EVROPSKÁ KOMISE

VYSOKÁ PŘEDSTAVITELKA UNIE PRO ZAHRANIČNÍ VĚCI A BEZPEČNOSTNÍ POLITIKU

V Bruselu dne 13.6.2018
JOIN(2018) 16 final

SPOLEČNÉ SDĚLENÍ EVROPSKÉMU PARLAMENTU, EVROPSKÉ RADĚ A RADĚ

Zvýšení odolnosti a posílení kapacit pro řešení hybridních hrozeb

1. ÚVOD

Hybridní činnosti státních a nestátních aktérů nadále představují závažnou a akutní hrozbu pro EU a její členské státy. Úsilí zaměřené na destabilizaci zemí oslabením důvěry veřejnosti ve vládní instituce a zpochybněním základních hodnot společností je čím dál tím běžnější. Naše společnosti čelí závažným problémům způsobeným těmi, kteří se snaží škodit EU a jejím členským státům počínaje kybernetickými útoky, které narušují hospodářství a veřejné služby, přes cílené dezinformační kampaně až po agresivní vojenské akce.

Hybridní kampaně jsou vícerozměrné, kombinují nátlaková a rozvratná opatření, při nichž jsou využívány konvenční i nekonvenční nástroje a taktiky (diplomatické, vojenské, ekonomické a technologické) k destabilizaci protivníka. Jsou koncipovány tak, aby bylo obtížné je odhalit nebo zjistit, kdo je za ně odpovědný, a mohou je použít jak státní, tak i nestátní subjekty. Útok nervovou látkou v Salisbury v březnu[1] dále upozornil na univerzálnost hybridních hrozeb a množství taktik, které jsou nyní k dispozici. V reakci na něj Evropská rada[2] zdůraznila potřebu zvýšit schopnost EU a jejích členských států odhalovat hybridní hrozby, předcházet jim a reagovat na ně v oblastech jako kybernetická bezpečnost, strategická komunikace a kontrašpionáž. Upozornila zejména na potřebu odolnosti v souvislosti s chemickými, biologickými, radiologickými a jadernými hrozbami.

Hrozby, které představují nekonvenční zbraně, spadají do samostatné kategorie z důvodu možného rozsahu škod, které mohou způsobit. A jelikož je těžké odhalit je a zjistit jejich původce, jejich náprava je složitá. Chemické, biologické, radiologické a jaderné hrozby, které překračují rámec hybridních hrozeb a zahrnují rovněž teroristické útoky, jsou rovněž předmětem všeobecného zájmu mezinárodního společenství[3], zejména vyvíjející se riziko jejich šíření jak zeměpisně, tak i v rámci nestátních subjektů.

Zvyšování odolnosti vůči těmto hrozbám a posílení souvisejících schopností je sice převážně odpovědností členských států. Orgány EU však již přijaly řadu opatření, která mají pomoci posílit úsilí jednotlivých států v této oblasti. Patří mezi ně úzká spolupráce s jinými mezinárodními aktéry, zejména s Organizací Severoatlantické smlouvy (NATO)[4], a tato činnost by se mohla dále prohloubit na podporu členských států v takových oblastech, jako je rychlá reakce[5].

Toto společné sdělení je reakcí na výzvu Evropské rady, aby tato práce pokračovala. Je součástí širšího balíčku zahrnujícího také poslední zprávu o pokroku bezpečnostní unie[6], v níž se zvažují a představují další kroky v provádění akčního plánu v oblasti chemické, biologické, radiologické a jaderné bezpečnosti z října 2017[7], a rovněž druhou zprávu o

---

1 Pokud jde o útok v Salisbury, vyjádřila Evropská rada na svém zasedání dne 22. března 2018 souhlas se závěry vlády Spojeného království, podle nichž je za útok s vysokou pravděpodobností odpovědná Ruská federace a žádné jiné věrohodné vysvětlení neexistuje.

2 Závěry ze zasedání Evropské rady z března 2018.

3 Zabývala se jimi i rezoluce Rady bezpečnosti Organizace spojených národů S/RES/2325 (2016), 14. prosince 2016.

4 Boj proti hybridním hrozbám je jednou ze sedmi oblastí spolupráce s Organizací Severoatlantické smlouvy uvedených ve společném prohlášení podepsaném ve Varšavě v červenci 2016 předsedou Evropské rady, předsedou Evropské komise a generálním tajemníkem Organizace Severoatlantické smlouvy.

5 Skupina G7, která se sešla na summitu v Charlevoix v červnu 2018, se rovněž dohodla na vývoji mechanismu rychlé reakce skupiny G7 pro řešení hrozeb pro demokracii: https://g7.gc.ca/en/official-documents/charlevoix-commitment-defending-democracy-from-foreign-threats/

6 Patnáctá zpráva o pokroku na cestě k účinné a skutečné bezpečnostní unii (COM(2018) 470).

7 COM(2017) 610 final.

pokroku[8] v provádění 22 opatření společného rámce pro boj proti hybridním hrozbám – reakce Evropské unie[9].

