PARLAMENT ČESKÉ REPUBLIKY

SENÁT

10. funkční období

K 082 / 10

Společné sdělení Evropskému parlamentu a Radě Společný rámec pro boj proti hybridním hrozbám Reakce Evropské unie

(73. týden)

2016

Rada
Evropské unie

Brusel 7. dubna 2016
(OR. en)

7688/16

COPS 102	**PROCIV 21**
CSDP/PSDC 193	**CYBER 31**
CFSP/PESC 282	**EF 75**
JAI 263	**ECOFIN 272**
POLMIL 33	**ENER 100**
EUMC 39	**POLMAR 1**
CIVCOM 60	**TRANS 97**
COEST 86	**ESPACE 20**
COAFR 97	**SAN 121**
COTER 33	**CSC 88**

PRŮVODNÍ POZNÁMKA

Odesílatel:	Jordi AYET PUIGARNAU, ředitel, za generálního tajemníka Evropské komise
Datum přijetí:	7. dubna 2016
Příjemce:	Jeppe TRANHOLM-MIKKELSEN, generální tajemník Rady Evropské unie
Č. dok. Komise:	JOIN(2016) 18 final
Předmět:	SPOLEČNÉ SDĚLENÍ EVROPSKÉMU PARLAMENTU A RADĚ Společný rámec pro boj proti hybridním hrozbám Reakce Evropské unie

Delegace naleznou v příloze dokument JOIN(2016) 18 final.

Příloha: JOIN(2016) 18 final

EVROPSKÁ
KOMISE

VYSOKÁ PŘEDSTAVITELKA
UNIE PRO ZAHRANIČNÍ
VĚCI A BEZPEČNOSTNÍ
POLITIKU

V Bruselu dne 6.4.2016
JOIN(2016) 18 final

SPOLEČNÉ SDĚLENÍ EVROPSKÉMU PARLAMENTU A RADĚ

Společný rámec pro boj proti hybridním hrozbám

Reakce Evropské unie

1. ÚVOD

Bezpečnostní situace Evropské unie se v posledních letech dramaticky změnila. Problémy se zajištěním míru a stability ve východním a jižním sousedství EU svědčí i nadále o tom, že Unie musí přizpůsobit a znásobit své kapacity, aby mohla splnit svou úlohu zajišťovatele bezpečnosti, a zaměřit se přitom zejména na vzájemnou provázanost mezi vnější a vnitřní bezpečností. Mnoho problémů v oblasti zajišťování míru, bezpečnosti a prosperity způsobuje v současné době nestabilita v zemích, jež bezprostředně sousedí s EU, a proměnlivý charakter hrozeb. Předseda Evropské komise Jean-Claude Juncker zdůraznil ve svých politických směrech z roku 2014, že je nutné „pracovat na posílení Evropy, pokud jde o záležitosti bezpečnosti a obrany" a skloubit evropské a národní nástroje efektivněji než v minulosti. Také vysoká představitelka věnovala v návaznosti na výzvu Rady pro zahraniční věci ze dne 18. května 2015 v úzké spolupráci s útvary Komise a Evropskou obrannou agenturou (EDA) a po konzultaci s členskými státy EU své úsilí tomu, aby představila tento společný rámec obsahující realizovatelné návrhy pro boj proti hybridním hrozbám a pro posílení odolnosti EU a jejích členských států i partnerů[1]. Evropská rada v červnu 2015 připomněla, že pro účely boje proti hybridním hrozbám je nutné mobilizovat nástroje EU[2].

Definice hybridních hrozeb jsou sice různé a musí zůstat flexibilní, aby mohly reagovat na proměnlivou povahu těchto hrozeb, ovšem jde o to vystihnout soubor různých nátlakových a podvratných činností a konvenčních i nekonvenčních metod (např. diplomatických, vojenských, ekonomických a technologických), které mohou různí státní i nestátní aktéři koordinovaným způsobem využívat k tomu, aby dosáhli konkrétních cílů, aniž by formálně vyhlásili válku. Snahou je obvykle využívat zranitelnosti cíle a vytvářet nepřehledné situace s cílem narušit rozhodovací procesy. Nástrojem těchto hybridních hrozeb mohou být masivní dezinformační kampaně a využívání sociálních médií k propagandě nebo k radikalizaci, náboru a přímému ovládání příznivců.

Jelikož boj proti hybridním hrozbám souvisí s národní bezpečností a obranou a zachováním práva a veřejného pořádku, hlavní odpovědnost nesou členské státy, neboť jednotlivé slabiny jsou většinou specifické pro jednotlivé země. Mnoho členských států EU se však potýká i se společnými hrozbami, jejichž cílem mohou být rovněž přeshraniční sítě nebo infrastruktury. Takovým hrozbám je možné účinněji čelit pomocí koordinované reakce na úrovni EU, a sice prostřednictvím politik a nástrojů EU, využitím evropské solidarity, vzájemné pomoci a plného potenciálu Lisabonské smlouvy. Politiky a nástroje EU mohou hrát – a ve významné míře již hrají – zásadní úlohu při zvyšování informovanosti. Tím se zlepšuje schopnost reakce členských států na společné hrozby. Vnější činnost Unie navrhovaná podle tohoto rámce odpovídá zásadám stanoveným v článku 21 Smlouvy o Evropské unii (SEU), mezi něž patří demokracie,

[1] Závěry Rady o společné bezpečnostní a obranné politice (SBOP), květen 2015 [Consilium 8971/15].
[2] Závěry Evropské rady, červen 2015 [EUCO 22/15].

právní stát, univerzálnost a nedělitelnost lidských práv a dodržování zásad Charty Organizace spojených národů a mezinárodního práva[3].

Cílem tohoto společného sdělení je usnadnit vznik komplexního přístupu, který umožní Evropské unii v koordinaci s členskými státy bojovat s konkrétními hrozbami hybridní povahy tím, že všechny příslušné nástroje budou fungovat v součinnosti a zlepší se spolupráce mezi všemi příslušnými aktéry[4]. Navrhovaná opatření vycházejí ze stávajících strategií a odvětvových politik, které přispívají k dosažení větší bezpečnosti. Mezi nástroje, které tak mohou rovněž napomoci v boji proti hybridním hrozbám, patří zejména Evropský program pro bezpečnost[5], nová globální strategie Evropské unie pro pro zahraniční a bezpečnostní politiku a Akční plán pro evropskou obranu[6], Strategie kybernetické bezpečnosti EU[7], strategie energetické bezpečnosti[8] a strategie Evropské unie pro námořní bezpečnost[9].

Jelikož proti hybridním hrozbám bojuje i NATO a jelikož Rada pro zahraniční věci navrhla posílit spolupráci a koordinaci v této oblasti, cílem některých návrhů je upevnit spolupráci mezi EU a NATO v oblasti boje proti hybridním hrozbám.

Navrhovaná reakce se zaměřuje na tyto prvky: zlepšování informovanosti, posilování odolnosti, prevence, reakce na krize a zotavení.

2. IDENTIFIKACE HYBRIDNÍ POVAHY HROZBY

Hybridní hrozby využívají zranitelnosti určité země a často se snaží oslabit základní demokratické hodnoty a svobody. Vysoká představitelka a Komise budou v první řadě spolupracovat s členskými státy, aby získaly více informací o situaci, a to prostřednictvím sledování a posuzování rizik, která mohou hrozit na zranitelných místech v EU. Komise vyvíjí metody pro hodnocení bezpečnostních rizik, které mají poskytovat informace subjektům s rozhodovací pravomocí a podporovat vytváření politik na základě hodnocení rizik v oblastech sahajících od bezpečnosti leteckého provozu až po financování terorismu a praní peněz. Kromě toho by bylo vhodné provést v členských státech průzkum za účelem identifikace oblastí náchylných k hybridním hrozbám. Jeho cílem by bylo určit ukazatele hybridních hrozeb, začlenit je do mechanismů včasného varování a stávajících mechanismů pro hodnocení rizik a v případě potřeby je sdílet.

