EURÓPSKA
KOMISIA

VYSOKÁ PREDSTAVITEĽKA
ÚNIE PRE
ZAHRANIČNÉ VECI
A BEZPEČNOSTNÚ POLITIKU

V Bruseli 19. 7. 2017
JOIN(2017) 30 final

SPOLOČNÁ SPRÁVA EURÓPSKEMU PARLAMENTU A RADE

o vykonávaní Spoločného rámca pre boj proti hybridným hrozbám – reakcia Európskej únie

1. ÚVOD

EÚ čelí najväčšej bezpečnostnej výzve v celej svojej histórii: Hrozby majú čoraz častejšie nekonvenčnú podobu, niektoré sú fyzickej povahy, ako napr. nové podoby terorizmu, niektoré využívajú digitálny priestor na komplexné kybernetické útoky. Iné sú subtílnejšej povahy a zamerané na donucovacie praktiky vyvíjania tlaku vrátane dezinformačných kampaní a mediálnej manipulácie. Ich cieľom je podkopať základné európske hodnoty, akými sú ľudská dôstojnosť, sloboda a demokracia. Nedávne koordinované kybernetické útoky na celom svete, pri ktorých sa ukázalo, že je zložité zistiť pôvodcov, preukázali zraniteľnosť našich spoločností a inštitúcií.

V apríli 2016 Európska komisia a vysoká predstaviteľka prijali Spoločné oznámenie pre boj proti hybridným hrozbám[1] (spoločný rámec). Vzhľadom na cezhraničnú a komplexnú povahu hybridných hrozieb sa v tomto rámci navrhuje prístup na úrovni celej verejnej správy s cieľom posilniť celkovú odolnosť našej spoločnosti. Rada[2] uvítala túto iniciatívu a navrhované opatrenia a vyzvala Komisiu a vysokú predstaviteľku, aby v júli 2017 predložili správu o pokroku. Hoci EÚ môže členským štátom pomôcť vybudovať odolnosť proti hybridným hrozbám, hlavnú zodpovednosť nesú členské štáty, keďže boj proti hybridným hrozbám súvisí s národnou bezpečnosťou a obranou.

Tento Spoločný rámec pre boj proti hybridným hrozbám tvorí dôležitú súčasť celkového integrovanejšieho prístupu EÚ k bezpečnosti a obrane. Prispieva k vytvoreniu Európy, ktorá chráni, ako žiadal predseda Juncker vo svojom prejave o stave Únie v septembri 2016. Európska únia v roku 2016 vytvorila takisto základy pre silnejšiu európsku obrannú politiku s cieľom reagovať na očakávania občanov, pokiaľ ide o väčšiu ochranu. V rámci Globálnej stratégie EÚ pre zahraničnú a bezpečnostnú politiku Európskej únie[3] bola do detailu vypracovaná argumentácia potreby integrovaného prístupu na prepojenie vnútornej odolnosti s vonkajšou činnosťou EÚ a obsahovala výzvu na synergiu medzi obrannou politikou a politikami zahŕňajúcimi vnútorný trh, priemysel, orgány presadzovania práva a spravodajské služby. V novembri 2016 po prijatí akčného plánu v oblasti európskej obrany Komisia predložila konkrétne iniciatívy, ktoré prispejú k posilneniu schopnosti EÚ reagovať na hybridné hrozby prostredníctvom posilňovania odolnosti obranného dodávateľského reťazca a posilňovania jednotného trhu v oblasti obrany. Komisia konkrétne 7. júna 2017 vytvorila Európsky obranný fond s navrhovaným financovaním vo výške 600 mil. EUR do roku 2020 a 1,5 mld. EUR ročne po roku 2020. V oznámení o bezpečnostnej únii[4] sa uznala potreba bojovať proti hybridným hrozbám a dôležitosť zabezpečiť väčšiu súdržnosť medzi vnútornými a vonkajšími opatreniami v oblasti bezpečnosti.

Vedúci predstavitelia EÚ postavili bezpečnosť a obranu do centra pozornosti v rámci diskusie o budúcnosti Európy[5]. To bolo potvrdené v Rímskej deklarácii z 25. marca 2017, v ktorej sa stanovila vízia bezpečnej a chránenej Únie odhodlanej posilniť svoju spoločnú bezpečnosť

[1] Spoločné oznámenie Európskemu parlamentu a Rade s názvom *Spoločný rámec pre boj proti hybridným hrozbám – reakcia Európskej únie*, JOIN (2016) 18 final.
[2] *Závery Rady o boji proti hybridným hrozbám*, tlačová správa 196/16, 19. apríl 2016.
[3] Dokument predložený vysokou predstaviteľkou na zasadnutí Európskej rady 28. júna 2016.
[4] COM(2016) 230 final z 20. 4. 2016.
[5] Bratislavský plán Európskej rady zo 16. septembra 2016 a Rímska deklarácia vedúcich predstaviteľov 27 členských štátov a Európskej rady, Európskeho parlamentu a Európskej komisie z 25. marca 2017.

a obranu. Predsedovia Európskej rady a Európskej komisie a generálny tajomník NATO podpísali 8. júla 2016 spoločné vyhlásenie vo Varšave s cieľom poskytnúť nový impulz a nový obsah pre strategické partnerstvo EÚ a NATO. V spoločnom vyhlásení sa uvádza sedem konkrétnych oblastí vrátane boja proti hybridným hrozbám, v ktorých by sa spolupráca medzi týmito dvomi organizáciami mala posilniť. Spoločný súbor 42 návrhov na vykonanie následne schválila tak Rada EÚ, ako aj Rada NATO a prvá správa, vykazujúca značný pokrok, bola vydaná v júni 2017[6].

V Diskusnom dokumente Komisie o budúcnosti európskej obrany[7] predloženom v júni 2017 sa uvádzajú rôzne scenáre toho, akým spôsobom reagovať na narastajúce hrozby, ktorým Európa čelí v oblasti bezpečnosti a obrany, a ako do roku 2025 posilniť vlastné schopnosti Európy v oblasti obrany. Vo všetkých troch scenároch sa bezpečnosť a obrana považujú za integrálnu súčasť európskeho projektu s cieľom chrániť a podporovať naše záujmy doma i v zahraničí. Európa sa musí stať poskytovateľom bezpečnosti a zabezpečiť postupne svoju vlastnú bezpečnosť. Žiaden členský štát nemôže čeliť výzvam sám, a to najmä v boji proti hybridným hrozbám. Spolupráca v oblasti obrany a bezpečnosti preto nie je schodným riešením; je nevyhnutné, aby sme vytvorili Európu, ktorá chráni.

Cieľom tejto správy je poskytnúť prehľad o pokroku a ďalších vykonávacích opatreniach v rámci činností vykonávaných v štyroch oblastiach navrhnutých v rámci spoločného rámca: zlepšenie situačného povedomia; budovanie odolnosti; posilňovanie schopnosti členských štátov a Únie predchádzať krízam a reagovať na ne a zabezpečiť koordinovanú obnovu; a posilnenie spolupráce s NATO s cieľom zabezpečiť komplementárnosť opatrení. Mala by sa vykladať v spojení s mesačnými správami o pokroku dosiahnutom smerom k vytvoreniu účinnej a skutočnej bezpečnostnej únie.

2. IDENTIFIKÁCIA HYBRIDNEJ POVAHY HROZBY

Hybridné činnosti sa stávajú častou črtou bezpečnostného prostredia Európy. Intenzita týchto činností sa zvyšuje, pričom narastajú obavy z ovplyvňovania volieb, dezinformačných kampaní, zlomyseľných aktivít v kybernetickom priestore a z toho, že sa páchatelia hybridných činov pokúšajú radikalizovať zraniteľných členov spoločnosti ako svojich zástupcov. Zraniteľnosť vo vzťahu k hybridným hrozbám sa neobmedzuje na štátne hranice. Hybridné hrozby si vyžadujú koordinovanú reakciu na úrovni EÚ a NATO. Vývoj od apríla 2016 ukazuje, že hoci hrozby sú stále často posudzované izolovane, v rámci Únie existuje rastúce uznanie a chápanie hybridnej povahy niektorých pozorovaných činností a potreba koordinovaných krokov. EÚ bude pokračovať vo svojom úsilí o zlepšenie situačného povedomia a spolupráce.