2. REAKCE EU

Komise a vysoká představitelka vynaložily značné úsilí na zvýšení způsobilosti EU a na účinnou podporu členských států v boji proti hybridním a chemickým, biologickým, radiologickým a jaderným hrozbám. V oblastech, jako je strategická komunikace, informovanost o situaci, posílení připravenosti a odolnosti a zvýšení způsobilosti reagovat na krize, už bylo dosaženo hmatatelných výsledků.

Pracovní skupina East StratCom zřízená po zasedání Evropské rady v březnu 2015 vedla činnost zaměřenou na oblast předvídání a zpětného sledování dezinformací pocházejících ze zahraničních zdrojů a na boj proti nim. Její odborné analýzy a zveřejněné výstupy[10] výrazně zvýšily povědomí o ruských dezinformacích. Během posledních dvou let odhalila přes 4 000 jednotlivých případů dezinformací, z nichž byly mnohé úmyslně zaměřeny na Evropu. Činnost pracovní skupiny East StratCom se rovněž soustředila na zlepšení poskytování kladných sdělení s větším dosahem ve východním sousedství. Po tomto úspěchu byly vytvořeny dvě pracovní skupiny s různým zeměpisným zaměřením – pracovní skupina pro západní Balkán a zvláštní pracovní skupina „Jih“ pro arabsky mluvící země.

Byly učiněny důležité kroky pro vybudování struktur potřebných ke zlepšení informovanosti o situaci a podpory rozhodování. V rámci střediska EU pro analýzu zpravodajských informací, které je součástí Evropské služby pro vnější činnost, bylo v roce 2016 založeno středisko pro hybridní hrozby. Toto středisko dostává a analyzuje utajované informace a informace z otevřených zdrojů od různých zúčastněných stran týkající se hybridních hrozeb. Do současnosti bylo zpracováno víc než 100 hodnocení a informačních materiálů, které jsou zpřístupněné v rámci EU a mezi členskými státy s cílem informovat o rozhodování EU. Středisko pro hybridní hrozby úzce spolupracuje s Evropským střediskem excelence pro boj proti hybridním hrozbám v Helsinkách. Středisko excelence zřízené v dubnu 2017 na podporu strategického dialogu a provádění výzkumu a analýzy hybridních hrozeb se rozšířilo, jeho členem je nyní 16 zemí[11] a dostává trvalou podporu z EU.

Byla rovněž provedena důležitá opatření k posílení připravenosti a odolnosti, zejména proti chemickým, biologickým, radiologickým a jaderným hrozbám. Za posledních šest měsíců byly učiněny významné kroky ve zjišťování nedostatků týkajících se připravenosti na chemické, biologické, radiologické a jaderné bezpečnostní incidenty, zejména pokud jde o schopnost odhalování, s cílem pomoci předcházet chemickým, biologickým, radiologickým a jaderným útokům. Konsorcium národních odborníků vypracovalo z podnětu Komise analýzu nedostatků u detekčních zařízení pro různé druhy chemických, biologických, radiologických a jaderných scénářů. Zpráva o analýze nedostatků byla poskytnuta členským státům a umožňuje jim přijímat informovaná rozhodnutí týkající se strategií odhalování a činit operativní opatření k řešení zjištěných nedostatků.

---

[8] Společná zpráva o provádění společného rámce pro boj proti hybridním hrozbám v období od července 2017 do července 2018, (JOIN(2018) 14).

[9] JOIN(2016) 18 final.

[10] Viz www.euvsdisinfo.eu.

[11] Mezi současnými 16 členy je 14 členských států EU: Česká republika, Dánsko, Estonsko, Finsko, Francie, Itálie, Německo, Lotyšsko, Litva, Nizozemí, Polsko, Španělsko, Švédsko a Spojené království. Iniciativa pro jeho vytvoření vzešla ze společného rámce pro boj proti hybridním hrozbám. Středisko aktivně podporovala také EU a Organizace Severoatlantické smlouvy v rámci jejich spolupráce.

Tato činnost byla podpořena cvičeními, která ověřovala míru dosaženého pokroku. Souběžné a koordinované cvičení v roce 2017 (PACE17) s Organizací Severoatlantické smlouvy umožnilo podrobně otestovat schopnosti EU reagovat na rozsáhlou hybridní krizi. Cvičení bylo z hlediska svého rozsahu bezprecedentní a podrobilo zkoušce nejenom Operační protokol EU pro boj proti hybridním hrozbám (EU Playbook), různé mechanismy reakce EU a jejich schopnost účinné interakce, ale i součinnost reakce EU na hybridní hrozby s opatřeními organizace Severoatlantické smlouvy. Cvičení na rok 2018 je ve fázi plánování s cílem zavést je nejenom jako každoroční praxi, ale také pomoci členským státům posílit jejich schopnost reagovat na hybridní krizi.

