vyžadují, aby organizace zavedly příslušná bezpečnostní opatření s cílem řešit relevantní rizika kybernetické bezpečnosti.

energetiky, zdravotní péče, bankovnictví, finančních trhů a pitné vody nebo digitální infrastruktury[23].

I když u žádného produktu, systému nebo služby IKT není možné zaručit „stoprocentní“ bezpečnost, existuje několik dobře známých a podrobně zdokumentovaných nedostatků v návrhu produktů IKT, které lze využít pro útoky. Přístup na základě „bezpečnosti již od fáze návrhu“ přijatý výrobci propojených zařízení, softwaru a IT vybavení by zajistil, že by se kybernetická bezpečnost řešila před uvedením nových produktů na trh. Mohlo by to být součástí zásady „náležité péče“, která by se podrobněji rozpracovala ve spolupráci s průmyslem a mohla by snížit zranitelnost produktů/softwaru pomocí řady metod uplatňovaných od fáze návrhu až po zkoušení a ověřování, včetně případného formálního ověření, dlouhodobé údržby a používání bezpečných procesů životního cyklu vývoje, jakož i vývoje aktualizací a bezpečnostních záplat pro řešení dříve nezjištěných zranitelností a zajištění rychlých aktualizací a oprav[24]. Zvýšilo by to rovněž důvěru spotřebitelů v digitální produkty.

Kromě toho je třeba uznat důležitou úlohu nezávislých výzkumných pracovníků v oblasti bezpečnosti při zjišťování zranitelností existujících produktů a služeb a ve všech členských státech by se měly vytvořit podmínky, které umožní koordinované zveřejňování informací o zranitelnostech[25] na základě osvědčených postupů[26] a příslušných norem[27].

Konkrétní sektory současně čelí specifickým problémům a měly by být podněcovány k tomu, aby si vyvinuly vlastní přístup. Všeobecné strategie kybernetické bezpečnosti by tak byly doplněny odvětvovými strategiemi kybernetické bezpečnosti v oblastech, jako jsou finanční služby[28], energetika, doprava a zdravotnictví[29].

Komise už zdůraznila konkrétní otázky ohledně **odpovědnosti**, které nové digitální technologie přináší[30], a probíhá práce na analýze důsledků; další kroky budou dokončeny do června 2018. Kybernetická bezpečnost staví podniky a dodavatelské řetězce před otázky týkající se připisování škod a jejich neřešení bude brzdit rozvoj silného jednotného trhu v oblasti produktů a služeb kybernetické bezpečnosti.

A v neposlední řadě závisí rozvoj jednotného trhu EU rovněž na začlenění kybernetické bezpečnosti do politiky v oblasti obchodu a investic. Vliv pořizování kritických technologií v zahraničí – jejichž významným příkladem je kybernetická bezpečnost – je klíčovým

---

[23] Odvětví spadající do oblasti působnosti směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

[24] Kybernetická bezpečnost na evropském jednotném digitálním trhu, skupina vědeckých poradců na vysoké úrovni, březen 2017.

[25] Koordinované zveřejňování informací o zranitelnostech je forma spolupráce, která usnadňuje a umožňuje výzkumným pracovníkům v oblasti bezpečnosti hlásit zranitelnosti vlastníkovi nebo prodejci informačního systému a dát organizaci možnost správně a včas diagnostikovat a napravit danou zranitelnost dříve, než jsou podrobnosti o zranitelnosti sděleny třetím stranám nebo veřejnosti.

[26] Například příručka „Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations“ (Příručka osvědčených postupů při zveřejňování zranitelností. Od výzev k doporučením), ENISA, 2016.

[27] ISO/IEC 29147:2014 – Informační technologie – Bezpečnostní techniky – Zveřejňování informací o zranitelnostech.

[28] Nadcházející práce Komise na finančních technologiích bude zahrnovat kybernetickou bezpečnost pro finanční sektor.

[29] Například v odvětví energetiky jde o spojení velmi starých informačních technologií se špičkovými a zejména s požadavky energetické sítě v reálném čase.

[30] COM(2017) 228.

aspektem rámce pro **prověřování přímých zahraničních investic v Evropské unii**[31], jehož cílem je umožnit prověřování investic z třetích zemí z důvodů bezpečnosti a veřejného pořádku. Obdobně už požadavky na kybernetickou bezpečnost vytvořily obchodní překážky pro zboží a služby EU v důležitých odvětvích v řadě ekonomik třetích zemí. Rámec EU pro certifikaci kybernetické bezpečnosti dále posílí mezinárodní postavení Evropy a měl by být doplněn trvalým úsilím zaměřeným na vypracování celosvětových norem vysoké bezpečnosti a dohod o vzájemném uznávání.

2.3 Plné provedení směrnice o bezpečnosti sítí a informací

Jelikož hlavní nástroje v oblasti kybernetické bezpečnosti jsou v současné době ve vnitrostátních rukou, EU identifikovala potřebu prosazovat vyšší normy. Kybernetické bezpečnostní incidenty velkého rozsahu se málokdy dotýkají pouze jednoho členského státu, neboť klíčová odvětví, jako jsou bankovnictví, energetika a doprava, jsou svou povahou ve stále větší míře globalizovaná, závislá na digitálních technologiích a vzájemně propojená.

Směrnice o bezpečnosti sítí a informací je prvním celounijním právním předpisem o kybernetické bezpečnosti[32]. Má zajistit vytvoření odolnosti prostřednictvím zlepšení vnitrostátních kapacit v oblasti kybernetické bezpečnosti, podpory lepší spolupráce mezi členskými státy a požadavku, aby podniky v důležitých hospodářských odvětvích přijaly účinné postupy řízení rizik a hlásily vnitrostátním orgánům závažné incidenty. Tyto povinnosti se vztahují také na tři typy poskytovatelů klíčových internetových služeb: cloud computing, internetové vyhledávače a on-line tržiště. Cílem směrnice je důkladnější a systematičtější přístup a lepší tok informací.

Pro kybernetickou odolnost EU je důležité plné provedení směrnice všemi členskými státy do května 2018. Členské státy tento postup podporují společnou prací, jejímž výsledkem do podzimu 2017 budou pokyny na podporu harmonizovanějšího provádění, zejména pokud jde o provozovatele základních služeb. Komise rovněž jako součást tohoto balíčku o kybernetické bezpečnosti vydává sdělení[33] s cílem podpořit toto úsilí, a to poskytnutím osvědčených postupů od členských států významných pro provádění směrnice a pokynů, jak by směrnice měla fungovat v praxi.

Oblastí, kde směrnice bude muset být doplněna, je tok informací. Směrnice například zahrnuje pouze klíčová strategická odvětví – ale logicky bude nutný podobný přístup všech zúčastněných stran postižených kybernetickými útoky, aby bylo k dispozici systematické posuzování zranitelností a vstupních bodů využívaných pachateli kybernetických útoků. Kromě toho spolupráce a výměna informací mezi veřejným a soukromým sektorem naráží na řadu překážek. Vládní instituce a orgány veřejné správy se zdráhají sdílet informace důležité pro kybernetickou bezpečnost, neboť mají obavy z narušení národní bezpečnosti nebo konkurenceschopnosti. Soukromé podniky se zdráhají sdílet informace o svých kybernetických zranitelnostech a utrpěných ztrátách kvůli obavám z prozrazení citlivých obchodních informací, riziku poškození svého dobrého jména nebo riziku porušení pravidel o ochraně údajů[34]. Musí se posílit důvěra v partnerství veřejného a soukromého sektoru, aby

---

[31] COM(2017) 478.

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

[33] COM(2017) 476.