<u>Opatření č. 1</u>: Členské státy, případně s podporou Komise a vysoké představitelky, se vyzývají k tomu, aby zahájily průzkum týkající se hybridních rizik s cílem určit hlavní

[3] V okamžiku, kdy orgány a členské státy provádí právní předpisy Unie, je pro ně závazná Listina základních práv EU.
[4] Případné legislativní návrhy budou podléhat požadavkům Komise na zlepšování právní úpravy, a to v souladu s pokyny Komise pro zlepšování právní úpravy, SWD(2015) 111.
[5] COM(2015) 185 final.
[6] Měly by být předloženy v roce 2016.
[7] Politický rámec EU pro kybernetickou obranu [Consilium 15585/14] a společné sdělení s názvem „Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor“, únor 2013 [JOIN(2013)1].
[8] Společné sdělení s názvem „Evropská strategie energetické bezpečnosti“, květen 2014 [SWD(2014) 330].
[9] Společné sdělení s názvem „Za otevřenou a bezpečnou globální námořní oblast: prvky pro námořní bezpečnostní strategii Evropské unie“ – JOIN(2014) 9 final – 6. března 2014.

slabiny, včetně konkrétních ukazatelů hybridních hrozeb, které mohou potenciálně ovlivnit vnitrostátní a celoevropské struktury a sítě.

3. ORGANIZACE REAKCE NA ÚROVNI EU: ZLEPŠOVÁNÍ INFORMOVANOSTI

3.1 Středisko EU pro hybridní hrozby

Je velmi důležité, aby EU v koordinaci s členskými státy měla dostatek informací o situaci, aby mohla odhalit jakoukoli změnu v oblasti bezpečnosti týkající se hybridní činnosti vyvíjené státními a/nebo nestátními aktéry. Abychom mohli proti hybridním hrozbám bojovat účinně, je třeba zlepšit výměnu informací a podporovat sdílení příslušných zpravodajských informací napříč odvětvími a mezi Evropskou unií, jejími členskými státy a partnery.

Středisko EU pro hybridní hrozby zřízené v rámci Střediska Evropské unie pro analýzu zpravodajských informací (EU INTCEN) Evropské služby pro vnější činnost (dále jen „ESVČ“) se zaměří na analýzu hybridních hrozeb. Toto středisko bude shromažďovat, analyzovat a sdílet utajované informace a informace z otevřených zdrojů, které se konkrétně týkají ukazatelů a varování v souvislosti s hybridními hrozbami, od různých zúčastněných stran v rámci ESVČ (včetně delegací EU), Komise (včetně agentur EU[10]) a členských států. Ve spolupráci s podobnými stávajícími subjekty na úrovni EU[11] a na vnitrostátní úrovni by zmíněné středisko analyzovalo vnější aspekty hybridních hrozeb, které postihují EU a její sousedy, aby bylo možné urychleně vyhodnotit relevantní incidenty a zajistit informace nutné pro strategické rozhodovací procesy v EU, mimo jiné tím, že bude poskytovat informace potřebné pro hodnocení bezpečnostních rizik prováděná na úrovni EU. Analytické výstupy tohoto střediska by byly zpracovávány a bylo by s nimi nakládáno v souladu s pravidly Evropské unie pro ochranu utajovaných informací a údajů[12]. Středisko by mělo udržovat spojení s již existujícími subjekty na úrovni EU a na vnitrostátní úrovni. Členské státy by měly zřídit národní kontaktní místa propojená se střediskem EU pro hybridní hrozby. Zaměstnanci uvnitř i mimo EU (včetně těch, kteří jsou vysláni do delegací, operací a misí EU) a v členských státech by měli být rovněž proškoleni, aby dokázali rozeznat první signály hybridních hrozeb.

<u>Opatření č. 2</u>: Vytvořit v rámci stávající struktury EU INTCEN středisko EU pro hybridní hrozby, které bude schopné shromažďovat a analyzovat utajované informace a informace z otevřených zdrojů o hybridních hrozbách. Členské státy se vyzývají k tomu, aby zřídily národní kontaktní místa pro hybridní hrozby s cílem zajistit spolupráci a komunikaci se střediskem EU pro hybridní hrozby.

[10] V souladu s jejich mandáty.
[11] Například Evropské centrum pro boj proti kyberkriminalitě a Evropské centrum pro boj proti terorismu v rámci Europolu, agentura Frontex, skupina EU pro reakci na počítačové hrozby ((CERT)-EU).
[12] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995.

3.2 Strategická komunikace

Pachatelé hybridních hrozeb mohou systematicky šířit falešné informace, mimo jiné prostřednictvím cílených kampaní v sociálních médiích, a tím se snažit o radikalizaci jednotlivců, destabilizaci společnosti a politickou propagandu. Zásadní význam má proto schopnost reagovat na hybridní hrozby prostřednictvím spolehlivé **strategické komunikace**. Odolnost společnosti je možné posílit zejména tím, že budou zajištěny okamžité konkrétní reakce a že se zlepší veřejné povědomí o hybridních hrozbách.

Strategická komunikace by měla plně využívat nástrojů sociálních medií, jakož i tradičních audio- a videomédií a internetových médií. ESVČ by měla v návaznosti na aktivity pracovních skupin East StratCom a Arab StratCom optimalizovat využívání lingvistů plynně ovládajících relevantní jazyky zemí mimo EU a odborníků na sociální média, kteří mohou monitorovat informace ze zemí mimo EU a zajistit cílenou komunikaci, která by reagovala na šíření falešných informací. Členské státy by navíc měly vypracovat koordinované mechanismy pro strategickou komunikaci na podporu zjišťování původu falešných informací a boje proti nim, aby hybridní hrozby byly odhaleny.

<u>Opatření č. 3</u>: Vysoká představitelka spolu s členskými státy prozkoumá možnosti, jak aktualizovat a koordinovat kapacity pro aktivní strategickou komunikaci a jak optimalizovat využití jazykových odborníků a monitorování médií.

3.3 Středisko excelence pro boj proti hybridním hrozbám

Na základě zkušeností některých členských států a partnerských organizací[13] by jedna nadnárodní instituce nebo síť takových institucí mohla fungovat jako středisko excelence, které se bude zabývat řešením hybridních hrozeb. Takové středisko by se mohlo zaměřit na výzkum využívání hybridních strategií a mohlo by podnítit rozvoj nových konceptů a technologií v rámci soukromého i průmyslového sektoru s cílem pomoci členským státům při posilování jejich odolnosti. Výzkum by mohl přispět ke sladění politik, doktrín a koncepcí EU a jednotlivých států, a zajistit, aby při rozhodování bylo možné zohlednit složitost a nejednoznačnost spojenou s hybridními hrozbami. Toto středisko by mělo navrhovat programy podporující výzkum a výcvik s cílem nalézt praktická řešení stávajících problémů způsobených hybridními hrozbami. Práce tohoto střediska by vycházela z odborných znalostí jeho spolupracovníků z různých zemí a oborů, z civilního i vojenského a soukromého i akademického sektoru.

Toto středisko by mohlo úzce spolupracovat s již existujícími středisky excelence EU[14] a NATO[15], aby bylo možné využít informací o hybridních hrozbách, jež byly získány prostřednictvím kybernetické obrany, strategické komunikace, civilně-vojenské spolupráce, energetické a krizové reakce.