Tyto konkrétní kroky ilustrují, jaké výsledky přinášejí politické rámce zavedené Evropskou unií: v posledních dvou letech bylo vytvořeno několik rámců, které mají přispět k nasměrování a cílenému zaměření činnosti EU.

Společný rámec pro boj proti hybridním hrozbám – reakce Evropské unie[12] z dubna 2016 podpořil přístup na úrovni celé státní správy, přičemž bylo určeno 22 oblastí činnosti zaměřených na pomoc v boji proti **hybridním hrozbám** a posílení odolnosti EU a členských států, jakož i mezinárodních partnerů. Většina opatření stanovených ve společném rámci se zaměřuje na zlepšení informovanosti o situaci a budování odolnosti s větší schopností reagovat. Jde o celou řadu opatření, od posílení způsobilosti EU analyzovat zpravodajské informace až po zvýšení ochrany kritické infrastruktury a kybernetické bezpečnosti s cílem bojovat proti radikalizaci a násilnému extremismu. Hrozby související s kybernetickou bezpečností a kybernetické útoky jsou rovněž klíčovým prvkem společného rámce. Ve druhé zprávě o pokroku v provádění společného rámce, která byla přijata souběžně s tímto společným sdělením, se prokazuje hmatatelný pokrok v těchto opatřeních a potvrzuje posílení a prohloubení úsilí EU v boji proti hybridním hrozbám[13].

Pokud jde o **kybernetickou bezpečnost**, 9. květen 2018 byl významným mezníkem jako konečný termín pro všechny členské státy EU, aby provedly první právně závazný soubor pravidel o kybernetické bezpečnosti v rámci celé EU – směrnici o bezpečnosti sítí a informací. Je to významná součást širšího přístupu stanoveného ve *společném sdělení: Odolnost, odrazování a obrana: Budování silné kybernetické bezpečnosti pro EU*[14] ze září 2017 s rozsáhlými konkrétními opatřeními k zajištění zásadní podpory struktur a způsobilosti EU v oblasti kybernetické bezpečnosti. Zaměřuje se na budování odolnosti EU vůči kybernetickým útokům a na posílení kapacity EU v oblasti kybernetické bezpečnosti, vytvoření účinné trestněprávní odezvy a posílení globální stability prostřednictvím mezinárodní spolupráce. Součástí byl návrh aktu o kybernetické bezpečnosti za účelem posílení podpory na úrovni EU[15] společně s řadou návrhů, které je třeba realizovat (viz níže).

Dezinformace poškozují naše demokracie tím, že omezují schopnost občanů přijímat informovaná rozhodnutí a účastnit se demokratického procesu. Internet výrazně zvýšil množství a rozmanitost zpráv, které mají občané k dispozici. Nové technologie však lze použít v nebývalém rozsahu a s bezprecedentní rychlostí k šíření dezinformací, které jsou přesně zaměřeny na rozsévání nedůvěry a vytváření společenského napětí. *Sdělení* Komise *Boj proti dezinformacím na internetu: evropský přístup*[16] stanoví evropský přístup v reakci na problém dezinformací tím, že vyzývá různé zúčastněné strany, zejména internetové platformy, ale také mediální společnosti, aby přijaly opatření. Tato opatření zahrnují

---

13 První zpráva o provádění (červenec 2017): JOIN(2017) 30 final.
14 JOIN(2017) 450 final.
15 COM(2017) 477, viz níže.
16 COM(2018) 236 final.

širokou škálu příslušných oblastí, včetně větší transparentnosti, důvěryhodnosti a odpovědnosti internetových platforem, bezpečnější a odolnější volební procesy, podporu vzdělávání a mediální gramotnost, podporu kvalitní žurnalistiky a boj proti dezinformacím prostřednictvím strategické komunikace. Prvním konkrétním krokem je kodex zásad boje proti šíření dezinformací, jenž má vypracovat fórum mnoha zainteresovaných subjektů o dezinformacích a síť ověřovatelů faktů, která má být zavedena do léta. První zasedání fóra mnoha zainteresovaných subjektů o dezinformacích se konalo dne 29. května 2018 a byly na něm dohodnuty kroky potřebné k přijetí kodexu v červenci 2018. Komise do konce roku 2018 posoudí pokrok dosažený v řešení tohoto problému a rozhodne, zda je v této oblasti potřebný další zásah. Plánované činnosti budou v souladu s činnostmi pracovní skupiny East StratCom a budou je doplňovat.