***Opatrenie č. 1*: Členské štáty, s primeranou podporou Komisie a vysokej predstaviteľky, sa vyzývajú, aby začali prieskum týkajúci sa hybridných rizík s cieľom určiť hlavné slabiny vrátane konkrétnych ukazovateľov hybridných hrozieb, ktoré môžu potenciálne ovplyvniť vnútroštátne a celoeurópske štruktúry a siete.**

Rada zriadila skupinu „priateľov predsedníctva“, ktorá spája odborníkov z členských štátov s cieľom vytvoriť všeobecný prieskum, ktorý by im umožnil lepšiu identifikáciu kľúčových

[6] http://www.consilium.europa.eu/sk/press/press-releases/2017/06/19-conclusions-eu-nato-cooperation.
[7] Diskusný dokument o budúcnosti európskej obrany, 7. 6. 2017, https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_sk.pdf.

ukazovateľov hybridných hrozieb, ich začlenenie do mechanizmov včasného varovania a existujúcich mechanizmov hodnotenia rizík a v prípade potreby ich spoločné využívanie. Dohodol sa referenčný rámec a činnosť sa už rozbehla. Všeobecný prieskum by mal byť pripravený do konca roku 2017, pričom osobitné prieskumy by sa mali začať krátko potom. Prvky ochrany proti hybridným hrozbám by sa mali vzájomne dopĺňať. Členské štáty sa preto vyzývajú, aby vykonali tieto prieskumy čo možno najrýchlejšie, keďže budú zdrojom cenných informácií o rozsahu zraniteľnosti a pripravenosti v rámci Európy.

a) ZLEPŠOVANIE POVEDOMIA

Spoločné využívanie analýzy spravodajských informácií a činností posudzovania je kľúčovým nástrojom na znižovanie neistoty a posilnenie situačného povedomia. Významný pokrok sa dosiahol v uplynulom roku. Stredisko EÚ pre hybridné hrozby bolo zriadené a je v súčasnosti už plne funkčné, takisto je zriadená pracovná skupina East StratCom a Fínsko otvorilo Európske centrum pre boj proti hybridným hrozbám. Veľa práce sa zameriava na analýzu nástrojov a pák dezinformácií alebo propagandy, pričom v tejto oblasti je dobrá spolupráca medzi pracovnou skupinou East StratCom, strediskom EÚ pre hybridné hrozby a NATO. Je to dobrý základ, aby bolo možné pokračovať v budovaní väčšmi zakorenenej kultúry analyzovania a posudzovania hrozieb pre našu vnútornú a vonkajšiu bezpečnosť prostredníctvom optiky hybridných hrozieb.

Stredisko pre hybridné hrozby

Opatrenie č. 2: Vytvoriť v rámci existujúcej štruktúry Centra EÚ pre analýzu spravodajských informácií stredisko EÚ pre hybridné hrozby, ktoré bude schopné zbierať a analyzovať utajované informácie a informácie z otvorených zdrojov o hybridných hrozbách. Členské štáty sa vyzývajú, aby zriadili národné kontaktné miesta pre hybridné hrozby s cieľom zaistiť spoluprácu a komunikáciu so strediskom EÚ pre hybridné hrozby.

Stredisko EÚ pre hybridné hrozby bolo zriadené v rámci Centra EÚ pre analýzu spravodajských informácií s cieľom prijímať a analyzovať utajované informácie a informácie z otvorených zdrojov od rôznych zainteresovaných subjektov týkajúce sa hybridných hrozieb. Analýza sa potom spoločne využíva v rámci EÚ a medzi členskými štátmi, a tak sa získavajú informácie potrebné na rozhodovacie procesy v EÚ vrátane informácií potrebných na hodnotenie bezpečnostných rizík vykonávané na úrovni EÚ. Spravodajský útvar Vojenského štábu EÚ prispieva k činnosti strediska vojenskými analýzami. Na tému hybridných hrozieb bolo doteraz vypracovaných viac ako 50 hodnotení a brífingov. Od januára 2017 vydáva stredisko periodikum s názvom „Hybrid Bulletin“, v ktorom analyzuje súčasné hrozby a hybridné problémy a tieto analýzy priamo poskytuje inštitúciám a orgánom EÚ, ako aj národným kontaktným miestam[8]. V máji 2017 sa tak, ako sa plánovalo, dosiahla plná prevádzková kapacita strediska. Okrem toho prebiehajú pracovné kontakty s práve sa formujúcim oddelením NATO pre hybridné hrozby, a to výmenou tak skúseností získaných pri zriaďovaní strediska pre hybridné hrozby, ako aj informácií (pri plnom dodržiavaní pravidiel EÚ pre výmenu utajovaných informácií). Stredisko EÚ pre hybridné hrozby identifikuje v súčasnosti ďalšie iniciatívy s cieľom posilniť budúcu spoluprácu a bude zohrávať kľúčovú úlohu pri paralelných cvičeniach EÚ a NATO naplánovaných na jeseň 2017, pri ktorých sa bude testovať reakcieschopnosť strediska EÚ pre hybridné hrozby, pričom identifikované poznatky sa zohľadnia pri pracovných postupoch strediska.

[8] K dnešnému dňu 21 členských štátov vymenovalo národné kontaktné miesta. Ide o jednotlivcov pracujúcich v hlavných mestách členských štátov vo funkcii úradníkov zodpovedných za oblasť politiky/odolnosti.

Strategická komunikácia

Opatrenie č. 3: Vysoká predstaviteľka spolu s členskými štátmi preskúma možnosti aktualizácie a koordinácie kapacity na proaktívnu strategickú komunikáciu a možnosti optimalizácie využívania monitorovania médií a jazykových odborníkov.

V uplynulých mesiacoch patrí zvyšujúci sa počet dezinformačných kampaní a systematické šírenie falošných správ v sociálnych médiách k širokému spektru opatrení používaných na oslabenie protivníkov. Keď sú sociálne médiá uprednostňovanou platformou, informácie, ktoré sa zdajú spoľahlivé a legitímne, môžu zmeniť verejnú mienku v prospech niektorých jednotlivcov, organizácií alebo vlád. Celkovým cieľom týchto hybridných taktík je vyvolanie zmätku v spoločnosti a diskreditácia demokratických štátnych správ a našich štruktúr, inštitúcií a volieb. Prostredníctvom online platforiem sa často šíria falošné správy (pozri aj opatrenie 17). Komisia a vysoká predstaviteľka vítajú opatrenia, ktoré nedávno prijali online platformy a vydavateľstvá na boj proti nepravdivým informáciám. Komisia bude aj naďalej podporovať takéto dobrovoľné opatrenia.

Vysoká predstaviteľka zriadila pracovnú skupinu East StratCom, ktorá vypracúva prognózy a poskytuje stanoviská k prípadom a kampaniam šírenia dezinformácií Týmto sa výrazne zlepšuje komunikácia o politikách Únie v krajinách východného susedstva a zároveň posilňuje mediálne prostredie v týchto krajinách. Táto pracovná skupina odhalila v uplynulých dvoch rokoch viac ako 3 000 individuálnych prípadov šírenia nepravdivých informácií v 18 jazykoch. Nadchádzajúce spustenie novej internetovej stránky: *„#EUvsdisinformation*“ s online vyhľadávacím nástrojom významne zlepší prístup používateľov. Z výskumnej a analytickej činnosti však vyplýva, že počet kanálov šírenia nepravdivých informácií a správ na každodennom základe je oveľa vyšší. V rámci projektu EU-STRAT financovaného v rámci programu Horizont 2020 sa analyzuje politika a médiá v krajinách Východného partnerstva.

Vysoká predstaviteľka vyzýva členské štáty, aby podporovali činnosť pracovných skupín East StratCom s cieľom účinnejšie bojovať proti nárastu hybridných hrozieb. To pomôže pracovnej skupine pre Juh zlepšiť komunikáciu a informačnú osvetu vo vzťahu k arabskému svetu, a to aj v arabčine, v záujme vyvrátenia mýtov o Európskej únii a jej politikách a poskytnutia pravdivých informácií. Interakcia s miestnou novinárskou obcou pomôže zabezpečiť, aby boli tlačové produkty v súlade s miestnou kultúrou. Obe pracovné skupiny s podporou strediska EÚ pre hybridné hrozby sú zamerané na podporu a doplnenie úsilia členských štátov. Okrem toho Komisia spolufinancuje Európsku sieť pre strategickú komunikáciu, sieť spolupráce 26 členských štátov, ktorá informuje o analýzach, osvedčených postupoch a nápadoch pri využívaní strategickej komunikácie v boji proti násilnému extrémizmu, a to aj pokiaľ ide o dezinformácie.

Centrum excelentnosti pre boj proti hybridným hrozbám

Opatrenie č. 4: Členské štáty sa vyzývajú, aby zvážili zriadenie centra excelentnosti pre boj proti hybridným hrozbám.

V reakcii na výzvu na vytvorenie centra excelentnosti Fínsko otvorilo v apríli 2017 Európske centrum pre boj proti hybridným hrozbám. K členom daného centra patrí desať členských

štátov EÚ[9], Nórsko a USA, pričom Európska únie a NATO boli vyzvané, aby podporili jeho riadiacu radu[10]. Poslaním centra je podporovať strategický dialóg, ako aj vykonávať výskum a analýzy v spolupráci so záujmovými spoločenstvami v záujme zlepšenia odolnosti a schopnosti reagovať s cieľom pomôcť v boji proti hybridným hrozbám. Očakáva, že centrum bude slúžiť aj ako miesto pre budúce cvičenia týkajúce sa hybridných hrozieb. Centrum už nadviazalo úzke styky so strediskom EÚ pre hybridné hrozby a práca týchto dvoch organizácií by sa mala navzájom dopĺňať. EÚ v súčasnosti posudzuje spôsoby, ako možno centru poskytnúť konkrétnu podporu.

b) BUDOVANIE ODOLNOSTI

V spoločnom rámci sa pri opatreniach EÚ kladie primárny dôraz na odolnosť (napr. dopravy, komunikácií, energetiky, financií alebo regionálnej bezpečnostnej infraštruktúry) s cieľom odolávať propagande a informačným kampaniam, pokusom o narušenie činnosti podnikov, spoločností a hospodárskych tokov, ako aj kybernetickým útokom na informačné technológie a kybernetickú infraštruktúru. Posilnenie odolnosti sa považuje za preventívne a odstrašujúce opatrenie s cieľom utužiť spoločnosti a zabrániť vystupňovaniu kríz v rámci EÚ i mimo nej. Pridaná hodnota EÚ spočíva v poskytovaní pomoci členským štátom a partnerom pri budovaní ich odolnosti, opierajúc sa o širokú paletu existujúcich nástrojov a programov. Značný pokrok sa dosiahol opatreniami na budovanie odolnosti v oblastiach, ako je kybernetická bezpečnosť, kritická infraštruktúra, ochrana finančného systému pred nezákonným využívaním a boj proti násilnému extrémizmu a radikalizácii.

