EURÓPSKA
KOMISIA

VYSOKÁ PREDSTAVITEĽKA
ÚNIE PRE
ZAHRANIČNÉ VECI
A BEZPEČNOSTNÚ POLITIKU

V Bruseli 6. 4. 2016
JOIN(2016) 18 final

SPOLOČNÉ OZNÁMENIE EURÓPSKEMU PARLAMENTU A RADE

Spoločný rámec pre boj proti hybridným hrozbám

reakcia Európskej únie

1. ÚVOD

Bezpečnostná situácia Európskej únie sa v posledných rokoch dramaticky zmenila. Problémy so zabezpečením mieru a stability vo východnom a južnom susedstve EÚ svedčia aj naďalej o tom, že Únia musí prispôsobiť a znásobiť svoje kapacity, aby si mohla plniť úlohu poskytovateľky bezpečnosti, a zamerať sa pritom najmä na vzájomnú prepojenosť medzi vonkajšou a vnútornou bezpečnosťou. Mnoho problémov v oblasti zabezpečovania mieru, bezpečnosti a prosperity spôsobuje v súčasnosti nestabilita v krajinách, ktoré bezprostredne susedia s EÚ, a premenlivý charakter hrozieb. Predseda Európskej komisie Jean-Claude Juncker vo svojich politických usmerneniach z roku 2014 zdôraznil, že je potrebné „pracovať na posilnení Európy, pokiaľ ide o záležitosti bezpečnosti a obrany“, a skĺbiť európske a národné nástroje efektívnejšie než v minulosti. Aj vysoká predstaviteľka venovala v nadväznosti na výzvu Rady pre zahraničné veci z 18. mája 2015 v úzkej spolupráci s útvarmi Komisie a Európskou obrannou agentúrou (EDA) a po konzultácii s členskými štátmi EÚ svoje úsilie tomu, aby predstavila tento spoločný rámec obsahujúci realizovateľné návrhy pre boj proti hybridným hrozbám a pre posilnenie odolnosti EÚ a jej členských štátov a partnerov[1]. Európska rada v júni 2015 pripomenula, že na účely boja proti hybridným hrozbám je potrebné mobilizovať nástroje EÚ[2].

Definície hybridných hrozieb sú síce rôzne a musia zostať flexibilné, aby mohli reagovať na premenlivú povahu týchto hrozieb, ide však o to, aby sa podarilo vystihnúť súbor rôznych nátlakových a podvratných činností a konvenčných a nekonvenčných metód (napríklad diplomatických, vojenských, ekonomických a technologických), ktoré môžu rôzne štátne aj neštátne subjekty koordinovaným spôsobom využívať na to, aby dosiahli konkrétne ciele bez toho, aby formálne vyhlásili vojnu. Snahou je obyčajne zneužívať zraniteľnosť cieľa a vytvárať neprehľadné situácie s cieľom narušiť rozhodovacie procesy. Nástrojom týchto hybridných hrozieb môžu byť masívne dezinformačné kampane a využívanie sociálnych médií na propagandu alebo radikalizáciu, nábor a priame ovládanie priaznivcov.

Keďže boj proti hybridným hrozbám súvisí s národnou bezpečnosťou a obranou a zachovaním práva a verejného poriadku, hlavnú zodpovednosť nesú členské štáty, pretože jednotlivé slabiny sú väčšinou špecifické pre jednotlivé krajiny. Mnoho členských štátov EÚ sa však stretáva aj so spoločnými hrozbami, ktorých cieľom môžu byť aj cezhraničné siete alebo infraštruktúry. Takýmto hrozbám je možné účinnejšie čeliť pomocou koordinovanej reakcie na úrovni EÚ, konkrétne prostredníctvom politík a nástrojov EÚ, využitím európskej solidarity, vzájomnej pomoci a plného potenciálu Lisabonskej zmluvy. Politiky a nástroje EÚ môžu zohrávať – a vo významnej miere už aj zohrávajú – zásadnú úlohu pri zvyšovaní informovanosti. Tým sa zlepšuje odolnosť členských štátov a ich schopnosť reagovať na spoločné hrozby. Vonkajšia činnosť Únie navrhovaná podľa tohto rámca zodpovedá zásadám stanoveným v článku 21 Zmluvy o Európskej únii (ZEÚ), ku ktorým patrí demokracia, právny štát, univerzálnosť

[1] Závery Rady o spoločnej bezpečnostnej a obrannej politike (SBOP), máj 2015 [Consilium 8971/15].
[2] Závery Európskej rady, jún 2015 [EUCO 22/15].

a nedeliteľnosť ľudských práv a dodržiavanie zásad Charty Organizácie spojených národov a medzinárodného práva[3].

Cieľom tohto spoločného oznámenia je uľahčiť vznik komplexného prístupu, ktorý umožní Európskej únii v koordinácii s členskými štátmi bojovať s konkrétnymi hrozbami hybridnej povahy tým, že sa medzi všetkými príslušnými nástrojmi vytvoria synergie a že sa zlepší spolupráca medzi všetkými príslušnými aktérmi[4]. Navrhované opatrenia vychádzajú z existujúcich stratégií a sektorových politík, ktoré prispievajú k dosiahnutiu vyššieho stupňa bezpečnosti. Medzi nástroje, ktoré môžu tiež pomôcť v boji proti hybridným hrozbám, patrí najmä Európsky program v oblasti bezpečnosti[5], nová globálna stratégia Európskej únie v oblasti zahraničnej a bezpečnostnej politiky a akčný plán v oblasti európskej obrany[6], stratégia kybernetickej bezpečnosti EÚ[7], stratégia energetickej bezpečnosti[8] a stratégia námornej bezpečnosti Európskej únie[9].

Keďže proti hybridným hrozbám bojuje aj NATO a keďže Rada pre zahraničné veci navrhla posilniť spoluprácu a koordináciu v tejto oblasti, cieľom niektorých návrhov je upevniť spoluprácu medzi EÚ a NATO v oblasti boja proti hybridným hrozbám.

Navrhovaná reakcia sa zameriava na tieto prvky: zlepšovanie informovanosti, posilňovanie odolnosti, prevenciu, reakciu na krízu a obnovu.

2. IDENTIFIKÁCIA HYBRIDNEJ POVAHY HROZBY

Hybridné hrozby využívajú zraniteľnosti určitej krajiny a často sa snažia oslabiť základné demokratické hodnoty a slobody. Vysoká predstaviteľka a Komisia budú v prvom rade spolupracovať s členskými štátmi, aby získali viac informácií o situácii, a to prostredníctvom sledovania a posudzovania rizík, ktoré môžu hroziť na zraniteľných miestach v EÚ. Komisia vyvíja metódy hodnotenia bezpečnostných rizík, ktoré majú poskytovať informácie subjektom s rozhodovacou právomocou a podporovať vytváranie politík na základe hodnotenia rizík v oblastiach od bezpečnosti leteckej prevádzky až po financovanie terorizmu a pranie špinavých peňazí. Okrem toho by bolo vhodné uskutočniť v členských štátoch prieskum s cieľom identifikovať oblasti potenciálne zraniteľné hybridnými hrozbami. Cieľom by bolo určiť ukazovatele hybridných hrozieb, začleniť ich do mechanizmov včasného varovania a existujúcich mechanizmov hodnotenia rizík a v prípade potreby ich zdieľať.