[34] Kybernetická bezpečnost na evropském jednotném digitálním trhu, skupina vědeckých poradců na vysoké úrovni, březen 2017. Konkrétní problém se týká obchodních tajemství, kdy ve sdělení „Posílení evropského systému kybernetické odolnosti“ z července 2016 byla zaznamenána zdrženlivost v hlášení kybernetických krádeží obchodních tajemství a význam důvěryhodných oznamovacích kanálů, které zaručují důvěrnost.

se podpořila širší spolupráce a výměna informací mezi větším počtem odvětví. Při vytváření potřebné důvěry pro sdílení informací mezi soukromým a veřejným sektorem je obzvláště důležitá úloha středisek pro sdílení a analýzu informací. Byly učiněny některé první kroky v konkrétních kritických odvětvích, například v letectví vytvořením Evropského střediska pro kybernetickou bezpečnost v letectví[35] a v energetice rozvojem středisek pro sdílení a analýzu informací[36]. Komise za podpory agentury ENISA plně přispěje k tomuto přístupu, přičemž je třeba zintenzivnit úsilí zejména s ohledem na odvětví, která poskytují základní služby uvedené ve směrnici o bezpečnosti sítí a informací.

2.4 Odolnost díky rychlé reakci v případě mimořádných událostí

Když dojde ke kybernetickému útoku, rychlá a účinná reakce může zmírnit jeho dopad. Může rovněž ukázat, že orgány veřejné správy nejsou vůči kybernetickým útokům bezmocné, a přispívá k vytváření důvěry. Co se týče reakce orgánů EU, kybernetické aspekty by se měly v první řadě začlenit do existujících mechanismů EU pro řešení krizí: integrovaných opatření EU pro politickou reakci na krize, koordinovaných předsednictvím Rady[37], a obecných systémů včasného varování, kterými EU disponuje[38]. Potřeba reagovat na mimořádně závažný kybernetický incident nebo útok by mohl danému členskému státu zavdat dostatečný důvod k uplatnění doložky solidarity EU[39].

Rychlá a účinná reakce se rovněž opírá o mechanismus rychlé výměny informací mezi všemi klíčovými subjekty na vnitrostátní úrovni a úrovni EU, což však vyžaduje jasné rozdělení a chápání jejich úloh a povinností. Komise uskutečnila konzultace s orgány a členskými státy o plánu, jak zavést účinný proces pro operativní reakci na úrovni Unie a členských států na rozsáhlý kybernetický incident. **Plán** předložený v doporučení[40] v tomto balíčku vysvětluje, jak je kybernetická bezpečnost začleněna do existujících mechanismů pro řešení krizí na úrovni EU, a stanoví cíle a způsoby spolupráce mezi členskými státy navzájem, jakož i mezi členskými státy a příslušnými orgány, útvary, agenturami a institucemi EU[41] při reakci na krize a rozsáhlé kybernetické bezpečnostní incidenty. V doporučení se od členských států a orgánů EU také požaduje, aby vytvořily rámec EU pro reakci na kybernetické krize za účelem uvedení plánu do praxe. Plán se bude pravidelně ověřovat na cvičeních v oblasti řešení kybernetických a jiných krizí[42] a podle potřeby se bude aktualizovat.

Vzhledem k tomu, že kybernetické bezpečnostní incidenty by mohly podstatně ovlivnit fungování ekonomik a každodenní životy lidí, jednou z variant by bylo zkoumání možnosti vytvoření **fondu pro reakce při mimořádných událostech v oblasti kybernetické bezpečnosti** podle vzoru podobných krizových mechanismů v jiných oblastech politiky EU. Členské státy by tak během významného incidentu nebo po něm mohly žádat o pomoc na úrovni EU, avšak za předpokladu, že daný členský stát měl před incidentem zaveden rozumný

---

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

36 Jde o neziskové organizace řízené svými členy, které vytvořily soukromé a veřejné subjekty za účelem výměny informací o kybernetických hrozbách, rizicích, prevenci, zmírňování a reakci. Viz např. evropská střediska pro sdílení a analýzu informací v energetice (http://www.ee-isac.eu).

37 Lze tak koordinovat reakce na velké meziodvětvové krize na nejvyšší politické úrovni.

38 Umožňují interní výměnu informací a koordinaci v případě vznikajících víceodvětvových krizí nebo předvídatelných či bezprostředních hrozbách, které vyžadují opatření na úrovni EU.

39 Na základě článku 222 Smlouvy o fungování Evropské unie.

40 COM(2017) 6100.

41 Včetně Europolu, agentury ENISA, týmu CERT pro orgány, instituce a agentury EU (CERT-EU) a Střediska EU pro analýzu zpravodajských informací (INTCEN).

42 Například těch, která pořádá ENISA: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme

systém kybernetické bezpečnosti včetně plného provedení směrnice o bezpečnosti sítí a informací, vyspělého řízení rizik a rámců dohledu na vnitrostátní úrovni. Tento fond, který by doplnil existující mechanismy pro řešení krizí na úrovni EU, by mohl aktivovat schopnost rychlé reakce v zájmu solidarity a financovat specifické kroky v reakci na mimořádné události, jako je náhrada napadeného zařízení nebo aktivace nástrojů pro reakci či zmírnění následků, a to s využitím vnitrostátních odborných znalostí, podobně jako mechanismus civilní ochrany EU.

2.5 Odborná síť pro kybernetickou bezpečnost s Evropským výzkumným a odborným střediskem pro kybernetickou bezpečnost

Technologické nástroje kybernetické bezpečnosti jsou strategickými aktivy a rovněž klíčovými technologiemi růstu pro budoucnost. Je strategickým zájmem EU zajistit, aby si EU udržela a rozvíjela důležité dovednosti v zájmu zabezpečení digitální ekonomiky, společnosti a demokracie, ochrany kritického hardwaru a softwaru a poskytování klíčových služeb v oblasti kybernetické bezpečnosti.

Partnerství veřejného a soukromého sektoru v oblasti kybernetické bezpečnosti[43] vytvořené v roce 2016 bylo významným prvním krokem, který dal podnět k investicím ve výši 1,8 miliardy EUR do roku 2020. Rozsah investic vynakládaných v jiných částech světa[44] však ukazuje, že EU musí dělat více, pokud jde o investice, a překonat roztříštěnost kapacit rozprostřených po celé EU.

Vzhledem k propracovanosti technologií kybernetické bezpečnosti, rozsahu potřebných investic a potřebě řešení, která fungují v celé EU, může EU poskytnout přidanou hodnotu. Na základě práce členských států a partnerství veřejného a soukromého sektoru by dalším krokem bylo posílení kapacit EU v oblasti kybernetické bezpečnosti prostřednictvím **sítě odborných středisek v oblasti kybernetické bezpečnosti**[45], jejímž ústředním prvkem by bylo **Evropské výzkumné a odborné středisko pro kybernetickou bezpečnost**. Tato síť a její středisko by stimulovaly rozvoj a zavádění technologií v oblasti kybernetické bezpečnosti a doplnily by úsilí zaměřené na budování kapacit v této oblasti na úrovni EU a na vnitrostátní úrovni. Komise zahájí posouzení dopadů za účelem prozkoumání dostupných možností – včetně možnosti zřízení společného podniku – s cílem vytvořit tuto strukturu v roce 2018.

Komise jako první krok a v zájmu získání informací pro budoucí úvahy navrhne, aby byla v rámci programu Horizont 2020 zahájena pilotní fáze, která pomůže zapojit vnitrostátní střediska do sítě, a dodat tak nový impuls rozvoji kompetencí a technologií v oblasti kybernetické bezpečnosti. Za tímto účelem plánuje navrhnout krátkodobou finanční injekci ve výši 50 milionů EUR. Tato činnost doplní probíhající provádění partnerství veřejného a soukromého sektoru v oblasti kybernetické bezpečnosti.

Základem sítě a počátečním zaměřením střediska by bylo soustředění a formování výzkumného úsilí. V zájmu podpory rozvoje průmyslových kapacit by středisko mohlo působit jako projektový manažer v oblasti kapacit, schopný řídit mezinárodní projekty. Tím by se také dodal další stimul inovacím a konkurenceschopnosti průmyslu EU na celosvětové scéně, pokud jde o rozvoj digitálních technologií příští generace, včetně umělé inteligence,

[43] C(2016) 4400 final.

