EVROPSKÁ
KOMISE

VYSOKÁ PŘEDSTAVITELKA
UNIE PRO ZAHRANIČNÍ
VĚCI A BEZPEČNOSTNÍ
POLITIKU

V Bruselu dne 19.7.2017
JOIN(2017) 30 final

SPOLEČNÁ ZPRÁVA EVROPSKÉMU PARLAMENTU A RADĚ

o provádění společného rámce pro boj proti hybridním hrozbám – reakce Evropské unie

1. ÚVOD

EU stojí před největším úkolem v oblasti bezpečnosti ve své historii. Hrozby stále častěji nabývají méně obvyklých podob, některé probíhají ve skutečném světě, jako například nové formy terorismu, některé využívají digitální prostor ke složitým kybernetickým útokům. Jiné jsou rafinovanější a zaměřují na vyvíjení tlaku prostřednictvím dezinformačních kampaní a mediální manipulace. Snaží se otřást základními evropskými hodnotami, jako je lidská důstojnost, svoboda a demokracie. Nedávné koordinované kybernetické útoky, které zasáhly celý svět a u nichž je problematické určit pachatele, ukázaly, jak jsou naše společnost a naše instituce zranitelné.

Evropská komise a vysoká představitelka přijaly v dubnu 2016 společné sdělení o boji proti hybridním hrozbám[1] (dále jen „společný rámec“). Tento rámec zohledňuje přeshraniční a komplexní povahu hybridních hrozeb a navrhuje celostní vládní přístup, aby se posílila celková odolnost naší společnosti. Rada[2] iniciativu a navrhovaná opatření uvítala a vyzvala Komisi a vysokou představitelku k tomu, aby v červenci 2017 podaly zprávu o dosaženém pokroku. EU sice může členským státům pomoci při zvyšování jejich odolnosti proti hybridním hrozbám, ale hlavní odpovědnost nesou členské státy, jelikož boj proti hybridním hrozbám souvisí s národní bezpečností a obranou.

Tento společný rámec pro boj proti hybridním hrozbám tvoří důležitou část celkového integrovanějšího přístupu EU k bezpečnosti a obraně. Přispívá k budování Evropy, která chrání, po níž volal předseda Juncker ve svém projevu o stavu Unie ze září 2016. V roce 2016 Evropská unie také položila základy pro silnější evropskou obrannou politiku, aby zohlednila skutečnost, že občané očekávají větší ochranu. Globální strategie zahraniční a bezpečnostní politiky Evropské unie[3] zdůraznila potřebu integrovaného přístupu, aby se propojila vnitřní odolnost s vnějšími opatřeními EU, a vyzdvihla důležitost synergií mezi obrannou politikou a politikami upravujícími vnitřní trh, průmysl, vymáhání práva a zpravodajskými službami. Po přijetí evropského obranného akčního plánu v listopadu 2016 Komise navrhla konkrétní kroky, které přispějí k posílení schopnosti EU reagovat na hybridní hrozby posílením odolnosti dodavatelského řetězce v sektoru obrany a podporou vnitřního trhu v oblasti obrany Konkrétně Komise 7. června 2017 zahájila činnost Evropského obranného fondu s navrhovaným financováním ve výši 600 milionů EUR do roku 2020 a 1,5 miliardy EUR ročně po roce 2020. Sdělení o bezpečnostní unii[4] upozornilo na potřebu bojovat proti hybridním hrozbám a na důležitost posílení soudržnosti mezi vnitřními a vnějšími opatřeními na poli bezpečnosti.

Vedoucí představitelé EU v diskuzi o budoucnosti Evropy považují bezpečnost a obranu za ústřední téma.[5] Tuto skutečnost uznává i Římské prohlášení z 25. března 2017, v němž byla formulována vize bezpečné a chráněné Unie, která se bude zasazovat o posilování společné bezpečnosti a obrany. Předsedové Evropské rady a Evropské komise a generální tajemník

[1] Společné sdělení Evropskému parlamentu a Radě nazvané *Společný rámec pro boj proti hybridním hrozbám – reakce Evropské unie*, JOIN(2016) 18 final.
[2] *Závěry Rady o boji proti hybridním hrozbám*, tisková zpráva 196/16, 19. dubna 2016.
[3] Předloženo vysokou představitelkou na zasedání Evropské rady dne 28. června 2016.
[4] COM(2016) 230 final, 20. 4. 2016.
[5] Bratislavský plán Evropské rady ze dne 16. září 2016 a Římské prohlášení vedoucích představitelů 27 členských států a Evropské rady, Evropského parlamentu a Evropské komise ze dne 25. března 2017.

NATO dne 8. července 2016 ve Varšavě podepsali společné prohlášení se záměrem dát nový impuls a nový rozměr strategickému partnerství mezi EU a NATO. Společné prohlášení vyzdvihlo sedm konkrétních oblastí, včetně boje proti hybridním hrozbám, kde by měla být posílena spolupráce mezi oběma organizacemi. Společný soubor 42 návrhů na provedení schválily následně Rada EU i NATO a v červnu 2017 byla vydána první zpráva, která vykazuje podstatný pokrok[6].

Diskusní dokument Komise o budoucnosti evropské obrany[7] představený v červnu 2017 nastiňuje různé scénáře toho, jak přistupovat k narůstajícím hrozbám v oblasti bezpečnosti a obrany, jimž Evropa čelí, a jak lze do roku 2025 posílit její vlastní obranyschopnost. Ve všech třech scénářích se bezpečnost a obrana považují za nedílné složky evropského projektu sloužící tomu, abychom mohli doma i v zahraničí bránit a prosazovat naše zájmy. Evropa se musí stát subjektem zajišťujícím bezpečnost a postupně musí zajistit svou vlastní bezpečnost. Žádný členský stát nemůže sám za sebe čelit úkolům, které před ním stojí, zejména pokud jde o boj proti hybridním hrozbám. Spolupráce v oblasti obrany a bezpečnosti proto není volbou; je to nutnost, aby se vytvořila Evropa, která ochraňuje.