Ochrana kritickej infraštruktúry

Opatrenie č. 5: Komisia v spolupráci s členskými štátmi a zúčastnenými stranami identifikuje spoločné nástroje vrátane ukazovateľov na zlepšenie ochrany a odolnosti kritických infraštruktúr proti hybridným hrozbám v príslušných odvetviach.

V rámci Európskeho programu na ochranu kritickej infraštruktúry (EPCIP) Komisia pokračovala v práci s cieľom určiť spoločné nástroje vrátane ukazovateľov zraniteľnosti na zlepšenie odolnosti kritickej infraštruktúry proti hybridným hrozbám v príslušných odvetviach. V máji 2017 Komisia zorganizovala seminár o hybridných hrozbách pre kritickú infraštruktúru, ktorej účastníkmi boli takmer všetky členské štáty, prevádzkovatelia kritickej infraštruktúry, stredisko EÚ pre hybridné hrozby a NATO ako pozorovateľ. Bol dohodnutý spoločný plán, ako aj kroky pre budúcu prácu, a to na základe dotazníka zaslaného vnútroštátnym orgánom v členských štátoch. Komisia bude ďalej konzultovať so zainteresovanými stranami v jeseni s cieľom dosiahnuť dohodu o ukazovateľoch do konca roku 2017.

Európska obranná agentúra pracuje na identifikácii spoločných spôsobilostí a nedostatkov výskumu vyplývajúcich z prepojenia energetických infraštruktúr a obranných spôsobilostí. Európska obranná agentúra vypracuje koncepčný dokument na jeseň roku 2017, ako aj pilotné akcie holistickej metodiky.

[9] Fínsko, Francúzsko, Nemecko, Lotyšsko, Litva, Poľsko, Švédsko a Spojené kráľovstvo, Estónsko, Španielsko.
[10] Centrum je otvorené aj pre ostatné členské štáty EÚ a spojencov NATO, ktorí by sa chceli k nemu pripojiť.

Zvýšenie bezpečnosti dodávok energie v rámci EÚ

Opatrenie č. 6: Komisia v spolupráci s členskými štátmi podporí úsilie o diverzifikáciu zdrojov energie a bude presadzovať normy v oblasti bezpečnosti a zabezpečenia s cieľom zvýšiť odolnosť jadrových infraštruktúr.

Komisia predložila konkrétne návrhy v balíku opatrení v oblasti bezpečnosti dodávok v decembri 2016 a v apríli 2017, Rada a Európsky parlament dosiahli dohodu o novom nariadení o bezpečnosti dodávok plynu, ktorého cieľom je zabránenie krízam v oblasti dodávok plynu. Novými pravidlami sa zabezpečí spoločný prístup koordinovaný na regionálnej úrovni týkajúci sa opatrení na zaistenie bezpečnosti dodávok medzi členskými štátmi. Vďaka tomu bude mať EÚ lepšie predpoklady pripraviť sa na nedostatok plynu v prípade krízy alebo hybridného útoku a zvládať ho. Po prvýkrát sa bude uplatňovať zásada solidarity: členské štáty budú schopné pomôcť susedným krajinám v prípade vážnej krízy alebo útoku tak, aby európske domácnosti a podniky netrpeli výpadkami dodávok.

EÚ dosiahla pokrok aj pri rozvoji kľúčových projektov na diverzifikáciu trás a zdrojov dodávok energie v súlade s rámcovou stratégiou energetickej únie a európskou stratégiou energetickej bezpečnosti. V južnom koridore zemného plynu prebiehajú napríklad konkrétne stavebné práce na všetkých dôležitých plynovodných projektoch: predĺženie Zakaukazského plynovodu, Transanatolského plynovodu a Transjadranského plynovodu, ťažobného plynovodu Shah Deniz II, ako aj rozšírenie Južného koridoru zemného plynu do Strednej Ázie, najmä do Turkménska. Dovoz skvapalneného zemného plynu (LNG) do Európy narastá a LNG sa dováža z nových zdrojov, napríklad z USA. Príklad terminálu v Litve ukazuje, ako diverzifikačné projekty môžu znížiť závislosť od jediného dodávateľa. Posilnenie úsilia o diverzifikáciu zdrojov energie a lepšie využívanie domácich zdrojov energie, najmä obnoviteľných zdrojov, zároveň prispieva k diverzifikácii energetických zásobovacích trás a zdrojov energie.

V oblasti jadrovej bezpečnosti Komisia najmä prostredníctvom seminárov s vnútroštátnymi orgánmi a regulačnými orgánmi aktívne podporuje konzistentné a účinné vykonávanie dvoch smerníc (o jadrovej bezpečnosti a základných bezpečnostných normách), ktoré musia členské štáty transponovať do konca roka 2017, respektíve 2018. Okrem toho program Euratomu pre výskum a vzdelávanie prispieva k zvýšeniu jadrovej bezpečnosti.

Bezpečnosť dopravy a dodávateľských reťazcov

Opatrenie č. 7: Komisia bude monitorovať vznikajúce hrozby v celom odvetví dopravy a vo vhodných prípadoch bude aktualizovať právne predpisy. Pri vykonávaní stratégie a akčného plánu EÚ pre námornú bezpečnosť a stratégie EÚ pre riadenie rizík v oblasti ciel, ako aj akčných plánov v rámci nich Komisia a vysoká predstaviteľka (v rámci svojich právomocí) preskúmajú v spolupráci s členskými štátmi, ako treba reagovať na hybridné hrozby, najmä na také, ktoré sa týkajú kritickej dopravnej infraštruktúry.

V súlade s oznámením o bezpečnostnej únii Komisia uľahčuje posúdenia bezpečnostných rizík na úrovni EÚ s členskými štátmi, Centrom EÚ pre analýzu spravodajských informácií a príslušnými agentúrami s cieľom identifikovať hrozby pre bezpečnosť dopravy a podporovať rozvoj účinných a primeraných opatrení na zníženie rizika. Zostrelenie lietadla spoločnosti Malaysia Airlines (let MH17) nad východnou Ukrajinou v roku 2014 poukázalo

na riziko, ktoré predstavujú prelety nad zónami konfliktu: V súlade s odporúčaniami Európskej pracovnej skupiny na vysokej úrovni pre vojnové zóny[11] Komisia vypracovala metodiku „spoločného posúdenia rizika na úrovni EÚ“ s podporou vnútroštátnych odborníkov v oblasti bezpečnosti letectva a ESVČ, ktoré umožňuje výmenu utajovaných informácií a vymedzenie spoločnej predstavy o riziku. Na základe výsledkov tohto spoločného posúdenia rizika na úrovni EÚ vydala Európska agentúra pre bezpečnosť letectva (EASA) v marci 2017 prvý „Informačný bulletin o vojnových zónach“[12]. Komisia zvažuje rozšírenie činností posudzovania rizík vykonávaných v oblasti bezpečnostnej ochrany letectva aj na iné druhy dopravy (napr. železničná, námorná), pričom príslušné návrhy sa predložia v roku 2018. V júni 2017 Komisia, ESVČ a členské štáty spustili svoje vlastné posúdenie rizika v oblasti železničnej bezpečnosti s cieľom identifikovať nedostatky a možné opatrenia na zmiernenie rizík.

Značné úsilie v oblasti bezpečnosti letectva a manažmentu letovej prevádzky sa vyvinulo pri výskumných projektoch v oblasti bezpečnosti v rámci 7. rámcového programu a programu Horizont 2020. V oblasti civilného letectva Komisia spolu s Európskou agentúrou pre bezpečnosť letectva a zainteresovanými stranami vyvíja dve nové iniciatívy na posilnenie kybernetickej bezpečnosti, ako aj pre boj proti hybridným hrozbám: vytvorenie tímu reakcie na núdzové počítačové situácie v oblasti letectva a zriadenie pracovnej skupiny pre kybernetickú bezpečnosť v rámci Spoločného podniku pre výskum manažmentu letovej prevádzky jednotného európskeho neba (SESAR) zodpovedného za oblasť manažmentu letovej prevádzky jednotného európskeho neba. Európska obranná agentúra poskytuje vojenské vstupné informácie súvisiace s kybernetickou bezpečnosťou letectva spoločnému podniku SESAR, ako aj Európskej agentúre pre bezpečnosť letectva, a to prostredníctvom „európskej strategickej koordinačnej platformy pre oblasť kybernetickej bezpečnosti“, ktorá bude na žiadosť členských štátov a odvetvia pomáhať koordinovať všetky činnosti v leteckej doprave na úrovni EÚ. V súlade s plánom pre kybernetickú bezpečnosť v letectve Európska agentúra pre bezpečnosť letectva vykonala v roku 2016 analýzy nedostatkov existujúcich pravidiel, a najmä vymedzenie a zriadenie Európskeho centra pre kybernetickú bezpečnosť v letectve. Toto centrum je už v prevádzke a spolupracuje s tímom reakcie na núdzové počítačové situácie (CERT-EU) (memorandum o porozumení podpísané vo februári 2017) pri tvorbe analýzy hrozieb v leteckej doprave a s organizáciou EUROCONTROL (plán spolupráce schválený), pričom webové sídlo pre distribúciu analýz z verejných zdrojov sa už vyvinulo. Do jesene 2017 bude prijatý normalizačný program a zabezpečená výmena informácií.