[44] USA budou do kybernetické bezpečnosti jenom v roce 2017 investovat 19 miliard dolarů, což je o 35 % více oproti roku 2016. Bílý dům, Úřad tiskového tajemníka: „Fact Sheet: Cybersecurity National Action Plan“ (Informativní přehled: Vnitrostátní akční plán v oblasti kybernetické bezpečnosti), 9. února 2016.

[45] Síť by zahrnovala stávající a budoucí střediska kybernetické bezpečnosti zřízená v členských státech, jejichž členy by zpravidla byly veřejné výzkumné organizace a laboratoře.

kvantové výpočetní techniky, blockchainu a bezpečných digitálních identit, jakož i o zajištění přístupu společností se sídlem v EU k hromadným údajům, což bude vše v budoucnosti pro kybernetickou bezpečnost klíčové. Středisko by rovněž využilo práci EU v oblasti rozšiřování infrastruktury vysoce výkonné výpočetní techniky: ta je důležitá pro analýzu velkých objemů dat, rychlé šifrování a dešifrování dat, kontrolu identit, simulaci kybernetických útoků a analýzu videomateriálů[46].

Síť odborných středisek by mohla být také schopna odvětví podpořit formou zkoušek a simulací s cílem dát základ certifikaci kybernetické bezpečnosti popsané v oddílu 2.2. Její zapojení do celého rozsahu činností EU v oblasti kybernetické bezpečnosti by zajistilo průběžnou aktualizaci jejího zacílení podle potřeby. Cílem střediska by bylo prosazovat vysoké normy kybernetické bezpečnosti nejen v oblasti technologií a systémů kybernetické bezpečnosti, ale také v rozvoji špičkových dovedností odborníků, a to poskytováním řešení a modelů pro vnitrostátní úsilí v oblasti rozvoje digitálních dovedností. V tomto ohledu by také zvýšilo kapacity v oblasti kybernetické bezpečnosti na úrovni EU a stavělo na synergiích zejména s agenturou ENISA, týmem CERT-EU, Europolem, případným budoucím fondem pro reakce při mimořádných událostech v oblasti kybernetické bezpečnosti a vnitrostátními bezpečnostními týmy CSIRT.

Práce odborné sítě se musí zaměřit zejména na chybějící evropské kapacity pro posuzování **šifrování** v produktech a službách, které občané, podniky a vlády používají v rámci jednotného digitálního trhu. Silné šifrování je základem pro bezpečné digitální identifikační systémy, které hrají klíčovou úlohu v účinné kybernetické bezpečnosti[47]; rovněž udržuje v bezpečí duševní vlastnictví lidí, umožňuje chránit základní práva, jako je svoboda projevu a ochrana osobních údajů, a zajišťuje bezpečné obchodování on-line[48].

Jelikož civilní a obranné trhy v oblasti kybernetické bezpečnosti v EU sdílejí společné výzvy[49] a technologie dvojího užití, což vyžaduje úzkou spolupráci v kritických oblastech, mohla by se druhá fáze sítě a jejího střediska dále rozvíjet s dimenzí kybernetické obrany, přičemž je třeba plně dodržet ustanovení Smlouvy týkající se společné bezpečnostní a obranné politiky. Podobně jako technologické zaměření by i obranná dimenze mohla přispívat ke spolupráci mezi členskými státy v oblasti kybernetické obrany, včetně výměny informací, informovanosti o situaci, vytváření odborných znalostí, koordinované reakce a podpory rozvoje společných schopností členských států. Mohla by rovněž působit jako platforma umožňující členským státům určit priority pro kybernetickou obranu EU, hledat společná řešení, přispívat k rozvoji společných strategií, usnadňovat společný výcvik, cvičení a zkoušky v oblasti kybernetické obrany na evropské úrovni a podporovat práci na taxonomiích a normách kybernetické obrany, přičemž středisko by mělo podpůrnou a poradenskou úlohu. Při provádění uvedených činností by středisko muselo v oblasti kybernetické obrany úzce a plně spolupracovat s Evropskou obrannou agenturou a v oblasti kybernetické odolnosti s agenturou ENISA. Tato obranná dimenze by zohledňovala proces zahájený diskusním dokumentem o budoucnosti evropské obrany.

Vysoká úroveň odolnosti potřebná pro kybernetickou obranu vyžaduje specifické zaměření úsilí ve výzkumu a technologiích. Projekty nebo technologie kybernetické obrany vyvíjené

---

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

[47] Komise v rámci programu Horizont 2020 zahájí novou soutěž o cenu Horizon, v níž nejlepší inovační řešení pro bezproblémové metody ověřování online získá 4 miliony eur.

[48] Kybernetická bezpečnost na evropském jednotném digitálním trhu, skupina vědeckých poradců na vysoké úrovni, březen 2017.

[49] „Study on synergies between the civilian and the defence cybersecurity markets“ (Studie o synergiích mezi civilními a obrannými trhy v oblasti kybernetické bezpečnosti, Optimity, SMART 2014-0059).

podniky by mohly využít financování z Evropského obranného fondu, a to ve fázi výzkumu i vývoje[50]. Mimořádně důležité by v této souvislosti mohly být konkrétní oblasti, jako jsou šifrovací systémy založené na kvantových technologiích, informovanost o kybernetické situaci, biometrické systémy řízení přístupu, detekce sofistikovaných trvalých hrozeb nebo vytěžování dat. Vysoká představitelka, Evropská obranná agentura a Komise podpoří členské státy v určování oblastí, v kterých lze zvážit financování společných projektů kybernetické bezpečnosti z Evropského obranného fondu.

2.6 Vytváření silné základny kybernetických dovedností EU

Kybernetická bezpečnost zahrnuje významnou dimenzi vzdělávání. Účinná kybernetická bezpečnost se do značné míry opírá o dovednosti příslušných pracovníků. Předpokládá se však, že do roku 2022 bude v Evropě v soukromém sektoru chybět 350 000 odborníků na oblast kybernetické bezpečnosti[51]. Vzdělávání v oblasti kybernetické bezpečnosti by se mělo rozvíjet na všech úrovních, počínaje pravidelnou odbornou přípravou pracovníků v kybernetických oborech, další odbornou přípravou pro všechny odborníky v oboru IKT a novými specifickými učebními osnovami v oblasti kybernetické bezpečnosti. K uspokojení poptávky po zrychleném vzdělávání a odborné přípravě by se měla zřídit silná vědecká odborná střediska, která by mohla vycházet z pokynů Evropského výzkumného a odborného střediska pro kybernetickou bezpečnost a agentury ENISA. Cílem by mělo být, aby bylo přirozené navrhovat produkty a systémy IKT tak, aby od samého začátku zohledňovaly zásady bezpečnosti. Vzdělávání v oblasti kybernetické bezpečnosti by se nemělo omezovat na odborníky v IT, ale mělo by se začlenit do učebních osnov pro jiné obory, jako je strojírenství, řízení podniků nebo právo, a také do odvětvových vzdělávacích programů. A v neposlední řadě by učitelé a žáci na základních a středních školách měli být poučeni o kyberkriminalitě a kybernetické bezpečnosti při osvojování si digitálních dovedností ve škole.

EU spolu s členskými státy by měla k tomuto úsili také přispět, a to tím, že vyjde z práce velké koalice pro dovednosti a pracovní místa[52] a například zavede systémy učňovského vzdělávání v oblasti kybernetické bezpečnosti pro malé a střední podniky.

2.7 Podpora kybernetické hygieny a informovanosti

Přibližně 95 % incidentů údajně nastane kvůli „nějaké lidské chybě – ať už úmyslné, nebo neúmyslné“[53], takže zde působí významný lidský faktor. Kybernetická bezpečnost je tedy odpovědností každého. To znamená, že chování osob, podniků a veřejné správy se musí změnit, aby každý chápal hrozbu a byl vybaven nástroji a dovednostmi k tomu, aby mohl útoky rychle zjistit a sám se před nimi chránit. Lidé si musí osvojit návyky kybernetické hygieny a podniky a organizace musí přijmout vhodné programy kybernetické bezpečnosti na základě rizik a pravidelně je aktualizovat, aby odrážely měnící se situaci v oblasti rizik.