Cílem této zprávy je popsat dosažený pokrok a další prováděcí opatření ve čtyřech oblastech navržených ve společném rámci: zlepšení informovanosti o situaci; zvyšování odolnosti; posilování schopnosti členských států a Unie, pokud jde o předcházení krizím, jejich řešení a koordinovanou obnovu a posilování spolupráce s NATO, aby se zajistilo, že jednotlivá opatření budou komplementární. Měla by být čtena společně s měsíčními zprávami o pokroku na cestě k účinné a skutečné bezpečnostní unii.

2. ZOHLEDNĚNÍ HYBRIDNÍ POVAHY HROZBY

Hybridní aktivity se stávají častým rysem evropského bezpečnostního prostředí. Intenzita těchto aktivit se zvyšuje s narůstajícími obavami ohledně nekalého ovlivňování voleb, dezinformačních kampaní, nepřátelských činností v kyberprostoru a pachatelů hybridních aktů, kteří se snaží zradikalizovat náchylnější členy společnosti jako své prostředníky. Zranitelná místa, která jsou vystavena hybridním hrozbám, se neomezují pouze na hranice jednotlivých států. Hybridní hrozby vyžadují koordinovanou reakci na úrovni EU a NATO. Vývoj od dubna 2016 ukazuje, že ačkoli se hrozby nadále řeší izolovaně, narůstá v rámci Unie uznání a pochopení hybridní povahy některých činností a také toho, že je zapotřebí jednat koordinovaně. EU bude pokračovat ve svých snahách o zlepšení informovanosti o situaci a spolupráce.

***Opatření 1*: Členské státy, případně s podporou Komise a vysoké představitelky, se vyzývají k tomu, aby zahájily průzkum týkající se hybridních rizik s cílem určit hlavní slabiny, včetně konkrétních ukazatelů hybridních hrozeb, které mohou potenciálně ovlivnit vnitrostátní a celoevropské struktury a sítě.**

Rada zřídila „Skupinu přátel předsednictví“, která sdružuje odborníky z členských států, aby vypracovala obecný přehled, který pomůže určit klíčové ukazatele hybridních hrozeb, a ty zapracovat do mechanismů včasného varování a stávajících mechanismů pro hodnocení rizik

[6] http://www.consilium.europa.eu/cs/press/press-releases/2017/06/19-conclusions-eu-nato-cooperation

[7] Diskusní dokument o budoucnosti evropské obrany, 7. 6. 2017, https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_cs.pdf

a případně je sdílet. Byl dohodnut mandát a již došlo k zahájení činnosti. Do konce roku 2017 by měl být k dispozici obecný průzkum, přičemž aktuální průzkumy začnou následně. Ochrana před hybridními hrozbami by měla být vzájemně provázaná. Členské státy se proto vyzývají k tomu, aby tyto průzkumy provedly co nejrychleji, a získaly tak cenné informace o míře zranitelnosti a připravenosti v celé Evropě.

a. ZVYŠOVÁNÍ INFORMOVANOSTI

Hlavním nástrojem pro snižování nejistoty a posílení informovanosti o situaci je sdílení výsledků analýz a posuzování informačních zdrojů. Za loňský rok se dosáhlo značného pokroku. Bylo zřízeno středisko EU pro hybridní hrozby, které je nyní plně v provozu. Zároveň došlo ke zřízení pracovní skupiny East StratCom a Finsko zahájilo činnost Evropského střediska pro boj proti hybridním hrozbám. Velký díl práce se zaměřuje na analýzu nástrojů a mechanismů tvorby dezinformací a propagandy, přičemž funguje dobrá spolupráce mezi pracovní skupinou EU East StratCom, střediskem pro hybridní hrozby a organizací NATO. To vytváří solidní základ pro další rozvíjení tradice analyzování a posuzování hrozeb pro naši vnitřní a vnější bezpečnost prizmatem hybridních jevů.

Středisko EU pro hybridní hrozby

Opatření 2: Vytvořit v rámci stávající struktury Střediska EU pro analýzu zpravodajských informací 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.

Středisko EU pro hybridní hrozby bylo zřízeno v rámci Střediska Evropské unie pro analýzu zpravodajských informací, aby přijímalo a analyzovalo utajované informace a informace z otevřených zdrojů o hybridních hrozbách od různých zúčastněných stran. Analýza se následně sdílí v rámci EU a mezi členskými státy a poskytuje informace nutné pro rozhodovací procesy EU, včetně podkladů pro hodnocení bezpečnostních rizik prováděná na úrovni EU. V oblasti vojenské analýzy se středisko pro hybridní hrozby opírá o pomoc ředitelství EU pro vojenské zpravodajské pracovníky. K dnešnímu dni bylo vypracováno přes 50 posouzení a informačních dokumentů o hybridních hrozbách. Od ledna 2017 vydává středisko periodikum „Hybrid Bulletin“ (bulletin o hybridních hrozbách) určené čtenářům přímo v rámci institucí a orgánů EU a vnitrostátních kontaktních míst[8], v němž analyzuje současné hrozby a problémy hybridních hrozeb. Plné operační schopnosti střediska bylo dle plánu dosaženo v květnu 2017. V neposlední řadě také pokračuje mezipersonální spolupráce v rámci rodícího se úseku NATO pro analýzu hybridních hrozeb, při níž se sdílejí zkušenosti získané při zřizování střediska EU pro hybridní hrozby a informace (což se provádí při plném dodržování pravidel EU o výměně utajovaných informací). Středisko EU pro hybridní hrozby v současnosti vymezuje další iniciativy k posílení budoucí spolupráce a bude hrát klíčovou úlohu v paralelních cvičeních mezi EU a NATO, která se plánují na podzim 2017 a při nichž se bude testovat reakceschopnost střediska EU pro hybridní hrozby a budou zohledněny získané zkušenosti a poznatky.

[8] K dnešnímu dni jmenovalo své vnitrostátní kontaktní osoby 21 členských států. Jedná se o odborníky, kteří se na svých pozicích v hlavních městech členských států zabývají problémem hybridních hrozeb a odolnosti.

Strategická komunikace

Opatření 3: 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.