[3] Keď orgány a členské štáty vykonávajú právne predpisy Únie, Charta základných práv EÚ je pre ne záväzná.
[4] Prípadné legislatívne návrhy budú podliehať požiadavkám Komisie na lepšiu právnu reguláciu, a to v súlade s usmerneniami Komisie pre lepšiu právnu reguláciu [SWD(2015) 111].
[5] COM(2015) 185 final.
[6] Mali by sa predložiť v roku 2016.
[7] Politický rámec EÚ pre kybernetickú obranu [Consilium 15585/14] a spoločné oznámenie s názvom „Stratégia kybernetickej bezpečnosti Európskej únie: Otvorený, bezpečný a chránený kybernetický priestor “, február 2013 [JOIN(2013)1].
[8] Spoločné oznámenie s názvom „Európska stratégia energetickej bezpečnosti“, máj 2014 [SWD(2014) 330].
[9] Spoločné oznámenie s názvom „Za otvorené a bezpečné svetové oceány: prvky stratégie námornej bezpečnosti Európskej únie“ – JOIN(2014) 9 final – 6. marca 2014.

<u>Opatrenie č. 1</u>: 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.

3. ORGANIZÁCIA REAKCIE NA ÚROVNI EÚ: ZLEPŠOVANIE INFORMOVANOSTI

3.1. Stredisko EÚ pre hybridné hrozby

Je veľmi dôležité, aby EÚ v koordinácii s členskými štátmi mala dostatok informácií o situácii, aby mohla odhaliť akúkoľvek zmenu v oblasti bezpečnosti týkajúcu sa hybridnej činnosti vyvíjanej štátnymi a/alebo neštátnymi subjektmi. Aby sme mohli účinne bojovať proti hybridným hrozbám, treba zlepšiť výmenu informácií a podporovať zdieľanie príslušných spravodajských informácií medzi všetkými sektormi a medzi Európskou úniou a jej členskými štátmi a partnermi.

Stredisko EÚ pre hybridné hrozby zriadené v rámci Centra EÚ pre analýzu spravodajských informácií (EU INTCEN) Európskej služby pre vonkajšiu činnosť (ESVČ) bude zamerané výlučne na analýzu hybridných hrozieb. Toto stredisko bude zbierať, analyzovať a zdieľať tajné informácie a informácie z otvorených zdrojov, ktoré sa konkrétne týkajú ukazovateľov a varovaní v súvislosti s hybridnými hrozbami, od rôznych zúčastnených strán v rámci ESVČ (vrátane delegácií EÚ), Komisie (vrátane agentúr EÚ[10]) a členských štátov. V spolupráci s podobnými existujúcimi subjektmi na úrovni EÚ[11] a na vnútroštátnej úrovni by uvedené stredisko analyzovalo vonkajšie aspekty hybridných hrozieb, ktoré postihujú EÚ a jej susedov, aby bolo možné urýchlene vyhodnocovať relevantné incidenty a zaistiť informácie potrebné na strategické rozhodovacie procesy v EÚ, okrem iného tým, že bude poskytovať informácie potrebné na hodnotenie bezpečnostných rizík vykonávané na úrovni EÚ. Analytické výstupy tohto strediska by sa spracúvali a nakladalo by sa s nimi v súlade s pravidlami Európskej únie pre ochranu utajovaných informácií a údajov[12]. Stredisko by malo udržiavať kontakt s existujúcimi subjektmi na úrovni EÚ a na vnútroštátnej úrovni. Členské štáty by mali zriadiť národné kontaktné miesta prepojené so strediskom EÚ pre hybridné hrozby. Zamestnanci vnútri aj mimo EÚ (vrátane tých, ktorí sú vyslaní do delegácií, operácií a misií EÚ) a v členských štátoch by takisto mali absolvovať prípravu, aby dokázali rozoznávať prvé náznaky hybridných hrozieb.

<u>Opatrenie č. 2</u>: Vytvoriť v rámci existujúcej štruktúry EU INTCEN 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.

[10] V súlade s ich mandátmi.
[11] Napríklad Európske centrum boja proti počítačovej kriminalite a Európske centrum pre boj proti terorizmu, agentúra Frontex, tím EÚ pre reakciu na núdzové počítačové situácie (CERT-EU).
[12] Smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995.

3.2. Strategická komunikácia

Pôvodcovia hybridných hrozieb môžu systematicky šíriť nepravdivé informácie, okrem iného prostredníctvom cielených kampaní cez sociálne médiá, a tým sa snažiť o radikalizáciu jednotlivcov, destabilizáciu spoločnosti a politickú propagandu. Zásadný význam má preto schopnosť reagovať na hybridné hrozby prostredníctvom spoľahlivej **strategickej komunikácie**. Hlavnými faktormi budovania odolnosti spoločnosti sú zabezpečenie okamžitých adresných reakcií a zvyšovanie informovanosti verejnosti o hybridných hrozbách.

Pri strategickej komunikácii by sa mali v plnom rozsahu využívať nástroje sociálnych médií, ako aj tradičné vizuálne, zvukové a webové médiá. ESVČ by mala v nadväznosti na aktivity pracovných skupín East StratCom a Arab StratCom optimalizovať využívanie lingvistov plynule hovoriacich príslušnými jazykmi krajín mimo EÚ a odborníkov na sociálne médiá, ktorí môžu monitorovať informácie z krajín mimo EÚ a zabezpečovať cielenú komunikáciu na účely reakcie na šírenie dezinformácií. Členské štáty by navyše mali vypracovať koordinované mechanizmy strategickej komunikácie na podporu zisťovania pôvodu dezinformácií a boja proti nim s cieľom odhaľovať hybridné hrozby.

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.

3.3. Centrum excelentnosti pre boj proti hybridným hrozbám

Na základe skúseností niektorých členských štátov a partnerských organizácií[13] by jedna nadnárodná inštitúcia alebo sieť takýchto inštitúcií mohla fungovať ako stredisko excelentnosti, ktoré sa bude zapodievať riešením hybridných hrozieb. Takéto stredisko by sa mohlo zamerať na výskum využívania hybridných stratégií a mohlo by podnietiť rozvoj nových koncepcií a technológií v súkromnom aj priemyselnom sektore s cieľom pomôcť členským štátom s budovaním odolnosti. Výskum by mohol prispieť k zladeniu politík, doktrín a koncepcií EÚ a jednotlivých štátov a zabezpečiť, aby v rozhodovaní bolo možné zohľadniť zložitosť a nejednoznačnosť, ktoré sú príznačné pre hybridné hrozby. Toto stredisko by malo navrhovať programy na podporu výskumu a výcvik s cieľom nájsť praktické riešenia existujúcich problémov spôsobených hybridnými hrozbami. Sila tohto strediska by spočívala v tom, že by vychádzalo z odborných znalostí svojich spolupracovníkov z rôznych krajín a odborov, z civilného aj vojenského, ako aj súkromného a akademického sektora.

Toto stredisko by mohlo úzko spolupracovať s existujúcimi centrami excelentnosti EÚ[14] a NATO[15], aby bolo možné využívať informácie o hybridných hrozbách získaných

[13] Centrá excelentnosti NATO.
[14] Napríklad Inštitút Európskej únie pre bezpečnostné štúdie (EU ISS), tematické centrá excelentnosti EÚ v oblasti CBRN.
[15] http://www.nato.int/cps/en/natohq/topics_68372.htm.

prostredníctvom kybernetickej obrany, strategickej komunikácie, civilno-vojenskej spolupráce, energetickej a krízovej reakcie.