Riadenie colných rizík

Z colného hľadiska sa Komisia zameriava na významné zlepšenie systému analýzy predbežných informácií o náklade a systému riadenia colných rizík. Toto sa vzťahuje na celú škálu colných rizík, a to aj v súvislosti s hrozbami pre bezpečnosť a integritu medzinárodných dodávateľských reťazcov a príslušných kľúčových infraštruktúr (napr. priame hrozby pre zariadenia v námorných prístavoch, letiská a pozemné hranice, ktoré predstavuje dovoz). Cieľom modernizácie je zabezpečiť, aby colné správy v EÚ získavali všetky potrebné informácie od obchodníkov, pokiaľ ide o pohyb tovaru; aby boli schopné efektívnejšie si vymieňať tieto informácie medzi členskými štátmi; aby uplatňovali spoločné pravidlá

[11] https://www.easa.europa.eu/system/files/dfu/208599_EASA_CONFLICT_ZONE_CHAIRMAN_REPORT_no_B_update.pdf.
[12] https://ad.easa.europa.eu/czib-docs/page-1.

týkajúce sa rizík, ako aj pravidlá týkajúce sa rizík osobitné pre daný členský štát; a aby boli schopné efektívnejšie sa zamerať na rizikové zásielky tým, že budú intenzívnejšie spolupracovať s inými orgánmi, najmä s ostatnými orgánmi presadzovania práva a bezpečnostnými agentúrami. Vývoj IT nevyhnutný pre vykonanie tejto aktualizácie zo strany Komisie je v súčasnosti vo svojej počiatočnej fáze a príslušné investície na ústrednej úrovni sa uskutočnia v najbližších mesiacoch.

Vesmír

Opatrenie č. 8: V kontexte kozmickej stratégie a akčného plánu v oblasti európskej obrany navrhne Komisia posilniť odolnosť kozmických infraštruktúr proti hybridným hrozbám, najmä prípadným rozšírením pôsobnosti dohľadu a sledovania v kozmickom priestore tak, aby do nej boli zahrnuté hybridné hrozby, ďalej prípravu budúcej generácie GovSatCom na európskej úrovni a použitie systému Galileo pri kritických infraštruktúrach, ktoré závisia od časovej synchronizácie.

Komisia v roku 2018 pri príprave regulačného rámca v oblasti vládnej satelitnej komunikácie (GovSatCom) a sledovania kozmického priestoru a dohľadu nad ním začlení do svojho posudzovania aspekty odolnosti proti hybridným hrozbám. V súlade so Stratégiou pre Európu v oblasti kozmického priestoru Komisia pri prípravách na vývoji projektu Galileo a Copernicus posúdi potenciál týchto služieb s cieľom pomôcť zmierniť zraniteľnosť kritických infraštruktúr. Hodnotiaca správa by mala byť hotová na jeseň 2017 a návrh k ďalšej generácii programov Copernicus a Galileo v roku 2018. Európska obranná agentúra pracuje na projektoch na rozvoj spôsobilostí formou spolupráce v oblasti vesmírnych komunikácií, vojenského určovania polohy, navigácie a načasovania, ako aj pozorovania Zeme. Všetky projekty budú zamerané na požiadavky na odolnosť vzhľadom na súčasné a nové hybridné hrozby.

Obranná spôsobilosť

Opatrenie č. 9: Vysoká predstaviteľka, v prípade potreby s podporou členských štátov a v spolupráci s Komisiou, navrhne projekty týkajúce sa toho, ako prispôsobiť obrannú spôsobilosť a vývoj EÚ konkrétne na boj proti hybridným hrozbám namiereným proti jednému alebo viacerým členským štátom.

V rokoch 2016 a 2017 Európska obranná agentúra vykonala tri simulačné cvičenia zamerané na scenáre hybridných hrozieb spolu s Komisiou, ESVČ a expertmi z členských štátov. Ich zistenia budú podkladom pre revíziu plánu rozvoja spôsobilostí tak, aby výsledný vývoj kľúčových spôsobilostí potrebných na boj proti hybridným hrozbám bol zahrnutý v nových prioritách EÚ týkajúcich sa rozvoja spôsobilostí. Pri činnosti týkajúcej sa revízie zoznamu požiadaviek na rok 2005 sa zohľadní rozmer hybridných hrozieb. Európska obranná agentúra dokončila v apríli 2017 analytickú správu o vojenských dôsledkoch plynúcich z hybridných útokov namierených proti kritickej prístavnej infraštruktúre, ktoré budú prediskutované na seminári s odborníkmi z oblasti námorníctva v októbri 2017. Ďalšia osobitná analýza vojenskej úlohy v rámci boja proti minidrónom je naplánovaná na rok 2018. Priority spôsobilostí s cieľom posilniť odolnosť proti hybridným hrozbám identifikovaným členskými štátmi by mohli byť od roku 2019 okrem toho takisto oprávnené na podporu z Európskeho fondu pre obranu. Komisia vyzýva spoluzákonodarcov, aby zabezpečili rýchle prijatie, a členské štáty, aby predložili návrhy projektov týkajúcich sa spôsobilostí na posilnenie odolnosti EÚ proti hybridným hrozbám.

<u>Opatrenie č. 10</u>: Komisia bude v spolupráci s členskými štátmi zlepšovať informovanosť o hybridných hrozbách a odolnosť proti týmto hrozbám v rámci existujúcich mechanizmov pripravenosti a koordinácie, najmä v rámci Výboru pre zdravotnú bezpečnosť.

S cieľom posilniť pripravenosť a odolnosť proti hybridným hrozbám vrátane budovania kapacít v rámci systémov ochrany v zdravotnej a potravinárskej oblasti Komisia podporuje členské štáty prostredníctvom odbornej prípravy a simulačných cvičení, ako aj uľahčovaním výmeny skúseností a financovaním spoločných opatrení. Podpora sa uskutočňuje predovšetkým v súvislosti s rámcom EÚ pre bezpečnosť zdravia – pri závažných cezhraničných hrozbách pre zdravie, ako aj v rámci programu verejného zdravia na vykonávanie medzinárodných zdravotných predpisov, legislatívneho piliera záväzného pre 196 krajín vrátane členských štátov, ktorého cieľom je predchádzať a reagovať na akútne verejné cezhraničné riziká pre zdravie na celom svete. Na testovanie medziodvetvovej pripravenosti a reakcie v sektore zdravotníctva útvary Komisie vykonajú cvičenie týkajúce sa komplexných a viacrozmerných hybridných hrozieb na jeseň 2017. Komisia a členské štáty pripravujú spoločné opatrenie týkajúce sa vakcinácie vrátane zásobovania vakcínami, ako aj prognóz dopytu a výskumu o postupoch výroby inovatívnych vakcín s cieľom posilniť zásobovanie vakcínami a zlepšiť zdravotnú bezpečnosť na úrovni EÚ (2018 – 2020). Komisia takisto spolupracuje s Európskym úradom pre bezpečnosť potravín a Európskym centrom pre prevenciu a kontrolu chorôb s cieľom prispôsobiť svoju politiku najnovším poznatkom v oblasti techniky analýzy potravín v záujme presnejšej identifikácie a zisťovania zdrojov ohrozenia zdravia a výsledného rýchleho riadenia ohnísk predstavujúcich hrozbu pre bezpečnosť potravín. Komisia vytvorila sieť subjektov financujúcich výskum – Globálna výskumná spolupráca pre pripravenosť v prípade infekčných chorôb – v záujme koordinovanej núdzovej reakcie výskumníkov do 48 hodín od akéhokoľvek významného výskytu ohniska choroby.

<u>Opatrenie č. 11</u>: Komisia vyzýva členské štáty, aby prioritne zriadili sieť 28 tímov CSIRT a tímu CERT-EU (tím reakcie na núdzové počítačové situácie) a v plnej miere ich využívali, rovnako ako aj rámec pre strategickú spoluprácu. Komisia by v spolupráci s členskými štátmi mala zabezpečiť, aby odvetvové iniciatívy v oblasti kybernetických hrozieb (napríklad v oblasti letectva, energetiky a v námornej oblasti) boli v súlade s kapacitami jednotlivých odvetví, na ktoré sa vzťahuje smernica NIS, aby bolo možné spoločne využívať informácie, znalosti a rýchle reakcie.