Pokud jde o **chemická, biologická, radiologická a jaderná** rizika, v *akčním plánu*[17] Komise z října 2017 bylo navrženo 23 praktických opatření a opatření zaměřených na lepší ochranu občanů a infrastruktur před těmito hrozbami, kromě jiného i prostřednictvím spolupráce mezi EU a jejími členskými státy, jakož i s Organizací Severoatlantické smlouvy. Jako součást opatření v oblasti bezpečnostní unie pro zlepšení ochrany před terorismem a zvýšení odolnosti proti němu se vycházelo z preventivního přístupu založeného na základním principu, podle něhož jsou sice chemická, biologická, radiologická a jaderná rizika méně pravděpodobná, ale v případě útoku mají vážný a dlouhotrvající dopad. Útok v Salisbury a také rostoucí obavy z toho, jaký mají teroristé zájem a schopnost využívat chemické, biologické, radiologické a jaderné materiály a látky v EU i mimo ni[18], mezitím ukazují, že hrozba, kterou tyto látky a materiály představují, je reálná. Tato skutečnost dále posiluje naléhavou potřebu plně provádět akční plán. Ten se řídí přístupem zohledňujícím veškerá rizika a zaměřuje se na čtyři cíle: omezení dostupnosti chemických, biologických, radiologických a jaderných materiálů a látek, zajištění lepší připravenosti a reakce na chemické, biologické, radiologické a jaderné bezpečnostní incidenty, budování silnějších vnitřních a vnějších vazeb v oblasti chemické, biologické, radiologické a jaderné bezpečnosti s klíčovými regionálními a mezinárodními partnery EU a zlepšení znalostí o chemických, biologických, radiologických a jaderných rizicích. Podrobná zpráva o hmatatelném pokroku v provádění akčního plánu je uvedena v poslední zprávě o pokroku bezpečnostní unie přijaté souběžně s tímto společným sdělením.

S cílem zvýšit úsilí v boji proti hybridním hrozbám a posílit myšlenku jednoty mezi členskými státy a Organizací Severoatlantické smlouvy (NATO) byla spolupráce v boji proti hybridním hrozbám určena za klíčovou oblast **spolupráce mezi EU a NATO**, jak je uvedeno ve *varšavském společném prohlášení* z července 2016[19]. Téměř jedna třetina všech současných společných návrhů na spolupráci se zaměřuje na hybridní hrozby[20]. Cvičení a „Operační protokol EU“ (EU Playbook)[21] popsané výše vycházejí z prohloubené spolupráce v letošním roce.

---

17 COM(2017) 610 final.

18 Europol, Terrorism Situation and Trend report (TE-SAT) 2017 (Zpráva o stavu a vývoji terorismu v EU), s. 16, k dispozici na adrese: www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf. Viz také prohlášení generálního ředitele Organizace pro zákaz chemických zbraní (OPCW): www.globaltimes.cn/content/1044644.shtml.

19 Prohlášení podepsané předsedou Junckerem, předsedou Tuskem a generálním tajemníkem NATO Stoltenbergem představuje současný základ pro spolupráci mezi EU a NATO.

20 15283/16 a 14802/17.

21 Pracovní dokument útvarů Komise SWD(2016) 227 final.

3. ZINTENZIVNĚNÍ REAKCE NA VYVÍJEJÍCÍ SE HROZBY

3.1. Informovanost o situaci – lepší schopnost odhalovat hybridní hrozby

Úsilí bojovat proti hybridním hrozbám a reagovat na ně musí být podpořeno schopností včas odhalit škodlivé hybridní činnosti a zdroje, jak vnitřní, tak i vnější, a pochopit možné souvislosti mezi často zdánlivě nepropojenými událostmi. Za tímto účelem je nezbytné využít veškeré dostupné datové toky, včetně informací z veřejně dostupných zdrojů.

Středisko pro hybridní hrozby zřízené v rámci Evropské služby pro vnější činnost jako centrální místo EU zaměřené na analýzu hybridních hrozeb je důležitým přínosem, musí však mít k dispozici potřebné odborné znalosti pro řešení celého spektra hybridních hrozeb, kromě jiného i v oblasti chemických, biologických, radiologických a jaderných rizik a také v oblasti kontrašpionáže. Rozšíření odborných znalostí by zvýšilo podporu případné budoucí reakce EU na krizi poskytnutím úplnějších produktů civilních a vojenských zpravodajských služeb v těchto konkrétních oblastech. Mohlo by se opírat o opatření členských států, která by rozšířila poskytování zpravodajských příspěvků jejich vnitrostátních služeb středisku pro hybridní hrozby a dále posílila schopnost vytvořené sítě národních kontaktních míst pro středisko pro hybridní hrozby poskytovat a zpracovávat informace, u nichž kritickou úlohu hraje čas. Dalším krokem by bylo zaměření členských států na rozšíření zpravodajských příspěvků jejich vnitrostátních útvarů pro Středisko EU pro analýzu zpravodajských informací (INTCEN), aby bylo možné provádět hlubší analýzu potenciálních hrozeb.