[13] Střediska excelence NATO.
[14] Např. Ústav EU pro studium bezpečnosti (EU ISS), tematická střediska excelence EU v oblasti CBRN.
[15] http://www.nato.int/cps/en/natohq/topics_68372.htm.

<u>Opatření č. 4</u>: Členské státy se vyzývají, aby zvážily zřízení střediska excelence pro boj proti hybridním hrozbám.

4. ORGANIZACE REAKCE NA ÚROVNI EU: POSÍLENÍ ODOLNOSTI

Odolnost je schopnost odolávat stresu a zotavit se a poučit se z problematických situací. Aby bylo možné bojovat proti hybridním hrozbám účinně, je třeba řešit potenciální slabá místa nejdůležitějších infrastruktur, dodavatelských řetězců a společnosti. S využitím nástrojů a politik EU lze posílit odolnost infrastruktury na úrovni EU.

4.1 Ochrana kritické infrastruktury

Je nutné chránit kritické infrastruktury (například dodavatelské řetězce energií a dopravu), protože nekonvenční útok ze strany původců hybridních hrozeb na jakýkoli „měkký cíl“ by mohl způsobit vážný ekonomický nebo sociální rozvrat. Aby byla zajištěna ochrana kritické infrastruktury, poskytuje Evropský program na ochranu kritické infrastruktury[16] (EPCIP) meziodvětvový systémový přístup, který zohledňuje veškerá rizika, soustředí se na vzájemnou provázanost a funguje na základě prevence, připravenosti a reakce. Směrnice o evropských kritických infrastrukturách[17] zavádí postup pro určování a označování evropských kritických infrastruktur (EKI) a společný přístup pro posouzení potřeby zvýšit jejich ochranu. Zejména by se podle této směrnice mělo obnovit úsilí k posílení odolnosti kritických infrastruktur v oblasti dopravy (například hlavních letišť a obchodních přístavů v EU). Komise posoudí, zda je vhodné vypracovat společné nástroje, včetně ukazatelů, pro zlepšení odolnosti kritických infrastruktur proti hybridním hrozbám ve všech příslušných odvětvích.

<u>Opatření č. 5</u>: Komise ve spolupráci s členskými státy a zúčastněnými stranami identifikuje společné nástroje, včetně ukazatelů, pro zlepšení ochrany a odolnosti kritických infrastruktur proti hybridním hrozbám v příslušných odvětvích.

4.1.1 Energetické sítě

Nerušená výroba a distribuce energie má pro EU zásadní význam a významné výpadky energie by mohly způsobit škody. Zásadním prvkem v boji proti hybridním hrozbám je další diverzifikace zdrojů energie v EU, jejích dodavatelů a tras, aby se zajistily bezpečnější a odolnější dodávky energie. Komise rovněž provádí posouzení rizik a bezpečnosti (tzv. zátěžové testy) jaderných elektráren EU. Pro zajištění diverzifikace energetických zdrojů se zintenzivňuje úsilí Strategie pro energetickou unii: například jižní koridor pro přepravu plynu, který umožní dopravu plynu z oblasti Kaspického moře do Evropy, a zbudování terminálů pro zkapalněný zemní plyn s více dodavateli v severní Evropě. Tento příklad je třeba následovat i ve střední a východní Evropě

[16] Sdělení Komise o Evropském programu na ochranu kritické infrastruktury, 12.12.2006, KOM(2006) 786 v konečném znění.

[17] Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu (Úř. věst. L 345, 23.12.2008).

a ve Středomoří, kde se takový terminál právě vyvíjí[18]. K dosažení tohoto cíle rovněž pozitivně přispěje vývoj trhu se zkapalněným zemním plynem.

Pokud jde o jaderný materiál a jaderná zařízení, Komise podporuje tvorbu a přijímání nejvyšších bezpečnostních norem, které posilují odolnost. Komise vyzývá k jednotnému provádění a uplatňování směrnice o jaderné bezpečnosti[19], která stanoví pravidla pro předcházení haváriím a zmírnění jejich následků, a ustanovení směrnice o základních bezpečnostních standardech[20] týkající se mezinárodní spolupráce v oblasti havarijní připravenosti a odezvy na havarijní situaci, zejména mezi sousedními členskými státy a se sousedními zeměmi.

Opatření č. 6: Komise ve spolupráci s členskými státy podpoří úsilí o diverzifikaci zdrojů energie a bude prosazovat normy v oblasti bezpečnosti a zabezpečení s cílem zvýšit odolnost jaderných infrastruktur.

4.1.2 Bezpečnost dopravy a dodavatelských řetězců

Doprava má pro fungování Unie zásadní význam. Hybridní útoky na dopravní infrastrukturu (jako jsou letiště, silniční infrastruktura, přístavy a železnice) mohou mít závažné důsledky vedoucí k narušení dopravy a dodavatelských řetězců. V rámci provádění předpisů o letecké a námořní bezpečnosti[21] organizuje Komise pravidelné inspekce[22] a prostřednictvím své práce v oblasti bezpečnosti pozemní dopravy se snaží řešit hybridní hrozby. V této souvislosti je rámec EU projednáván v revidovaném nařízení o bezpečnosti letectví[23] jakožto součást strategie pro evropské letectví[24]. Kromě toho se hrozbami pro námořní bezpečnost zabývá strategie Evropské unie pro námořní bezpečnost a její akční plán[25]. Tento plán umožňuje EU a jejím členským státům komplexně řešit problémy v oblasti námořní bezpečnosti, včetně boje proti hybridním hrozbám, a to díky meziodvětvové spolupráci mezi civilními a vojenskými subjekty pro účely ochrany kritické námořní infrastruktury, celosvětového dodavatelského řetězce, námořního obchodu a mořských přírodních zdrojů a zdrojů energie. Bezpečnost

---

[18] Informace o pokroku, jehož bylo dosud dosaženo, jsou uvedeny ve Zprávě o stavu energetické unie za rok 2015 (COM(2015) 572 final).

[19] Směrnice Rady 2009/71/Euratom ze dne 25. června 2009, kterou se stanoví rámec Společenství pro jadernou bezpečnost jaderných zařízení, ve znění směrnice Rady 2014/87/Euratom ze dne 8. července 2014.

[20] Směrnice Rady 2013/59/Euratom ze dne 5. prosince 2013, kterou se stanoví základní bezpečnostní standardy ochrany před nebezpečím vystavení ionizujícímu záření a zrušují se směrnice 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom a 2003/122/Euratom.

[21] Nařízení Evropského parlamentu a Rady (ES) č. 300/2008 ze dne 11. března 2008 o společných pravidlech v oblasti ochrany civilního letectví před protiprávními činy a o zrušení nařízení (ES) č. 2320/2002. Prováděcí nařízení Komise (EU) 2015/1998 ze dne 5. listopadu 2015, kterým se stanoví prováděcí opatření ke společným základním normám letecké bezpečnosti. Směrnice Evropského parlamentu a Rady 2005/65/ES ze dne 26. října 2005 o zvýšení zabezpečení přístavů. Nařízení Evropského parlamentu a Rady (ES) č. 725/2004 ze dne 31. března 2004 o zvýšení bezpečnosti lodí a přístavních zařízení.

[22] Podle práva EU je Komise povinna provádět inspekce, aby zajistila, že členské státy řádně provedou požadavky na leteckou a námořní bezpečnost. Jedná se mimo jiné o inspekce příslušného orgánu v členském státě a kontroly na letištích, v přístavech, u leteckých dopravců, lodí a subjektů provádějících bezpečnostní opatření. Cílem inspekcí Komise je zajistit, aby členské státy v úplnosti provedly normy EU.