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

4. ORGANIZÁCIA REAKCIE NA ÚROVNI EÚ: BUDOVANIE ODOLNOSTI

Odolnosť je schopnosť odolávať stresu, zabezpečiť obnovu a poučiť sa z ťažkých situácií. Aby bolo možné bojovať proti hybridným hrozbám účinne, treba riešiť potenciálne slabé miesta najdôležitejších infraštruktúr, dodávateľských reťazcov a spoločnosti. Využitím nástrojov a politík EÚ je možné posilniť odolnosť infraštruktúry na úrovni EÚ.

4.1. Ochrana kritickej infraštruktúry

Dôležité je chrániť kritické infraštruktúry (napríklad dodávateľské reťazce energie a dopravu), pretože nekonvenčný útok pôvodcov hybridných hrozieb na akýkoľvek „mäkký cieľ“ by mohol spôsobiť vážny ekonomický alebo sociálny rozvrat. Na zabezpečenie ochrany kritickej infraštruktúry Európsky program na ochranu kritickej infraštruktúry[16] (EPCIP) poskytuje medziodvetvový systémový prístup, v ktorom sa zohľadňujú všetky riziká, ktorý je zameraný na vzájomnú prepojenosť a ktorý funguje na základe vykonávania činností v oblastiach prevencie, pripravenosti a reakcie. Smernicou o európskych kritických infraštruktúrach[17] sa zavádza postup pre určovanie a označovanie európskych kritických infraštruktúr (EKI) a spoločný prístup pre posudzovanie potreby zvýšiť ich ochranu. Podľa tejto smernice by sa malo obnoviť najmä úsilie o posilnenie odolnosti kritických infraštruktúr v oblasti dopravy (napríklad hlavných letísk a obchodných prístavov v EÚ). Komisia posúdi, či je vhodné vo všetkých príslušných odvetviach vypracovať spoločné nástroje vrátane ukazovateľov na zlepšenie odolnosti kritických infraštruktúr proti hybridným hrozbám.

<u>Opatrenie č. 5</u>: 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.

4.1.1. Energetické siete

Nerušená výroba a distribúcia energie má pre EÚ zásadný význam a významné výpadky energie by mohli spôsobiť škody. Základným prvkom v boji proti hybridným hrozbám je ďalšia diverzifikácia zdrojov energie v EÚ, ich dodávateľov a trás, aby sa zaistili bezpečnejšie a odolnejšie dodávky energie. Komisia zároveň vykonáva posúdenie rizík a bezpečnosti (tzv. záťažové skúšky) atómových elektrární EÚ. Aby sa zabezpečila diverzifikácia dodávok energie, zintenzívňuje sa úsilie v rámci stratégie pre energetickú

[16] Oznámenie Komisie o Európskom programe na ochranu kritickej infraštruktúry, 12.12.2006, KOM(2006) 786 v konečnom znení.

[17] Smernica Rady 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu (Ú. v. EÚ L 345, 23.12.2008).

úniu: napríklad južný koridor dodávky zemného plynu, ktorý umožní dopravu plynu z oblasti Kaspického mora do Európy a vybudovanie terminálov pre skvapalnený zemný plyn s viacerými dodávateľmi v severnej Európe. Tento príklad treba nasledovať aj v strednej a východnej Európe a v Stredomorí, kde sa v súčasnosti pracuje na vývoji plynárenského uzla.[18] Aj vývoj trhu so skvapalneným zemným plynom pozitívne prispeje k dosiahnutiu tohto cieľa.

Pokiaľ ide o atómový materiál a atómové zariadenia, Komisia podporuje tvorbu a prijímanie najvyšších bezpečnostných noriem, ktorými sa zvyšuje odolnosť. Komisia vyzýva na konzistentnú transpozíciu a vykonávanie smernice o jadrovej bezpečnosti[19], v ktorej sa stanovujú pravidlá predchádzania haváriám a zmierňovania ich následkov, a ustanovení smernice o základných bezpečnostných štandardoch[20] týkajúcich sa medzinárodnej spolupráce v oblasti havarijnej pripravenosti a odozvy na havarijnú situáciu, najmä medzi susednými členskými štátmi a so susednými krajinami.

***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.**

4.1.2 Bezpečnosť dopravy a dodávateľských reťazcov

Doprava má zásadný význam pre fungovanie Únie. Hybridné útoky na dopravnú infraštruktúru (ako sú letiská, cestná infraštruktúra, prístavy a železnice) môžu mať závažné dôsledky, ktoré môžu viesť k narušeniu dopravy a dodávateľských reťazcov. V rámci vykonávania predpisov o leteckej a námornej bezpečnosti[21] Komisia organizuje pravidelné inšpekcie[22] a prostredníctvom svojej práce v oblasti bezpečnosti pozemnej dopravy sa snaží riešiť nové hybridné hrozby. V tejto súvislosti sa o rámci EÚ diskutuje v revidovanom nariadení o bezpečnosti letectva[23] ako súčasti Stratégie v oblasti letectva

[18] Informácie o dosiahnutom pokroku sú uvedené v Správe o stave energetickej únie za rok 2015 [COM(2015) 572 final].

[19] Smernica Rady 2009/71/Euratom z 25. júna 2009, ktorou sa zriaďuje rámec Spoločenstva pre jadrovú bezpečnosť jadrových zariadení, zmenená smernicou Rady 2014/87/Euratom z 8. júla 2014.

[20] Smernica Rady 2013/59/Euratom z 5. decembra 2013, ktorou sa stanovujú základné bezpečnostné normy ochrany pred nebezpečenstvami vznikajúcimi v dôsledku ionizujúceho žiarenia, a ktorou sa zrušujú smernice 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom a 2003/122/Euratom.

[21] Nariadenie Európskeho parlamentu a Rady (ES) č. 300/2008 z 11. marca 2008 o spoločných pravidlách v oblasti bezpečnostnej ochrany civilného letectva a o zrušení nariadenia (ES) č. 2320/2002; Vykonávacie nariadenie Komisie (EÚ) 2015/1998 z 5. novembra 2015, ktorým sa stanovujú podrobné opatrenia na vykonávanie spoločných základných noriem bezpečnostnej ochrany letectva; Smernica Európskeho parlamentu a Rady 2005/65/ES z 26. októbra 2005 o zvýšení bezpečnosti prístavov; Nariadenie (ES) č. 725/2004 Európskeho parlamentu a Rady z 31. marca 2004 o zvýšení bezpečnosti lodí a prístavných zariadení.

[22] Podľa práva EÚ má Komisia povinnosť vykonávať inšpekcie, aby zabezpečila, že členské štáty riadne vykonávajú požiadavky na leteckú a námornú bezpečnosť. Ide o inšpekcie príslušného orgánu v členskom štáte a kontroly na letiskách, v prístavoch, kontroly leteckých dopravcov, lodí a subjektov vykonávajúcich bezpečnostné opatrenia. Cieľom inšpekcií Komisie ja zabezpečiť, aby členské štáty plne vykonávali normy EÚ.