Další kroky v budoucnosti

- Vysoká představitelka rozšíří středisko EU pro hybridní hrozby o specializované analytické složky pro chemické, biologické, radiologické a jaderné záležitosti, kontrarozvědku a také o kybernetickou složku. Členské státy se vyzývají, aby zintenzívnily poskytování zpravodajských příspěvků středisku pro hybridní hrozby za účelem analýzy existujících a vznikajících hybridních hrozeb.

- Komise v koordinaci s vysokou představitelkou dokončí práci na ukazatelích zranitelnosti, aby členské státy mohly lépe posoudit potenciální hybridní hrozby v různých odvětvích. Tato činnost podpoří rovněž analýzu EU týkající se trendů v oblasti hybridních hrozeb.

3.2. Posílená opatření proti chemickým, biologickým, radiologickým a jaderným hrozbám

Akční plán z října 2017 pro zlepšení připravenosti na chemická, biologická, radiologická a jaderná bezpečnostní rizika poskytuje rámec pro opatření k posílení připravenosti, odolnosti a koordinace na úrovni EU. Činnosti, které jsou v něm stanoveny, zahrnují celou řadu opatření na podporu členských států sdružováním odborných poznatků a společným budováním kapacit, výměnou znalostí a osvědčených postupů a zvýšením operační spolupráce. Je nutné, aby členské státy a Komise spolupracovaly za účelem urychleného plného provádění akčního plánu. Kromě toho by nyní Unie na základě již dosaženého pokroku v analýze nedostatků ve schopnostech odhalování a výměně osvědčených postupů v rámci nově vytvořené poradní skupiny pro chemickou, biologickou, radiologickou a jadernou bezpečnost měla přijmout další opatření pro řešení vznikajících a vyvíjejících se hrozeb. Týká se to zejména chemických hrozeb. Je třeba, aby EU podle

vzoru přijatých opatření k omezení přístupu k prekurzorům výbušnin[22] urychleně učinila operativní opatření, která zlepší kontrolu přístupu k vysoce rizikovým chemickým látkám a schopnost co nejdříve takové látky odhalit. Členské státy by měly zvážit rovněž provedení další analýzy nedostatků a mapování situace na úrovni EU, například v oblasti chemické, biologické, radiologické a jaderné odolnosti a dekontaminačních schopností a přístupů v této oblasti. Příprava na chemické, biologické, radiologické a jaderné útoky a zvládání jejich následků vyžaduje posílenou spolupráci a koordinaci mezi členskými státy, a to i mezi orgány civilní ochrany. Mechanismus civilní ochrany Unie může v tomto procesu hrát klíčovou úlohu s cílem posílit společnou kapacitu Evropy v oblasti připravenosti a reakce na tyto hrozby.

Mezinárodní spolupráce je také důležitým prvkem v této činnosti a EU může stavět na vazbách s regionálními chemickými, biologickými, radiologickými a jadernými středisky excelence, včetně hledání synergií s Organizací Severoatlantické smlouvy a programy prevence přírodních katastrof a katastrof způsobených člověkem a připravenosti a reakce na ně v zemích jižního a východního partnerství[23].

Další kroky v budoucnosti

- EU by měla prozkoumat opatření, jež by podpořila dodržování mezinárodních pravidel a norem zaměřených proti používání chemických zbraní, mimo jiné prostřednictvím zvláštního režimu sankcí EU týkajícího se chemických zbraní.

- Aby se pokročilo v akčním plánu v oblasti chemické, biologické, radiologické a jaderné bezpečnosti, bude Komise spolupracovat s členskými státy na dokončení těchto kroků do konce roku 2018:
  - vypracování seznamu chemických látek, které představují mimořádnou hrozbu, jako základ operativního opatření ke snížení jejich dostupnosti,
  - navázání dialogu se soukromými subjekty v dodavatelském řetězci v zájmu společné práce na řešení vyvíjejících se hrozeb vyplývajících z chemických látek, které mohou být použity jako prekurzory,
  - urychlení přezkumu scénářů ohrožení a analýzy existujících metod odhalování, aby se zlepšilo odhalování chemických hrozeb, s cílem zpracovat operativní pokyny pro členské státy za účelem zvýšení jejich schopnosti odhalování hrozeb.

- Členské státy by měly vytvořit soupisy zásob základních lékařských protiopatření, laboratoří, kapacit pro péči a dalších kapacit. Komise bude spolupracovat s členskými státy na pravidelném mapování dostupnosti těchto zásob v EU, aby se zlepšil přístup k nim a umožnilo jejich rychlé nasazení v případě útoků.

[22] Komise v rámci činnosti v oblasti bezpečnostní unie zaměřené na minimalizaci prostoru pro působení teroristů a zločinců přijala rázná opatření pro omezení přístupu k prekurzorům výbušnin, které lze zneužít k domácí výrobě výbušnin. V říjnu 2017 Komise předložila doporučení, v němž se stanoví okamžitá opatření k zamezení zneužívání prekurzorů výbušnin na základě existujících pravidel (doporučení C(2017) 6950 final). Na základě toho Komise v dubnu 2018 přijala návrh na revizi a posílení existujícího nařízení č. 98/2013 o uvádění prekurzorů výbušnin na trh a o jejich používání (COM(2018) 209 final).