Směrnice o bezpečnosti sítí a informací stanoví nejenom povinnost členských států vyměňovat si informace o kybernetických útocích na úrovni EU, ale také povinnost zavést v oblasti kybernetické bezpečnosti vyspělé národní strategie a rámce pro bezpečnost sítí

[50] Evropský program rozvoje obranného průmyslu už teď dává prioritu projektům kybernetické obrany a kybernetická obrana bude jedním z témat výzvy k předkládání návrhů, která bude zahájena v roce 2018.

[51] „Global Information Security Workforce Study“ (celosvětová studie o pracovní síle v informační bezpečnosti), 2017. Celosvětový nedostatek je 1,8 milionu.

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

[53] IBM, „The Cybersecurity Intelligence Index“ (Ukazatel informovanosti o kybernetické bezpečnosti), 2014, uvedeno v Securitymagazine.com, 19. června 2014.

a informačních systémů. Veřejné správy na úrovni EU a na vnitrostátní úrovni by měly hrát výraznější vedoucí úlohu v prosazování těchto úsilí.

Za prvé, členské státy by měly maximalizovat dostupnost nástrojů kybernetické bezpečnosti pro podniky i jednotlivce. Více by se mělo udělat zejména pro prevenci a zmírnění dopadů kyberkriminality na koncové uživatele. V práci Europolu již existuje jeden příklad – kampaň „NoMoreRansom“[54] vytvořená v úzké spolupráci mezi donucovacími orgány a společnostmi v oblasti kybernetické bezpečnosti s cílem pomoci uživatelům předejít infekcím ransomwaru a dešifrovat data, pokud se stanou obětmi útoku. Takové systémy by se měly zavést i pro jiné typy škodlivého softwaru a v dalších oblastech a EU by měla vyvinout **společný portál, kde budou na jednom místě dostupné všechny takové nástroje** a který nabídne uživatelům poradenství o prevenci a detekci škodlivého softwaru a odkazy na ohlašovací mechanismy.

Za druhé, členské státy by měly urychlit **používání kyberneticky bezpečnějších nástrojů při rozvoji elektronické veřejné správy (e-Government)**, a rovněž plně využít přínosy odborné sítě. Mělo by se podporovat přijetí bezpečných prostředků identifikace na základě rámce EU pro elektronickou identifikaci a služby vytvářející důvěru pro elektronické transakce na vnitřním trhu, který je účinný od roku 2016 a poskytuje předvídatelné regulační prostředí za účelem umožnění bezpečné a bezproblémové elektronické interakce mezi podniky, občany a orgány veřejné správy[55]. Kromě toho by veřejné instituce, zejména ty, které poskytují základní služby, měly dbát, aby jejich pracovníci absolvovali odbornou přípravu v oblastech spojených s kybernetickou bezpečností.

Za třetí, členské státy by měly informovanost o kybernetické bezpečnosti považovat za prioritu **v kampaních ke zvýšení povědomí**, včetně kampaní zaměřených na školy, univerzity, podnikatelskou sféru a výzkumné instituce. Měsíc kybernetické bezpečnosti, který se koná každý rok v říjnu za koordinace agentury ENISA, se rozšíří, aby jako společné komunikační úsilí na úrovni EU i na vnitrostátní úrovni oslovil širší publikum. Stejně důležité je zvýšení informovanosti o online **dezinformačních kampaních a falešných zprávách** v sociálních mediích, jejichž cílem je zejména podkopat demokratické procesy a evropské hodnoty. I když hlavní odpovědnost zůstává na vnitrostátní úrovni, a to i při volbách do Evropského parlamentu, sdílení odborných znalostí a výměna zkušeností na evropské úrovni se osvědčily jako přidaná hodnota, která opatřením dává jasný cíl[56].

Velkou roli obecně hraje i **průmysl**, ale zvláštní pozornost je třeba věnovat poskytovatelům digitálních služeb a výrobcům. Průmysl musí uživatelům (jednotlivcům, podnikům a veřejné správě) poskytnout podporu v podobě nástrojů, které jim umožní převzít odpovědnost za jejich činnost online, a dát jasně najevo, že kybernetická hygiena je nedílnou součástí nabídky pro spotřebitele[57]. V zájmu zjišťování a odstraňování zranitelností by průmysl měl usilovat o to, aby měl zavedeny vnitřní procesy pro vyšetřování, třídění a řešení zranitelností bez

---

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

[55] Nařízení (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (nařízení eIDAS). Evropská komise také poskytuje stavební prvky a nástroje pro interoperabilitu elektronické identifikace (eID) a elektronických podpisů (např. prohlížeč důvěryhodných seznamů „Trusted List Browser“) prostřednictvím Nástroje pro propojení Evropy.

[56] Příkladem je Pracovní skupina East StratCom, kterou v roce 2015 zřídily členské státy a vysoká představitelka za účelem řešení probíhajících ruských dezinformačních kampaní. Skupina se účastní vývoje komunikačních produktů a kampaní zaměřených na vysvětlování politik EU v regionu Východního partnerství.

[57] Někteří výrobci už s touto koncepcí pracují, neboť některé evropské právní předpisy týkající se výrobků (jako je směrnice 2006/42/ES o strojních zařízeních) stanoví zásady pro „bezpečnost jako nedílnou součást návrhu“.

ohledu na to, zda se zdroj potenciální zranitelnosti nacházel vně nebo uvnitř dotčené společnosti.

Klíčová opatření

- plné provedení směrnice o bezpečnosti sítí a informací,
- rychlé přijetí nařízení o novém mandátu pro agenturu ENISA a evropském rámci pro certifikaci[58] Evropským parlamentem a Radou,
- společná iniciativa Komise a průmyslu ohledně stanovení zásady „povinné péče“ za účelem snížení zranitelností produktů/softwaru a podpory „bezpečnosti již od fáze návrhu“,
- rychlé provedení plánu reakce na velké přeshraniční incidenty,
- zahájení posouzení dopadů s cílem prověřit, zda může Komise v roce 2018 předložit návrh na zřízení odborné sítě pro kybernetickou bezpečnost a Evropského výzkumného a odborného střediska pro kybernetickou bezpečnost na základě bezprostřední pilotní fáze,
- podpora členských států při určování oblastí, v kterých lze zvážit podporu společných projektů kybernetické bezpečnosti z Evropského obranného fondu,
- jednotné kontaktní místo v celé EU pro pomoc obětem kybernetických útoků, které by poskytovalo informace o nejnovějších hrozbách a soustředilo na jednom místě praktické rady a nástroje v oblasti kybernetické bezpečnosti,
- opatření ze strany členských států pro začlenění kybernetické bezpečnosti do programů dovedností, elektronické veřejné správy a kampaní ke zvýšení povědomí,
- opatření ze strany průmyslu na zintenzivnění odborné přípravy pracovníků v oblasti kybernetické bezpečnosti a přijetí přístupu „bezpečnost již od fáze návrhu“, pokud jde o výrobky, služby a procesy.