[23] Nariadenie Komisie (EÚ) 2016/4 z 5. januára 2016, ktorým sa mení nariadenie Európskeho parlamentu a Rady (ES) č. 216/2008, pokiaľ ide o základné požiadavky ochrany životného prostredia; Nariadenie Európskeho parlamentu a Rady (ES) č. 216/2008 z 20. februára 2008 o spoločných pravidlách v oblasti civilného letectva a o zriadení Európskej agentúry pre bezpečnosť letectva.

pre Európu[24]. Hrozbami pre námornú bezpečnosť sa ďalej zaoberá stratégia Európskej únie pre námornú bezpečnosť a jej akčný plán[25]. Tento plán umožňuje EÚ a jej členským štátom komplexne riešiť problémy v oblasti námornej bezpečnosti vrátane boja proti hybridným hrozbám, a to vďaka medziodvetvovej spolupráci medzi civilnými a vojenskými subjektmi na účely ochrany kritickej námornej infraštruktúry, celosvetového dodávateľského reťazca, námorného obchodu a morských prírodných zdrojov a zdrojov energie. Bezpečnosť medzinárodného dodávateľského reťazca je zároveň predmetom stratégie a akčného plánu Európskej únie pre riadenie rizík v oblasti ciel[26].

<u>Opatrenie č. 7</u>: 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 a akčného plánu EÚ pre riadenie rizík v oblasti ciel preskúma Komisia a vysoká predstaviteľka (v rámci svojich právomocí) v spolupráci s členskými štátmi, ako treba reagovať na hybridné hrozby, najmä na také, ktoré sa týkajú kritickej dopravnej infraštruktúry.

4.1.3 Vesmír

Hybridné hrozby by sa mohli zamerať na kozmické infraštruktúry, s následkami pre viacero odvetví naraz. EÚ vytvorila rámec na podporu dohľadu nad kozmickým priestorom a sledovania tohto priestoru[27], aby tieto prostriedky vo vlastníctve členských štátov prepojila s cieľom zabezpečiť služby dohľadu nad kozmickým priestorom a jeho sledovania[28] pre určených používateľov (členské štáty, orgány a inštitúcie EÚ, vlastníkov a prevádzkovateľov vesmírnych lodí a orgány civilnej ochrany). V súvislosti s vytvorením kozmickej stratégie pre Európu Komisia preskúma jej ďalší rozvoj, aby bolo možné monitorovať hybridné hrozby pre kozmické infraštruktúry.

Družicové komunikačné systémy (SatComs) predstavujú kľúčové nástroje na riadenie kríz, reakciu na katastrofy, policajný, pohraničný a pobrežný dohľad. Tvoria kostru rozsiahlych infraštruktúr, ako sú dopravné a kozmické systémy alebo diaľkovo riadené letecké systémy. V súlade s výzvou Európskej rady týkajúcou sa prípravy budúcej generácie družicovej komunikácie v rámci štátnej správy (GovSatCom) Komisia v spolupráci s Európskou obrannou agentúrou posudzuje možné spôsoby zdieľania dopytu v kontexte novej kozmickej stratégie a akčného plánu v oblasti európskej obrany.

Mnohé kritické infraštruktúry potrebujú na synchronizáciu svojich sietí (napríklad energetika a telekomunikácie) alebo transakcií s časovou pečiatkou (napríklad finančné

[24] Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: Stratégia v oblasti letectva pre Európu [COM(2015) 0598 final, 7.12.2015].
[25] V decembri 2014 Rada prijala akčný plán pre vykonávanie stratégie námornej bezpečnosti Európskej únie; http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf
[26] Oznámenie Komisie Európskemu parlamentu, Rade a Európskemu hospodárskemu a sociálnemu výboru – Stratégia EÚ pre riadenie colných rizík: Riešenie rizík, posilnenie bezpečnosti dodávateľského reťazca a uľahčenie obchodu, COM(2014) 527 final.
[27] Pozri rozhodnutie Európskeho parlamentu a Rady 541/2014/EÚ.
[28] Ako sú varovania na účely zabránenia kolízii na obežnej dráhe, varovania týkajúce sa rozpadu alebo kolízie a riskantných vstupov vesmírnych objektov nazad do atmosféry Zeme.

trhy) presné časové údaje. Závislosť od jediného signálu časovej synchronizácie globálneho družicového navigačného systému nezaručuje odolnosť potrebnú na boj proti hybridným hrozbám. Európsky globálny družicový navigačný systém Galileo by mohol ponúknuť druhý spoľahlivý zdroj časových údajov.

Opatrenie č. 8: V kontexte novej 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.

4.2. Obranná spôsobilosť

Na zvýšenie odolnosti EÚ proti hybridným hrozbám je potrebné posilniť obrannú spôsobilosť. Treba určiť najdôležitejšie oblasti, ako sú schopnosti sledovania a vyhľadávania informácií. Európska obranná agentúra by mohla byť katalyzátorom rozvoja vojenských kapacít, ktoré sa týkajú hybridných hrozieb (napríklad skrátením cyklov vývoja obranných schopností, investíciami do technológií, systémov a prototypov, sprístupnením inovatívnych obchodných technológií pre obranný priemysel). Prípadné opatrenia by sa mohli preskúmať v rámci nového akčného plánu v oblasti európskej obrany.

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 význam EÚ konkrétne v boji proti hybridným hrozbám namiereným proti jednému alebo viacerým členským štátom.

4.3. Ochrana verejného zdravia a potravinová bezpečnosť

Zdravie obyvateľov by mohlo byť ohrozené manipuláciou s prenosnými chorobami alebo kontamináciou potravín, pôdy, vzduchu a pitnej vody chemickými, biologickými, rádiologickými a jadrovými látkami (CBRN). Okrem toho môže úmyselné šírenie chorôb zvierat alebo rastlín vážne ohroziť potravinovú bezpečnosť Únie a mať významné hospodárske a sociálne následky pre kľúčové články potravinového reťazca v EÚ. Existujúce štruktúry EÚ na ochranu zdravia, životného prostredia a bezpečnosti potravín možno využiť na reakciu na hybridné hrozby používajúce uvedené metódy.

Podľa právnych predpisov EÚ týkajúcich sa cezhraničných zdravotných hrozieb[29] existujúce mechanizmy koordinujú pripravenosť na závažné cezhraničné ohrozenia zdravia a prepájajú členské štáty, agentúry EÚ a vedecké výbory[30] prostredníctvom systému včasného varovania a reakcie. Výbor pre zdravotnú bezpečnosť, ktorý

[29] Rozhodnutie Európskeho parlamentu a Rady č. 1082/2013/EÚ z 22. októbra 2013 o závažných cezhraničných ohrozeniach zdravia, ktorým sa zrušuje rozhodnutie č. 2119/98/ES (Ú. v. EÚ L 293, 5.11.2013).

[30] Rozhodnutie Komisie C(2015) 5383 zo 7. augusta 2015 o zriadení vedeckých výborov v oblasti verejného zdravia, bezpečnosti spotrebiteľov a životného prostredia.

koordinuje reakciu členských štátov na hrozby, môže fungovať ako kontaktné miesto pre zraniteľnosť v oblasti verejného zdravia[31] s cieľom začleniť hybridné hrozby (najmä bioterorizmus) do usmernení pre krízovú komunikáciu a do nácviku budovania kapacít (simulácia krízy) s členskými štátmi. Pokiaľ ide o bezpečnosť potravín, príslušné orgány si prostredníctvom systému rýchleho varovania pre potraviny a krmivá (RASFF) a spoločného colného systému na riadenie rizík (CRMS) vymieňajú informácie o analýze rizík, aby mohli monitorovať zdravotné riziká, ktoré predstavujú kontaminované potraviny. Pokiaľ ide o zdravie zvierat a rastlín, prieskum právneho rámca EÚ[32] do súboru existujúcich nástrojov [33]doplní nové prvky, aby bol lepšie pripravený aj na hybridné hrozby.