Nedávne celosvetové kybernetické útoky s použitím ransomvéru a malvéru s cieľom paralyzovať tisícky počítačových systémov opäť poukázali na naliehavú potrebu zvýšiť kybernetickú odolnosť a bezpečnostné opatrenia v rámci EÚ. Ako bolo oznámené v rámci preskúmania jednotného digitálneho trhu v polovici trvania, Komisia a vysoká predstaviteľka v súčasnosti vykonávajú preskúmanie stratégie kybernetickej bezpečnosti EÚ z roku 2013 predovšetkým prostredníctvom prijatia balíka naplánovaného na september 2017. Cieľom bude poskytovať účinnejšie medziodvetvové reakcie na tieto hrozby, čím sa zvýši dôvera v digitálnu spoločnosť a hospodárstvo. Preskúma sa tiež mandát Agentúry EÚ pre sieťovú a informačnú bezpečnosť (ENISA) s cieľom vymedziť jej úlohy v zmenenom ekosystéme kybernetickej bezpečnosti. Európska rada[13] privítala zámer Komisie prehodnotiť stratégiu kybernetickej bezpečnosti.

[13] Pozri závery zo zasadnutia Európskej rady, ktoré sa konalo 22. až 23. júna 2017.

Prijatie smernice o kybernetickej bezpečnosti (NIS)[14] v júli 2016 bolo kľúčovým krokom smerom k budovaniu odolnosti v oblasti kybernetickej bezpečnosti na európskej úrovni. V smernici sa stanovujú prvé pravidlá EÚ v oblasti kybernetickej bezpečnosti, ktoré zlepšujú spôsobilosti v oblasti kybernetickej bezpečnosti, a posilňuje sa spolupráca medzi členskými štátmi. Smernicou sa takisto od spoločností v kritických odvetviach požaduje, aby prijali vhodné bezpečnostné opatrenia a oznamovali akékoľvek závažné kybernetické incidenty príslušným vnútroštátnym orgánom. K týmto odvetviam patrí energetika, doprava, vodné hospodárstvo, zdravotná starostlivosť, bankovníctvo a infraštruktúra finančného trhu. Online trhy, služby cloud computingu a internetové vyhľadávače budú musieť prijať podobné opatrenia. Jednotné vykonávanie v rôznych odvetviach, ako aj cez hranice, sa zabezpečí prostredníctvom skupiny pre spoluprácu v oblasti sieťových informačných služieb (zriadenej Komisiou v roku 2016), ktorej úlohou je zabrániť rozdrobeniu trhu. V tejto súvislosti sa smernica NIS považuje za referenčný rámec pre všetky odvetvové iniciatívy v oblasti kybernetickej bezpečnosti. Prostredníctvom smernice sa okrem toho vytvára sieť jednotiek pre riešenie počítačových bezpečnostných incidentov (CSIRT), ktorá združuje všetky príslušné zainteresované subjekty. Komisia súbežne s tímom CERT-EU aktívne monitoruje situáciu, pokiaľ ide o kybernetické hrozby, a vymieňa si informácie s vnútroštátnymi orgánmi s cieľom zabezpečiť, aby boli informačné systémy inštitúcií EÚ bezpečné a odolné proti kybernetickým útokom. Ransomvérový incident „WannaCry“ z mája 2017 bol prvou príležitosťou siete zapojiť sa do operatívnej výmeny informácií a spolupráce prostredníctvom šírenia poradenstva. Tím reakcie na núdzové počítačové situácie EÚ bol takisto v úzkom kontakte s Európskym centrom boja proti počítačovej kriminalite (EC3) pri Europole, jednotkami dotknutých krajín pre riešenie počítačových bezpečnostných incidentov (CSIRT), jednotkami pre počítačovú kriminalitu a kľúčovými partnermi z odvetvia s cieľom zmierniť hrozbu a pomôcť obetiam útoku. Výmenou vnútroštátnych situačných správ sa dosiahlo spoločné situačné povedomie v celej EÚ. Táto skúsenosť umožnila sieti lepšie sa pripraviť na ďalšie incidenty (napr. „NonPetya“). Boli identifikované aj ďalšie problémy, ktoré sa v súčasnosti riešia.

<u>Opatrenie č. 12</u>: Komisia bude v koordinácii s členskými štátmi v rámci zmluvného verejno-súkromného partnerstva pre kybernetickú bezpečnosť spolupracovať s odvetvím na vývoji a testovaní technológií, aby boli používatelia a infraštruktúry lepšie chránení pred kybernetickými aspektmi hybridných hrozieb.

V júli 2016 Komisia v koordinácii s členskými štátmi podpísala s odvetvím zmluvné verejno-súkromné partnerstvo v oblasti kybernetickej bezpečnosti, pričom z rámcového programu EÚ pre výskum a inováciu (Horizont 2020) investuje až 450 mil. EUR s cieľom vyvinúť a otestovať technológie, ktoré by používateľov a infraštruktúry lepšie ochránili pred kybernetickými a hybridnými hrozbami. Výsledkom tohto partnerstva je prvý celoeurópsky strategický výskumný program, ktorý sa zameriava na posilnenie odolnosti kritickej infraštruktúry, ako aj občanov voči kybernetickým útokom. Vďaka tomuto partnerstvu sa zlepšila koordinácia medzi zainteresovanými stranami, čo vedie k zvýšeniu efektívnosti a účinnosti v oblasti financovania kybernetickej bezpečnosti v rámci programu Horizont 2020. Toto partnerstvo sa takisto zameriava na otázky týkajúce sa technológie certifikácie informácií a komunikácie z hľadiska kybernetickej bezpečnosti, ako aj na riešenie akútneho nedostatku kvalifikovaných odborníkov v oblasti kybernetickej bezpečnosti na trhu. Vzhľadom na značnú potrebu civilného výskumu a vysokú odolnosť požadovanú v oblasti

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

obrany, skupina pre výskum kybernetických hrozieb a technológie v rámci Európskej obrannej agentúry prispieva k výskumu oblastí, ktoré identifikovala Európska organizácia kybernetickej bezpečnosti vo svojom strategickom programe v oblasti výskumu a inovácií.

Opatrenie č. 13: Komisia vydá usmernenie pre vlastníkov aktív inteligentných sietí na zvýšenie kybernetickej bezpečnosti ich zariadení. V rámci iniciatívy o usporiadaní trhu s elektrinou zváži Komisia možnosť, že navrhne plány pripravenosti na riziká a procesné pravidlá pre spoločné využívanie informácií a zabezpečenie solidarity medzi členskými štátmi v čase krízy vrátane pravidiel týkajúcich sa prevencie a zmierňovania kybernetických útokov.

V odvetví energetiky Komisia pripravuje návrh odvetvovej stratégie v oblasti kybernetickej bezpečnosti spolu so zriadením platformy expertov v oblasti kybernetickej bezpečnosti v odvetví energetiky s cieľom posilniť vykonávanie smernice NIS. V rámci štúdie z februára 2017 sa určili najlepšie dostupné techniky na zvýšenie úrovne kybernetickej bezpečnosti inteligentných meracích systémov, ktoré podporujú túto platformu. Komisia vytvorila aj webovú platformu známu ako „Stredisko EÚ pre zdieľanie informácií o hrozbách a incidentoch“, v rámci ktorej sa analyzujú a zdieľajú informácie o počítačových hrozbách a incidentoch v energetickom sektore.

Zvýšenie odolnosti finančného sektora voči hybridným hrozbám

Opatrenie č. 14: Komisia bude v spolupráci s agentúrou ENISA[15], členskými štátmi, príslušnými medzinárodnými, európskymi a vnútroštátnymi orgánmi a finančnými inštitúciami podporovať a zjednodušovať platformy a siete pre spoločné využívanie informácií o hrozbách a bude sa zaoberať faktormi, ktoré výmenu informácií brzdia.

Uznávajúc, že kybernetické hrozby patria medzi hlavné riziká finančnej stability, Komisia preskúmala v súčasnosti platný regulačný rámec týkajúci sa platobných služieb v Európskej únii. Revidovanou smernicou o platobných službách[16] sa zaviedli nové opatrenia na posilnenie bezpečnosti platobných nástrojov a silnej autentifikácie zákazníka s cieľom znížiť výskyt podvodov, najmä v oblasti online platieb. Nový legislatívny rámec sa bude uplatňovať od januára 2018. V súčasnosti Komisia s pomocou Európskeho orgánu pre bankovníctvo a v rámci konzultácií so zainteresovanými stranami vyvíja regulačné technické predpisy, ktorých uverejnenie sa očakáva do konca roku 2017, týkajúce sa silnej autentifikácie zákazníka a spoločnej a bezpečnej komunikácie s cieľom zabezpečiť bezpečnosť platobných transakcií. Okrem toho, pokiaľ ide o medzinárodnú scénu, Komisia úzko spolupracovala s príslušnými partnermi zo skupiny G7 na „*základných zásadách kybernetickej bezpečnosti G7 vo finančnom sektore*“, ktoré boli schválené v októbri 2016 ministrami financií skupiny G7 a guvernérmi centrálnych bánk. Tieto zásady sú určené pre subjekty finančného sektora (verejné a súkromné) a prispievajú ku koordinovanému prístupu v oblasti kybernetickej bezpečnosti v rámci finančného sektora s cieľom spoločne bojovať proti kybernetickým hrozbám vrátane komplexnejších a sofistikovanejších kybernetických hrozieb.

[15] Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť.

[16] Smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, Ú. v. EÚ L 337, 23.12.2015, s. 35.

Doprava

Opatrenie č. 15: Komisia a vysoká predstaviteľka (v rámci svojich právomocí) v koordinácii s členskými štátmi preskúmajú, ako treba reagovať na hybridné hrozby, najmä na kybernetické útoky v odvetví dopravy.