V posledních měsících došlo k nárůstu dezinformačních kampaní a systematického šíření falešných zpráv v rámci sociálních médií, což patří k paletě prostředků využívaných k oslabení protivníků. Vzhledem k tomu, že sociální média představují oblíbenou platformu, mohou informace, které působí spolehlivě a legitimně, změnit veřejné mínění ve prospěch jednotlivců, organizací či vlád. Tyto hybridní taktiky mají širší cíl, jímž je vyvolat zmatení v naší společnosti a zdiskreditovat demokratické vlády i naše struktury, instituce a volby. Falešné zprávy se často šíří prostřednictvím on-line platforem (viz rovněž opatření 17). Komise a vysoká představitelka vítají nedávné kroky, které podnikly platformy on-line a vydavatelé zpravodajských médií s cílem řešit problém dezinformací. Komise bude taková dobrovolná opatření nadále podporovat.

Vysoká představitelka zřídila pracovní skupinu East StratCom, která dezinformace a dezinformační kampaně předvídá a reaguje na ně. To výrazně zlepšuje komunikaci týkající se politik Unie ve východním sousedství a současně také posiluje mediální prostředí v těchto zemích. Tato pracovní skupina za poslední dva roky odhalila více než 3 000 jednotlivých případů dezinformací v 18 jazycích. Plánované spuštění nové internetové stránky: „*#EUvsdisinformation*“ s nástrojem pro on-line vyhledávání výrazně zlepší přístup pro uživatele. Výzkum a analýzy ovšem ukazují, že počet dezinformačních kanálů i každodenně šířených falešných zpráv je podstatně vyšší. Analýza politiky a médií v zemích Východního partnerství je prováděna v rámci projektu EU-STRAT financovaného z programu Horizont 2020.

Vysoká představitelka vyzývá členské státy, aby podpořily činnost pracovních skupin StratCom v zájmu účinnějšího boje proti nárůstu hybridních hrozeb. Podpoří se tím i činnost pracovní skupiny South s cílem zlepšit komunikaci a interakci s arabským světem (i v arabštině), bořit mýty a poskytovat pravdivé informace o Evropské unii a jejích politikách. Spolupráce s místními novináři pomůže zajistit, aby byly zpravodajské produkty kulturně sladěné. Obě pracovní skupiny – s podporou střediska EU pro hybridní hrozby – mají za cíl podpořit a doplnit úsilí členských států v této oblasti. Kromě toho Komise spolufinancuje Evropskou strategickou komunikační síť, což je platforma, v jejímž rámci sdílí 26 členských států analýzy, osvědčené postupy a nápady na využití strategické komunikace v boji proti násilnému extremismu či dezinformacím.

Středisko excelence pro boj proti hybridním hrozbám

Opatření 4: Členské státy se vyzývají, aby zvážily zřízení střediska excelence pro boj proti hybridním hrozbám.

V reakci na výzvu ke zřízení střediska excelence zahájilo Finsko v dubnu 2017 činnost evropského střediska pro boj proti hybridním hrozbám. Členem je deset členských států EU[9], Norsko a USA, přičemž Evropská unie i NATO byly vyzvány k podpoře jeho řídící rady[10].

[9] Finsko, Francie, Německo, Lotyšsko, Litva, Polsko, Švédsko, Spojené království, Estonsko, Španělsko.
[10] Středisko je otevřeno i dalším členským státům EU a spojencům NATO, kteří se chtějí připojit.

Posláním střediska je podporovat strategický dialog a provádět výzkum a analýzu ve spolupráci s příslušnými společenstvími, aby zvyšovalo odolnost a reakceschopnost, a pomáhalo tak v boji proti hybridním hrozbám. Očekává se, že středisko bude rovněž sloužit jako platforma pro budoucí cvičení v oblasti hybridních hrozeb. Středisko již navázalo úzké styky se střediskem EU pro hybridní hrozby a činnosti těchto dvou organizací by se měly navzájem doplňovat. EU v současnosti posuzuje způsoby, jak středisku poskytnout konkrétní podporu.

b. ZVYŠOVÁNÍ ODOLNOSTI

Společný rámec staví v rámci opatření EU odolnost (např. dopravy, komunikace, energetiky, financí či regionálních bezpečnostních infrastruktur) na přední místo, neboť je třeba vzdorovat propagandě a informačním kampaním, snahám o rozvracení podniků, společnosti a narušování hospodářských toků, jakož i útokům na informační technologie a kybernetickou infrastrukturu. O zvyšování odolnosti uvažuje jako o preventivním a odrazujícím opatření, které má posílit společnost a zamezit eskalaci krizí uvnitř a vně EU. Přínos EU spočívá v pomoci členským státům a partnerům při zvyšování odolnosti s využitím širokého rejstříku existujících nástrojů a programů. V oblasti opatření, která mají posilovat odolnost, se dosáhlo značného pokroku, např. pokud jde o kybernetickou bezpečnost, kritickou infrastrukturu, ochranu finančního systému před nezákonným využíváním či boj proti násilnému extremismu a radikalizaci.

Ochrana kritické infrastruktury

Opatření 5: 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.

V kontextu Evropského programu na ochranu kritické infrastruktury (EPCIP) pokračuje Komise v úsilí vymezit společné nástroje, včetně ukazatelů zranitelnosti, aby zvýšila odolnost kritické infrastruktury proti hybridním hrozbám v relevantních odvětvích. Komise v květnu 2017 uspořádala pracovní seminář na téma hybridní ohrožení kritické infrastruktury, jehož se zúčastnili zástupci téměř všech členských států, provozovatelé kritické infrastruktury, středisko EU pro hybridní hrozby a NATO jakožto pozorovatel. Byl dohodnut společný plán a jednotlivé kroky pro budoucí práci, a to na základě dotazníku zaslaného vnitrostátním orgánům v členských státech. Komise bude na podzim dále konzultovat zúčastněné strany, aby se do konce roku 2017 dohodly ukazatele.

Evropská obranná agentura pracuje na tom, aby identifikovala nedostatky, pokud jde o společnou kapacitu a výzkum, které se projevují v souvislosti s obranou energetických infrastruktur a obranných schopností. Evropská obranná agentura vypracuje na podzim 2017 koncepční dokument a představí pilotní akce pro komplexní metodiky.

