EURÓPSKA
KOMISIA

VYSOKÁ PREDSTAVITEĽKA
ÚNIE PRE
ZAHRANIČNÉ VECI
A BEZPEČNOSTNÚ POLITIKU

V Bruseli 13. 6. 2018
JOIN(2018) 16 final

SPOLOČNÉ OZNÁMENIE EURÓPSKEMU PARLAMENTU, EURÓPSKEJ RADE A RADE

Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby

1. ÚVOD

Hybridné činnosti štátnych a neštátnych aktérov naďalej predstavujú závažnú a akútnu hrozbu pre EÚ a jej členské štáty. Úsilie zamerané na destabilizáciu krajín tým, že sa oslabí dôvera verejnosti vo vládne inštitúcie, a spochybnením základných hodnôt spoločností sa stáva stále bežnejším. Naše spoločnosti čelia vážnym problémom spôsobeným tými, čo sa snažia škodiť EÚ a jej členským štátom, počnúc kybernetickými útokmi, ktoré narúšajú hospodárstvo a verejné služby, cez cielené dezinformačné kampane až po agresívne vojenské akcie.

Hybridné kampane sú majú viacrozmerný charakter, kombinujú v sebe donucovacie a podvratné opatrenia, pričom využívajú konvenčné aj nekonvenčné nástroje a taktiky (diplomatické, vojenské, ekonomické a technologické) s cieľom destabilizovať protivníka. Sú navrhnuté tak, aby ich bolo ťažké odhaliť alebo nájsť ich pôvodcu, a môžu ich použiť tak štátne, ako aj neštátne subjekty. Útok nervovou látkou v Salisbury v marci[1] ďalej poukázal na univerzálnosť hybridných hrozieb a na množstvo taktík, ktoré sú v súčasnosti k dispozícii. Európska rada[2] v reakcii na to zdôraznila potrebu zvýšiť schopnosť EÚ a jej členských štátov odhaľovať hybridné hrozby, predchádzať im a reagovať na ne v takých oblastiach, ako je kybernetická bezpečnosť, strategická komunikácia a kontrarozviedna činnosť. Osobitnú pozornosť pripísala aj potrebe odolnosti proti chemickým, biologickým, rádiologickým a jadrovým hrozbám.

Hrozby, ktoré predstavujú nekonvenčné zbrane, patria do samostatnej kategórie z dôvodu možného rozsahu škody, ktorú môžu spôsobiť. Nielenže je ťažké ich odhaliť a nájsť ich pôvodcu, je veľmi zložité riešiť ich. Chemické, biologické, rádiologické a jadrové hrozby, ktoré prekračujú rámec hybridných hrozieb a zahŕňajú aj teroristické útoky, takisto vzbudzujú všeobecné obavy medzinárodného spoločenstva[3], najmä vyvíjajúce sa riziko šírenia zbraní tak geograficky, ako aj v rámci neštátnych subjektov.

Za zvýšenie odolnosti voči týmto hrozbám a posilnenie spôsobilostí zodpovedajú prevažne členské štáty. Inštitúcie EÚ však už prijali niekoľko opatrení, ktoré majú pomôcť posilniť vnútroštátne úsilie. To zahŕňalo úzku spoluprácu s inými medzinárodnými aktérmi, najmä s Organizáciou Severoatlantickej zmluvy (NATO)[4], a táto práca by sa mohla ďalej prehlbovať tak, aby poskytovala podporu členským štátom v oblastiach, ako je napríklad rýchla reakcia[5].

Toto spoločné oznámenie je reakciou na výzvu Európskej rady, aby sa v tejto činnosti napredovalo. Je súčasťou širšieho balíka zahŕňajúceho tiež poslednú správu o pokroku dosiahnutom pri budovaní bezpečnostnej únie[6], v ktorej sa hodnotia a uvádzajú ďalšie

---

1 Pokiaľ ide o útok v Salisbury, Európska rada 22. marca 2018 „vyjadrila súhlas s názorom vlády Spojeného kráľovstva, že zodpovednosť za útok nesie s vysokou pravdepodobnosťou Ruská federácia a že neexistuje iné vierohodné vysvetlenie“.

2 Závery Európskej rady z marca 2018.

3 Vrátane rezolúcie Bezpečnostnej rady Organizácie Spojených národov S/RES/2325 (2016) zo 14. decembra 2016.

4 Boj proti hybridným hrozbám je jednou zo siedmich oblastí spolupráce s Organizáciou Severoatlantickej zmluvy uvedenej v spoločnom vyhlásení podpísanom vo Varšave v júli 2016 predsedom Európskej rady, predsedom Európskej komisie a generálnym tajomníkom Organizácie Severoatlantickej zmluvy.

5 Na zasadnutí skupiny G7 v rámci samitu v Charlevoix v júni 2018 sa tiež odsúhlasilo vypracovanie mechanizmu rýchlej reakcie G7 s cieľom riešiť hrozby pre demokracie: https://g7.gc.ca/en/official-documents/charlevoix-commitment-defending-democracy-from-foreign-threats/

6 Pätnásta správa o pokroku dosiahnutom pri budovaní účinnej a skutočnej bezpečnostnej únie, COM(2018) 470.

kroky v plnení akčného plánu v oblasti chemickej, biologickej, rádiologickej a jadrovej bezpečnosti z októbra 2017[7], ako aj druhú správa o pokroku[8] pri vykonávaní 22 opatrení Spoločného rámca pre boj proti hybridným hrozbám – reakcia Európskej únie[9].