[23] Nařízení Komise (EU) 2016/4 ze dne 5. ledna 2016, kterým se mění nařízení Evropského parlamentu a Rady (ES) č. 216/2008, pokud jde o hlavní požadavky na ochranu životního prostředí. Nařízení (ES) č. 216/2008 ze dne 20. února 2008 o společných pravidlech v oblasti civilního letectví a o zřízení Evropské agentury pro bezpečnost letectví.

[24] Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: Strategie pro evropské letectví (COM/2015/0598 final, 7.12.2015).

[25] V prosinci 2014 přijala Rada akční plán pro provádění strategie Evropské unie pro námořní bezpečnost; http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf

mezinárodního dodavatelského řetězce je rovněž předmětem strategie a akčního plánu Evropské unie pro řízení rizik v oblasti cel[26].

<u>Opatření č. 7</u>: Komise bude monitorovat vznikající hrozby v celém odvětví dopravy a ve vhodných případech bude aktualizovat právní předpisy. Při provádění strategie a akčního plánu EU pro námořní bezpečnost a strategie a akčního plánu EU pro řízení rizik v oblasti cel přezkoumá Komise a vysoká představitelka (v rámci svých pravomocí) ve spolupráci s členskými státy, jak reagovat na hybridní hrozby, zejména ty, které se týkají kritické dopravní infrastruktury.

4.1.3 Vesmír

Hybridní hrozby by se mohly zaměřit na vesmírné infrastruktury, což by mělo dopad na mnoho odvětví. EU vytvořila rámec na podporu pozorování a sledování vesmíru[27], aby tato aktiva, jež jsou ve vlastnictví členských států, propojila, aby byly zajištěny služby pozorování a sledování vesmíru[28] určeným uživatelům (členským státům, orgánům a institucím EU, vlastníkům a provozovatelům kosmických lodí a orgánům civilní ochrany). V souvislosti s vytvořením kosmické strategie pro Evropu Komise prozkoumá její další rozvoj, aby bylo možné monitorovat hybridní hrozby pro vesmírné infrastruktury.

Zásadními nástroji pro řízení krizí, reakci na katastrofy, policejní, pohraniční a pobřežní dohled jsou družicové komunikační systémy (SatComs). Jsou páteří rozsáhlých infrastruktur, jako jsou dopravní a kosmické systémy nebo systémy dálkově řízených letadel. V souladu s výzvou Evropské rady týkající se přípravy příští generace družicové komunikace v rámci státní správy (GovSatCom) posuzuje Komise ve spolupráci s Evropskou obrannou agenturou způsoby, jak sdílet poptávku v kontextu nové kosmické strategie a evropského obranného akčního plánu.

Mnoho kritických infrastruktur potřebuje k synchronizaci svých sítí (např. energetika a telekomunikace) nebo transakcí s časovým razítkem (např. finanční trhy) přesné časové údaje. Závislost na jediném signálu časové synchronizace globálního družicového navigačního systému nezajišťuje odolnost nutnou pro boj proti hybridním hrozbám. Evropský globální družicový navigační systém Galileo by mohl nabídnout druhý spolehlivý zdroj pro časové údaje.

<u>Opatření č. 8</u>: V kontextu nové kosmické strategie a evropského obranného akčního plánu navrhne Komise posílit odolnost vesmírných infrastruktur proti hybridním hrozbám, zejména případným rozšířením působnosti pozorování a sledování vesmíru tak, aby do ní byly zahrnuty hybridní hrozby, dále přípravu příští generace GovSatCom

[26] Sdělení Komise Evropskému parlamentu, Radě a Evropskému hospodářskému a sociálnímu výboru o strategii a akčním plánu EU pro řízení rizik v oblasti cel: čelit rizikům, posilovat bezpečnost dodavatelského řetězce a usnadňovat obchod (COM(2014) 527 final).
[27] Viz rozhodnutí Evropského parlamentu a Rady 541/2014/EU.
[28] Jako jsou varování pro účely zabránění kolize na oběžné dráze, varování ohledně rozpadu nebo kolize a riskantních vstupů vesmírných objektů zpět do zemské atmosféry.

na evropské úrovni a použití systému Galileo u kritických infrastruktur, jež jsou závislé na časové synchronizaci.

4.2 Obranné schopnosti

Aby se zvýšila odolnost EU vůči hybridním hrozbám, je nutno posílit obranné schopnosti. Je třeba určit nejdůležitější oblasti, jako jsou schopnosti pro sledování a vyhledávání informací. Evropská obranná agentura by mohla být katalyzátorem rozvoje vojenských kapacit, které se týkají hybridních hrozeb (například zkrácením cyklů vývoje obranných schopností, investicemi do technologií, systémů a prototypů, zpřístupněním inovativních obchodních technologií pro obranný průmysl). Případná opatření by mohla být přezkoumána v rámci nového evropského obranného akčního plánu.

Opatření č. 9: Vysoká představitelka, v případě potřeby s podporou členských států a ve spolupráci s Komisí, navrhne projekty týkající se toho, jak přizpůsobit obranné schopnosti a význam EU konkrétně v boji proti hybridním hrozbám namířeným proti jednomu nebo několika členským státům.

4.3 Ochrana veřejného zdraví a potravinového zabezpečení

Zdraví obyvatel by mohlo být ohroženo manipulací s přenosnými nemocemi či kontaminací potravin, půdy, vzduchu a pitné vody chemickými, biologickými, radiologickými a jadernými látkami (tzv. látky CBRN). Kromě toho může úmyslné šíření nákaz zvířat či rostlin vážně ohrozit potravinové zabezpečení Unie a mít významné hospodářské a sociální dopady na klíčové články potravinového řetězce v EU. Stávající struktury EU pro ochranu zdraví, životního prostředí a bezpečnosti potravin lze využít pro reakci na hybridní hrozby používající uvedených metod.

Podle právních předpisů EU týkajících se přeshraničních zdravotních hrozeb[29] koordinují stávající mechanismy připravenost na vážné přeshraniční zdravotní hrozby a propojují členské státy, agentury EU a vědecké výbory[30] prostřednictvím systému včasného varování a reakce. Výbor pro zdravotní bezpečnost, který koordinuje reakci členských států na hrozby, může fungovat jako kontaktní místo pro zranitelnost v oblasti veřejného zdraví[31], začlenit hybridní hrozby (zejména bioterorismus) do pokynů pro krizovou komunikaci a do nácviku budování kapacit (simulace krize) s členskými státy. Pokud jde o bezpečnost potravin, příslušné orgány si prostřednictvím systému včasné výměny informací pro potraviny a krmiva (RASFF) a společného celního systému pro řešení rizik (CRMS) vyměňují informace o analýze rizik, aby mohly monitorovat zdravotní rizika, jež představují kontaminované potraviny. Pokud jde o zdraví zvířat a rostlin, doplní

[29] Rozhodnutí Evropského parlamentu a Rady č. 1082/2013/EU ze dne 22. října 2013 o vážných přeshraničních zdravotních hrozbách a o zrušení rozhodnutí č. 2119/98/ES (Úř. věst. L 293, 5.11.2013, s. 1).
[30] Rozhodnutí Komise C(2015) 5383 ze dne 7.8.2015 o zřízení vědeckých výborů v oblasti veřejného zdraví, bezpečnosti spotřebitele a životního prostředí.
[31] V souladu s rozhodnutím Evropského parlamentu a Rady č. 1082/2013/EU ze dne 22. října 2013 o vážných přeshraničních zdravotních hrozbách a o zrušení rozhodnutí č. 2119/98/ES (Úř. věst. L 293, s. 1).

přezkum právního rámce EU[32] do souboru stávajících nástrojů[33] nové prvky, aby byl lépe připraven také na hybridní hrozby.