Opatrenie č. 10: ***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.***

4.4. Kybernetická bezpečnosť

EÚ vo významnej miere profituje zo svojej prepojenej a digitalizovanej spoločnosti. Kybernetické útoky by mohli narušiť digitálne služby v celej EÚ a tieto útoky by mohli využívať pôvodcovia hybridných hrozieb. Zvýšená odolnosť komunikačných a informačných systémov v Európe má význam pre podporu jednotného digitálneho trhu. Stratégia kybernetickej bezpečnosti EÚ a Európsky program v oblasti bezpečnosti predstavujú celkový strategický rámec pre iniciatívy EÚ v oblasti kybernetickej bezpečnosti a kybernetickej kriminality. EÚ sa aktívne zapája do tvorby mechanizmov na zvyšovanie informovanosti, mechanizmov spolupráce a reakcie v rámci plnenia stratégie kybernetickej bezpečnosti. Riziká pre kybernetickú bezpečnosť v rámci širokej škály poskytovateľov hlavných služieb v oblasti energetiky, dopravy, financií a zdravotnej starostlivosti sa riešia konkrétne v navrhovanej smernici o bezpečnosti sietí a informácií (BSI)[34]. Títo poskytovatelia, rovnako ako poskytovatelia kľúčových digitálnych služieb (napr. cloud computing), by mali prijať vhodné bezpečnostné opatrenia a ohlasovať vnútroštátnym orgánom závažné incidenty, pričom je vždy potrebné uviesť prípadný hybridný charakter incidentu. Keď spoluzákonodarcovia uvedenú smernicu prijmú, jej skutočnou transpozíciou a vykonávaním sa posilnia kapacity v oblasti kybernetickej bezpečnosti vo všetkých členských štátoch a ich spolupráca v oblasti kybernetickej

[31] V súlade s rozhodnutím Európskeho parlamentu a Rady č. 1082/2013/EÚ z 22. októbra 2013 o závažných cezhraničných ohrozeniach zdravia, ktorým sa zrušuje rozhodnutie č. 2119/98/ES (Ú. v. EÚ L 293/1).

[32] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/429 z 9. marca 2016 o prenosných chorobách zvierat a zmene a zrušení určitých aktov v oblasti zdravia zvierat („právna úprava v oblasti zdravia zvierat“) (Ú. v. EÚ L 84, 31.3.2016). Pokiaľ ide o nariadenie Európskeho parlamentu a Rady o ochranných opatreniach proti škodcom rastlín („právne predpisy o zdraví rastlín“), 16. decembra 2015 sa podarilo dosiahnuť politickú dohodu medzi Európskym parlamentom a Radou na znení tohto textu.

[33] Napríklad banky vakcín EÚ, dômyselný elektronický informačný systém pre choroby zvierat, prísnejšia povinnosť prijímať opatrenia pre laboratóriá a ďalšie subjekty, ktoré sa zaoberajú patogénmi.

[34] Komisiou predložený návrh smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii, COM(2013) 48 final, 7.2.2013. Rada EÚ a Európsky parlament dosiahli politickú dohodu, pokiaľ ide o túto navrhovanú smernicu, a smernica by mala byť čoskoro formálne prijatá.

bezpečnosti bude intenzívnejšia vďaka výmene informácií a osvedčených postupov v oblasti boja proti hybridným hrozbám. V smernici sa konkrétne stanovuje zriadenie siete 28 vnútroštátnych tímov pre reakciu na incidenty v oblasti počítačovej bezpečnosti (CSIRT) a tímu CERT-EU[35] na účely dobrovoľnej operačnej spolupráce.

S cieľom podporiť spoluprácu verejného a súkromného sektora a celoeurópskych prístupov v oblasti kybernetickej bezpečnosti Komisia zriadila platformu pre bezpečnosť sietí a a informácií (BSI), ktorá vydáva usmernenia s osvedčenými postupmi pre riadenie rizík. Kým členské štáty určujú bezpečnostné požiadavky a postupy oznamovania incidentov, ktoré sa vyskytnú v jednotlivých štátoch, Komisia vyzýva na vyššiu mieru zbližovania prístupov k riadeniu rizík a opiera sa pritom najmä o Agentúru Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA).

<u>Opatrenie č. 11</u>: Komisia vyzýva členské štáty, aby prioritne zriadili sieť 28 tímov CSIRT a tímu CERT-EU 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 o sieťovej a informačnej bezpečnosti, aby bolo možné zdieľať informácie, znalosti a rýchle reakcie.

4.4.1. Priemysel

Keďže sa čoraz viac využívajú služby ako cloud computing a big data, zvyšuje sa aj zraniteľnosť hybridnými hrozbami. Stratégia pre jednotný digitálny trh stanovuje zmluvné partnerstvo verejného a súkromného sektora v oblasti kybernetickej bezpečnosti[36], ktoré má byť zamerané na výskum a inovácie a má pomôcť Európskej únii zachovať vysokú úroveň technologických kapacít v tejto oblasti. Zmluvné verejno-súkromné partnerstvo vybuduje dôveru medzi jednotlivými účastníkmi trhu a bude rozvíjať súčinnosť medzi dopytom a ponukou. Zmluvné verejno-súkromné partnerstvo a súvisiace opatrenia sa síce budú zameriavať primárne na civilné produkty a služby kybernetickej bezpečnosti, výsledkom týchto iniciatív by však mala byť lepšia ochrana používateľov týchto technológií aj proti hybridným hrozbám.

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

4.4.2. Energetika

Vznik inteligentných domácností a spotrebičov a rozvoj inteligentných sietí a rastúca digitalizácia energetického systému tiež vedú k zvýšenej zraniteľnosti kybernetickými

[35] Tím pre reakciu na núdzové počítačové situácie pre inštitúcie EÚ (CERT-EU).
[36] Má sa začať v polovici roka 2016.

útokmi. Európska stratégia energetickej bezpečnosti[37] a stratégia pre energetickú úniu[38] podporujú prístup zohľadňujúci všetky riziká, do ktorého je začlenená aj odolnosť proti hybridným hrozbám. Tematická sieť pre ochranu kritickej energetickej infraštruktúry podporuje spoluprácu medzi subjektmi v odvetví energetiky (ropy, plynu, elektriny). Komisia spustila webovú platformu pre analýzu a výmenu informácií o hrozbách a incidentoch[39]. S cieľom obmedziť zraniteľnosť spoločne so zúčastnenými stranami[40] pracuje na vývoji komplexnej stratégie pre odvetvie energetiky v súvislosti s kybernetickou bezpečnosťou prevádzok inteligentných sietí. Zatiaľ čo trhy s elektrinou sú stále viac integrované, pravidlá a postupy pre riešenie krízových situácií ešte vždy určujú jednotlivé krajiny. Musíme zabezpečiť, aby vlády navzájom spolupracovali na príprave na krízové situácie a na prevencii a zmierňovaní rizík a aby sa všetci príslušní aktéri riadili spoločným súborom pravidiel.

<u>Opatrenie č. 13</u>: 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 zdieľanie informácií a zabezpečenie solidarity medzi členskými štátmi v čase krízy vrátane pravidiel týkajúcich sa prevencie a zmierňovania kybernetických útokov.