2. REAKCIA EÚ

Komisia a vysoká predstaviteľka vynaložili veľké úsilie na vybudovanie spôsobilostí EÚ a na účinnú podporu členských štátov v boji proti hybridným a chemickým, biologickým, rádiologickým a jadrovým hrozbám. V oblastiach, ako je strategická komunikácia, situačné povedomie, posilnenie pripravenosti a odolnosti a zvýšenie kapacít reagovať na krízy, sa už dosiahli hmatateľné výsledky.

Pracovná skupina East StratCom zriadená po zasadnutí Európskej rady v marci 2015 viedla činnosť zameranú na oblasť predpovedania a spätného sledovania dezinformácií pochádzajúcich zo zahraničných zdrojov, ako aj boja proti nim. Jej odborné analýzy a uverejnenia[10] výrazne zvýšili informovanosť o vplyve ruských dezinformácií. V priebehu posledných dvoch rokov odhalila viac ako 4 000 jednotlivých prípadov dezinformácií, z ktorých mnohé sa úmyselne zameriavali na Európu. Činnosť pracovnej skupiny East StratCom sa takisto zamerala na kvalitnejšie poskytovanie pozitívnych oznámení, s väčším dosahom vo východnom susedstve. Na základe tohto úspechu boli vytvorené dve ďalšie pracovné skupiny s rôznym geografickým zameraním – osobitná pracovná skupina pre západný Balkán a osobitná pracovná skupina Juh pre arabský svet.

Podnikli sa dôležité kroky na vybudovanie štruktúr potrebných na zlepšenie situačného povedomia a podporu rozhodovania. Stredisko pre hybridné hrozby bolo zriadené v roku 2016 v rámci Spravodajského a situačného centra EÚ Európskej služby pre vonkajšiu činnosť. Stredisko EÚ pre hybridné hrozby prijíma a analyzuje utajované informácie a informácie z otvorených zdrojov od rôznych zainteresovaných subjektov týkajúce sa hybridných hrozieb. K dnešnému dňu bolo vypracovaných viac ako 100 posúdení a brífingov, ktoré sú sprístupnené v rámci EÚ a medzi členskými štátmi s cieľom formovať rozhodovací proces EÚ. Stredisko pre hybridné hrozby má úzke pracovné vzťahy s Európskym centrom excelentnosti pre boj proti hybridným hrozbám, ktoré má sídlo v Helsinkách. Toto centrum, ktoré bolo zriadené v apríli 2017 na posilnenie strategického dialógu a vykonávanie výskumu a analýzy hybridných hrozieb, teraz rozšírilo svoje členstvo na 16 krajín[11], pričom sa mu dostáva nepretržitej podpory z EÚ.

Urobili sa aj dôležité opatrenia zamerané na posilnenie pripravenosti a odolnosti, najmä proti chemickým, biologickým, rádiologickým a jadrovým hrozbám. Za posledných šesť mesiacov boli zaznamenané významné kroky pri odhaľovaní nedostatkov v pripravenosti na chemické, biologické, rádiologické a jadrové bezpečnostné incidenty, najmä pokiaľ ide o detekčnú kapacitu s cieľom pomôcť predchádzať chemickým, biologickým, rádiologickým a jadrovým útokom. Na podnet Komisie vykonalo združenie národných expertov analýzu nedostatkov v detekčných zariadeniach pre rôzne typy scenárov

---

7 COM (2017) 610 final.

8 Spoločná správa o uplatňovaní spoločného rámca pre boj proti hybridným hrozbám (júl 2017 – júl 2018), JOIN(2018) 14.

9 JOIN (2016) 18 final.

10 Pozri www.euvsdisinfo.eu.

11 Zo súčasných 16 členských štátov je 14 členskými štátmi EÚ: Česká republika, Dánsko, Estónsko, Fínsko, Francúzsko, Taliansko, Nemecko, Lotyšsko, Litva, Holandsko, Poľsko, Španielsko, Švédsko, Spojené kráľovstvo. Iniciatíva na jeho vytvorenie vzišla zo Spoločného rámca pre boj proti hybridným hrozbám. Centrum aktívne podporovala aj EÚ a Organizácia Severoatlantickej zmluvy v rámci vzájomnej spolupráce.

chemických, biologických, rádiologických a jadrových útokov. Správa o analýze nedostatkov bola sprístupnená členským štátom, čo im umožňuje prijímať informované rozhodnutia o stratégiách detekcie a operačné opatrenia na riešenie zistených nedostatkov.

Táto práca bola podporená cvičeniami, ktorými sa testovala miera dosiahnutého pokroku. Paralelné a koordinované cvičenia v roku 2017 (PACE17) s Organizáciou Severoatlantickej zmluvy umožnili podrobne otestovať kapacity EÚ reagovať na rozsiahlu hybridnú krízu. Cvičenie bolo z hľadiska svojho rozsahu bezprecedentné a podrobilo skúške nielen „Operatívny protokol EÚ pre hybridné hrozby“, rôzne mechanizmy reakcie EÚ a ich schopnosť efektívne vzájomne pôsobiť, ale súčinnosť reakcie EÚ na hybridné hrozby s opatreniami Organizácie Severoatlantickej zmluvy. Cvičenie na rok 2018 je vo fáze plánovania s cieľom zaviesť ho nielen ako každoročnú prax, ale aj pomôcť členským štátom posilniť ich kapacity reagovať na hybridné krízy.