Opatření č. 10: Komise bude ve spolupráci s členskými státy zlepšovat informovanost o hybridních hrozbách a odolnost vůči těmto hrozbám v rámci stávajících mechanismů připravenosti a koordinace, zejména v rámci Výboru pro zdravotní bezpečnost.

4.4 Kybernetická bezpečnost

EU významnou měrou profituje ze své propojené a digitalizované společnosti. Kybernetické útoky by mohly narušit digitální služby v celé EU a tyto útoky by mohli využívat původci hybridních hrozeb. Zvýšená odolnost komunikačních a informačních systémů v Evropě má význam pro podporu jednotného digitálního trhu. Strategie kybernetické bezpečnosti EU a Evropský program pro bezpečnost představují celkový strategický rámec pro iniciativy EU v oblasti kybernetické bezpečnosti a kyberkriminality. EU se aktivně zapojuje do tvorby mechanismů pro zvyšování informovanosti, mechanismů spolupráce a reakce v rámci plnění Strategie kybernetické bezpečnosti. Konkrétně se rizika pro kybernetickou bezpečnost u široké škály hlavních poskytovatelů služeb v oblasti energetiky, dopravy, financí a zdravotní péče řeší v navrhované směrnici o bezpečnosti sítí a informací[34]. Tito poskytovatelé, stejně jako poskytovatelé zásadních digitálních služeb (např. „cloud computingu“) by měli přijmout vhodná bezpečnostní opatření a hlásit vnitrostátním orgánům závažné incidenty, přičemž by měli zmínit jakýkoli náznak hybridní povahy incidentu. Jakmile bude uvedená směrnice přijata spoluzákonodárci, její efektivní provedení a uplatňování posílí kapacity v oblasti kybernetické bezpečnosti ve všech členských státech a jejich spolupráce v oblasti kybernetické bezpečnosti bude intenzivnější díky výměně informací a osvědčených postupů v oblasti boje proti hybridním hrozbám. Směrnice konkrétně stanoví zřízení sítě 28 vnitrostátních skupin pro reakci na incidenty v oblasti počítačové bezpečnosti (CSIRT) a skupiny CERT-EU[35] pro účely dobrovolné operativní spolupráce.

Za účelem podpory spolupráce veřejného a soukromého sektoru a celoevropských přístupů v oblasti kybernetické bezpečnosti zřídila Komise platformu pro bezpečnost sítí a informací (NIS), která vydává pokyny s osvědčenými postupy pro řízení rizik. Zatímco členské státy stanoví bezpečnostní požadavky a postupy, jak oznamovat incidenty, k nimž došlo v jednotlivých státech, Komise vybízí k vyšší míře sbližování přístupů k řízení rizik a opírá se přitom zejména o Agenturu Evropské unie pro bezpečnost sítí a informací (ENISA).

[32] Nařízení Evropského parlamentu a Rady (EU) 2016/429 o nákazách zvířat a o změně a zrušení některých aktů v oblasti zdraví zvířat („právní rámec pro zdraví zvířat“) (Úř. věst. L 84, 31.3.2016). Pokud jde o nařízení Evropského parlamentu a Rady o ochranných opatřeních proti škodlivým organismům rostlin („právní rámec pro zdraví rostlin“), dne 16. prosince 2015 bylo dosaženo politické dohody mezi Evropským parlamentem a Radou o znění tohoto textu.

[33] Například banky očkovacích látek EU, moderní elektronický informační systém pro nákazy zvířat, přísnější povinnost přijímat opatření pro laboratoře a další subjekty, které se zabývají patogeny.

[34] Návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii (COM(2013) 48 final – 7.2.2013), který předložila Komise. Rada EU a Evropský parlament dosáhly politické dohody, pokud jde o tuto navrhovanou směrnici, a směrnice by měla být brzy formálně přijata.

[35] Skupina pro reakci na počítačové hrozby (CERT-EU) pro orgány EU.

<u>Opatření č. 11</u>: Komise vyzývá členské státy, aby prioritně zřídily síť 28 skupin CSIRT a skupiny CERT-EU a plně ji využívaly rovněž jako rámec pro strategickou spolupráci. Komise by ve spolupráci s členskými státy měla zajistit, aby odvětvové iniciativy v oblasti kybernetických hrozeb (např. v oblasti letectví, energetiky a v námořní oblasti) byly v souladu s kapacitami jednotlivých odvětví, na něž se vztahuje směrnice o bezpečnosti sítí a informací, aby bylo možné sdílet informace, znalosti a rychlé reakce.

4.4.1 Průmysl

Jelikož se stále více využívají služby jako cloud computing a data velkého objemu, zvyšuje se i zranitelnost vůči hybridním hrozbám. Strategie pro jednotný digitální trh stanoví smluvní partnerství veřejného a soukromého sektoru v oblasti kybernetické bezpečnosti[36], které se zaměří na výzkum a inovace a pomůže Evropské unii zachovat vysokou úroveň technologických kapacit v této oblasti. Smluvní partnerství veřejného a soukromého sektoru vybuduje důvěru mezi jednotlivými účastníky trhu a bude rozvíjet součinnost mezi poptávkou a nabídkou. Smluvní partnerství veřejného a soukromého sektoru a doprovodná opatření se sice primárně zaměří na civilní produkty a služby kybernetické bezpečnosti, výsledkem těchto iniciativ by však měla být lepší ochrana uživatelů těchto technologií také proti hybridním hrozbám.

<u>Opatření č. 12</u>: Komise bude v koordinaci s členskými státy v rámci smluvního partnerství veřejného a soukromého sektoru pro kybernetickou bezpečnost spolupracovat s průmyslem na vývoji a zkoušení technologií, aby uživatelé a infrastruktury byli lépe chráněni před kybernetickými aspekty hybridních hrozeb.

4.4.2 Energetika

Vznik inteligentních domácností a spotřebičů a rozvoj inteligentních sítí a rostoucí digitalizace energetického systému také vedou ke zvýšené zranitelnosti vůči kybernetickým útokům. Evropská strategie energetické bezpečnosti[37] a Strategie pro energetickou unii[38] podporují přístup zohledňující veškerá rizika, do nějž je začleněna také odolnost vůči hybridním hrozbám. Tématická síť pro ochranu kritické energetické infrastruktury podporuje spolupráci mezi subjekty v odvětví energetiky (ropy, plynu, elektřiny). Komise spustila webovou platformu pro analýzu a výměnu informací o hrozbách a incidentech[39]. Aby omezila zranitelnost, společně se zúčastněnými stranami[40] také vypracovává komplexní strategii pro odvětví energetiky ohledně kybernetické bezpečnosti při operacích inteligentních sítí. Zatímco trhy s elektřinou jsou stále více integrované, pravidla a postupy pro řešení krizových situací stále ještě určují jednotlivé země. Musíme zajistit, aby vlády vzájemně spolupracovaly při přípravě na

[36] Bude zahájeno v polovině roku 2016.
[37] Sdělení Komise Evropskému parlamentu a Radě: Evropská strategie energetické bezpečnosti – COM/2014/0330 final.
[38] Sdělení s názvem „Rámcová strategie k vytvoření odolné energetické unie s pomocí progresivní politiky v oblasti změny klimatu“ – COM/2015/080 final.
[39] Středisko EU pro sdílení informací o hrozbách a incidentech – ITIS.
[40] V podobě platformy odborníků na kybernetickou bezpečnost v odvětví energetiky (EECSP).

krizové situace, prevenci a zmírňování rizik a aby se všichni příslušní aktéři řídili společným souborem pravidel.