3. ZAVEDENÍ ÚČINNÉHO KYBERNETICKÉHO ODRAZOVÁNÍ ZE STRANY EU

Účinné odrazování znamená zavést rámec opatření, která jsou jak důvěryhodná, tak i odrazující pro potenciální útočníky a pachatele kybernetických trestných činů. Dokud se pachatelé kybernetických útoků – nestátní i státní – kromě neúspěchu nebudou mít čeho obávat, budou mít jen malou motivaci, aby se o ně přestali pokoušet. Ústředním prvkem účinného odrazování je účinnější reakce donucovacích orgánů zaměřená na odhalení, vysledování a stíhání pachatelů kybernetických trestných činů. K tomu se připojuje potřeba, aby EU podporovala své členské státy v rozvoji kapacit kybernetické bezpečnosti dvojího užití. Kybernetické útoky můžeme zvrátit, pouze když zvýšíme šance na dopadení a stíhání těch, kteří je páchají. Kybernetické útoky by se měly bezodkladně vyšetřit a pachatelé by měli být pohnáni před spravedlnost, nebo by měla být přijata opatření umožňující patřičnou politickou nebo diplomatickou reakci. V případě velké krize s významným mezinárodním a obranným rozměrem by vysoká představitelka mohla možnosti, jak adekvátně reagovat, předložit Radě.

Jeden krok ke zlepšení trestněprávní reakce na kybernetické útoky už byl učiněn přijetím směrnice o útocích na informační systémy[59] v roce 2013. Tím se stanovila minimální pravidla týkající se definice trestných činů a sankcí v oblasti útoků na informační systémy, jakož i operativní opatření ke zlepšení spolupráce mezi orgány. Směrnice zajistila významný

[58] COM(2017) 477.

[59] Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy.

pokrok, pokud jde o srovnatelnou úroveň kriminalizace kybernetických útoků v členských státech, což usnadňuje přeshraniční spolupráci donucovacích orgánů, které tyto typy trestných činů vyšetřují. Stále však existuje prostor k dosažení plného potenciálu směrnice, pokud členské státy v plném rozsahu provedou všechna její ustanovení[60]. Komise bude i nadále poskytovat podporu členským státům v provádění směrnice a v současné době nevidí potřebu navrhnout její změny.

3.1 Identifikace zlovolných subjektů

Aby se zvýšily šance pohnat pachatele ke spravedlnosti, musíme naléhavě zlepšit schopnost identifikovat osoby odpovědné za kybernetické útoky. Nalezení užitečných informací pro vyšetřování kyberkriminality, většinou ve formě digitálních stop, je pro donucovací orgány velkým problémem. Musíme proto posílit své technologické schopnosti, abychom mohli účinně vést vyšetřování, včetně posílení centra Europolu pro boj proti kyberkriminalitě o odborníky na kybernetiku. Europol se stal klíčovým hráčem, pokud jde o podporu členských států při vedení vyšetřování ve více jurisdikcích. Měl by se stát odborným centrem pro donucovací orgány členských států, pokud jde o vyšetřováních online a kybernetické forenzní vědy.

Vyšetřování nekalého chování online technicky značně znesnadňuje velmi rozšířená praxe umisťování četných uživatelů – někdy až tisíců – za jedinou IP adresu. Kvůli tomu je někdy nutné, například v případě závažné trestné činnosti, jako je sexuální zneužívání dětí, k odhalení jednoho zlovolného subjektu zahrnout do vyšetřování velký počet uživatelů. EU proto podpoří zavádění nového protokolu (IPv6), neboť ten umožňuje přidělit každému jednotlivému uživateli jinou IP adresu, což je jasným přínosem pro prosazování práva a vyšetřování v oblasti kybernetické bezpečnosti. Jako první krok na podporu jeho zavádění Komise začlení požadavek přechodu na IPv6 do řady svých politik, včetně požadavků při zadávání veřejných zakázek a financování projektů a výzkumu, a podpoří potřebné materiály pro odbornou přípravu. Členské státy by kromě toho s cílem podnítit zavádění IPv6 měly zvážit dobrovolné dohody s poskytovateli internetových služeb.

Belgie představuje světovou špičku[61] v míře přijetí IPv6 mimo jiné díky spolupráci veřejného a soukromého sektoru: příslušné zúčastněné strany jako součást dobrovolného samoregulačního opatření zvážily omezení spočívající v používání jedné IP adresy maximálně pro 16 uživatelů, což bylo motivací k přechodu na IPv6[62].

Obecněji řečeno by se měla více podporovat odpovědnost online. To znamená podporu opatření k zamezení zneužívání doménových jmen pro rozesílání nevyžádaných zpráv nebo phishingové útoky. Komise bude za tímto účelem pracovat na zlepšení fungování systémů

[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.

doménových jmen a IP WHOIS[63] a dostupnosti a přesnosti informací v těchto systémech souběžně s úsilím sdružení ICANN[64].

3.2 Posílení reakce donucovacích orgánů

Klíčovým odrazujícím prvkem, pokud jde o kybernetické útoky, je účinné **vyšetřování** a **stíhání** trestné činnosti související s kyberprostorem. Současný procedurální rámec se však musí lépe přizpůsobit internetovému věku[65]. Rychlost kybernetických útoků může přemoci naše postupy a zvláště si žádá rychlou přeshraniční spolupráci. Jak bylo oznámeno v Evropském programu pro bezpečnost, Komise začátkem roku 2018 předloží za tímto účelem návrhy na **usnadnění přeshraničního přístupu k elektronickým důkazům**. Komise současně provádí praktická opatření s cílem zlepšit přeshraniční přístup k elektronickým důkazům při vyšetřování trestné činnosti, včetně financování odborné přípravy v oblasti přeshraniční spolupráce, rozvoje elektronické platformy pro výměnu informací v rámci EU a standardizace forem soudní spolupráce používaných mezi členskými státy.

Další překážkou účinného stíhání jsou rozdílné forenzní postupy pro shromažďování elektronických důkazů při vyšetřování kyberkriminality v členských státech. Zlepšení by mohla přinést práce na stanovení společných forenzních norem. Kromě toho se musí posílit forenzní schopnosti, aby se podpořila sledovatelnost a schopnost určit pachatele. Jedním krokem by bylo prohloubení forenzních schopností v Europolu a přizpůsobení existujících rozpočtových a lidských zdrojů Evropského centra Europolu pro boj proti kyberkriminalitě, aby se uspokojila rostoucí potřeba operativní podpory v přeshraničních vyšetřováních kyberkriminality. Dalším krokem by bylo reflektovat výše uvedené technologické zaměření na šifrování, a to prozkoumáním, jak jeho zneužívání pachateli trestných činů působí značné problémy v boji proti závažným trestným činům, včetně terorismu a kyberkriminality. Komise předloží výsledky současných diskusí o **roli šifrování ve vyšetřováních trestné činnosti**[66] do října 2017[67].

Vzhledem k tomu, že internet svou povahou není omezen hranicemi, dává rámec mezinárodní spolupráce stanovený **budapešťskou Úmluvou Rady Evropy o kyberkriminalitě**[68] možnost, aby různé skupiny zemí využily optimální právní standard pro různé vnitrostátní právní předpisy, které se zabývají kyberkriminalitou. V současné době se zkoumá případné připojení protokolu k úmluvě[69], který by mohl rovněž poskytnout dobrou příležitost zabývat se otázkou přeshraničního přístupu k elektronickým důkazům v mezinárodním kontextu. Spíše než vytvoření nových mezinárodních právních nástrojů pro otázky kyberkriminality

---

[63] Dotazovací protokol používaný v širokém měřítku pro vyhledávání v databázích, v nichž se uchovávají registrovaní uživatelé nebo uživatelé, kterým byl přidělen daný internetový zdroj.

[64] Internetové sdružení pro přidělování jmen a čísel (Internet Corporation for Assigned Names and Numbers – ICANN) je nezisková organizace odpovědná za koordinaci údržby a postupů několika databází souvisejících s jmennými prostory internetu.

[65] Aby byl uveden alespoň jeden příklad, (virtuální) centrální řídicí server botnetu Avalanche se přesouval mezi fyzickými servery a doménami každých pět minut.

[66] Předsednictví Rady, „Výsledky zasedání Rady pro spravedlnost a vnitřní věci ve dnech 8. a 9. prosince 2016“, č. 15391/16.

[67] Osmá zpráva o pokroku na cestě k účinné a skutečné bezpečnostní unii ze dne 29. června 2017, COM(2017) 354 final.