Tieto konkrétne kroky ilustrujú, ako politické rámce zavedené Európskou úniou prinášajú ovocie: v posledných dvoch rokoch sa podarilo uviesť do života niekoľko rámcov s cieľom pomôcť usmerniť a zamerať prácu EÚ.

V oznámení *Spoločný rámec pre boj proti hybridným hrozbám – reakcia Európskej únie*[12] z apríla 2016 sa podporil nadrezortný prístup, pričom bolo identifikovaných 22 oblastí činnosti na pomoc v boji proti **hybridným hrozbám** a posilnenie odolnosti EÚ a členských štátov, ako aj medzinárodných partnerov. Väčšina opatrení vymedzených v spoločnom rámci sa zameriava na zlepšenie situačného povedomia a budovanie odolnosti s väčšou schopnosťou reagovať. Ide o celé spektrum opatrení, od posilnenia kapacity EÚ analyzovať spravodajské informácie až po zvýšenie ochrany kritickej infraštruktúry a kybernetickej bezpečnosti s cieľom bojovať proti radikalizácii a násilnému extrémizmu. Hrozby súvisiace s kybernetickou bezpečnosťou a kybernetické útoky tvoria takisto kľúčový prvok spoločného rámca. V druhej správe o pokroku vo vykonávaní spoločného rámca, ktorá bola prijatá súbežne s týmto spoločným oznámením, sa preukazuje hmatateľný pokrok v týchto opatreniach a potvrdzuje posilnenie a prehĺbenie úsilia EÚ v boji proti hybridným hrozbám[13].

Pokiaľ ide o **kybernetickú bezpečnosť**, 9. máj 2018 bol dôležitým medzníkom ako konečný termín pre všetky členské štáty EÚ na transpozíciu prvého právne záväzného súboru pravidiel týkajúcich sa kybernetickej bezpečnosti v rámci EÚ, a to smernice o bezpečnosti sietí a informačných systémov. Je významnou súčasťou širšieho prístupu stanoveného v *Spoločnom oznámení o odolnosti, odrádzaní a obrane*: *budovanie silnej kybernetickej bezpečnosti v Európe*[14] zo septembra 2017 s rozsiahlymi konkrétnymi opatreniami na zabezpečenie zásadnej podpory štruktúr a spôsobilosti EÚ v oblasti kybernetickej bezpečnosti. Zameriava sa na budovanie odolnosti EÚ voči kybernetickým útokom a na posilnenie kapacity EÚ v oblasti kybernetickej bezpečnosti; vytvorenie účinnej trestnoprávnej reakcie, a zvýšenie globálnej stability prostredníctvom medzinárodnej spolupráce. Súčasťou bol návrh zákona o kybernetickej bezpečnosti s cieľom posilniť podporu na úrovni EÚ[15] spolu so sériou návrhov, ktoré je potrebné realizovať (pozri ďalej).

Dezinformácie poškodzujú naše demokracie tým, že obmedzujú schopnosť občanov prijímať informované rozhodnutia a zúčastňovať sa na demokratickom procese. Internet výrazne zvýšil množstvo a rozmanitosť správ, ktoré majú občania k dispozícii. Nové technológie sa však môžu použiť na šírenie dezinformácií v nebývalom rozsahu

---

13 Prvá správa o vykonávaní (júl 2017): JOIN (2017) 30 final.
14 JOIN (2017) 450 final.
15 COM (2017) 477, pozri nižšie.

a bezprecedentnou rýchlosťou, pričom môžu byť presne zamerané na rozsievanie nedôvery a vytváranie spoločenského napätia. *Oznámenie* Komisie o *boji proti dezinformáciám na internete: európsky prístup*[16] stanovuje európsky prístup v reakcii na problém dezinformácií, a to tým, že vyzýva rôzne zainteresované strany, najmä online platformy, ale aj mediálne spoločnosti, aby prijali opatrenia. Tieto opatrenia zahŕňajú širokú škálu príslušných oblastí vrátane väčšej transparentnosti, dôveryhodnosti a zodpovednosti online platforiem, bezpečnejšie a odolnejšie volebné procesy; podporu vzdelávania a mediálnej gramotnosti; podporu kvalitnej žurnalistiky; a boj proti dezinformáciám prostredníctvom strategickej komunikácie. Prvým konkrétnym krokom je Kódex postupov v oblasti dezinformácií, ktorý má vypracovať multilaterálne fórum zainteresovaných strán pre otázku dezinformácií a sieť overovateľov faktov, ktorá sa má zaviesť do leta. Prvé zasadnutie multilaterálneho fóra zainteresovaných strán pre otázku dezinformácií sa uskutočnilo 29. mája 2018, pričom sa dohodli kroky potrebné na prijatie kódexu v júli 2018. Komisia do konca roka 2018 posúdi pokrok dosiahnutý pri riešení tohto problému a rozhodne, či je v tejto oblasti potrebná ďalšia intervencia. Plánované činnosti budú v súlade s činnosťami pracovnej skupiny East StratCom a budú ich dopĺňať.