Zvyšování bezpečnosti dodávek energie EU

Opatření 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.

Komise v prosinci 2016 v balíčku týkajícím se bezpečnosti dodávek učinila konkrétní návrhy a v dubnu 2017 pak Rada a Evropský parlament dosáhly dohody ohledně nového nařízení o

zajištění bezpečnosti dodávek zemního plynu, jehož účelem je zabránit krizím v oblasti dodávek zemního plynu. Nová pravidla zaručí regionálně koordinovaný a společný přístup k opatřením pro zajištění bezpečnosti dodávek mezi členskými státy. To postaví EU do lepší pozice k tomu, aby se v případě krize či hybridního útoku mohla připravit na výpadky dodávek plynu nebo takové výpadky řešit. Poprvé se uplatní zásada solidarity: členské státy budou schopny pomoci svým sousedům v případě závažné krize či útoku, aby evropské domácnosti a a podniky nepostihly výpadky dodávek energie.

EU rovněž pokročila v rozvoji klíčových projektů diverzifikace svých zásobovacích tras a zdrojů dodávek energie v souladu se strategickým rámcem energetické unie a evropskou strategií energetické bezpečnosti. V jižním koridoru pro přepravu plynu kupříkladu probíhají konkrétní stavební práce na všech hlavních projektech plynovodů: rozšíření jihokavkazského plynovodu, transanatolský a transjadranský plynovod, ložisko Shah Deniz II, jakož i rozšíření jižního koridoru pro přepravu plynu do Střední Asie, zejména do Turkmenistánu. Dovoz zkapalněného zemního plynu do Evropy narůstá a přichází z nových zdrojů, např. Spojených států. Příklad terminálu v Litvě je důkazem toho, jak mohou diverzifikační projekty snížit závislost na jediném dodavateli. K diverzifikaci energetických tras a zdrojů přispívá i posilování snah v oblasti energetiky a lepší využívání domácích zdrojů energie, zejména zdrojů obnovitelných.

V oblasti jaderné bezpečnosti Komise aktivně podporuje – zejména prostřednictvím pracovních seminářů s vnitrostátními veřejnými a regulačními orgány – důsledné a účinné provádění dvou směrnic o jaderné bezpečnosti a základních bezpečnostních standardech, které musí členské státy provést do konce roku 2017 a 2018. Ke zvyšování jaderné bezpečnosti kromě toho přispívá program Euratomu v oblasti výzkumu a odborné přípravy.

Bezpečnost dopravy a dodavatelských řetězců

Opatření 7: Komise bude monitorovat vznikající hrozby v celém odvětví dopravy a ve vhodných případech bude aktualizovat právní předpisy. Při provádění strategie EU pro námořní bezpečnost a strategie EU pro řízení rizik v oblasti cel a akčních plánů těchto strategií 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.

Komise v souladu se sdělením o bezpečnostní unii usnadňuje posuzování bezpečnostního rizika na úrovni EU s členskými státy, Střediskem Evropské unie pro analýzu zpravodajských informací a příslušnými agenturami, aby se odhalily hrozby pro dopravní bezpečnost a podpořil se rozvoj efektivních a přiměřených opatření ke zmírnění rizik. Sestřelení letadla Malajsijských aerolinií MH17 v roce 2014 nad východní Ukrajinou upozornilo na riziko, které představují přelety nad konfliktními zónami. V souladu s doporučeními evropské pracovní skupiny na vysoké úrovni pro konfliktní zóny[11] vypracovala Komise metodiku pro „společné posouzení rizik EU“ za podpory vnitrostátních odborníků v oblasti letectví a bezpečnosti a ESVČ, která umožňuje výměnu utajovaných informací a zmapování situace společných rizik. Evropská agentura pro bezpečnost letectví (EASA) na základě výsledků tohoto společného posouzení rizik EU vydala v březnu 2017 první „informační bulletin o konfliktních zónách“[12]. Komise uvažuje o rozšíření činností týkajících se posouzení rizik,

[11] https://www.easa.europa.eu/system/files/dfu/208599_EASA_CONFLICT_ZONE_CHAIRMAN_REPORT_no_B_update.pdf

[12] https://ad.easa.europa.eu/czib-docs/page-1

které jsou prováděny v oblasti bezpečnosti letectví, na další druhy dopravy (např. železniční a námořní dopravu) a v roce 2018 budou představeny návrhy. Komise, ESVČ a členské státy v červnu 2017 zahájily posouzení rizik v oblasti železniční bezpečnosti, aby odhalily nedostatky a stanovily možná opatření ke zmírnění rizik.

Značné úsilí, pokud jde o bezpečnost letectví a uspořádání letového provozu (ATM), bylo též vyvinuto v rámci výzkumných projektů v oblasti bezpečnosti programu Horizont 2020 a sedmého rámcového programu pro výzkum a technologický rozvoj. V oblasti civilního letectví rozvíjí Komise společně s Evropskou agenturou pro bezpečnost letectví a zúčastněnými stranami dvě nové iniciativy pro posílení kybernetické bezpečnosti a také k řešení hybridních hrozeb: zřízení skupiny pro reakci na počítačové hrozby v oblasti letectví, jakož i pracovní skupiny pro kybernetickou bezpečnost v rámci společného podniku výzkumu uspořádání letového provozu jednotného evropského nebe (SESAR) odpovídající za uspořádání letového provozu jednotného evropského nebe. Evropská obranná agentura poskytuje vojenské podklady, pokud jde o kybernetickou bezpečnost letectví, společnému podniku SESAR, jakož i Evropské agentuře pro bezpečnost letectví prostřednictvím „evropské strategické koordinační platformy pro kybernetickou bezpečnost“, která na žádost členských států napomůže koordinaci všech činností v oblasti letectví na úrovni EU. Evropská agentura pro bezpečnost letectví provedla v souladu s plánem v oblasti kybernetické bezpečnosti letectví v roce 2016 analýzy nedostatků stávajících pravidel a zejména vymezení a zřízení Evropského centra pro kybernetickou bezpečnost v letectví; toto centrum je nyní v provozu a spolupracuje se skupinou pro reakci na počítačové hrozby v evropských orgánech, institucích a jiných subjektech (CERT-EU) (memorandum o porozumění bylo podepsáno v únoru 2017), která provádí analýzy hrozeb v oblasti letectví, a s agenturou EUROCONTROL (byl přijat plán spolupráce), přičemž byla zároveň zřízena internetová stránka pro šíření analýz z otevřených zdrojů. Do podzimu 2017 bude přijat program normalizace a zavedena zabezpečená výměna informací.