[68] Úmluva je první mezinárodní smlouvou o trestných činech páchaných prostřednictvím internetu a jiných počítačových sítí a zabývá se zejména porušováním autorského práva, počítačovými podvody, dětskou pornografií a narušeními bezpečnosti sítí. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. K roku 2017 Úmluvu Rady Evropy o kyberkriminalitě ratifikovalo nebo k ní přistoupilo 55 vlád.

[69] Mandát pro přípravu návrhu 2. dodatkového protokolu k Budapešťské úmluvě o kyberkriminalitě, T-CY (2017)3.

vyzývá EU všechny země, aby vypracovaly vhodné vnitrostátní právní předpisy a pokračovaly ve spolupráci v existujícím mezinárodním rámci.

Všeobecná dostupnost nástrojů anonymizace usnadňuje zločincům utajení. „**Darknet**“[70] otevřel pachatelům trestných činů nové cesty přístupu k dětské pornografii, drogám nebo palným zbraním, často s malým rizikem dopadení[71]. V současné době je také hlavním zdrojem nástrojů používaných v kyberkriminalitě, jako je škodlivý software a hackerské nástroje. Komise spolu s příslušnými zúčastněnými stranami provede analýzu vnitrostátních přístupů s cílem určit nová řešení. Europol by měl usnadnit a podpořit vyšetřování na darknetu, posoudit hrozby, pomáhat určit jurisdikci a dát prioritu vysoce rizikovým případům, a EU může hrát vedoucí úlohu v koordinaci mezinárodních opatření[72].

Jednou z rozšiřujících se oblastí kyberkriminality je zneužívání údajů z kreditních karet nebo jiných elektronických platebních prostředků. Identifikační údaje pro platby získané kybernetickými útoky na online maloobchodníky nebo jiné legitimní podniky se potom prodávají online a zločinci je mohou použít k páchání podvodů[73]. Komise předkládá návrh na silnější odrazování ve formě **směrnice o potírání podvodů v oblasti bezhotovostních prostředků pro placení a jejich padělání**[74]. Jejím cílem je aktualizovat existující pravidla v této oblasti a posílit schopnost donucovacích orgánů řešit tuto formu trestné činnosti.

Rovněž se musí zlepšit schopnosti donucovacích orgánů členských států vyšetřovat kyberkriminalitu, jakož i chápání trestné činnosti související s kyberprostorem a vyšetřovací možnosti státních zástupců a justice. Eurojust a Europol přispívají k tomuto cíli a ke zvýšené koordinaci v úzké spolupráci se specializovanými poradenskými skupinami v rámci střediska Europolu pro kyberkriminalitu a se sítěmi vedoucích útvarů zabývajících se kyberkriminalitou a státními zástupci specializovanými na kyberkriminalitu. Komise vyčlení 10,5 milionu EUR na financování boje proti kyberkriminalitě, primárně v rámci **policejního programu Fondu pro vnitřní bezpečnost**. Významným prvkem je odborná příprava a Evropská skupina pro odbornou přípravu a vzdělání v oblasti kyberkriminality zpracovala řadu užitečných materiálů. Tyto materiály by se nyní měly ve velkém měřítku rozšířit mezi odborníky v oblasti prosazování práva s podporou Agentury Evropské unie pro vzdělávání a výcvik v oblasti prosazování práva (CEPOL).

3.3 Spolupráce veřejného a soukromého sektoru v boji proti kyberkriminalitě

Rysy digitálního světa, který se většinou skládá z infrastruktury v soukromém vlastnictví a řady různých subjektů v rozličných jurisdikcích, zpochybňují účinnost tradičních mechanismů prosazování práva. Proto je pro orgány veřejné správy velmi důležitá spolupráce se soukromým sektorem, včetně průmyslu a občanské společnosti, aby mohly proti kriminalitě účinně bojovat. V této souvislosti je klíčový i finanční sektor a spolupráce s ním

---

[70] Darknet se skládá z obsahu v překryvných sítích, které používají internet, ale vyžadují zvláštní software, konfigurace nebo povolení přístupu. Darknet tvoří malou část hlubokého webu („deep web“), což je část webu, kterou neindexují internetové vyhledávače.

[71] Pozoruhodnou výjimkou je nedávné uzavření dvou největších tržišť na dark webu spojených s trestnou činností, 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 této oblasti hraje významnou roli. Poslední příklad viz: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

[73] Výnosy z podvodů jsou významným zdrojem příjmů organizovaného zločinu, a tudíž umožňují páchání jiné trestné činnosti, jako je terorismus a obchodování s drogami a lidmi.

[74] COM(2017) 489.

by se měla zintenzivnit. V kontextu kyberkriminality by se měla například posílit úloha finančních zpravodajských jednotek[75].

Některé členské státy už učinily klíčové kroky. V Nizozemsku finanční instituce a donucovací orgány vzájemně spolupracují při řešení online podvodů a kyberkriminality v pracovní skupině pro elektronickou trestnou činnost. Německé odborné středisko pro boj proti kyberkriminalitě poskytuje svým členům operativní platformu pro výměnu informací v úzké spolupráci s německým spolkovým policejním úřadem a vypracovává opatření zaměřená na zajištění ochrany před kyberkriminalitou. 16 členských států[76] vytvořilo střediska excelence v oblasti kyberkriminality, aby usnadnily spolupráci mezi donucovacími orgány, akademickou sférou a soukromými partnery za účelem vývoje a výměny osvědčených postupů, odborné přípravy a budování kapacit.
Komise podporuje vytváření partnerství veřejného a soukromého sektoru a mechanismů spolupráce prostřednictvím zvláštních projektů, jako je kybernetické středisko a odborná síť pro řešení podvodů online[77], které uplatňují model a standard výměny informací s cílem analyzovat a zmírnit rizika elektronických trestných činů a podvodů online.

V souvislosti s kyberkriminalitou musí mít soukromé podniky možnost vyměňovat si informace o konkrétních incidentech – včetně osobních údajů – s donucovacími orgány, ale přitom plně dodržet pravidla o ochraně údajů. Reforma ochrany údajů v EU, která vstoupí v platnost v květnu 2018, poskytuje společný soubor pravidel, která stanoví podmínky, za nichž mohou donucovací orgány a soukromé subjekty spolupracovat. Evropská komise bude spolupracovat s Evropským sborem pro ochranu osobních údajů a příslušnými zúčastněnými stranami za účelem určení osvědčených postupů v této oblasti a v příslušných případech poskytne pokyny.

3.4 Posílení politické reakce

Nedávno přijatý **rámec pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru**[78] („soubor nástrojů pro diplomacii v oblasti kybernetiky“) stanoví opatření na základě společné zahraniční a bezpečnostní politiky, včetně restriktivních opatření, jež lze použít pro posílení reakce EU na aktivity, které poškozují její politické, bezpečnostní a ekonomické zájmy. Rámec tvoří důležitý krok v rozvoji signalizačních a reaktivních schopností na úrovni EU a členských států. Zvýší naši schopnost určit původce nepřátelských činností v kyberprostoru s cílem ovlivnit chování potenciálních útočníků a současně přihlédnout k potřebě zajistit přiměřenost reakce. Označení státního nebo nestátního subjektu za původce zůstává suverénním politickým rozhodnutím, které se opírá o všechny zdroje zpravodajských informací. Práce spojená s prováděním rámce v současné době probíhá v členských státech a pokračovala by rovněž v plné koordinaci s plánem reakce na rozsáhlé kybernetické incidenty[79]. Informovanost o situaci, která je pro použití opatření obsažených

[75] Finanční zpravodajské jednotky slouží jako vnitrostátní střediska pro příjem a analýzu oznámení o podezřelých obchodech a dalších informací týkajících se praní peněz, souvisejících predikativních trestných činů a financování terorismu, jakož i pro šíření výsledků této analýzy.
[76] Belgie, Bulharsko, Česká republika, Estonsko, Francie, Irsko, Kypr, Litva, Německo, Polsko, Rakousko, Rumunsko, Řecko, Slovinsko, Spojené království a Španělsko.
[77] Cílem iniciativy EU-OF2CEN je umožnit v rámci celé EU systematickou výměnu informací souvisejících s internetovými podvody mezi bankami a donucovacími orgány za účelem zamezení plateb podvodníkům a bílým koňům a v zájmu vyšetřování a stíhání pachatelů. Spolufinancuje ji EU (Fond vnitřní bezpečnosti – policejní program).
[78] http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/
[79] COM(2017) 6100.

v rámci potřebná, by mělo shromáždit, analyzovat a sdílet zpravodajské středisko INTCEN[80] v úzké spolupráci s členskými státy a orgány EU.