[23] Ve východním a jižním sousedství je organizována odborná příprava a cvičení civilní ochrany v rámci regionálních programů prevence přírodních katastrof a katastrof způsobených člověkem a připravenosti a rekce na ně.

3.3. **Strategická komunikace – ucelené šíření informací**

Důležitou výzvou v souvislosti s hybridními hrozbami je zvýšení informovanosti a vzdělávání veřejnosti, aby běžní občané byli schopni odlišit informace od dezinformací. Na základě zkušeností pracovní skupiny East StratCom, střediska EU pro hybridní hrozby a Evropského střediska excelence pro boj proti hybridním hrozbám, jakož i dalšího úsilí Komise[24], bude Komise a vysoká představitelka dále rozvíjet a profesionalizovat kapacity EU pro strategickou komunikaci tím, že zajistí systematickou interakci a soudržnost mezi stávajícími strukturami. Tato možnost bude ještě rozšířena na další orgány EU a členské státy, včetně využití ohlášené zabezpečené platformy online zabývající se dezinformacemi.

Zlepšení koordinace a spolupráce v oblasti strategické komunikace mezi orgány EU, členskými státy, partnery a mezinárodními organizacemi bude důležitá a bude vyžadovat přípravu a nácvik před reakcí na krize v reálném čase.

Ukázalo se, že období voleb je zvláště strategickým a citlivým cílem kybernetických útoků a obcházení obvyklých („off-line“) záruk a pravidel na internetu, jako jsou tzv. období ticha před konáním voleb, transparentní pravidla financování a stejné zacházení s uchazeči. Patří sem útoky na volební infrastrukturu a na informační systémy kampaní a také politicky motivované masové dezinformační kampaně a kybernetické útoky ze strany třetích zemí, jejichž cílem je zdiskreditovat demokratické volby a zpochybnit jejich legitimitu. Na úrovni EU se provádí několika pracovních okruhů pro zvýšení informovanosti členských států v oblasti přípravy a reakce na tyto vyvíjející se hrozby. Orgány členských států pro kybernetickou bezpečnost[25] vydají v Radě dobrovolné pokyny a určí společné osvědčené postupy pro zajištění kybernetické bezpečnosti volebních technologií po dobu volebního cyklu. To se týká informačních systémů a řešení IKT používaných pro registraci voličů a kandidátů, shromažďování a počítání hlasů a výsledků vysílání a také pomocných systémů přímo spojených se zákonností výsledků voleb.

Je rovněž nutné zajistit rychlé, spolehlivé a úplné informace pro širokou veřejnost v případě hybridních útoků. Jakýkoli chemický, biologický, radiologický a jaderný incident nebo událost s podobným dopadem vyvolává veřejný protest, protože občané žádají rychlé odpovědi. Strategické zprávy hrají klíčovou úlohu, mimo jiné i mezi mezinárodními organizacemi, které mohou samostatně stanovit své plány reakce.

[24] Například zastoupení Komise působí i v oblasti prověřování faktů a popírání mýtů. Některá vyvinula místně přizpůsobené nástroje, jako je *Les Décodeurs de l'Europe* ve Francii, UE Vero Falso v Itálii, veřejná soutěž EU s kreslenými figurkami na vyvracení mýtů v Rakousku, podobná komiksová série v Rumunsku a tzv. Euromyths A–Z ve Spojeném království. Další podobné projekty se připravují.

[25] Pod záštitou skupiny pro spolupráci zřízené podle směrnice o bezpečnosti sítí a informačních systémů.

Další kroky v budoucnosti

- Evropská služba pro vnější činnost a Komise budou v rámci svých příslušných pravomocí spolupracovat, aby byla navázána strukturovanější spolupráce v oblasti strategické komunikace za účelem řešení dezinformací pocházejících z EU i ze třetích zemí a odrazování od vytváření nepřátelských dezinformací a hybridních zásahů cizích vlád.

- Komise na podzim uspořádá setkání na vysoké úrovni s členskými státy a příslušnými zúčastněnými stranami, včetně kolokvia o základních právech věnovaného demokracii, aby podpořila osvědčené postupy a poskytla pokyny, jak předcházet kybernetickým a dezinformačním hrozbám v období voleb, zmírňovat je a reagovat na ně.

- Vysoká představitelka a Komise přezkoumají možnosti, jak lépe podpořit činnost tří pracovních skupin StratCom, pokud jde o nástroje a zdroje, aby se zajistilo dostatečné zvýšení úsilí EU s ohledem na komplexitu dezinformačních kampaní, které vedou nepřátelské subjekty.