Pokiaľ ide o chemické, biologické, rádiologické a jadrové (CBRN) riziká, v *akčnom pláne*[17] Komisie z októbra 2017 sa navrhlo 23 praktických akcií a opatrení zameraných na lepšiu ochranu občanov a infraštruktúr pred týmito hrozbami, a to aj prostredníctvom užšej spolupráce medzi EÚ a jej členskými štátmi, ako aj s Organizáciou Severoatlantickej zmluvy. Ako súčasť opatrení v oblasti bezpečnostnej únie s cieľom zlepšiť ochranu a odolnosť proti terorizmu sa vychádzalo z preventívneho prístupu založeného na základnom princípe, podľa ktorého sú chemické, biologické, rádiologické a jadrové riziká menej pravdepodobné, ale v prípade takýchto útokov je dosah vážny a dlhotrvajúci. Medzitým útok v Salisbury a tiež rastúce obavy z toho, aký majú teroristi záujem a spôsobilosť využívať chemické, biologické, rádiologické a jadrové materiály a látky v EÚ i mimo nej[18], ukazujú, že hrozba, ktorú predstavujú chemické, biologické, rádiologické a jadrové materiály a látky, je reálna. Táto skutočnosť ďalej posilňuje naliehavú potrebu plne vykonať akčný plán. Riadi sa prístupom zohľadňujúcim všetky riziká a zameriava sa na štyri ciele: zníženie dostupnosti chemických, biologických, rádiologických a jadrových materiálov a látok; zabezpečenie dôkladnejšej pripravenosti a reakcie na chemické, biologické, rádiologické a jadrové bezpečnostné incidenty; budovanie silnejších väzieb medzi vonkajšími a vnútornými aspektmi chemickej, biologickej, rádiologickej a jadrovej bezpečnosti s kľúčovými regionálnymi a medzinárodnými partnermi EÚ; prehĺbenie vedomostí o chemických, biologických, rádiologických a jadrových rizikách. Podrobná správa o hmatateľnom pokroku pri vykonávaní akčného plánu je uvedená v najnovšej správe o pokroku bezpečnostnej únie prijatej súbežne s týmto spoločným oznámením.

Napokon, s cieľom zvýšiť účinnosť úsilia v boji proti hybridným hrozbám a posilniť myšlienku jednoty medzi členskými štátmi EÚ a spojencami Organizácie Severoatlantickej zmluvy (NATO), sa spolupráca v boji proti hybridným hrozbám vymedzila ako kľúčová oblasť **spolupráce medzi EÚ a NATO**, ako sa uvádza v *spoločnom vyhlásení z Varšavy* z júla 2016[19]. Takmer jedna tretina všetkých súčasných

---

16 COM (2018) 236 final.

17 COM (2017) 610 final.

18 Europol, Správa o stave a trendoch v oblasti terorizmu (TE-SAT) 2017, s. 16, k dispozícii na adrese: www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf. Pozri aj vyhlásenia generálneho riaditeľa Organizácie pre zákaz chemických zbraní (OPCW): www.globaltimes.cn/content/1044644.shtml.

19 Vyhlásenie podpísané predsedom Junckerom, predsedom Tuskom a generálnym tajomníkom NATO Stoltenbergom predstavuje súčasný základ pre spoluprácu medzi EÚ a NATO.

spoločných návrhov týkajúcich sa spolupráce sa zameriava na hybridné hrozby[20]. Cvičenia a „operatívny protokol EÚ“[21] vychádzajú z prehĺbenej spolupráce v tomto roku.

3. ZINTENZÍVNENIE REAKCIE NA VYVÍJAJÚCE SA HROZBY

3.1. Situačné povedomie – lepšia schopnosť odhaľovať hybridné hrozby

Úsilie bojovať proti hybridným hrozbám a reagovať na ne sa musí opierať o schopnosť včas odhaliť zlomyseľné hybridné činnosti a zdroje, vnútorné aj vonkajšie, a pochopiť možné súvislosti medzi často zdanlivo neprepojenými udalosťami. Na tento účel je nevyhnutné využiť všetky dostupné dátové toky vrátane spravodajských informácií z verejne dostupných zdrojov.

Stredisko pre hybridné hrozby zriadené v rámci Európskej služby pre vonkajšiu činnosť ako jediné miesto EÚ zamerané na analýzu hybridných hrozieb je dôležitým aktívom, potrebuje však nevyhnutnú expertízu na riešenie celého spektra hybridných hrozieb tak v oblasti chemických, biologických, rádiologických a jadrových materiálov a látok, ako aj v oblasti kontrarozviednej činnosti. Rozšírenie odborných znalostí by zvýšilo podporu akejkoľvek budúcej reakcie EÚ na krízu poskytnutím úplnejších civilných a vojenských spravodajských výstupov v týchto konkrétnych oblastiach. Mohlo by sa to opierať o opatrenia členských štátov na zintenzívnenie prispievania spravodajskými informáciami ich národných útvarov stredisku pre hybridné hrozby a na ďalšie posilnenie schopnosti vytvorenej siete národných kontaktných miest pre stredisko pre hybridné hrozby s cieľom poskytovať a spracúvať informácie, pre ktoré je dôležitý časový faktor. Ďalším krokom by bolo, aby sa členské štáty zamerali na zintenzívnenie prispievania spravodajskými informáciami ich národných útvarov Spravodajskému a situačnému centru EÚ (INTCEN) s cieľom umožniť hlbšiu analýzu potenciálnych hrozieb.

Budúce kroky

- Vysoká predstaviteľka rozšíri stredisko EÚ pre hybridné hrozby o špecializované chemické, biologické, rádiologické a jadrové spravodajské, ako aj kybernetické analytické zložky. Členské štáty sa vyzývajú, aby zintenzívnili prispievanie spravodajskými informáciami stredisku pre hybridné hrozby na analýzu existujúcich a vznikajúcich hybridných hrozieb.