Vykonávanie akčného plánu stratégie námornej bezpečnosti EÚ[17] napomôže prelomenie uzavretého spôsobu myslenia pri výmene informácií a spoločné využívanie aktív medzi civilnými a vojenskými orgánmi. Celý prístup verejnej správy viedol k zvýšenej spolupráci rôznych aktérov. Spoločný civilno-vojenský strategický výskumný program Komisie a ESVČ by sa mal dokončiť do konca roka 2017, a to záverečným seminárom o ochrane kritickej námornej infraštruktúry. Táto činnosť by sa mohla v budúcnosti rozšíriť na novú hrozbu pre podmorské potrubia, prenos energie, optické vlákna a tradičné komunikačné káble, ktorú predstavujú zásahy mimo vnútroštátnych vôd.

V jednej nedávnej štúdii[18] sa vyhodnotili kapacity posudzovania rizík vnútroštátnych orgánov vykonávajúcich úlohy pobrežnej stráže. Určili sa v nej najdôležitejšie prekážky spolupráce a odporučili praktické spôsoby na zlepšenie spolupráce medzi námornými orgánmi na úrovni EÚ a na vnútroštátnej úrovni v tejto osobitnej oblasti. Posúdenie rizika je dôležité pre boj proti námorným hrozbám a ešte nápomocnejšie pre hodnotenie a prevenciu hybridných hrozieb, pretože tieto si vyžadujú zohľadnenie dodatočných a zložitejších faktorov. Výsledky tejto štúdie budú predložené rozličným fóram pôsobiacim v oblasti pobrežnej stráže tak, aby sa navrhované odporúčania mohli posúdiť a vykonať s cieľom zintenzívniť spoluprácu v tejto oblasti, pričom hlavnými cieľmi sú pripravenosť a reakcia na hybridné hrozby.

Boj proti financovaniu terorizmu

Opatrenie č. 16: Komisia využije vykonávanie akčného plánu pre boj proti financovaniu terorizmu na to, aby prispel aj k boju proti hybridným hrozbám.

Pôvodcovia hybridných hrozieb a ich podporovatelia potrebujú finančné prostriedky na to, aby vykonávali svoje plány. Úsilie EÚ v boji proti financovaniu trestnej činnosti a terorizmu vyvíjané v rámci Európskeho programu v oblasti bezpečnosti a akčného plánu pre boj proti financovaniu terorizmu môže takisto prispieť k boju proti hybridným hrozbám. V decembri 2016 Komisia predložila tri legislatívne návrhy vrátane návrhu týkajúceho sa trestných sankcií za pranie špinavých peňazí a nezákonné platby v hotovosti, ako aj zmrazenia a konfiškácie majetku[19].
Všetky členské štáty museli do 26. júna 2017 transponovať 4. smernicu o boji proti praniu špinavých peňazí[20] a v júli 2016 Komisia predložila cielený legislatívny návrh na doplnenie a posilnenie tejto smernice prostredníctvom dodatočných opatrení[21].

---

[17] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf a 2. správa o vykonávaní akčného plánu námornej bezpečnosti EÚ (EUMSS AP) predložená členským štátom 21. júna 2017.

[18] Štúdia na tému „Hodnotenie kapacity posudzovania rizika na úrovni orgánov členských štátov vykonávajúcich úlohy pobrežnej stráže“ (Evaluation of risk assessment capacity at the level of Member States' authorities performing coast guard functions), 2017, https://ec.europa.eu/maritimeaffairs/documentation/studies.

[19] Tretia správa o pokroku smerom k dosiahnutiu účinnej a skutočnej bezpečnostnej Únie, COM(2016) 831 final.

[20] Smernica Európskeho parlamentu a Rady (EÚ) 2015/849 z 20. mája 2015 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu, ktorou sa mení nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 a zrušuje smernica Európskeho parlamentu a Rady 2005/60/ES a smernica Komisie 2006/70/ES (Text s významom pre EHP), Ú. v. EÚ L 141, 5.6.2015, s. 73 – 117).

Dňa 26. júna 2017 Komisia vydala nadnárodné posúdenie rizík v zmysle 4. smernice o boji proti praniu špinavých peňazí. Takisto predložila návrh nariadenia s cieľom zabrániť dovozu a uskladneniu tovaru kultúrneho charakteru nezákonne vyvezeného z tretích krajín v EÚ[22]. Neskôr v tomto roku Komisia predloží správu o svojom prebiehajúcom posudzovaní potreby možných dodatočných opatrení na sledovanie financovania terorizmu v EÚ. Komisia tiež vykonáva preskúmanie právnych predpisov o boji proti podvodom a falšovaniu bezhotovostných platobných prostriedkov[23].

Ôsma správa o pokroku smerom k dosiahnutiu účinnej a skutočnej bezpečnostnej Únie obsahuje viac informácií o aktuálnom stave vykonávania akčného plánu boja proti financovaniu terorizmu.

Presadzovanie spoločných hodnôt EÚ a inkluzívnych, otvorených a odolných spoločenstiev

Budovanie odolnosti proti radikalizácii a násilnému extrémizmu

Náboženská a ideologická radikalizácia, etnický konflikt a menšinové konflikty môžu byť vyvolané vonkajšími aktérmi prostredníctvom podpory osobitných skupín alebo úsilia podnecovať konflikty medzi skupinami. Objavujú sa nové problémy, ako sú hrozby zo strany osamelých aktérov, nové spôsoby radikalizácie vrátane potenciálne v súvislosti s migračnou krízou, ako aj nárast pravicového extrémizmu (vrátane násilia voči migrantom) a riziko polarizácie. Zatiaľ čo sa v rámci bezpečnostnej únie napreduje v činnosti v súvislosti s radikalizáciou, môže byť tiež z hľadiska hybridných hrozieb nepriamo relevantné, že ľudia náchylní na radikalizáciu môžu byť manipulovaní páchateľmi hybridných hrozieb.

***Opatrenie č. 17:* Komisia vykonáva opatrenia proti radikalizácii stanovené v Európskom programe v oblasti bezpečnosti a analyzuje potrebu posilniť postupy pre odstraňovanie nelegálneho obsahu, pričom vyzýva sprostredkovateľov sietí a systémov na náležitú starostlivosť pri ich riadení.**

Predchádzanie radikalizácii

Komisia pokračuje vo vykonávaní svojich komplexných opatrení zameraných proti radikalizácii, ako bolo stanovené v oznámení na podporu predchádzania radikalizácii vedúcej k násilnému extrémizmu[24] z júna 2016, a to konkrétne opatrení, ako napr. podpora inkluzívneho vzdelávania a spoločných hodnôt, boj proti extrémistickej propagande na internete a radikalizácii vo väzeniach, posilnenie spolupráce s tretími krajinami a posilnenie výskumu s cieľom lepšie porozumieť meniacej sa povahe radikalizácie a získať lepšie predpoklady pre strategické reakcie. Sieť na zvyšovanie povedomia o radikalizácii (RAN) má popredné postavenie v rámci práce Komisie na podporu členských štátov v tejto oblasti, v spolupráci s miestnymi odborníkmi z praxe na miestnej úrovni. Ďalšie podrobnosti sú

[21] Viac informácií nájdete v Tretej správe o pokroku smerom k dosiahnutiu účinnej a skutočnej bezpečnostnej Únie [COM(2016) 831 final] a v Ôsmej správe o pokroku smerom k dosiahnutiu účinnej a skutočnej bezpečnostnej Únie [COM(2017) 354 final].

[22] COM(2017) z 26. 6. 2017, COM(2017) 340 final, SWD(2017) 275 final 0.

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

[24] http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf.

uvedené v Ôsmej správe o pokroku smerom k dosiahnutiu účinnej a skutočnej bezpečnostnej Únie[25].

Radikalizácia prostredníctvom internetu a nenávistné prejavy

V súlade s európskym programom v oblasti bezpečnosti[26] Komisia podnikla kroky s cieľom obmedziť dostupnosť nezákonného obsahu na internete, a to najmä prostredníctvom jednotky EÚ pre nahlasovanie internetového obsahu pri Europole a internetového fóra EÚ[27]. Významný pokrok sa dosiahol aj vďaka kódexu správania zameraného na boj proti nelegálnym nenávistným prejavom na internete[28]. Ďalšie podrobnosti sú uvedené v Ôsmej správe o pokroku smerom k dosiahnutiu účinnej a skutočnej bezpečnostnej Únie[29]. Tieto činnosti sa posilnia, a to aj vzhľadom na závery Európskej rady[30], samit skupiny G7[31] a samit G20 v Hamburgu[32].

Online platformy zohrávajú kľúčovú úlohu v boji proti nezákonnému alebo potenciálne škodlivému obsahu. V rámci stratégie v oblasti jednotného digitálneho trhu, ako sa uvádza v preskúmaní v polovici trvania[33], Komisia zabezpečí lepšiu koordináciu dialógov platformy zameraných na mechanizmy a technické riešenia na odstránenie nezákonného obsahu. V prípade potreby by cieľom mala byť podpora týchto mechanizmov s usmerneniami o aspektoch, ako je oznamovanie a odstraňovanie nezákonného obsahu. Komisia poskytne aj usmernenia k pravidlám týkajúcim sa zodpovednosti.