3.4. **Budování odolnosti a odrazování v odvětví kybernetické bezpečnosti**

Kybernetická bezpečnost je velmi důležitá pro naši prosperitu i bezpečnost. Se stále větší závislostí našeho každodenního života i ekonomiky na digitálních technologiích jsme čím dál víc vystaveni kybernetickým hrozbám.

Překážkou účinné kybernetické bezpečnosti v EU jsou v současné době nedostatečné investice a nedostatečná koordinace. EU se nyní snaží řešit tuto otázku budováním kapacit prostřednictvím podpůrných opatření, důkladnější koordinace a nových struktur pro pokročilé technologie a jejich zavedení v oblasti kybernetické bezpečnosti.[26] Ve směrnici o bezpečnosti sítí a informačních systémů byla stanovena minimální úroveň bezpečnosti sítí a informačních systémů[27] v celé Unii. Její úplné provádění všemi členskými státy je důležité pro zvýšení kybernetické odolnosti: jde o první klíčový krok. Obecné nařízení o ochraně osobních údajů zavádí povinnost oznamovat porušení ochrany osobních údajů příslušnému orgánu dohledu. K dalším klíčovým opatřením patří silnější a modernizovaná Agentura Evropské unie pro kybernetickou bezpečnost a rámec EU pro certifikaci produktů a služeb IKT[28] za účelem budování důvěry spotřebitelů. Probíhá rovněž práce na pomoc síti odborných středisek členských států s cílem stimulovat rozvoj a zavádění řešení kybernetické bezpečnosti a doplnit úsilí zaměřené na budování kapacit v této oblasti na úrovni EU a na vnitrostátní úrovni. Bude se opírat o činnost programu Digitální Evropa předloženého Komisí dne 6. června[29], který pokládá investice EU do kybernetické bezpečnosti za novou prioritu.

Doporučení pro koordinovanou reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize („návrh doporučení“)[30] zároveň stanovilo, jak by měla fungovat spolupráce mezi členskými státy a různými subjekty EU v reakci na rozsáhlý přeshraniční kybernetický útok. Bylo v něm zdůrazněno, jak důležitou úlohu pro účinnou koordinaci na technických,

[26] V rámci posílení inovací v regionech Evropy byla v prosinci 2017 zahájena nová meziregionální pilotní akce s cílem zintenzivnit činnosti regionů EU v oblasti kybernetické bezpečnosti.

[27] 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.

[28] COM(2017) 477.

[29] Návrh nařízení, kterým se zavádí program Digitální Evropa na období 2021–2027, (COM(2018) 434).

[30] C(2017) 6100.

operativních a strategických/politických úrovních hraje informovanost o situaci. Skupina pro spolupráci zřízená podle směrnice o bezpečnosti sítí a informačních systémů pracuje rovněž na zlepšení výměny informací mezi příslušnými stranami a jejich společného využívání a na vytváření společné taxonomie pro popis incidentu. Tento přístup bude otestován v nadcházejících cvičeních. Středisko pro hybridní hrozby poskytuje strategickou analýzu současných a vznikajících kybernetických hrozeb na základě příspěvků zpravodajských služeb členských států.

Rámec pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru („soubor nástrojů pro diplomacii v oblasti kybernetiky“) byl z operativního hlediska významným krokem vpřed a stanovil 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. Čím více jej členské státy budou naplno využívat, tím víc bude působit jako účinný odrazující prostředek. V dubnu Rada pro zahraniční věci přijala závěry o nepřátelské činnosti v kyberprostoru, v nichž bylo důrazně odsouzeno nepřátelské využívání informačních a komunikačních technologií, včetně útoků Wannacry a NotPetya, které způsobily značné škody a hospodářské ztráty v EU a mimo ni.

EU a její členské státy musí zlepšit svou schopnost zjistit, kdo je za kybernetické útoky odpovědný, v neposlední řadě prostřednictvím rozšířeného společného využívání zpravodajských informací. Určení viníků by odradilo potenciální útočníky a zvýšilo šance, že odpovědné osoby se budou náležitě zodpovídat. Zvýšení odrazujícího účinku je klíčovým cílem strategického přístupu Komise pro zvýšení kybernetické bezpečnosti. Nedávné návrhy Komise zaměřené na zlepšení přeshraničního shromažďování elektronických důkazů pro trestní řízení by rovněž podstatně zlepšily schopnost donucovacích orgánů vyšetřovat a stíhat kybernetickou kriminalitu.

Silná kybernetická odolnost vyžaduje kolektivní a široký přístup. K tomu jsou zapotřebí silnější a účinnější struktury na podporu kybernetické bezpečnosti a reakce na kybernetické útoky v členských státech, ale také v orgánech, agenturách, delegacích, misích a operacích EU: skutečnost, že v evropských orgánech chybí společná bezpečná komunikační síť, je závažným nedostatkem. Informovanost o kybernetické bezpečnosti v rámci orgánů EU a jejich zaměstnanců by se měla zvýšit zlepšením bezpečnostní kultury a intenzivnějším školením.