- Komisia v koordinácii s vysokou predstaviteľkou dokončí práce na ukazovateľoch zraniteľnosti s cieľom umožniť členským štátom lepšie posúdiť potenciál hybridných hrozieb v rôznych odvetviach. Touto prácou sa podporí aj analýza EÚ týkajúca sa hybridných trendov.

3.2. Posilnené opatrenia proti chemickým, biologickým, rádiologickým a jadrovým hrozbám

Akčný plán z októbra 2017 proti chemickým, biologickým, rádiologickým a jadrovým bezpečnostným rizikám poskytuje rámec pre opatrenia na posilnenie pripravenosti, odolnosti a koordinácie na úrovni EÚ. Činnosti, ktoré sa v ňom stanovujú, pokrývajú celý rad opatrení na podporu členských štátov zhromažďovaním odborných znalostí a spoločným budovaním kapacít, výmenou poznatkov a najlepších postupov

[20] 15283/16 a 14802/17.
[21] SWD (2016) 227 final.

a zintenzívnením operačnej spolupráce. Členské štáty a Komisia musia prioritne spolupracovať pri vykonávaní akčného plánu v plnom rozsahu. Okrem toho by Únia mala v súčasnosti prijať ďalšie opatrenia na riešenie vznikajúcich a vyvíjajúcich sa hrozieb, a to na základe už dosiahnutého pokroku, pokiaľ ide o analýzu nedostatkov detekčnej kapacity a výmeny najlepších postupov v novej poradnej skupine pre chemickú, biologickú, rádiologickú a jadrovú bezpečnosť. Týka sa to najmä chemických hrozieb. Podľa vzoru práce na obmedzení prístupu k prekurzorom výbušnín[22] musí EÚ urýchlene prijať operatívne opatrenia s cieľom zlepšiť kontrolu prístupu k vysoko rizikovým chemickým látkam a optimalizovať schopnosť čo najskôr odhaliť takéto látky. Členské štáty by mali zvážiť aj vykonanie ďalšej analýzy nedostatkov a mapovania situácie na úrovni EÚ, napríklad v oblasti chemickej, biologickej, rádiologickej a jadrovej odolnosti a dekontaminačných aktív a prístupov. Príprava a riadenie dôsledkov chemického, biologického, rádiologického a jadrového útoku si vyžaduje posilnenú spoluprácu a koordináciu medzi členskými štátmi vrátane orgánov civilnej ochrany. Mechanizmus Únie v oblasti civilnej ochrany môže hrať v tomto procese kľúčovú úlohu s cieľom posilniť spoločnú kapacitu Európy v oblasti pripravenosti a reakcie.

Medzinárodná spolupráca je tiež dôležitým prvkom v tejto práci a EÚ môže budovať na prepojeniach s regionálnymi centrami excelentnosti v oblasti zmierňovania chemického, biologického, rádiologického a jadrového rizika vrátane hľadania synergií s Organizáciou Severoatlantickej zmluvy a prevencie prírodných katastrof a katastrof spôsobených ľudskou činnosťou v južnom a východnom susedstve a pripravenosti a reakcie na ne[23].

[22] Komisia v rámci svojej činnosti v oblasti bezpečnostnej únie zameranej na obmedzenie priestoru, v ktorom pôsobia teroristi a zločinci, prijala rázne opatrenia na zníženie prístupu k prekurzorom výbušnín, ktoré môžu byť zneužité na účely podomácky vyrobených výbušnín. V októbri 2017 Komisia predložila odporúčanie, v ktorom sa stanovujú okamžité opatrenia na zabránenie zneužívaniu prekurzorov výbušnín na základe existujúcich pravidiel [odporúčanie C(2017) 6950 final]. Na základe uvedeného Komisia prijala v apríli 2018 návrh na revíziu a posilnenie existujúceho nariadenia č. 98/2013 o uvádzaní prekurzorov výbušnín na trh a ich používaní [COM (2018) 209 final].

[23] Vo východnom a južnom susedstve sa organizuje odborná príprava a cvičenia civilnej ochrany v rámci regionálnych programov prevencie prírodných katastrof a katastrof spôsobených ľudskou činnosťou a pripravenosti a reakcie na ne.

Budúce kroky

- EÚ by mala preskúmať opatrenia na podporu dodržiavania medzinárodných pravidiel a noriem proti používaniu chemických zbraní, a to aj prostredníctvom možného osobitného systému sankcií EÚ týkajúceho sa chemických zbraní.

- Aby sa pokročilo v akčnom pláne v oblasti chemickej, biologickej, rádiologickej a jadrovej bezpečnosti, Komisia bude spolupracovať s členskými štátmi s cieľom vykonať tieto kroky do konca roka 2018:
  - vypracovať zoznam chemických látok, ktoré predstavujú mimoriadnu hrozbu, ako základ operatívneho opatrenia na zníženie ich dostupnosti;
  - nadviazať dialóg so súkromnými subjektmi v dodávateľskom reťazci s cieľom spolupracovať pri riešení vyvíjajúcich sa hrozieb vyplývajúcich z chemických látok, ktoré sa môžu použiť ako prekurzory;
  - urýchliť preskúmanie scenárov ohrozenia a analýzu existujúcich metód detekcie v záujme zlepšenia detekcie chemických hrozieb s cieľom vypracovať operatívne usmernenia pre členské štáty na účel zvýšenia ich schopností detekcie.