Posilnenie spolupráce s tretími krajinami

Opatrenie č. 18: ***Vysoká predstaviteľka v koordinácii s Komisiou začne prieskum týkajúci sa hybridných rizík v susedných regiónoch. Vysoká predstaviteľka, Komisia a členské štáty budú využívať nástroje, ktoré majú k dispozícii, na účely budovania kapacít svojich partnerov a na posilnenie ich odolnosti proti hybridným hrozbám. Misie SBOP by sa mohli využívať (samostatne alebo ako doplnenie nástrojov EÚ) na pomoc partnerom pri posilňovaní ich kapacít.***

Európska únia venuje zvýšenú pozornosť budovaniu kapacít v oblasti bezpečnosti v partnerských krajinách okrem iného tým, že vychádza zo vzájomnej previazanosti prvkov bezpečnosti a rozvoja, rozpracúva bezpečnostný rozmer revidovanej európskej susedskej politiky a iniciuje rozhovory o boji proti terorizmu a o bezpečnosti s krajinami v oblasti Stredozemného mora. Na tento účel sa začal pilotný projekt prieskumu rizika v spolupráci

[25] COM(2017) 354 final.
[26] Viac informácií nájdete v Ôsmej správe o pokroku smerom k dosiahnutiu účinnej a skutočnej bezpečnostnej Únie, COM(2017) 354 final.
[27] Viac informácií nájdete v Ôsmej správe o pokroku smerom k dosiahnutiu účinnej a skutočnej bezpečnostnej Únie, COM(2017) 354 final.
[28] Kódex správania týkajúci sa nezákonných nenávistných prejavov na internete, 31. mája 2016, http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf.
[29] Viac informácií nájdete v Ôsmej správe o pokroku smerom k dosiahnutiu účinnej a skutočnej bezpečnostnej Únie, COM(2017) 354 final.
[30] Závery Rady z 22. až 23. júna 2017.
[31] Samit G7 v Taormine (Taliansko), 26. až 27. 5. 2017.
[32] Samit G20 v Hamburgu (Nemecko), 7. až 8. 7. 2017.
[33] Pozri vyššie oznámenie Komisie, COM (2017) 228 final.

s Moldavskou republikou. Jeho účelom je pomôcť identifikovať kľúčové slabé miesta v krajine a zabezpečiť, aby bola pomoc EÚ zacielená konkrétne na dané oblasti. Z výsledkov pilotného projektu vyplýva, že prieskum sa vyhodnotil ako užitočný. Na základe získaných skúseností Komisia a ESVČ budú predkladať odporúčania s cieľom určiť prioritné opatrenia v rámci okruhu účinnosť budov, strategická komunikácia, ochrana kritickej infraštruktúry a kybernetická bezpečnosť.

Pri pohľade do budúcnosti by aj ďalšie susedné krajiny mohli čerpať výhody z tohto prieskumu, vychádzajúc z tejto prvej skúsenosti; hoci s potrebou osobitne zohľadniť líšiacu sa miestnu situáciu a špecifické hrozby a zabrániť duplicite vo vzťahu k prebiehajúcim rozhovorom o boji proti terorizmu a o bezpečnosti. Dňa 7. júna 2017 Komisia a vysoká predstaviteľka prijali spoločné oznámenie s názvom „Strategický prístup k zvyšovaniu odolnosti vo vonkajšej činnosti EÚ“[34]. Cieľom je podporiť partnerské krajiny, aby sa stali odolnejšími proti globálnym výzvam súčasnosti. Uznáva sa v ňom potreba prejsť od zamedzovania šíreniu kríz k štruktúrovanejšiemu, dlhodobejšiemu prístupu k zraniteľnostiam s dôrazom na predvídanie, prevenciu a pripravenosť.

Kybernetická odolnosť v oblasti rozvoja

EÚ podporuje krajiny mimo Európy s cieľom posilniť odolnosť ich informačných sietí. Čoraz väčšia digitalizácia má vnútorný bezpečnostný rozmer, ktorý prináša osobitné výzvy pre odolnosť systémov informačných sietí na celom svete, keďže kybernetické útoky nepoznajú hranice. EÚ podporuje tretie krajiny pri budovaní ich schopnosti primerane predchádzať náhodným poruchám a kybernetickým útokom a reagovať na ne. V nadväznosti na pilotný projekt kybernetickej bezpečnosti v bývalej Juhoslovanskej republike Macedónsko, Kosove[35] a Moldavsku dokončený v roku 2016 Komisia začne nový program zameraný na zvýšenie kybernetickej odolnosti tretích krajín, najmä v Afrike a Ázii, na obdobie rokov 2017 – 2020, ale aj na Ukrajine. Jeho cieľom je zvýšenie bezpečnosti a pripravenosti kritickej informačnej infraštruktúry a sietí v tretích krajinách na základe celovládneho prístupu, pričom sa zaručí dodržiavanie ľudských práv a zásad právneho štátu.

Bezpečnostná ochrana letectva

Civilné letectvo zostáva hlavným a symbolickým cieľom pre teroristov, ale mohlo by byť tiež súčasťou hybridnej kampane. Zatiaľ čo EÚ vypracovala solídny rámec bezpečnostnej ochrany letectva, lety z tretích krajín môžu byť ohrozenejšie. V súlade s rezolúciou Bezpečnostnej rady OSN 2309 (2016) Komisia zintenzívňuje svoje úsilie o budovanie kapacít v tretích krajinách. V januári 2017 Komisia začala vykonávať nové integrované posudzovanie rizík s cieľom zabezpečiť stanovenie priorít a koordináciu úsilia o budovanie kapacít na úrovni EÚ a na úrovni členských štátov, ako aj s medzinárodnými partnermi. V roku 2016 Komisia začala realizovať 4-ročný projekt týkajúci sa bezpečnostnej ochrany civilného letectva v Afrike a na Arabskom polostrove na boj proti teroristickým hrozbám namiereným proti civilnému letectvu. Projekt sa zameriava na výmenu odborných znalostí medzi partnerskými štátmi a expertmi z členských štátov Európskej konferencie civilného letectva, mentorstvo, odbornú prípravu a školenia. Rozsah činností sa bude ďalej rozširovať v roku 2017.

[34] Spoločné oznámenie Európskemu parlamentu a Rade: Strategický prístup k zvyšovaniu odolnosti vo vonkajšej činnosti EÚ, JOIN (2017) 21 final.

[35] Týmto označením nie sú dotknuté pozície týkajúce sa štatútu a označenie je v súlade s rezolúciou Bezpečnostnej rady OSN č. 1244 a so stanoviskom Medzinárodného súdneho dvora k vyhláseniu nezávislosti Kosova.

c) PREVENCIA, REAKCIA NA KRÍZU A OBNOVA

Dôsledky je možné zmierniť prostredníctvom dlhodobých politík na vnútroštátnej úrovni a na úrovni EÚ, ale z krátkodobého hľadiska je veľmi dôležité posilniť kapacity členských štátov a Únie na prevenciu hybridných hrozieb, reakciu na ne a obnovu po nich, a to rýchlo a koordinovane. Kľúčová je rýchla reakcia na udalosti vyvolané hybridnými hrozbami. Za posledný rok sa v tejto oblasti dosiahol veľký pokrok, pričom v EÚ už v súčasnosti existuje operačný protokol, v ktorom sa stanovuje postup krízového riadenia v prípade hybridného útoku. V budúcnosti sa bude vykonávať pravidelné monitorovanie a precvičovanie.

Opatrenie č. 19: Vysoká predstaviteľka a Komisia v koordinácii s členskými štátmi vytvoria spoločný operačný protokol a budú vykonávať pravidelné cvičenia na zdokonalenie strategickej rozhodovacej kapacity v reakcii na komplexné hybridné hrozby, a to v rámci postupov pre riadenie kríz a integrovanej politickej reakcie na krízu.

Spoločný rámec obsahuje odporúčanie zaviesť mechanizmy rýchlej reakcie na udalosti vyvolané hybridnými hrozbami, na koordináciu medzi mechanizmami reakcie EÚ[36] a systémami včasného varovania. Na tento účel útvary Komisie a ESVČ vydali operatívny protokol pre boj proti hybridným hrozbám (operatívny protokol EÚ)[37], v ktorom sa uvádzajú rôzne spôsoby koordinácie, syntézy a analýzy spravodajských informácií, tvorby politík, cvičení a odbornej prípravy, ako aj spolupráce s partnerskými organizáciami, najmä s NATO, v prípade hybridnej hrozby. Podobne NATO vytvorilo operatívny protokol na posilnenie interakcie medzi EÚ a NATO pri predchádzaní a boji proti hybridným hrozbám v oblasti kybernetickej obrany, strategickej komunikácie, situačného povedomia a krízového riadenia. Operatívny protokol EÚ sa bude testovať na jeseň 2017 ako súčasť paralelných a koordinovaných cvičení Európskej únie, ktoré zahŕňajú interakciu s NATO.

Opatrenie č. 20: Komisia a vysoká predstaviteľka (v rámci svojich právomocí) preskúmajú uplatniteľnosť a praktické dôsledky uplatnenia článku 222 ZFEÚ a článku 42 ods. 7 ZEÚ v prípadoch, keď sa objaví rozsiahly a závažný hybridný útok.