Řízení rizik v oblasti cel

Pokud jde o cla, Komise se zaměřuje na to, aby se zásadním způsobem zmodernizoval systém pro předběžné informace o nákladu a celní systém pro řešení rizik. To se vztahuje na celou škálu rizik v oblasti cel, a to i ve vztahu k ohrožení bezpečnosti a neporušenosti mezinárodních dodavatelských řetězců a příslušných kritických infrastruktur (např. přímé ohrožení námořních přístavů, letišť a pozemních hranic, které představuje dovoz). Cílem modernizace je zajistit, aby celní správy v EU získávaly od obchodníků veškeré nezbytné informace, pokud jde o pohyb zboží; aby byly schopny tyto informace efektivněji sdílet mezi jednotlivými členskými státy; aby vedle pravidel specifických pro jednotlivé členské státy uplatňovaly i společná pravidla a aby byly schopny efektivněji se zaměřit na rizikové zásilky na základě prohloubené spolupráce s ostatními orgány, zejména donucovacími a bezpečnostními. Vývoj IT nezbytný k provedení této modernizace ze strany Komise je v současnosti v počáteční fázi a v nadcházejících měsících budou na centrální úrovni zahájeny příslušné investice.

Vesmír

Opatření 8: V kontextu 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 na evropské úrovni a použití systému Galileo u kritických infrastruktur, jež jsou závislé na časové synchronizaci.

Komise při přípravě regulačního rámce v oblasti vládní družicové komunikace (GovSatCom) a pozorování a sledování vesmíru v roce 2018 začlení do svého posouzení i hledisko odolnosti proti hybridním hrozbám. V souladu s kosmickou strategií Komise při přípravě rozvoje programů Galileo a Copernicus posoudí potenciál těchto služeb, pokud jde o zmírňování zranitelnosti kritických infrastruktur. Hodnotící zpráva by měla být hotova na podzim 2017 a návrh týkající se nové generace programů Copernicus a Galileo v roce 2018. Evropská obranná agentura pracuje na projektech společného rozvoje kapacit v oblastech komunikace využívající vesmír, vojenského určování polohy, navigace a načasování a pozorování země. Všechny projekty se zaměří na požadavky na odolnost z hlediska existujících a nově se objevujících hybridních hrozeb.

Obranné schopnosti

Opatření 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.

V letech 2016 a 2017 Evropská obranná agentura společně s Komisí, EEAS a odborníky z členských států provedla tři simulační cvičení zaměřená na scénáře hybridních hrozeb. Jejich zjištění budou využita při přezkumu plánu rozvoje schopností, takže výsledný rozvoj klíčových schopností požadovaný pro boj proti hybridním hrozbám bude začleněn do nových priorit EU v oblasti rozvoje schopností. Práce na revizi katalogu požadavků z roku 2005 zohlední i rovinu hybridních hrozeb. V dubnu 2017 Evropská obranná agentura dokončila svou analytickou zprávu o vojenských dopadech vyplývajících z hybridních útoků proti kritické přístavní infrastruktuře. Tato analytická zpráva se bude projednávat na pracovním semináři s námořními odborníky v říjnu 2017. Další zvláštní analýza vojenské úlohy v souvislosti s bojem proti minidronům se plánuje na rok 2018. Od roku 2019 mohou být navíc způsobilé pro podporu v rámci Evropského obranného fondu rovněž priority kapacit posílení odolnosti proti hybridním hrozbám, které určí členské státy. Komise vyzývá spoluzákonodárce, aby zajistili rychlé přijetí, a členské státy, aby předložily návrhy projektů kapacit na posílení odolnost EU vůči hybridním hrozbám.

Opatření 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.

Komise chce posílit připravenost na hybridní hrozby a odolnost vůči nim, včetně rozvoje kapacit v rámci systému zdravotní péče a potravinového systému, a proto členské podporuje státy prostřednictvím odborné přípravy, simulačních cvičení a pokynů pro usnadnění výměny osvědčených postupů a financování společných akcí. Činí tak zejména v rámci zdravotní bezpečnosti EU pro závažné přeshraniční zdravotní hrozby a v rámci programu veřejného zdraví k provádění mezinárodního zdravotního řádu – legislativního pilíře závazného pro 196 zemí včetně členských států –, který má zabránit akutním veřejným přeshraničním zdravotním rizikům po celém světě nebo je řešit. K ověření meziodvětvové připravenosti a reakceschopnosti v oblasti zdravotnictví provedou útvary Komise na podzim 2017 cvičení zaměřené na složité a vícerozměrné hybridní hrozby. Komise a členské státy připravují společnou akci v oblasti vakcinace, která zahrnuje dodávky vakcín, odhadování poptávky a výzkum v oblasti inovativních postupů pro výrobu vakcín, přičemž cílem je posílit dodávky vakcín a zlepšit zdravotní bezpečnost na úrovni EU (2018–2020). Komise rovněž

spolupracuje s Evropským úřadem pro bezpečnost potravin a Evropským střediskem pro prevenci a kontrolu nemocí s cílem přizpůsobit se vyspělým metodám vědeckého výzkumu, zajistit přesnější zjišťování zdravotních hrozeb a jejich příčin a díky tomu rychleji zvládat řešení naléhavých situací týkajících se bezpečnosti potravin. Komise vytvořila síť subjektů financujících výzkum – Globální spolupráce ve výzkumu připravenosti na infekční onemocnění –, jež má být schopna do 48 hodin od vypuknutí závažné nákazy zajistit koordinovanou reakci subjektů činných v oblasti výzkumu.