- Členské štáty by mali zostaviť inventárny súpis nevyhnutných zdravotníckych protiopatrení, ako aj laboratórnych, liečebných a iných kapacít. Komisia bude spolupracovať s členskými štátmi v pravidelnom mapovaní dostupnosti týchto kapacít v EÚ, aby sa zlepšil prístup k nim a ich rýchle použitie v prípade útoku.

3.3. **Strategická komunikácia – šírenie zrozumiteľných informácií**

Dôležitou výzvou v súvislosti s hybridnými hrozbami je zvýšenie informovanosti a vzdelávanie verejnosti, aby bežný občan dokázal rozlíšiť informácie od dezinformácií. Na základe skúseností pracovnej skupiny East StratCom, strediska EÚ pre hybridné hrozby a Európskeho centra excelentnosti pre boj proti hybridným hrozbám, ako aj ďalšieho úsilia Komisie[24], Komisia a vysoká predstaviteľka budú ďalej rozvíjať a profesionalizovať spôsobilosť EÚ v oblasti strategickej komunikácie zabezpečením sústavnej súčinnosti a súdržnosti medzi existujúcimi štruktúrami. To sa ďalej rozšíri aj na ostatné inštitúcie EÚ a členské štáty, a to aj využitím ohlásenej zabezpečenej internetovej platformy venovanej problematike dezinformácií.

Zlepšenie koordinácie a spolupráce v oblasti strategickej komunikácie v rámci inštitúcií EÚ, s členskými štátmi, s partnermi a medzinárodnými organizáciami bude mať zásadný význam a bude si vyžadovať prípravu a nácvik pred reakciou na krízové situácie v reálnom čase.

Ukázalo sa, že obdobie volieb je mimoriadne strategickým a citlivým cieľom pre kybernetické útoky a online obchádzanie platných („off-line“) záruk a pravidiel, ako napríklad období ticha, transparentných pravidiel financovania a rovnakého zaobchádzania s kandidátmi. Patrili sem útoky na volebnú infraštruktúru a informačné systémy kampaní, ako aj politicky motivované masové dezinformačné kampane online a kybernetické útoky zo strany tretích krajín s cieľom zdiskreditovať demokratické voľby

[24] Napríklad zastúpenia Komisie pôsobia aj v oblasti preverovania skutočností a vyvracania mýtov. Viaceré vyvinuli miestne prispôsobené nástroje, ako napr. *Les Décodeurs de l'Europe* vo Francúzsku, UE Vero Falso v Taliansku, verejnú komiksovú súťaž na tému vyvracania mýtov o EÚ v Rakúsku. Podobnú komiksovú sériu vymyslelo zastúpenie v Rumunsku a tiež v Spojenom kráľovstve, tzv. Euromyths A-Z. Viacero takýchto projektov sa navyše ešte len pripravuje.

a zneplatniť ich. Na úrovni EÚ sa uskutočňuje cielená činnosť na zvýšenie informovanosti členských štátov v oblasti prípravy a reakcie na tieto vyvíjajúce sa hrozby. V Rade vydajú orgány členských štátov pre kybernetickú bezpečnosť[25] dobrovoľné usmernenia a určia najlepšie spoločné postupy na riešenie kybernetickej bezpečnosti volebných technológií počas volebného cyklu. Patria sem informačné systémy a riešenia IKT používané na registráciu voličov a kandidátov, zber a počítanie hlasov a vysielanie výsledkov, ako aj pomocné systémy priamo spojené so zákonnosťou výsledkov volieb.

Takisto je potrebné zabezpečiť rýchle, spoľahlivé a úplné informácie pre širokú verejnosť v prípade hybridných útokov. Akýkoľvek chemický, biologický, rádiologický a jadrový incident alebo udalosť s podobným dosahom vedie k tomu, že občania požadujú rýchle odpovede. Strategické správy majú kľúčovú úlohu, a to aj medzi medzinárodnými organizáciami, ktoré môžu samostatne stanoviť svoje plány reakcie.

Budúce kroky

- Európska služba pre vonkajšiu činnosť a Komisia budú spolupracovať v rámci svojich príslušných právomocí s cieľom nadviazať štruktúrovanejšiu spoluprácu v oblasti strategickej komunikácie na riešenie dezinformácií pochádzajúcich z EÚ a mimo nej a na odradenie zahraničných vlád od vytvárania nepriateľských dezinformácií a hybridných zásahov.

- Komisia na jeseň zorganizuje stretnutia na vysokej úrovni s členskými štátmi a príslušnými zainteresovanými stranami vrátane kolokvia o základných právach, ktoré sa venuje demokracii, s cieľom podporiť najlepšie postupy a usmernenia o tom, ako predchádzať hrozbám umožnených počítačom, zmierňovať ich a reagovať na ne, ako aj dezinformáciám, ktoré predstavujú hrozbu pre volebný proces.

- Vysoká predstaviteľka a Komisia preskúmajú z hľadiska nástrojov a zdrojov spôsoby lepšej podpory činnosti, ktorú vykonávajú tri pracovné skupiny StratCom, s cieľom zabezpečiť, aby sa úsilie EÚ dostatočne vystupňovalo na vyriešenie zložitosti dezinformačných kampaní, ktoré vedú nepriateľské subjekty.

3.4. Budovanie odolnosti a odstrašujúceho účinku v sektore kybernetickej bezpečnosti

Kybernetická bezpečnosť má rozhodujúci význam pre našu prosperitu aj bezpečnosť. Keďže naše každodenné životy a naše hospodárstva čoraz viac závisia od digitálnych technológií, sme čím ďalej tým viac vystavení rizikám, ktoré sú s ich využívaním spojené.