4.4.3. Zabezpečenie zdravých finančných systémov

Na to, aby hospodárstvo EÚ fungovalo, potrebuje bezpečné finančné a platobné systémy. Ochrana finančného systému a jeho infraštruktúry pred kybernetickými útokmi, bez ohľadu na motívy alebo povahu útočníka, má zásadný význam. Aby bolo možné čeliť hybridným hrozbám namiereným proti finančným službám v EÚ, musí príslušné odvetvie hrozbu pochopiť, musí mať otestovanú svoju obranu a disponovať technológiami nevyhnutnými na vlastnú ochranu pred útokmi. Rozhodujúci význam má preto zdieľanie informácií o hrozbách medzi účastníkmi finančných trhov a s príslušnými orgánmi a najdôležitejšími poskytovateľmi služieb alebo zákazníkmi, ktoré však musí byť bezpečné a spĺňať požiadavky ochrany údajov. V súlade s úsilím, ktoré sa vyvíja na medzinárodných fórach, vrátane práce skupiny G7 v tomto odvetví sa Komisia bude usilovať identifikovať faktory, ktoré bránia náležitému zdieľaniu informácií o hrozbách, a navrhne riešenia. Treba zabezpečiť pravidelné testovanie a vylepšovanie protokolov na ochranu podnikov a príslušných infraštruktúr, okrem iného neustálym zdokonaľovaním technológií zvyšujúcich bezpečnosť.

<u>Opatrenie č. 14</u>: Komisia bude v spolupráci s agentúrou ENISA[41], členskými štátmi, príslušnými medzinárodnými, európskymi a vnútroštátnymi orgánmi a finančnými inštitúciami podporovať a zjednodušovať platformy a siete pre zdieľanie informácií

[37] Oznámenie Komisie Európskemu parlamentu a Rade: Európska stratégia energetickej bezpečnosti – COM(2014) 0330 final.
[38] Oznámenie „Rámcová stratégia odolnej energetickej únie s výhľadovou politikou v oblasti zmeny klímy“ – COM(2015) 080 final.
[39] Stredisko EÚ pre zdieľanie informácií o hrozbách a incidentoch – ITIS.
[40] Vo forme platformy expertov kybernetickej bezpečnosti v odvetví energetiky (EECSP).
[41] Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť.

o hrozbách a bude sa zaoberať faktormi, ktoré výmenu informácií brzdia.

4.4.4. Doprava

Moderné dopravné systémy (železničné, cestné, letecká a námorná doprava) sú závislé od informačných systémov, ktoré sú voči kybernetickým útokom zraniteľné. Vzhľadom na cezhraničnú povahu týchto systémov si svoju osobitnú úlohu musí plniť EÚ. Komisia bude v spolupráci s členskými štátmi naďalej analyzovať kybernetické hrozby a riziká súvisiace s protiprávnymi zásahmi do dopravných systémov. Komisia v spolupráci s Európskou agentúrou pre bezpečnosť letectva (EASA)[42] pracuje na pláne pre kybernetickú bezpečnosť v letectve. Na kybernetické hrozby pre námornú bezpečnosť je zameraná aj stratégia námornej bezpečnosti Európskej únie a jej akčný plán.

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.

4.5. Boj proti financovaniu hybridných hrozieb

Pôvodcovia hybridných hrozieb potrebujú na svoje aktivity finančné prostriedky. Financovanie takýchto činností sa môže používať na podporu teroristických skupín alebo skrytejších foriem destabilizácie, ako je podpora nátlakových skupín a okrajových politických strán. EÚ zintenzívnila svoje úsilie v boji proti financovaniu trestnej činnosti a terorizmu, ako je uvedené v Európskom programe v oblasti bezpečnosti, najmä prostredníctvom akčného plánu[43]. V tejto súvislosti napomáha v boji proti financovaniu terorizmu a praniu špinavých peňazí najmä revidovaný európsky rámec proti praniu špinavých peňazí, ktorý uľahčuje vnútroštátnym finančným spravodajským jednotkám (FIU) identifikáciu a sledovanie podozrivých prevodov peňazí a výmenu informácií a súčasne zabezpečuje vystopovateľnosť prevodov finančných prostriedkov v Európskej únii. Preto by mohol prispieť aj k boju proti hybridným hrozbám. V rámci nástrojov SZBP by sa mohli preskúmať primerane upravené a účinné obmedzujúce opatrenia boja proti hybridným hrozbám.

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

[42] V súčasnosti Európsky parlament a Rada rokujú o návrhu nového nariadenia o agentúre EASA, ktorý Komisia predložila v decembri 2015. Návrh nariadenia Európskeho parlamentu a Rady o spoločných pravidlách v oblasti civilného letectva a o zriadení Agentúry Európskej únie pre bezpečnosť letectva, ktorým sa zrušuje nariadenie Európskeho parlamentu a Rady (ES) č. 216/2008 [COM(2015) 613 final, 2015/0277 (COD)].

[43] Oznámenie Komisie Európskemu parlamentu a Rade o akčnom pláne na posilnenie boja proti financovaniu terorizmu [COM(2016) 50 final].

4.6. Budovanie odolnosti proti radikalizácii a násilnému extrémizmu

Napriek tomu, že teroristické činy a násilný extrémizmus nemajú sami osebe hybridnú povahu, pôvodcovia hybridných hrozieb sa môžu zamerať na zraniteľných členov spoločnosti, vykonávať ich nábor a radikalizáciu prostredníctvom moderných komunikačných kanálov (vrátane internetových sociálnych médií a skupín priaznivcov) a propagandy.

Aby bolo možné zakročiť proti extrémistickému obsahu na internete, Komisia v rámci stratégie pre jednotný digitálny trh analyzuje potrebu potenciálnych nových opatrení, s náležitým ohľadom na ich vplyv na základné práva, ako je sloboda prejavu a informácií. Mohlo by to zahŕňať dôkladné postupy na odstraňovanie nelegálneho obsahu tak, aby sa pritom neodstránil zákonný obsah (tzv. „mechanizmy oznamovania protiprávneho obsahu a prijatia opatrení“), a väčšiu zodpovednosť a náležitú starostlivosť zo strany sprostredkovateľov pri riadení ich sietí a systémov. Predstavovalo by to doplnok k existujúcemu dobrovoľnému prístupu, v rámci ktorého spoločnosti prevádzkujúce internet a sociálne médiá (v rámci internetového fóra EÚ) a v spolupráci s jednotkou EÚ pre nahlasovanie internetového obsahu pri Europole urýchlene odstraňujú teroristickú propagandu.

V rámci Európskeho programu v oblasti bezpečnosti sa proti radikalizácii bojuje prostredníctvom výmeny skúseností a tvorby osvedčených postupov vrátane spolupráce v tretích krajinách. Poradný tím pre strategickú komunikáciu o Sýrii sa zameriava na posilnenie vývoja a šírenie alternatívnych správ s cieľom boja proti teroristickej propagande. Sieť EÚ na zvyšovanie povedomia o radikalizácii poskytuje pomoc členským štátom a expertom, ktorí prichádzajú do styku s radikalizovanými osobami (vrátane zahraničných teroristických bojovníkov) alebo s osobami, ktoré sa považujú za náchylné na radikalizáciu. Sieť na zvyšovanie povedomia o radikalizácii poskytuje odbornú prípravu a poradenstvo a ponúka podporu prioritným tretím krajinám, ktoré sú ochotné angažovať sa v tomto smere. Okrem toho Komisia posilňuje justičnú spoluprácu medzi aktérmi v oblasti trestného súdnictva vrátane Eurojustu na účely boja proti terorizmu a radikalizácii vo všetkých členských štátoch vrátane stretávania sa so zahraničnými teroristickými bojovníkmi a tými, ktorí sa vrátili z cudziny.