<u>Opatření č. 13</u>: Komise vydá pokyny pro vlastníky aktiv inteligentních sítí ke zvýšení kybernetické bezpečnosti jejich zařízení. V rámci iniciativy o uspořádání trhu s elektřinou zváží Komise možnost, že navrhne plány připravenosti na rizika a procesní pravidla pro sdílení informací a zajištění solidarity mezi členskými státy v době krize, včetně pravidel týkajících se prevence a zmírňování kybernetických útoků.

4.4.3 Zajištění zdravých finančních systémů

Hospodářství EU ke svému fungování potřebuje, aby finanční a platební systémy byly bezpečné. Ochrana finančního systému a jeho infrastruktury před kybernetickými útoky, bez ohledu na motivy či povahu útočníka, má zásadní význam. Aby bylo možné čelit hybridním hrozbám namířeným proti finančním službám v EU, musí dané odvětví hrozbě rozumět, mít otestovánu svou obranu a disponovat technologiemi nezbytnými pro svoji ochranu před útoky. Zásadní význam má proto sdílení informací o hrozbách mezi účastníky finančních trhů a s příslušnými orgány a nejdůležitějšími poskytovateli služeb nebo zákazníky, avšak musí být bezpečné a splňovat požadavky na ochranu údajů. V souladu s úsilím, jež je vyvíjeno na mezinárodních fórech, včetně práce skupiny G7 v tomto odvětví, se Komise bude snažit identifikovat faktory, které brání náležitému sdílení informací o hrozbách, a navrhne řešení. Je nutné zajistit pravidelné testování a vylepšování protokolů na ochranu podniků a příslušných infrastruktur, mimo jiné neustálým zdokonalováním technologií zvyšujících bezpečnost.

<u>Opatření č. 14</u>: Komise bude ve spolupráci s agenturou ENISA[41], členskými státy, příslušnými mezinárodními, evropskými a vnitrostátními orgány a finančními institucemi podporovat a zjednodušovat platformy a sítě pro sdílení informací a bude se zabývat faktory, které výměnu informací brzdí.

4.4.4 Doprava

Moderní dopravní systémy (železniční, silniční, letecká a námořní doprava) jsou závislé na informačních systémech, které jsou zranitelné vůči kybernetickým útoků. Vzhledem k přeshraniční povaze těchto systémů zde musí svou úlohu sehrát EU. Komise bude ve spolupráci s členskými státy nadále analyzovat kybernetické hrozby a rizika související s protiprávními zásahy do dopravních systémů. Komise ve spolupráci s Evropskou agenturou pro bezpečnost letectví (EASA)[42] pracuje na plánu pro kybernetickou bezpečnost v letectví. Kybernetickými hrozbami pro námořní bezpečnost se zabývá rovněž strategie Evropské unie pro námořní bezpečnost a její akční plán.

[41] Agentura Evropské unie pro bezpečnost sítí a informací.

[42] V současné době projednává Evropský parlament a Rada návrh nového nařízení o agentuře EASA, který Komise předložila v prosinci 2015. Návrh nařízení Evropského parlamentu a Rady o společných pravidlech v oblasti civilního letectví a o zřízení Agentury Evropské unie pro bezpečnost letectví, kterým se ruší nařízení Evropského parlamentu a Rady (ES) č. 216/2008 (COM(2015) 613 final, 2015/0277 (COD)).

<u>Opatření č. 15</u>: Komise a vysoká představitelka (v rámci svých pravomocí) v koordinaci s členskými státy přezkoumají, jak reagovat na hybridní hrozby, zejména na kybernetické útoky v odvětví dopravy.

4.5 Boj proti financování hybridních hrozeb

Původci hybridních hrozeb potřebují pro své aktivity finanční prostředky. Finance mohou být použity na podporu teroristických skupin nebo subtilnějších forem destabilizace, jako je podpora nátlakových skupin a okrajových politických stran. EU zintenzivnila své úsilí v boji proti financování trestné činnosti a terorismu, jak je uvedeno v Evropském programu pro bezpečnost, zejména prostřednictvím akčního plánu[43]. V této souvislosti napomáhá v boji proti financování terorismu a praní peněz zejména revidovaný evropský rámec proti praní peněz, který usnadňuje vnitrostátním finančním zpravodajským jednotkám (FIU) identifikaci a sledování podezřelých převodů peněz a výměnu informací a současně zajišťuje dohledatelnost převodů finančních prostředků v Evropské unii. Mohl by tedy rovněž přispět k boji proti hybridním hrozbám. V rámci nástrojů SZBP by mohla být prozkoumána vhodně upravená a účinná omezující opatření k boji proti hybridním hrozbám.

<u>Opatření č. 16</u>: Komise využije provádění akčního plánu pro boj proti financování terorismu k tomu, aby přispěl také k boji proti hybridním hrozbám.

4.6 Posilování odolnosti proti radikalizaci a násilnému extremismu

Přestože teroristické činy a násilný extremismus nemají samy o sobě hybridní povahu, původci hybridních hrozeb se mohou zaměřit na zranitelné členy společnosti, rekrutovat je a radikalizovat prostřednictvím moderních komunikačních kanálů (včetně internetových sociálních médií a skupin příznivců) a propagandy.

Aby bylo možné zakročit proti extremistickému obsahu na internetu, analyzuje Komise v rámci strategie pro jednotný digitální trh potřebu potenciálních nových opatření, s náležitým ohledem na jejich dopad na základní práva, jako je svoboda projevu a informací. To by mohlo zahrnovat důkladné postupy pro odstraňování nelegálního obsahu a současné zabraňování tomu, aby byl zničen zákonný obsah (tzv. „mechanismy pro oznámení protiprávního obsahu a přijetí opatření“), a větší odpovědnost a náležitou péči ze strany zprostředkovatelů při řízení jejich sítí a informačních systémů. Představovalo by to doplněk ke stávajícímu dobrovolnému přístupu, kdy společnosti provozující internet a sociální média (zejména v rámci internetového fóra EU) a ve spolupráci s jednotkou EU pro oznamování internetového obsahu při Europolu urychleně odstraňují teroristickou propagandu.

[43] Sdělení Komise Evropskému parlamentu a Radě o akčním plánu pro zesílení boje proti financování terorismu – (COM(2016) 50 final).

V rámci Evropského programu pro bezpečnost se proti radikalizaci bojuje prostřednictvím výměny zkušeností a tvorbou osvědčených postupů, včetně spolupráce ve třetích zemích. Poradní tým pro strategickou komunikaci ohledně Sýrie se zaměřuje na posílení vývoje a šíření alternativních zpráv s cílem boje proti teroristické propagandě. Síť pro zvyšování povědomí o radikalizaci poskytuje pomoc členským státům a odborníkům, kteří potřebují jednat s radikalizovanými osobami (včetně zahraničních teroristických bojovníků) nebo s osobami, které se považují za náchylné k radikalizaci. Síť pro zvyšování povědomí o radikalizaci poskytuje odbornou přípravu a poradenství a nabízí podporu prioritním třetím zemím, které jsou ochotny se v tomto směru angažovat. Kromě toho Komise posiluje justiční spolupráci mezi aktéry v oblasti trestního soudnictví, včetně Eurojustu, za účelem boje proti terorismu a radikalizaci ve všech členských státech, včetně zacházení se zahraničními teroristickými bojovníky a navrátivšími se bojovníky.