Článok 42 ods. 7 ZEÚ odkazuje na ozbrojenú agresiu na území členského štátu, zatiaľ čo článok 222 ZFEÚ (doložka o solidarite) odkazuje na teroristický útok, alebo prírodnú katastrofu alebo katastrofu spôsobenú ľudskou činnosťou na území členského štátu. V prípade hybridných útokov, ktoré sú kombináciou trestných/podvratných činností, sa uplatňuje článok 222 ZFEÚ. Uplatnenie doložky o solidarite spúšťa koordináciu na úrovni Rady (dojednania o integrovanej politickej reakcii na krízu) a zapojenie príslušných inštitúcií, agentúr a orgánov EÚ, ako aj programov a mechanizmov pomoci EÚ. Rozhodnutím Rady 2014/415/EÚ sa stanovujú podrobnosti vykonávania doložky o solidarite Úniou. Tieto spôsoby uplatnenia zostanú platné a nie je potrebné revidovať rozhodnutie Rady. Ak hybridný útok zahŕňa ozbrojenú agresiu, bolo by možné uplatniť aj článok 42 ods. 7. V takom prípade poskytnú pomoc a podporu členské štáty aj EÚ. Komisia a vysoká predstaviteľka budú pokračovať v posudzovaní najúčinnejšieho spôsobu, ako riešiť takéto útoky.

[36] Dojednania v rámci integrovanej politickej reakcie Rady EÚ na krízu, systém Komisie ARGUS a CRM ESVČ.
[37] Pracovný dokument útvarov Komisie (2016) 227, prijatý 7. júla 2016.

Prijatím operačného protokolu EÚ uvedeného vyššie sa priamo podporuje toto posúdenie. Operačný protokol sa bude vykonávať ako súčasť paralelného a koordinovaného cvičenia EÚ s NATO (PACE) v októbri 2017. Počas tohto cvičenia sa otestujú rôzne mechanizmy EÚ a schopnosť interakcie s cieľom rýchlejšie prijímať rozhodnutia v prípade nejasnosti vyvolanej hybridnými hrozbami.

Opatrenie č. 21: Vysoká predstaviteľka v koordinácii s členskými štátmi bude takisto integrovať, využívať a koordinovať možnosti vojenskej akcie v boji proti hybridným hrozbám v rámci spoločnej bezpečnostnej a obrannej politiky.

V reakcii na poverenie integrovať vojenské spôsobilosti s cieľom podporiť SZBP/SBOP a v nadväznosti na seminár vojenských expertov v decembri 2016, ako aj v reakcii na usmernenie pracovnej skupiny Vojenského výboru z mája 2017 bolo v júli 2017 sfinalizované vojenské odporúčanie k „príspevku EÚ k boju proti hybridným hrozbám v rámci spoločnej bezpečnostnej a obrannej politiky“, ktoré bude ďalej rozpracované prostredníctvom vykonávacieho plánu pre vypracovanie koncepcie.

d) SPOLUPRÁCA MEDZI EÚ A NATO

Opatrenie č. 22: Vysoká predstaviteľka bude v koordinácii s Komisiou pokračovať v neformálnom dialógu a bude v boji proti hybridným hrozbám posilňovať spoluprácu a koordináciu s NATO v oblastiach situačného povedomia, strategickej komunikácie, kybernetickej bezpečnosti a „prevencie kríz a reakcie na ne“ tak, aby sa rešpektovali zásady inkluzívneho a autonómneho rozhodovania obidvoch organizácií.

Na základe spoločného vyhlásenia podpísaného predsedami Európskej rady a Európskej komisie spolu s generálnym tajomníkom NATO vo Varšave 8. júla 2016 EÚ a NATO vypracovali spoločný súbor 42 návrhov na vykonanie, ktorý bol následne potvrdený v rámci samostatných súbežných postupov 6. decembra 2016 tak Radou EÚ, ako aj Radou NATO[38]. Vysoká predstaviteľka a podpredsedníčka Komisie a generálny tajomník NATO prijali v júni 2017 správu o celkovom pokroku dosiahnutom pri 42 opatreniach spoločného vyhlásenia. Boj proti hybridným hrozbám je jednou zo siedmich oblastí spolupráce uvedených v spoločnom vyhlásení a je súčasťou desiatich zo štyridsiatich dvoch opatrení. Správa ukazuje, že spoločné úsilie vynaložené v posledných rokoch prinieslo významné výsledky. Mnohé osobitné opatrenia zamerané na boj proti hybridným hrozbám už boli uvedené, vrátane Európskeho centra excelentnosti pre boj proti hybridným hrozbám, lepšieho situačného povedomia, vytvorenia strediska EÚ pre hybridné hrozby a jeho interakcie s novovytvoreným oddelením NATO pre hybridné hrozby a spolupráce medzi tímami strategickej komunikácie. Po prvýkrát budú štáby EÚ a NATO spoločne nacvičovať reakciu na hybridný scenár. Pri tomto cvičení by sa malo otestovať vykonávanie viac než tretiny spoločných návrhov. EÚ bude vykonávať svoje vlastné paralelné a koordinované cvičenie v tomto roku a má v úmysle prevziať vedúcu úlohu v roku 2018.

Pokiaľ ide o odolnosť, štáby EÚ aj NATO sa zapojili do krížových brífingov vrátane mechanizmu EÚ pre integrovanú politickú reakciu na krízu. Pravidelné kontakty medzi štábmi EÚ a NATO, a to aj prostredníctvom seminárov a NATO alebo účasti v riadiacej rade Európskej obrannej agentúry umožnili výmenu informácií o základných požiadavkách NATO týkajúcich sa vnútroštátnej odolnosti. Na jeseň sa plánuje ďalšia výmena medzi Komisiou

[38] http://www.consilium.europa.eu/sk/press/press-releases/2016/12/06-eu-nato-joint-declaration/.

a NATO o posilnení odolnosti. V ďalšej správe o pokroku v spolupráci medzi EÚ a NATO sa navrhnú možnosti na rozšírenie spolupráce medzi týmito dvoma organizáciami.

3. ZÁVER

Spoločný rámec ponúka náčrt návrhov, ktorých cieľom je prispieť k boju proti hybridným hrozbám a posilniť odolnosť na úrovni EÚ a na vnútroštátnej úrovni, ako aj na úrovni partnerov. Zatiaľ čo Komisia a vysoká predstaviteľka v každej oblasti úzko spolupracujú s členskými štátmi a partnermi, je dôležité, aby sa tento trend zachoval vzhľadom na pretrvávajúce a neustále sa vyvíjajúce hybridné hrozby. Členské štáty nesú primárnu zodpovednosť za boj proti hybridným hrozbám súvisiacim s národnou bezpečnosťou a za zachovanie práva a poriadku. Vnútroštátnu odolnosť a kolektívne úsilie na ochranu proti hybridným hrozbám treba chápať ako vzájomne sa dopĺňajúce prvky rovnakého celkového úsilia. Členské štáty sa preto vyzývajú, aby vykonali tieto prieskumy týkajúce sa hybridných rizík čo možno najrýchlejšie, keďže budú zdrojom cenných informácií o rozsahu zraniteľnosti a pripravenosti v rámci Európy. Na základe významného pokroku pri zlepšovaní povedomia by sa mal potenciál strediska EÚ pre hybridné hrozby maximalizovať. Vysoká predstaviteľka vyzýva členské štáty, aby podporovali činnosť pracovných skupín East StratCom s cieľom účinnejšie bojovať proti nárastu hybridných hrozieb. EÚ bude v plnej miere podporovať Európske centrum pre boj proti hybridným hrozbám vedené Fínskom.

Jedinečná sila EÚ spočíva v poskytovaní pomoci členským štátom a partnerom pri budovaní ich odolnosti, opierajúc o širokú paletu existujúcich nástrojov a programov. Značný pokrok sa dosiahol opatreniami na budovanie odolnosti v oblastiach, ako je doprava, energetika, kybernetická bezpečnosť, kritická infraštruktúra, ochrana finančného systému pred nezákonným využívaním a boj proti násilnému extrémizmu a radikalizácii. EÚ bude pokračovať v činnosti pri budovaní odolnosti, keďže povaha hybridných hrozieb sa neustále mení. EÚ vypracuje predovšetkým ukazovatele na zlepšenie ochrany a odolnosti kritickej infraštruktúry proti hybridným hrozbám v príslušných odvetviach.

Fond môže spolu s členskými štátmi spolufinancovať priority spôsobilostí s cieľom posilniť odolnosť proti hybridným hrozbám. Nadchádzajúci balík kybernetickej bezpečnosti, ako aj opatrenia zamerané na vykonávanie smernice o bezpečnosti informačných sietí poskytnú nové platformy pre boj proti hybridným hrozbám v celej EÚ.

Komisia a vysoká predstaviteľka vyzývajú členské štáty a zainteresované subjekty, aby v prípade potreby rýchlo dosiahli dohodu a zabezpečili rýchle a účinné vykonávanie mnohých opatrení zameraných na posilnenie odolnosti uvedených v tomto oznámení. EÚ bude naďalej rozvíjať a prehlbovať svoju už teraz prínosnú spoluprácu s NATO.

Európska únia je i naďalej odhodlaná zmobilizovať všetky relevantné nástroje EÚ s cieľom riešiť komplexné hybridné hrozby. Podpora úsilia členských štátov zostáva prioritou Európskej únie, konajúcej v spolupráci so svojimi kľúčovými partnermi ako silnejší a pohotovejší zabezpečovateľ bezpečnosti.