Účinnej kybernetickej bezpečnosti v EÚ v súčasnosti bránia nedostatočné investície a nedostatočná koordinácia. EÚ sa v súčasnosti snaží riešiť túto otázku budovaním kapacít prostredníctvom podporných opatrení, dôkladnejšej koordinácie a nových štruktúr pre modernizáciu technológie a jej zavedenia v oblasti kybernetickej bezpečnosti[26]. Smernicou o bezpečnosti sietí a informačných systémov[27] sa stanovila minimálna úroveň bezpečnosti sietí a informačných systémov v celej Únii. Jej vykonávanie všetkými členskými štátmi v plnom rozsahu má zásadný význam pre posilnenie kybernetickej

[25] Pod záštitou skupiny pre spoluprácu zriadenej podľa smernice o bezpečnosti sietí a informačných systémov.

[26] V rámci posilnenia inovácie v európskych regiónoch sa v decembri 2017 začala nová medziregionálna pilotná akcia s cieľom zintenzívniť činnosť v oblasti kybernetickej bezpečnosti.

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

odolnosti: ide o prvý kľúčový krok. Všeobecným nariadením o ochrane údajov sa zavádza povinnosť oznamovať porušenie ochrany osobných údajov príslušnému dozornému orgánu. K ďalším kľúčovým opatreniam patrí silnejšia a modernizovaná Agentúra Európskej únie pre kybernetickú bezpečnosť a rámec EÚ pre certifikáciu produktov a služieb IKT[28] na budovanie dôvery spotrebiteľov. Pokračuje aj práca na pomoc sieti odborných stredísk členských štátov, aby sa stimuloval rozvoj a zavádzanie riešení kybernetickej bezpečnosti a doplnilo úsilie zamerané na budovanie kapacít v tejto oblasti na úrovni EÚ a na vnútroštátnej úrovni. Bude sa opierať o prácu programu Digitálna Európa predloženého Komisiou 6. júna[29], ktorým sa nanovo prioritizujú investície EÚ do kybernetickej bezpečnosti.

V odporúčaní o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu („Koncepcia“)[30] sa zároveň stanovilo, ako by mala fungovať spolupráca medzi členskými štátmi a rôznymi aktérmi EÚ pri reagovaní na rozsiahly cezhraničný kybernetický útok. Zdôraznila sa v ňom kľúčová úloha situačného povedomia v záujme účinnej koordinácie na technickej, operačnej a strategickej/politickej úrovni. Skupina pre spoluprácu zriadená podľa smernice o bezpečnosti sietí a informačných systémov pracuje aj na zlepšení výmeny informácií medzi príslušnými stranami a ich spoločného využívania a na vytváraní spoločnej taxonómie na opis incidentu. Tento prístup sa otestuje v nadchádzajúcich cvičeniach. Stredisko pre hybridné hrozby poskytuje strategickú analýzu súčasných a vznikajúcich kybernetických hrozieb na základe príspevkov spravodajských služieb členských štátov.

Rámec pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti („súbor nástrojov kybernetickej diplomacie“) bol významným krokom vpred z operačného hľadiska, pričom sa v ňom stanovili opatrenia v rámci spoločnej zahraničnej a bezpečnostnej politiky vrátane reštriktívnych opatrení, ktoré možno použiť na posilnenie reakcie EÚ na aktivity, ktoré poškodzujú jej politické, bezpečnostné a hospodárske záujmy. Čím viac ho budú členské štáty využívať, tým viac bude pôsobiť ako účinný odradzujúci prostriedok. V apríli Rada pre zahraničné veci prijala závery o škodlivých kybernetických činnostiach, v ktorých sa dôrazne odsúdilo zlomyseľné používanie informačných a komunikačných technológií vrátane útokov Wannaracry a NotPetya, ktoré spôsobili značné škody a hospodársku stratu v EÚ aj mimo nej.

EÚ a jej členské štáty musia zlepšiť svoju schopnosť určovať pôvodcov kybernetických útokov, v neposlednom rade prostredníctvom rozšíreného spoločného využívania spravodajských informácií. Kapacita vysledovať pôvodcov útokov by odradila potenciálnych útočníkov a zvýšila šance, že zodpovedné osoby ponesú náležitú zodpovednosť. Zvýšenie účinku odradenia je kľúčovým cieľom strategického prístupu Komisie k zvyšovaniu kybernetickej bezpečnosti. Nedávne návrhy Komisie zamerané na zlepšenie cezhraničného zhromažďovania elektronických dôkazov na účely trestného konania by takisto výrazne zlepšili schopnosť orgánov presadzovania práva vyšetrovať a stíhať kybernetickú kriminalitu.

Silná kybernetická odolnosť potrebuje kolektívny prístup so širokým záberom. Vyžaduje si to spoľahlivejšie a účinnejšie štruktúry na podporu kybernetickej bezpečnosti a reagovanie na kybernetické útoky v členských štátoch, ako aj vo vlastných inštitúciách, agentúrach, delegáciách, misiách a operáciách EÚ: Nedostatok spoločnej bezpečnej komunikačnej siete v európskych inštitúciách je vážnym nedostatkom. Informovanosť v inštitúciách EÚ, ako aj v prípade ich zamestnancov, pokiaľ ide o kybernetickú

[28] COM (2017) 477.
[29] Návrh nariadenia, ktorým sa stanovuje program Digitálna Európa na obdobie 2021 – 2027, COM(2018) 434.
[30] C(2017) 6100.

bezpečnosť, by sa mala zlepšiť zvýšením kultúry bezpečnosti a zintenzívnením odbornej prípravy.