<u>Opatření 11</u>: Komise vyzývá členské státy, aby prioritně zřídily síť 28 bezpečnostních týmů typu CSIRT a skupiny CERT-EU (skupina EU pro reakci na počítačové hrozby) 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.

Nedávný globální kybernetický útok, který využil ransomware a malware k tomu, aby vyřadil z provozu tisíce počítačových systémů, opět zdůraznil naléhavou potřebu zvýšit kybernetickou odolnost a posílit v rámci EU bezpečnostní opatření. Jak bylo oznámeno v přezkumu jednotného digitálního trhu v polovině období, Komise a vysoká představitelka nyní provádějí přezkum Strategie kybernetické bezpečnosti EU z roku 2013, a to zejména prostřednictvím přijetí balíčku plánovaného na září 2017. Půjde v něm o to, zajistit efektivnější meziodvětvovou reakci na zmíněné hrozby, která posílí důvěru v digitální společnost a ekonomiku. Přezkoumá se rovněž mandát agentury ENISA (Agentury EU pro bezpečnost sítí a informací), aby bylo možné definovat její úlohu ve změněném ekosystému kybernetické bezpečnosti. Evropská rada[13] uvítala záměr Komise provést přezkum strategie kybernetické bezpečnosti.

Zásadním krokem ke zvýšení odolnosti v oblasti kybernetické bezpečnosti na evropské úrovni bylo přijetí směrnice o sítích a informačních systémech (NIS)[14] v červenci 2016. Směrnice stanoví první celounijní pravidla pro kybernetickou bezpečnost, zlepšuje kapacity v oblasti kybernetické bezpečnosti a posiluje spolupráci mezi členskými státy. Rovněž po společnostech v kritických odvětvích požaduje, aby přijaly vhodná bezpečnostní opatření a oznamovaly příslušnému vnitrostátnímu orgánu závažné kybernetické incidenty. K těmto kritickým odvětvím patří energetika, doprava, vodohospodářství, zdravotnictví, bankovnictví a infrastruktura finančních trhů. Podobné kroky budou muset provést i on-line trhy, služby cloud computingu a vyhledávače. Důsledné provádění v různých odvětvích, jakož i napříč hranicemi, zajistí skupina pro spolupráci v oblasti bezpečnosti sítí a informací (založená Komisí v roce 2016), jež má za úkol zabránit roztříštění trhu. V této souvislosti se za referenční rámec pro všechny odvětvové iniciativy v oblasti kybernetické bezpečnosti považuje směrnice o sítích a informačních systémech. Směrnice dále vytváří síť bezpečnostních týmů typu CSIRT, která sdružuje všechny příslušné zúčastněné strany. Komise a skupina CERT-EU současně aktivně monitorují situaci v oblasti kybernetických hrozeb a provádějí výměnu informací s vnitrostátními orgány, aby systémy informačních technologií orgánů EU byly dobře zabezpečené a odolné vůči kybernetickým útokům. První příležitostí k tomu, aby se tato síť zapojila do operativní výměny informací a spolupráce šířením rad a pokynů, byl incident v souvislosti s ransomwarem WannaCry, k němuž došlo v

[13] Závěry Evropské rady ze zasedání ve dnech 22.–23. června 2017.

[14] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, Úř. věst. L 194, 19.7.2016, s. 1.

květnu 2017. Při zmírňování této hrozby a při pomoci obětem udržovala skupina EU pro reakci na počítačové hrozby úzké kontakty rovněž s Evropským centrem pro boj proti kyberkriminalitě (EC3) při úřadu Europol, bezpečnostními týmy typu CSIRT dotčených zemí, útvary pro boj proti kyberkriminalitě a klíčovými partnery z odvětví. Díky výměně vnitrostátních situačních zpráv se zajistila společná informovanost o situaci v celé EU. Tato zkušenost umožnila, aby se síť lépe připravila na další incidenty (např. „NonPetya“) Došlo také k odhalení několika problémů, které se momentálně řeší.

***Opatření 12*: Komise bude v koordinaci s členskými státy v rámci smluvního partnerství veřejného a soukromého sektoru pro kybernetickou bezpečnost spolupracovat se zástupci průmyslu na vývoji a zkoušení technologií, aby uživatelé a infrastruktury byli lépe chráněni před kybernetickými aspekty hybridních hrozeb.**

V červenci 2016 Komise, v koordinaci s členskými státy, podepsala se **zástupci průmyslu** smluvní partnerství veřejného a soukromého sektoru pro kybernetickou bezpečnost s investicemi až 450 milionů EUR v rámci programu pro vývoj a inovace Horizont 2020 na vývoj a testování technologií pro lepší ochranu uživatelů a infrastruktur před kybernetickými a hybridními hrozbami. Toto partnerství přineslo první celoevropský strategický výzkumný program, který se zaměřuje na zlepšování odolnosti kritických infrastruktur i občanů proti kybernetickým útokům. Partnerství zlepšilo koordinaci mezi zúčastněnými stranami, což zvyšuje efektivnost a účelnost financování kybernetické bezpečnosti v rámci programu Horizont 2020. Partnerství pracuje současně na řešení otázek souvisejících s kybernetickou bezpečností certifikace informačních a komunikačních technologií, jakož i otázek, jak řešit akutní nedostatek kvalifikovaných odborníků v oblasti kybernetické bezpečnosti na trhu. Skupina pro kybernetický výzkum a technologii Evropské obranné agentury s ohledem na značné potřeby civilního výzkumu a vysoké požadavky na odolnost, které s obranou souvisí, podporuje oblasti výzkumu, jež Evropská organizace pro kybernetickou bezpečnost určila ve svém strategickém programu výzkumu a inovací.

***Opatření 13*: Komise vydá pokyny pro vlastníky 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.**

V odvětví **energetiky** připravuje Komise odvětvové strategie zaměřené na kybernetickou bezpečnost s vytvořením platformy odborníků na kybernetickou bezpečnost v odvětví energetiky, aby se podpořilo provádění směrnice o bezpečnosti sítí a informací. Studie z února 2017 určila nejlepší dostupné techniky ke zvýšení úrovně kybernetické bezpečnosti inteligentních měřicích systémů, které tato platforma využívá. Komise rovněž vytvořila internetovou platformu „*Středisko EU pro sdílení informací o hrozbách a incidentech*“, které analyzuje a sdílí informace o kybernetických hrozbách a incidentech v odvětví energetiky.