Tím, že EU doplňuje výše uvedené přístupy v rámci své **vnější činnosti**, přispívá k boji proti násilnému extremismu, mimo jiné i prostřednictvím vnější angažovanosti a informačních činností, prevence (boj proti radikalizaci a financování terorismu), jakož i prostřednictvím opatření k řešení základních hospodářských, politických a společenských faktorů, které poskytují teroristickým skupinám příležitost k rozvoji.

<u>Opatření č. 17:</u> Komise provádí opatření proti radikalizaci stanovená v Evropském programu pro bezpečnost a analyzuje potřebu posílit postupy pro odstraňování nelegálního obsahu, přičemž vybízí zprostředkovatele sítí a systémů k náležité péči při jejich řízení.

4.7 Posílení spolupráce s třetími zeměmi

Jak je zdůrazněno v Evropském programu pro bezpečnost, EU věnuje zvýšenou pozornost budování kapacit v oblasti bezpečnosti v ***partnerských zemích***, mimo jiné tím, že vychází ze vzájemné provázanosti prvků bezpečnosti a rozvoje, a rozpracovává bezpečnostní rozměr revidované evropské politiky sousedství[44]. Tato opatření mohou také posilovat odolnost partnerů vůči hybridním činnostem.

Komise hodlá dále prohlubovat výměnu operativních a strategických informací se zeměmi procesu rozšíření a v rámci Východního partnerství a jižního sousedství, aby jim pomohla v boji proti organizovanému zločinu, terorismu, nelegální migraci a obchodu s lehkými zbraněmi. Pokud jde o boj proti terorismu, EU posiluje spolupráci se třetími zeměmi tím, že zahájila intenzivní dialogy o bezpečnosti a akční plány.

Cílem unijních nástrojů vnějšího financování je budování fungujících a odpovědných institucí ve třetích zemích[45], které jsou nezbytným předpokladem pro účinnou reakci

[44] Společné sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů, Přezkum evropské politiky sousedství, 18.11.2015 (JOIN(2015) 50 final).

[45] Tamtéž. Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: Strategie rozšíření EU, 10.11.2015 (COM(2015) 611 final). Sdělení Komise

na bezpečnostní hrozby a pro posilování odolnosti. V této souvislosti jsou nejdůležitějšími nástroji reforma bezpečnostního sektoru a budování kapacit na podporu bezpečnosti a rozvoje[46]. V rámci nástroje přispívajícího ke stabilitě a míru[47] vypracovala Komise opatření na posílení kybernetické odolnosti a těch schopností partnerů, jež jsou nutné k odhalování kybernetických útoků a kyberkriminality a k odpovídající reakci a jež mohou potírat hybridní hrozby ve třetích zemích. EU financuje činnosti v oblasti budování kapacit v partnerských zemích s cílem zmírnit bezpečnostní rizika související s látkami CBRN[48].

Členské státy by v duchu komplexního přístupu k řízení krizí mohly použít nástroje a mise společné bezpečnostní a obranné politiky (SBOP), a to buď samostatně, nebo jako doplněk k již zavedeným nástrojům EU, aby pomohly svým partnerům při posilování jejich kapacit. Lze uvažovat o následujících opatřeních: i) podpora pro strategickou komunikaci, ii) poradenství pro ministerstva vystavená hybridním hrozbám, iii) dodatečná podpora pro správu hranic v případě nouzových situací. Dále by bylo možné zkoumat synergie mezi nástroji SBOP a aktéry v oblasti bezpečnosti, cel a justice, včetně příslušných agentur EU[49], Interpolu nebo Evropských policejních sil (v souladu s jejich mandáty).

<u>Opatření č. 18</u>: Vysoká představitelka v koordinaci s Komisí zahájí průzkum o hybridních hrozbách v sousedních regionech.

Vysoká představitelka, Komise a členské státy budou využívat nástroje, které mají k dispozici, pro účely budování kapacit svých partnerů a pro posílení jejich odolnosti proti hybridním hrozbám. Mise SBOP by mohly být využity (samostatně nebo jako doplněk nástrojů EU) na pomoc partnerům při posilování jejich kapacit.

5. PREVENCE, REAKCE NA KRIZE A ZOTAVENÍ

Jak je uvedeno v oddíle 3.1, cílem navrhovaného střediska EU pro hybridní hrozby je analyzovat příslušné ukazatele v souvislosti s předcházením hybridním hrozbám a reakcí na ně a informovat subjekty s rozhodovací pravomocí v EU. Slabá místa lze posílit prostřednictvím dlouhodobých politik na vnitrostátní úrovni i na úrovni EU, ale z krátkodobého hlediska je zásadně důležité posílit kapacity členských států a Unie pro

---

Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: Zvýšení dopadu rozvojové politiky EU: Agenda pro změnu, 13.10.2011 (KOM(2011) 637 v konečném znění).

[46] Společné sdělení s názvem „Budování kapacity na podporu bezpečnosti a rozvoje – umožnit partnerům předcházet krizím a zvládat je“ (JOIN(2015) 17 final).

[47] Nařízení Evropského parlamentu a Rady (EU) č. 230/2014 ze dne 11. března 2014, kterým se zřizuje nástroj přispívající ke stabilitě a míru (Úř. věst. L 77, 15.3.2014, s. 1).

[48] Mezi relevantní oblasti patří sledování hranic, řízení krizí, první reakce, kontroly nedovoleného vývozu zboží dvojího užití, sledování a kontroly nemocí, jaderné forenzní vědy, zotavení po mimořádných událostech a ochrana rizikových zařízení. Osvědčené postupy, jež jsou výsledkem uplatnění nástrojů vytvořených v rámci akčního plánu EU v oblasti CBRN, například evropské vzdělávací středisko pro jadernou bezpečnost a účast EU v mezinárodní Pracovní skupině pro sledování hranic, lze sdílet i se třetími zeměmi.

[49] EUROPOL, FRONTEX, CEPOL, EUROJUST.

prevenci hybridních hrozeb, reakci na ně a zotavení se po nich, a to rychle a koordinovaně.

Zásadní význam má rychlá reakce na události vyvolané hybridními hrozbami. Podpora vnitrostátních opatření a kapacit v oblasti civilní ochrany prostřednictvím evropského střediska pro koordinaci odezvy na mimořádné události[50] by mohlo představovat účinný mechanismus reakce na ty aspekty hybridních hrozeb, které vyžadují reakci v oblasti civilní ochrany. Toho by bylo možné dosáhnout v koordinaci s dalšími mechanismy reakce a systémy včasného varování v EU, zejména se situačním střediskem ESVČ pro vnější rozměr bezpečnosti a útvarem pro strategickou analýzu a reakci v oblasti vnitřní bezpečnosti.

Doložka solidarity (článek 222 SFEU) stanoví, že pokud je některý členský stát cílem teroristického útoku nebo obětí přírodní nebo člověkem způsobené pohromy, může Unie i členské státy mezi sebou přijmout opatření. Opatření Unie na pomoc členskému státu se realizuje použitím rozhodnutí Rady 2014/415/EU[51]. Ujednání o koordinaci v Radě by měla vycházet z integrované politické reakce EU na krize[52]. Na základě těchto ujednání identifikuje Komise a vysoká představitelka (v rámci svých pravomocí) příslušné nástroje Unie a předloží Radě návrhy rozhodnutí o mimořádných opatřeních.

Článek 222 SFEU rovněž řeší situace, které zahrnují přímou pomoc ze strany jednoho nebo více členských států členskému státu, který se stal obětí teroristického útoku nebo pohromy. V tomto případě se rozhodnutí Rady 2014/415/EU nepoužije. Vzhledem k nejednoznačnosti spojené s hybridními činnostmi by eventuální uplatnění doložky solidarity jako poslední možnosti v případě, že se některý členský stát EU stane obětí značných hybridních hrozeb, měla posoudit Komise a vysoká představitelka (v rámci svých pravomocí).