Tým, že EÚ dopĺňa uvedené prístupy v rámci svojej **vonkajšej činnosti**, prispieva k boju proti násilnému extrémizmu, okrem iného aj prostredníctvom vonkajšej angažovanosti a informačných činností, prevencie (boj proti radikalizácii a financovaniu terorizmu), ako aj prostredníctvom opatrení na riešenie základných hospodárskych, politických a spoločenských faktorov, ktoré poskytujú teroristickým skupinám príležitosť na rozvoj.

<u>Opatrenie č. 17:</u> 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.

4.7. Posilnenie spolupráce s tretími krajinami

Ako sa zdôrazňuje v Európskom programe v oblasti bezpečnosti, EÚ venuje zvýšenú pozornosť budovaniu kapacít v oblasti bezpečnosti v ***partnerských krajinách*** okrem iného tým, že vychádza zo vzájomnej previazanosti prvkov bezpečnosti a rozvoja, a rozpracúva bezpečnostný rozmer revidovanej európskej susedskej politiky[44]. Tieto opatrenia môžu prispieť aj k posilneniu odolnosti partnerov proti hybridným činnostiam.

Komisia má v pláne ďalej prehlbovať výmenu operatívnych a strategických informácií s krajinami procesu rozširovania a v rámci Východného partnerstva a južného susedstva, aby im pomohla v boji proti organizovanej trestnej činnosti, terorizmu, nelegálnej migrácii a obchodu s ľahkými zbraňami. Pokiaľ ide o boj proti terorizmu, EÚ posilňuje spoluprácu s tretími krajinami tým, že začala realizovať intenzívnejšie dialógy o bezpečnosti a akčné plány.

Cieľom nástrojov na financovanie vonkajšej činnosti je budovanie fungujúcich a zodpovedných inštitúcií v tretích krajinách[45], ktoré sú nevyhnutným predpokladom pre účinnú reakciu na bezpečnostné hrozby a pre posilňovanie odolnosti. V tejto súvislosti sú kľúčovými nástrojmi reforma sektora bezpečnosti a budovanie kapacít na podporu bezpečnosti a rozvoja[46]. V rámci nástroja na podporu stability a mieru[47] vypracovala Komisia opatrenia na posilnenie kybernetickej odolnosti a schopností partnerov, ktoré sú potrebné na odhaľovanie kybernetických útokov a kybernetickej kriminality a na zodpovedajúcu reakciu na ne a ktorými je možné potláčať hybridné hrozby v tretích krajinách. EÚ financuje činnosti v oblasti budovania kapacít v partnerských krajinách s cieľom zmierniť bezpečnostné riziká súvisiace s látkami CBRN[48].

Členské štáty by napokon v duchu komplexného prístupu ku krízovému riadeniu mohli používať nástroje a misie spoločnej bezpečnostnej a obrannej politiky (SBOP) buď samostatne alebo ako doplnenie zavedených nástrojov EÚ, aby pomohli svojim partnerom s posilňovaním ich kapacít. Mohli by sa zvážiť tieto opatrenia: i) podpora strategickej komunikácie, ii) poradenstvo pre ministerstvá vystavené hybridným hrozbám, iii) dodatočná podpora pre riadenie hraníc v prípade núdzových situácií.

---

[44] Spoločné oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov – Preskúmanie európskej susedskej politiky [JOIN(2015) 50 final, 18.11.2015].

[45] Tamže; Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: Stratégia rozširovania EÚ [COM(2015) 611 final, 10.11.2015]. Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: Zvyšovanie vplyvu rozvojovej politiky EÚ: program zmien [KOM(2011) 637 v konečnom znení, 13.10.2011].

[46] Spoločné oznámenie „Budovanie kapacít na podporu bezpečnosti a rozvoja – umožnenie partnerom predchádzať krízam a zvládať ich“ [JOIN(2015) 17 final].

[47] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 230/2014 z 11. marca 2014, ktorým sa ustanovuje nástroj na podporu stability a mieru (Ú. v. EÚ L 77/1, 15.3.2014).

[48] Medzi príslušné oblasti patrí monitorovanie hraníc, krízové riadenie, prvá reakcia, kontroly nedovoleného vývozu tovaru s dvojakým použitím, sledovanie a kontroly chorôb, nukleárna forenzná veda, obnova po mimoriadnych udalostiach a ochrana rizikových zariadení. Osvedčené postupy, ktoré sú výsledkom uplatnenia nástrojov vytvorených v rámci akčného plánu EÚ v oblasti CBRN, napríklad európske vzdelávacie stredisko pre jadrovú bezpečnosť a účasť EÚ v medzinárodnej pracovnej skupine pre sledovanie hraníc, je možné zdieľať aj s tretími krajinami.

Preskúmať by sa mohli ďalšie synergie medzi nástrojmi SBOP a aktérmi v oblasti bezpečnosti, ciel a justície vrátane príslušných agentúr EÚ[49], Interpolu a európskych žandárskych síl v súlade s ich mandátmi.

<u>Opatrenie č. 18</u>: Vysoká predstaviteľka v koordinácii s Komisiou začne prieskum týkajúci sa hybridných hrozieb 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.

5. PREVENCIA, REAKCIA NA KRÍZU A OBNOVA

Ako sa uvádza v oddiele 3.1, cieľom navrhovaného strediska EÚ pre hybridné hrozby je analyzovať príslušné ukazovatele v súvislosti s prevenciou hybridných hrozieb a reakciou na ne a informovať subjekty EÚ s rozhodovacou právomocou. Zraniteľné miesta je možné posilniť 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. Podpora vnútroštátnych opatrení a kapacít v oblasti civilnej ochrany prostredníctvom Európskeho koordinačného centra pre reakcie na núdzové situácie[50] by mohla predstavovať účinný mechanizmus reakcie na aspekty hybridných hrozieb, ktoré si vyžadujú reakciu v oblasti civilnej ochrany. Dalo by sa to dosiahnuť v koordinácii s ďalšími mechanizmami reakcie a systémami včasného varovania v EÚ, najmä so situačným strediskom ESVČ pre vonkajší rozmer bezpečnosti a centrom pre strategickú analýzu a reakciu v oblasti vnútornej bezpečnosti.

Doložka o solidarite (článok 222 ZFEÚ) umožňuje konať na úrovni Únie, ako aj na úrovni členských štátov, ak sa členský štát stane cieľom teroristického útoku alebo obeťou prírodnej či človekom spôsobenej katastrofy. Opatrenie Únie na pomoc členskému štátu sa realizuje uplatnením rozhodnutia Rady 2014/415/EU[51]. Dojednania o koordinácii v Rade by mali vychádzať z integrovanej politickej reakcie EÚ na krízu[52]. Na základe týchto dojednaní Komisia a vysoká predstaviteľka (v rámci svojich právomocí) identifikujú príslušné nástroje Únie a predkladajú Rade návrhy rozhodnutí o mimoriadnych opatreniach.