Zvyšování odolnosti finančního sektoru vůči hybridním hrozbám

***Opatření 14*: Komise bude ve spolupráci s agenturou ENISA[15], členskými státy, příslušnými mezinárodními, evropskými a vnitrostátními orgány a finančními institucemi podporovat a**

[15] Evropská agentura pro bezpečnost sítí a informací.

zjednodušovat platformy a sítě pro sdílení informací a bude se zabývat faktory, které výměnu informací brzdí.

Vzhledem k tomu, že kybernetické hrozby patří mezi hlavní rizika pro finanční stabilitu, přezkoumala Komise regulační rámec pro platební služby v Evropské unii, který má být nyní proveden. Revidovaná směrnice o platebních službách[16] zavedla nová ustanovení s cílem posílit bezpečnost platebních prostředků a silné ověření klienta, aby se snížil výskyt podvodů, zejména pokud jde o on-line platby. Nový legislativní rámec bude použitelný od ledna 2018. Komise v současné době ve spolupráci s Evropským orgánem pro bankovnictví a v konzultaci se zúčastněnými stranami vypracovává regulační technické normy, které mají být zveřejněny do konce roku 2017, pro silné ověření klientů a bezpečnou komunikaci s cílem zprovoznit zabezpečení při platebních transakcích. Kromě toho Komise na mezinárodní úrovni úzce spolupracuje s příslušnými partnery ze skupiny G7 na „*základních zásadách kybernetické bezpečnosti skupiny G7 ve finančním sektoru*“, které v říjnu 2016 schválili ministři financí a guvernéři centrální banky G7. Tyto zásady jsou určeny pro subjekty finančního sektoru (soukromé i veřejné) a mají přispět k vytvoření koordinovaného přístupu v oblasti kybernetické bezpečnosti ve finančním sektoru, aby bylo možné společně řešit kybernetické hrozby, k nimž patří i narůstající a rafinovanější kybernetické hrozby.

Doprava

Opatření 15: 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.

Provádění akčního plánu strategie Evropské unie pro námořní bezpečnost[17] pomůže změnit nepružné a omezené uvažování v oblasti výměny informací a společného využívání prostředků mezi civilními a vojenskými orgány. Celostní vládní přístup vedl k prohloubení spolupráce mezi různými aktéry. Plánuje se, že do konce roku 2017 bude dokončen společný civilně-vojenský program strategického výzkumu Komise a ESVČ. Uzavře jej závěrečný praktický seminář na téma ochrana kritické námořní infrastruktury. Tato činnost by se mohla v budoucnosti rozšířit na oblast vznikajících hrozeb pro podmořská potrubí, přenos energie, optická vlákna a tradiční komunikační kabely, pokud jde o zásahy mimo národní vody.

Nedávná studie[18] zhodnotila schopnost posuzovat rizika u vnitrostátních orgánů, které vykonávají funkce pobřežní stráže. Identifikovala hlavní překážky spolupráce a doporučila praktické způsoby, jak v této konkrétní oblasti posílit spolupráci mezi námořními orgány na úrovni EU a na vnitrostátní úrovni. Posouzení rizik je zásadní pro boj proti námořním hrozbám a ještě prospěšnější pro hodnocení a prevenci hybridních hrozeb, neboť tyto hrozby vyžadují dodatečné a komplexnější úvahy. Výsledky studie budou představeny na různých fórech pro funkce pobřežní stráže, aby mohla být navrhovaná doporučení posouzena a provedena v zájmu posílení spolupráce v této oblasti. Hlavním cílem je přitom posílit připravenost a reakci na hybridní hrozby.

[16] Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu (Úř. věst. L 337, 23.12.2015, s. 35).
[17] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf a 2. zpráva o provádění akčního plánu EUMSS předložená členským státům dne 21. června 2017.
[18] Studie na téma „Hodnocení schopnosti posuzovat rizika na úrovni orgánů členských států vykonávajících funkce pobřežní stráže“, 2017, https://ec.europa.eu/maritimeaffairs/documentation/studies

Boj proti financování terorismu

Opatření 16: Komise využije provádění akčního plánu pro boj proti financování terorismu k tomu, aby tento plán také přispěl k boji proti hybridním hrozbám.

Původci hybridních hrozeb a jejich stoupenci potřebují k realizaci svých plánů finanční prostředky. K boji proti hybridním hrozbám mohou také přispět snahy EU zaměřené proti financování trestné činnosti a terorismu v rámci Evropského programu pro bezpečnost a akčního plánu pro boj proti financování terorismu. Komise v prosinci 2016 předložila tři legislativní návrhy, které se mimo jiné týkaly trestních sankcí za praní peněz a nezákonné hotovostní platby, jakož i zmrazování a konfiskace majetku[19].
Všechny členské státy musely do 26. června 2017 provést čtvrtou směrnici o boji proti praní peněz[20] a Komise v červenci 2016 předložila cílený legislativní návrh na doplnění a posílení této směrnice prostřednictvím dalších opatření[21].

Dne 26. června 2017 vydala Komise nadnárodní posouzení rizik podle čtvrté směrnice o boji proti praní peněz. Rovněž předložila návrh nařízení na prevenci dovozu a skladování kulturních statků nelegálně vyvezených ze třetích zemí na území EU[22]. V průběhu letošního roku podá Komise zprávu o probíhajícím posouzení potřeby možných dalších opatření pro sledování financování terorismu v EU. Komise rovněž provádí přezkum právních předpisů v oblasti boje proti podvodům a padělání bezhotovostních plateb[23].

Více podrobností o aktuálním stavu provádění akčního plánu pro boj proti financování terorismu obsahuje Osmá zpráva **o pokroku na cestě k účinné a skutečné bezpečnostní unii**.