Další kroky v budoucnosti

- Evropský parlament a Rada by měly urychlit práci zaměřenou na uzavření jednání o návrzích v oblasti kybernetické bezpečnosti dosažením dohody do konce letošního roku a urychleně se dohodnout na navrhovaných právních předpisech týkajících se shromažďování elektronických důkazů.

- Komise a vysoká představitelka budou úzce spolupracovat s členskými státy s cílem pokročit v kybernetických aspektech mechanismů krizového řízení a reakce v rámci celé EU. Členské státy se vyzývají, aby pokračovaly ve své práci v oblasti zjišťování viníků kybernetických útoků a v praktickém využívání souboru nástrojů pro diplomacii v oblasti kybernetiky za účelem posílení politické reakce na kybernetické útoky.

- V reakci na potřebu zvýšit naše schopnosti kybernetické obrany se zřizuje specializovaná platforma odborné přípravy a vzdělávání s cílem pomoci koordinovat možnosti odborné přípravy v oblasti kybernetické obrany, které poskytují členské státy. Bude vyvíjeno úsilí o synergie s podobnými činnostmi Organizace Severoatlantické smlouvy v této oblasti.

3.5. **Budování odolnosti vůči nepřátelské zpravodajské činnosti**

Boj proti nepřátelské zpravodajské činnosti v souladu s příslušnými unijními a vnitrostátními pravidly a opatřeními vyžaduje především zvýšenou a účinnou koordinaci mezi členskými státy. Je však rovněž nezbytné zvýšit schopnost orgánů EU čelit rostoucí hrozbě takových aktivit zaměřených výslovně na orgány a budovat kulturu informovanosti o bezpečnosti podporovanou lepší odbornou přípravou a fyzickým zabezpečením. Orgány by rovněž mohly spolupracovat s členskými státy na budování odolnějšího akreditačního systému EU. Takový systém by byl založen na aktivním podávání zpráv, které by umožňovalo lepší informovanost mezi členskými státy a orgány o případných nepřátelských aktérech, zejména těch, které už členské státy identifikovaly.

Koordinace mezi členskými státy a mezi členskými státy a jinými relevantními mezinárodními organizacemi, zejména Organizací Severoatlantické smlouvy, by pomohla mít pro kontrarozvědku proti nepřátelské činnosti v EU aktivační účinek. Příkladem oblasti, pro kterou by větší koordinace mezi členskými státy znamenala přínos, je prověřovací mechanismus pro investice na základě nařízení[31] o prověřování přímých zahraničních investic ze strany členských států v zájmu bezpečnosti a veřejného pořádku, jehož návrh Komise předložila v září 2017. Větší koordinace mezi členskými státy by byla rovněž důležitá pro kontrolu finančních transakcí, neboť nepřátelské zpravodajské služby ve stále větší míře financují svá aktivní opatření proti EU prostřednictvím důkladně rozpracovaných finančních systémů.

[31] Návrh nařízení Evropského parlamentu a Rady, kterým se stanoví rámec pro prověřování přímých zahraničních investic do Evropské unie, (COM(2017) 487).

Další kroky v budoucnosti

- Evropská služba pro vnější činnost a Komise zavedou zlepšená praktická opatření pro udržení a rozvoj schopnosti EU spolupracovat s členskými státy v boji proti nepřátelské zpravodajské činnosti zaměřené konkrétně na instituce.

- Rozšířené středisko pro hybridní hrozby bude doplněno odborníky v oblasti kontrašpionáže s cílem poskytnout podrobné analýzy a informace o povaze nepřátelské zpravodajské činnosti namířené pravděpodobně proti jednotlivým osobám a institucím.

- Evropský parlament a Rada by měly urychlit práci zaměřenou na uzavření jednání o návrhu týkajícím se prověřování investic do konce tohoto roku.

4. ZÁVĚR

Hybridní a chemické, biologické, radiologické a jaderné hrozby jsou v EU pozorně sledovanou oblastí. Březnový incident ve Spojeném království ukázal, jak široké je spektrum hybridních válek a že je mimořádně nutné vybudovat odolnost vůči chemickým, biologickým, radiologickým a jaderným hrozbám.

Komise a vysoká představitelka přijaly a navrhly několik iniciativ pro řešení výzev, které hybridní hrozby představují. Komise takto urychluje provádění akčního plánu z roku 2017 s cílem zvýšit připravenost na chemická, biologická, radiologická a jaderná bezpečnostní rizika.

Toto společné sdělení slouží k informování Evropské rady o probíhající práci a k určení oblastí, v nichž by se měla opatření zintenzivnit za účelem dalšího prohloubení a posílení zásadního příspěvku EU k řešení těchto hrozeb. Nyní je na členských státech, Komisi a vysoké představitelce, aby zajistily rychlá následná opatření.