Článok 222 ZFEÚ je určený aj na situácie, ktoré zahŕňajú priamu pomoc od jedného alebo viacerých členských štátov členskému štátu, ktorý sa stal obeťou teroristického

[49] EUROPOL, FRONTEX, CEPOL, EUROJUST.
[50] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en.
[51] Rozhodnutie Rady 2014/415/EÚ o podrobnostiach vykonávania doložky o solidarite Úniou (Ú. v. EÚ L 192, 1.7.2014, s. 53).
[52] http://www.consilium.europa.eu/en/documents-publications/publications/2014/eu-ipcr/

útoku alebo katastrofy. V takom prípade sa rozhodnutie Rady 2014/415/EU neuplatňuje. Vzhľadom na nejednoznačnosť spojenú s hybridnými činnosťami by Komisia a vysoká predstaviteľka (vrámci svojich právomocí) mali posúdiť prípadné uplatnenie doložky o solidarite ako poslednej možnosti v prípade, že sa niektorý členský štát EÚ stane obeťou značných hybridných hrozieb.

Na rozdiel od článku 222 ZFEÚ, pokiaľ niekoľkonásobné závažné hybridné hrozby zahŕňajú ozbrojenú agresiu proti niektorému členskému štátu EÚ, bolo by možné na účely primeranej a včasnej reakcie uplatniť článok 42 ods. 7 ZEÚ. Rozsiahle a závažné prejavy hybridných hrozieb si môžu vyžadovať aj intenzívnejšiu spoluprácu a koordináciu s NATO.

Členské štáty sa vyzývajú, aby počas prípravy svojich síl brali do úvahy potenciálne hybridné hrozby. Aby členské štáty boli schopné prijímať rýchle a účinné rozhodnutia v prípade hybridného útoku, musia organizovať pravidelné praktické a politické cvičenia, aby otestovali schopnosť prijímať rozhodnutia na vnútroštátnej aj medzinárodnej úrovni. Cieľom by bolo stanoviť spoločný operačný protokol medzi členskými štátmi, Komisiou a vysokou predstaviteľkou, v ktorom by sa opísali účinné postupy, ktorými sa treba riadiť v prípade hybridnej hrozby, a síce od začiatočnej fázy identifikácie až po konečnú fázu útoku, a úlohy každého orgánu či inštitúcie Únie a každého účastníka tohto procesu.

Ako dôležitý prvok SBOP by sa mohli ponúknuť: a) civilná a vojenská odborná príprava, b) poradné misie na zlepšenie bezpečnostnej a obrannej kapacity ohrozeného štátu, c) pohotovostné plánovanie s cieľom identifikovať signály hybridných hrozieb a posilnenie schopností včasného varovania, d) podpora riadenia ochrany hraníc v prípade mimoriadnej situácie a e) podpora v špecifických oblastiach, ako je zmierňovanie rizík CBRN a nebojová evakuácia.

<u>Opatrenie č. 19</u>: 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.

<u>Opatrenie č. 20</u>: 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.

<u>Opatrenie č. 21</u>: 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.

6. POSILNENIE SPOLUPRÁCE S NATO

Hybridné hrozby predstavujú problém nielen pre EÚ, ale aj pre ostatné významné partnerské organizácie vrátane Organizácie spojených národov (OSN), Organizácie pre bezpečnosť a spoluprácu v Európe (OBSE), a najmä NATO. Účinná reakcia si vyžaduje

dialóg a koordináciu medzi týmito organizáciami na politickej aj operačnej úrovni. Užšia spolupráca by EÚ a NATO umožnila lepšie sa pripraviť a účinne reagovať na hybridné hrozby, vzájomne sa dopĺňať a podporovať na základe zásady začlenenia a zároveň rešpektovať autonómiu oboch organizácií pri rozhodovaní a pravidlá ochrany údajov.

Tieto dve organizácie zdieľajú spoločné hodnoty a stretávajú sa s podobnými problémami. Členské štáty EÚ a spojenci NATO očakávajú, že tieto organizácie sa budú v prípade krízy navzájom podporovať a konať rýchlo, rozhodne a koordinovane, alebo v ideálnom prípade zabránia vzniku krízy. Identifikovalo sa niekoľko oblastí vhodných na užšiu spoluprácu a koordináciu medzi EÚ a NATO, okrem iného situačné povedomie, kybernetická bezpečnosť strategických komunikačných štruktúr a prevencia kríz a reakcia na ne. Prebiehajúci neformálny dialóg medzi EÚ a NATO na tému hybridných hrozieb by mal byť intenzívnejší, aby tieto dve organizácie mohli synchronizovať svoje aktivity.

S cieľom vypracovať spoločnú reakciu EÚ/NATO je potrebné, aby obidve organizácie mali pred krízou a počas nej o situácii rovnaký prehľad. Mohlo by sa to dosiahnuť prostredníctvom pravidelného zdieľania analýz a získaných skúseností, ale aj prostredníctvom priamej spolupráce medzi strediskom EÚ pre hybridné hrozby a strediskom NATO pre hybridné hrozby. Pre rýchlu a účinnú reakciu je zároveň dôležité informovať sa navzájom o príslušných postupoch v oblasti krízového riadenia. Odolnosť by sa mohla posilniť zabezpečením doplnkovosti pri stanovovaní spoločných štandardov pre kritické súčasti ich infraštruktúr, ako aj úzkej spolupráce v oblasti strategickej komunikácie a kybernetickej obrany. Úplne inkluzívne spoločné cvičenia na politickej aj technickej úrovni by prispeli k zvýšeniu rozhodovacích kapacít týchto dvoch organizácií. Využitie ďalších príležitostí na odbornú prípravu by pomohlo vytvoriť porovnateľnú úroveň znalostí v kritických oblastiach.

<u>Opatrenie č. 22</u>: 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.

7. ZÁVERY

Toto spoločné oznámenie 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. Keďže cieľom je najmä **zlepšiť informovanosť**, navrhuje sa, aby sa vytvorili osobitné mechanizmy na výmenu informácií s členskými štátmi a koordinovala sa kapacita EÚ na strategické komunikácie. Jednotlivými opatreniami sa má **budovať odolnosť** v oblastiach, ako je kybernetická bezpečnosť, kritická infraštruktúra, ochrana finančného systému pred nezákonným využívaním a boj proti násilnému extrémizmu a radikalizácii. V každej z týchto oblastí bude kľúčovým prvým krokom vykonávanie dohodnutých stratégií zo strany EÚ a členských štátov, ako aj úplné vykonávanie

existujúcich právnych predpisov členskými štátmi, pričom boli navrhnuté aj určité konkrétnejšie opatrenia na ďalšie posilnenie tohto úsilia.

Pokiaľ ide o **prevenciu hybridných hrozieb, reakciu na ne a obnovu po nich**, navrhuje sa, aby sa preskúmala uskutočniteľnosť uplatnenia doložky o solidarite stanovenej v článku 222 ZFEÚ (špecifikovanej v príslušných rozhodnutiach) a článku 42 ods. 7 ZEÚ v prípade rozsiahlych a závažných hybridných útokov. Strategická rozhodovacia právomoc by sa mohla posilniť vytvorením spoločného operačného protokolu.

Napokon sa navrhuje, aby sa **posilnila spolupráca** a **koordinácia medzi EÚ a NATO** v spoločnom boji proti hybridným hrozbám.

Vysoká predstaviteľka a Komisia sú odhodlané na účely vykonania tohto spoločného rámca mobilizovať príslušné nástroje EÚ, ktoré majú k dispozícii. Dôležité je, aby EÚ spolu s členskými štátmi pracovala na minimalizácii rizík spojených s vystavením štátnych a neštátnych subjektov hybridným hrozbám.