3.5 Budování odrazovacích schopností v oblasti kybernetické bezpečnosti prostřednictvím obranných schopností členských států

Členské státy už rozvíjejí schopnosti kybernetické obrany. Kromě toho, vzhledem ke stírání hranic mezi kybernetickou obranou a kybernetickou bezpečností, dvojímu užití kybernetických nástrojů a technologií a velkým rozdílům mezi přístupy členských států, má EU dobrou pozici pro podporu synergií mezi vojenským a civilním úsilím[81].

Členské státy, které disponují pokročilejšími schopnostmi v oblasti kybernetické bezpečnosti a jsou ochotny je spojit dohromady, by mohly zvážit začlenění kybernetické obrany do rámce „stálé strukturované spolupráce“ (PESCO), a to s podporou vysoké představitelky, Komise a Evropské obranné agentury. Mohlo by to být podpořeno výše uvedeným úsilím na podporu průmyslových kapacit a strategické autonomie EU. EU může také podporovat interoperabilitu, kromě jiného i podporou rozvoje schopností, koordinací odborné přípravy a vzdělávání a úsilím v oblasti normalizace dvojího užití.

Měl by se také plně využít společný rámec pro reakce na hybridní hrozby, které často zahrnují kybernetické útoky, a to zejména prostřednictvím střediska EU pro hybridní hrozby a nedávno zřízeného Evropského střediska pro boj proti hybridním hrozbám v Helsinkách, jehož posláním je podporovat strategický dialog a provádět výzkum a analýzu.

EU znovu položí důraz na politický rámec EU pro kybernetickou obranu z roku 2014[82] jako nástroj pro hlubší integraci kybernetické bezpečnosti a obrany do společné bezpečnostní a obranné politiky (SBOP). Důležitá je kybernetická odolnost samotných misí a operací v rámci SBOP: budou vypracovány normalizované postupy a technické schopnosti, které by mohly podpořit vysílané civilní i vojenské mise a operace, jakož i příslušné struktury útvarů schopnosti plánování a vedení a poskytovatele služeb informačních technologií Evropské služby pro vnější činnost. Aby se dosáhlo pokroku ve spolupráci členských států a lépe zacílilo úsilí EU v této oblasti, Evropská obranná agentura a Evropská služba pro vnější činnost ve spolupráci s útvary Komise usnadní strategickou spolupráci tvůrců politik kybernetické obrany členských států. EU rovněž podpoří vývoj evropských řešení kybernetické bezpečnosti jako součást svého úsilí na podporu evropské technologické a průmyslové základny obrany. To zahrnuje rovněž podporu regionálních klastrů excelence v oblasti kybernetické bezpečnosti a obrany.

Útvary Komise v úzké spolupráci s ESVČ, členskými státy a dalšími příslušnými institucemi EU zavedou do roku 2018 **platformu odborné přípravy a vzdělávání v oblasti kybernetické obrany** s cílem řešit současný nedostatek dovedností v kybernetické obraně. Doplní to práci Evropské obranné agentury v této oblasti a pomůže řešit současný nedostatek dovedností v kybernetické bezpečnosti a kybernetické obraně.

Klíčová opatření

- iniciativa Komise pro přeshraniční přístup k elektronickým důkazům (začátkem roku 2018),
- rychlé přijetí, ze strany Evropského parlamentu a Rady, navržené směrnice o potírání

[80] JOIN(2016) 018 final.

[81] EU chápe kyberprostor jako oblast operací podobně jako zemi, vzduch a moře. Úsilí v oblasti kybernetické obrany zahrnuje rovněž ochranu a odolnost vesmírných kapacit a souvisejících pozemních infrastruktur.

[82] www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515

podvodů v oblasti bezhotovostních prostředků pro placení a jejich padělání,
- zavedení požadavků na IPv6 do zadávání veřejných zakázek EU a financování výzkumu a projektů ze strany EU, dobrovolné dohody mezi členskými státy a poskytovateli internetových služeb s cílem prosazovat používání IPv6,
- obnovení/rozšíření pozornosti Europolu na kybernetickou forenzní vědu a monitorování darknetu,
- provedení rámce pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru,
- zvýšená finanční podpora pro vnitrostátní a mezinárodní projekty, které zlepšují trestní soudnictví v kyberprostoru,
- vzdělávací platforma související s kybernetickou bezpečností pro řešení současného nedostatku dovedností v kybernetické bezpečnosti a kybernetické obraně v roce 2018.

4. POSÍLENÍ MEZINÁRODNÍ SPOLUPRÁCE V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

Mezinárodní politika EU v oblasti kybernetické bezpečnosti se řídí klíčovými hodnotami EU a základními právy, jako je svoboda projevu, právo na soukromí a ochranu osobních údajů a podpora otevřeného, svobodného a bezpečného kyberprostoru a je koncipována tak, aby se zabývala neustále se vyvíjejícími výzvami spojenými s prosazováním celosvětové kybernetické stability a přispívala ke strategické autonomii Evropy v kyberprostoru.

4.1 Kybernetická bezpečnost ve vnějších vztazích

Důkazy ukazují, že lidé z celého světa řadí kybernetické útoky z jiných zemí mezi přední hrozby pro vnitrostátní bezpečnost[83]. Vzhledem ke globální povaze hrozby je zásadním prvkem pro předcházení kybernetickým útokům a odrazováním od nich vytváření a udržování pevných spojenectví a partnerství s třetími zeměmi, což je čím dál tím důležitější pro mezinárodní stabilitu a bezpečnost. EU bude ve svých bilaterálních, regionálních a multilaterálních vztazích a vztazích za účasti více zúčastněných stran klást důraz na vytvoření strategického rámce pro předcházení konfliktům a zajištění stability v kyberprostoru.

EU silně podporuje stanovisko, že v kyberprostoru platí mezinárodní právo, a zejména Charta OSN. EU jako doplněk k závaznému mezinárodnímu právu podporuje dobrovolné nezávazné normy, pravidla a zásady odpovědného chování států, které formulovala skupina vládních odborníků OSN[84]; podporuje také rozvoj a provádění regionálních opatření pro vytváření důvěry, a to jak v rámci Organizace pro bezpečnost a spolupráci v Evropě, tak i v ostatních regionech.

Na bilaterální úrovni budou dále probíhat dialogy o kyberprostoru[85], které budou doplněny úsilím zaměřeným na usnadnění spolupráce s třetími zeměmi za účelem posílení zásad náležité péče a odpovědnosti států v kyberprostoru. EU bude klást důraz na otázky mezinárodní bezpečnosti v kyberprostoru ve svých mezinárodních vztazích a současně dbát, aby se kybernetická bezpečnost nestala záminkou pro ochranu trhu a omezení základních práv a svobod, včetně svobody projevu a přístupu k informacím. Komplexní přístup ke kybernetické bezpečnosti vyžaduje dodržování lidských práv a EU bude i nadále celosvětově prosazovat své klíčové hodnoty v návaznosti na obecné zásady EU v oblasti lidských práv

[83] „Spring 2017 Global Attitudes Survey“ (Průzkum globálních postojů – jaro 2017), Pew Research Centre.
[84] A/68/98 a A/70/174.
[85] V září 2017 vedla EU dialogy o kyberprostoru s USA, Čínou, Japonskem, Korejskou republikou a Indií.

ohledně svobody na internetu[86]. V tomto ohledu EU zdůrazňuje význam zapojení všech zúčastněných stran do správy internetu.