Budúce kroky

- Európsky parlament a Rada by mali urýchliť svoju činnosť s cieľom uzavrieť rokovania o návrhoch v oblasti kybernetickej bezpečnosti dohodou do konca tohto roka a mali by sa urýchlene dohodnúť na navrhovaných právnych predpisoch týkajúcich sa zhromažďovania elektronických dôkazov.

- Komisia a vysoká predstaviteľka budú úzko spolupracovať s členskými štátmi s cieľom dosiahnuť pokrok v kybernetických aspektoch mechanizmov krízového riadenia a reakcie v rámci celej EÚ. Členské štáty sa vyzývajú, aby pokračovali vo svojej činnosti v súvislosti so zisťovaním pôvodcov kybernetických útokov a v praktickom využívaní súboru nástrojov kybernetickej diplomacie s cieľom posilniť politickú reakciu na kybernetické útoky.

- V reakcii na potrebu zvýšiť našu spôsobilosť kybernetickej obrany sa zriaďuje špecializovaná platforma odbornej prípravy a vzdelávania s cieľom pomôcť koordinovať možnosti odbornej prípravy v oblasti kybernetickej obrany, ktoré ponúkajú členské štáty. Bude sa vyvíjať úsilie o dosiahnutie súčinnosti s podobným úsilím Organizácie Severoatlantickej zmluvy.

3.5. **Budovanie odolnosti proti nepriateľskej spravodajskej činnosti**

Boj proti nepriateľskej spravodajskej činnosti si v súlade s príslušnými pravidlami a opatreniami EÚ a vnútroštátnymi pravidlami a opatreniami členských štátov vyžaduje v prvom rade zvýšenú a účinnú koordináciu medzi členskými štátmi. Je však takisto nevyhnutné zvýšiť spôsobilosť inštitúcií EÚ čeliť rastúcej hrozbe takejto aktivity zameranej výslovne na inštitúcie a vybudovať kultúru informovanosti o bezpečnosti, ktorú podporí lepšia odborná príprava a fyzická bezpečnosť. Inštitúcie by takisto mohli spolupracovať s členskými štátmi na budovaní odolnejšieho akreditačného systému EÚ. Takýto systém by bol založený na aktívnom podávaní správ, ktoré by umožňovalo lepšiu informovanosť medzi členskými štátmi a inštitúciami o možných nepriateľských subjektoch, najmä tých, ktoré už členské štáty identifikovali.

Koordinácia medzi členskými štátmi a medzi členskými štátmi a inými príslušnými medzinárodnými organizáciami, najmä Organizáciou Severoatlantickej zmluvy, by pomohla vytvoriť pákový efekt pre kontrarozviedku proti nepriateľskej činnosti v EÚ. Príkladom oblasti, ktorá by mala prospech zo zvýšenej koordinácie medzi členskými štátmi, je preverovanie investícií na základe nariadenia[31] navrhnutého Komisiou v septembri 2017 o preverovaní priamych zahraničných investícií členskými štátmi z dôvodov bezpečnosti alebo verejného poriadku. Zvýšená koordinácia medzi členskými štátmi by bola rovnako dôležitá pre preverovanie finančných transakcií, keďže nepriateľské spravodajské služby čoraz viac financujú svoje aktívne opatrenia voči EÚ prostredníctvom dôkladne rozpracovaných finančných systémov.

[31] Návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovuje rámec na preverovanie priamych zahraničných investícií do Európskej únie, COM(2017) 487.

Budúce kroky

- Európska služba pre vonkajšiu činnosť a Komisia zavedú zlepšené praktické opatrenia na udržanie a rozvoj schopnosti EÚ spolupracovať s členskými štátmi v boji proti nepriateľskej spravodajskej činnosti zameranej konkrétne na inštitúcie.

- Zdokonalené stredisko pre hybridné hrozby bude doplnené expertízou v oblasti kontrarozviednej činnosti s cieľom poskytnúť podrobné analýzy a brífingy o povahe nepriateľskej spravodajskej činnosti pravdepodobne vyvíjanej proti jednotlivcom a inštitúciám.

- Európsky parlament a Rada by mali urýchliť prácu, aby rokovania o návrhu týkajúceho sa preverovania investícií boli uzavreté do konca roka.

4. ZÁVER

Hybridné a chemické, biologické, rádiologické a jadrové hrozby sú v EÚ pozorne sledovanou oblasťou. Marcový incident v Spojenom kráľovstve zdôraznil široké spektrum vedenia hybridných vojen a mimoriadnu potrebu odolnosti vzhľadom na chemické, biologické, rádiologické a jadrové hrozby.

Komisia a vysoká predstaviteľka prijali a navrhli niekoľko iniciatív na riešenie výziev, ktoré predstavujú hybridné hrozby. Komisia takisto urýchľuje vykonávanie akčného plánu z roku 2017 s cieľom zvýšiť pripravenosť na chemické, biologické, rádiologické a jadrové bezpečnostné riziká.

Toto spoločné oznámenie slúži na informovanie Európskej rady o prebiehajúcej práci a na určenie oblastí, v ktorých by sa mali zintenzívniť opatrenia s cieľom ešte viac prehĺbiť a posilniť zásadný príspevok EÚ k riešeniu týchto hrozieb. Teraz je na členských štátoch, Komisii a vysokej predstaviteľke, aby zabezpečili rýchle následné opatrenia.