Na rozdíl od článku 222 SFEU, pokud několikanásobné závažné hybridní hrozby obnášejí ozbrojenou agresi vůči některému členskému státu EU, bylo by možné pro účely vhodné a včasné reakce použít čl. 42 odst. 7 SEU. Dalekosáhlé a závažné projevy hybridních hrozeb mohou rovněž vyžadovat intenzivnější spolupráci a koordinaci s NATO.

Členské státy se vyzývají, aby při přípravě svých sil braly v úvahu potenciální hybridní hrozby. Aby byly členské státy schopny přijmout rychlá a efektivní rozhodnutí v případě hybridního útoku, musí pořádat pravidelná praktická i politická cvičení, aby otestovaly schopnost přijímat rozhodnutí na vnitrostátní i mezinárodní úrovni. Cílem by bylo stanovit společný operační protokol mezi členskými státy, Komisí a vysokou představitelkou, v němž budou popsány účinné postupy, kterými je třeba se řídit v případě hybridní hrozby, a sice od počáteční fáze identifikace až po konečnou fázi útoku, a úlohy každého orgánu či instituce Unie a každého účastníka tohoto procesu.

[50] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en.
[51] Rozhodnutí Rady 2014/415/EU o způsobu provádění doložky solidarity Unií (Úř. věst. L 192, 1.7.2014, s. 53).
[52] http://www.consilium.europa.eu/cs/documents-publications/publications/2014/eu-ipcr/

Jako důležitý prvek SBOP by mohly být nabídnuty: a) civilní a vojenská odborná příprava, b) poradní mise ke zlepšení bezpečnostní a obranné kapacity ohroženého státu, c) pohotovostní plánování s cílem určit signály hybridních hrozeb a posílení schopností včasného varování, d) podpora řízení ochrany hranic v případě mimořádné situace a e) podpora ve specifických oblastech, jako je zmírňování rizik CBRN a nebojové evakuace.

Opatření č. 19: Vysoká představitelka a Komise v koordinaci s členskými státy vytvoří společný operační protokol a budou provádět pravidelná cvičení pro zdokonalení strategické rozhodovací kapacity v reakci na komplexní hybridní hrozby, a to v rámci postupů pro řízení krizí a integrované politické reakce na krize.

Opatření č. 20: Komise a vysoká představitelka (v rámci svých pravomocí) prozkoumají uplatnitelnost a praktické důsledky použití článku 222 SFEU a čl. 42 odst. 7 SEU v případech, kdy dojde k dalekosáhlým a závažným hybridním útokům.

Opatření č. 21: Vysoká představitelka v koordinaci s členskými státy bude rovněž integrovat, využívat a koordinovat možnosti vojenské akce v boji proti hybridním hrozbám v rámci společné bezpečnostní a obranné politiky.

6. POSÍLENÍ SPOLUPRÁCE S NATO

Hybridní hrozby představují problém nejen pro EU, ale i pro ostatní důležité partnerské organizace, včetně Organizace spojených národů (OSN), Organizace pro bezpečnost a spolupráci v Evropě (OBSE), a zejména NATO. Účinná reakce vyžaduje dialog a koordinaci mezi těmito organizacemi na politické i operační úrovni. Užší spolupráce by EU a NATO umožnila lépe se připravit a účinně reagovat na hybridní hrozby, vzájemně se doplňovat a podporovat na základě zásady začlenění a zároveň respektovat nezávislost obou organizací při rozhodování a pravidla pro ochranu údajů.

Tyto dvě organizace sdílejí společné hodnoty a potýkají se s podobnými problémy. Členské státy EU a spojenci NATO očekávají, že tyto organizace budou v případě krize jednat rychle, rozhodně a koordinovaně, nebo pokud možno krizi zabrání. Byla identifikována řada oblastí vhodných pro užší spolupráci a koordinaci mezi EU a NATO, mimo jiné situační orientace, kybernetická bezpečnost strategických komunikací a předcházení krizím a reakce na ně. Probíhající neformální dialog mezi EU a NATO na téma hybridních hrozeb by měl být intenzivnější, aby tyto dvě organizace mohly synchronizovat své aktivity.

Pro účely vypracování společné reakce EU/NATO je nutné, aby obě tyto organizace měly před krizí a během krize stejný přehled o situaci. Toho by mohlo být dosaženo prostřednictvím pravidelného sdílení analýz a získaných zkušeností, ale také prostřednictvím přímé spolupráce mezi střediskem EU pro hybridní hrozby a střediskem NATO pro hybridní hrozby. Pro rychlou a účinnou reakci je také důležité vzájemně se informovat o příslušných postupech řízení krizí. Odolnost by mohla být posílena

zajištěním doplňkovosti při stanovování společných standardů pro kritické součásti jejich infrastruktur, jakož i úzké spolupráce v oblasti strategické komunikace a kybernetické obrany. Plně inkluzivní společná cvičení na politické i technické úrovni by přispěla ke zvýšení rozhodovacích kapacit těchto dvou organizací. Využití dalších příležitostí k odborné přípravě by pomohlo vytvořit srovnatelnou úroveň znalostí v kritických oblastech.

Opatření č. 22: Vysoká představitelka bude v koordinaci s Komisí pokračovat v neformálním dialogu a bude při boji proti hybridním hrozbám posilovat spolupráci a koordinaci s NATO v oblastech situační orientace, strategické komunikace, kybernetické bezpečnosti a „předcházení krizím a reakce na ně", a to při respektování zásad inkluzivního a samostatného rozhodování každé organizace.

7. ZÁVĚRY

Toto společné sdělení nastiňuje návrhy, jejichž účelem je přispět k boji proti hybridním hrozbám a posílit odolnost na úrovni EU a na vnitrostátní úrovni, jakož i u partnerů. Jelikož cílem je zejména **zlepšit informovanost**, navrhuje se ustavit zvláštní mechanismy pro výměnu informací s členskými státy a koordinovat kapacitu EU pro strategické komunikace. Jednotlivá opatření mají **posilovat odolnost** v oblastech, jako je kybernetická bezpečnost, kritická infrastruktura, ochrana finančního systému před nezákonným využíváním a boj proti násilnému extremismu a radikalizaci. V každé z těchto oblastí bude zásadním prvním krokem provádění dohodnutých strategií ze strany EU a členských států, jakož i úplné provedení stávajících právních předpisů ze strany členských států, přičemž byla navržena i některá konkrétnější opatření pro další posílení těchto snah.

Pokud jde o **prevenci před hybridními hrozbami, reakci na ně a zotavení**, navrhuje se prozkoumat proveditelnost použití doložky solidarity stanovené v článku 222 SFEU (specifikované v příslušných rozhodnutích) a ustanovení čl. 42 odst. 7 SEU v případě dalekosáhlých a závažných hybridních útoků. Strategická rozhodovací pravomoc by mohla být posílena vytvořením společného operačního protokolu.

Kromě toho se navrhuje **posílit spolupráci** a **koordinaci mezi EU a NATO** při společném boji proti hybridním hrozbám.

Za účelem provedení tohoto společného rámce jsou vysoká představitelka a Komise odhodlány mobilizovat příslušné nástroje EU, které mají k dispozici. Je důležité, aby EU společně s členskými státy pracovaly na minimalizaci rizik spojených s expozicí možným hybridním hrozbám ze strany státních i nestátních aktérů.