Komise také předložila návrh[87] na modernizaci kontrol vývozu EU, včetně zavedení kontrol vývozu kritických technologií kybernetického dohledu, které by mohly vést k porušování lidských práv nebo být zneužity proti bezpečnosti EU, a zintenzivní dialogy s třetími zeměmi s cílem podpořit celosvětové sbližování a odpovědné chování v této oblasti.

4.2 Budování kapacit v oblasti kybernetické bezpečnosti

Globální stabilita v kyberprostoru se opírá o místní a vnitrostátní schopnost všech zemí předcházet kybernetickým incidentům a reagovat na ně, jakož i vyšetřovat a stíhat případy kyberkriminality. Podpora úsilí ve vytváření vnitrostátní odolnosti v třetích zemích zvýší úroveň kybernetické bezpečnosti na celém světě s kladnými dopady pro EU. Boj s rychle se vyvíjejícími kybernetickými hrozbami zřejmě ukazuje na potřebu úsilí v oblasti odborné přípravy, politiky a legislativy, jakož i účinného fungování týmů CSIRT a útvarů zabývajících se kyberkriminalitou ve všech zemích po celém světě.

Od roku 2013 má EU vedoucí postavení v budování mezinárodních kapacit v oblasti kybernetické bezpečnosti a systematicky toto úsilí spojuje s rozvojovou spoluprací. EU bude i nadále podporovat model budování kapacit založený na právech v souladu s přístupem „Digital4Development“[88]. Prioritami pro budování kapacit budou sousední země EU a rozvojové země, v nichž dochází k rychlému růstu konektivity a prudkému rozvoji hrozeb. Úsilí EU bude doplňkem rozvojového programu EU s přihlédnutím k Agendě pro udržitelný rozvoj 2030 a celkovému úsilí v budování institucionálních kapacit.

Aby si EU zlepšila schopnost mobilizovat své kolektivní odborné znalosti na podporu tohoto budování kapacit, měla by se vytvořit vyhrazená síť EU pro budování kybernetických kapacit, která by spojovala ESVČ, orgány členských států zabývající se kyberprostorem, agentury EU, útvary Komise, akademickou sféru a občanskou společnost. Budou zpracovány pokyny EU pro budování kybernetických kapacit s cílem pomoci poskytnout lepší politické vedení a stanovit priority, pokud jde o úsilí EU v pomoci třetím zemím.

EU bude rovněž spolupracovat s jinými dárci v této oblasti, aby se zamezilo zdvojování úsilí a usnadnilo cílenější budování kapacit v různých regionech.

4.3 Spolupráce EU a NATO

Na základě už dosaženého značného pokroku prohloubí EU spolupráci EU a NATO v oblasti kybernetické bezpečnosti, hybridních hrozeb a obrany, jak předpokládá společné prohlášení ze dne 8. července 2016[89]. Priority zahrnují podporu interoperability prostřednictvím soudržných požadavků a norem v oblasti kybernetické obrany, posílení spolupráce v odborné přípravě a cvičeních a harmonizaci požadavků na odbornou přípravu.

EU a NATO budou rovněž podporovat spolupráci ve výzkumu a inovacích v oblasti kybernetické obrany a stavět na stávajícím technickém mechanismu pro sdílení informací o kybernetické bezpečnosti mezi příslušnými orgány pro kybernetickou bezpečnost[90]. Mělo by se zintenzivnit nedávné společné úsilí v boji proti hybridním hrozbám, zejména spolupráce

---

86 Obecné zásady EU v oblasti lidských práv ohledně svobody projevu online a offline.
87 COM(2016) 616.
88 SWD(2017) 157.
89 http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/
90 CERT-EU a NCIRC (NATO Computer Incident Response Capability).

mezi střediskem EU pro hybridní hrozby a úseku NATO pro analýzu hybridních hrozeb, aby se posílila odolnost vůči kybernetickým krizím a reakce na ně. Další spolupráce EU a NATO bude podpořena cvičeními v kybernetické obraně s účastí ESVČ a dalších subjektů EU a příslušných protistran NATO, včetně střediska excelence NATO pro spolupráci při kybernetické obraně v Tallinnu. NATO a EU poprvé uskuteční souběžná a koordinovaná cvičení v reakci na hybridní scénář, přičemž vedení se v roce 2017 ujme NATO a v roce 2018 podobně EU. Příští zpráva o spolupráci EU a NATO, která má být příslušným radám předložena v prosinci 2017, poskytne příležitost zvážit možnosti dalšího rozšíření spolupráce, zejména zajištěním společné, bezpečné a odolné komunikace mezi všemi příslušnými orgány a institucemi, včetně agentury ENISA.

Klíčová opatření

- dosáhnout pokroku, pokud jde o strategický rámec pro předcházení konfliktům a zajištění stability v kyberprostoru,
- vytvořit novou síť pro budování kapacit na podporu schopnosti třetích zemí řešit kybernetické hrozby a vypracovat pokyny EU pro budování kapacit v oblasti kybernetické bezpečnosti, aby byly lépe stanoveny priority úsilí EU,
- prohloubit spolupráci EU a NATO, včetně účasti na souběžných a koordinovaných cvičeních a rozšíření interoperability v oblasti norem kybernetické bezpečnosti.

5. ZÁVĚR

Kybernetická připravenost EU je klíčová pro jednotný digitální trh i pro bezpečnostní a obrannou unii. Posílení evropské kybernetické bezpečnosti a řešení hrozeb pro civilní i vojenské cíle je nezbytností.

Nadcházející digitální summit, který dne 29. září 2017 pořádá estonské předsednictví, představuje příležitost projevit společné odhodlání, aby se kybernetická bezpečnost stala jádrem EU jakožto digitální společnosti. Jako součást tohoto společného závazku Komise vyzývá členské státy, aby se závazně vyjádřily, jak hodlají postupovat v oblastech, kde mají hlavní odpovědnost. Mělo by to zahrnovat posílení kybernetické bezpečnosti prostřednictvím:

- zajištění plného a účinného provedení směrnice o bezpečnosti sítí a informací do 9. května 2018, jakož i zdrojů potřebných pro to, aby orgány veřejné správy odpovědné za kybernetickou bezpečnost mohly efektivně plnit své úkoly,
- uplatňování stejných pravidel vůči veřejným správám vzhledem k roli, kterou sehrávají ve společnosti a ekonomice jako celku,
- poskytování odborné přípravy související s kybernetickou bezpečností ve veřejné správě,
- důrazu na povědomí o kybernetické bezpečnosti v informačních kampaních a zahrnutí kybernetické bezpečnosti do učebních osnov vzdělávání a odborné přípravy,
- využívání iniciativ v rámci „stálé strukturované spolupráce“ (PESCO) a Evropského obranného fondu na podporu rozvoje projektů v oblasti kybernetické obrany.

Toto společné sdělení uvedlo rozsah úkolu a řadu opatření, která může EU učinit. Potřebujeme Evropu, která je odolná a která je schopna účinně chránit své lidi tím, že předvídá možné kybernetické bezpečnostní incidenty, vytváří silnou ochranu ve svých strukturách a svém chování, z jakéhokoli kybernetického útoku se rychle zotaví a odrazuje ty, kdo za kybernetickými útoky stojí. V tomto sdělení se předkládají cílená opatření, která koordinovaným způsobem dále posílí struktury a kapacity EU v oblasti kybernetické bezpečnosti v úzké spolupráci s členskými státy a různými dotčenými strukturami EU při respektování jejich kompetencí a odpovědností. Jeho provádění jasně prokáže, že EU

a členské státy budou spolupracovat za účelem zavedení takové úrovně kybernetické bezpečnosti, jaká odpovídá neustále rostoucím výzvám, kterým Evropa v současné době čelí.