Prosazování společných hodnot EU a inkluzivní, otevřené a odolné společnosti

Zvyšování odolnosti proti radikalizaci a násilnému extremismu

Vnější činitelé mohou vyprovokovat náboženskou a ideologickou radikalizaci, etnické konflikty a konflikty menšin tím, že podporují konkrétní skupiny, nebo se snaží přiživovat konflikty mezi jednotlivými skupinami. Objevily se i další problémy, jako jsou např. hrozby ze strany tzv. osamělých vlků, nové formy radikalizace, a to potenciálně také v souvislosti s migrační krizí, jakož i nárůst pravicového extremismu (včetně násilí zaměřeného proti migrantům) a riziko polarizace. Práce v oblasti boje proti radikalizaci sice pokračuje v rámci bezpečnostní unie, ovšem z hlediska hybridních hrozeb může mít nepřímý přínos i v případech, kdy jde o osoby náchylné k radikalizaci, které mohou být pachateli hybridních hrozeb zmanipulovány.

[19] Třetí zpráva o pokroku na cestě k účinné a skutečné bezpečnostní unii (COM(2016) 831 final).
[20] Směrnice Evropského parlamentu a Rady (EU) 2015/849 ze dne 20. května 2015 o předcházení využívání finančního systému k praní peněz nebo financování terorismu, o změně nařízení Evropského parlamentu a Rady (EU) č. 648/2012 a o zrušení směrnice Evropského parlamentu a Rady 2005/60/ES a směrnice Komise 2006/70/ES (Text s významem pro EHP) (Úř. věst. L 141, 5.6.2015, s. 73).
[21] Více podrobností viz Třetí zpráva o pokroku na cestě k účinné a skutečné bezpečnostní unii (COM(2016) 831 final) a Osmá zpráva o pokroku na cestě k účinné a skutečné bezpečnostní unii (COM(2017) 354 final).
[22] COM(2017) ze dne 26. června 2017, COM(2017) 340 final, SWD(2017) 275 final.
[23] Osmá zpráva o pokroku na cestě k účinné a skutečné bezpečnostní unii (COM(2017) 354 final).

<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 správě.

Předcházení radikalizaci

Komise pokračuje v provádění svého komplexního řešení problému radikalizace podle sdělení o podpoře prevence radikalizace vedoucí k násilnému extremismu z června 2016[24], v němž jsou popsána klíčová opatření, jako např. prosazování inkluzivního vzdělávání a společných hodnot, potírání extremistické propagandy na internetu a radikalizace ve věznicích, prohloubení spolupráce se třetími zeměmi a posílení výzkumu, který umožní lépe pochopit vyvíjející se povahu radikalizace a poskytne lepší podklady pro politické kroky. Na předním místě činnosti Komise na podporu členských států v této oblasti je síť pro zvyšování povědomí o radikalizaci, která využívá spolupráce s místními odborníky z praxe na úrovni komunit. Více podrobností lze nalézt v Osmé zprávě o pokroku na cestě k účinné a skutečné bezpečnostní unii[25].

Radikalizace a nenávistné projevy na internetu

V souladu s Evropským programem pro bezpečnost[26] podnikla Komise kroky s cílem omezit dostupnost nedovoleného obsahu na internetu, a to zejména prostřednictvím jednotky EU pro oznamování internetového obsahu a internetového fóra EU[27]. Významného pokroku bylo též dosaženo v rámci kodexu chování pro boj proti on-line šíření nelegálních nenávistných projevů[28]. Více podrobností lze nalézt v Osmé zprávě o pokroku na cestě k účinné a skutečné bezpečnostní unii[29]. Tato opatření se ještě zintenzivní, a to i s ohledem na závěry Evropské rady[30], summit G7[31] a summit skupiny G20 v Hamburku[32].

Klíčovou úlohu v boji proti nezákonnému či potenciálně škodlivému obsahu hrají on-line platformy. Jak bylo stanoveno v rámci přezkumu v polovině období[33], zajistí Komise v rámci strategie pro jednotný digitální trh lepší koordinaci dialogů s on-line platformami, přičemž se pozornost bude soustředit na mechanismy a technická řešení pro odstraňování nezákonného obsahu. Cílem by mělo být tyto mechanismy v příslušných případech posílit prostřednictvím pokynů o aspektech typu oznamování a odstraňování nezákonného obsahu. Komise také poskytne pokyny týkající se pravidel odpovědnosti.

[24] http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf
[25] COM(2017) 354 final.
[26] Více podrobností viz Osmá zpráva o pokroku na cestě k účinné a skutečné bezpečnostní unii (COM(2017) 354 final).
[27] Více podrobností viz Osmá zpráva o pokroku na cestě k účinné a skutečné bezpečnostní unii (COM(2017) 354 final).
[28] Kodex chování pro boj proti on-line šíření nelegálních nenávistných projevů, 31. května 2016, http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf
[29] Více podrobností viz Osmá zpráva o pokroku na cestě k účinné a skutečné bezpečnostní unii (COM(2017) 354 final).
[30] Závěry Rady ze zasedání ve dnech 22.–23. června 2017.
[31] Summit G7 v Taormině, Itálie, 26.–27. 5. 2017.
[32] Summit G20 v Hamburku, Německo, 7.–8. 5. 2017.
[33] Viz výše uvedené sdělení Komise COM(2017) 228 final.

<u>Posílení spolupráce s třetími zeměmi</u>

<u>Opatření č. 18:</u> Vysoká představitelka zahájí v koordinaci s Komisí 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.

Evropská unie věnuje zvýšenou pozornost budování kapacit a zvyšování odolnosti v oblasti bezpečnosti v partnerských zemích, a to mimo jiné tím, že vychází ze vzájemné provázanosti prvků bezpečnosti a rozvoje, rozpracovává bezpečnostní rozměr revidované evropské politiky sousedství a navazuje rozhovory o boji proti terorismu a bezpečnosti se zeměmi kolem Středozemního moře. Za tímto účelem byl zahájen průzkum rizik v rámci pilotního projektu ve spolupráci s Moldavskou republikou. Má pomáhat při identifikaci hlavních zranitelných míst této země a zajistit, aby se pomoc EU zaměřila konkrétně na tyto oblasti. Výsledky pilotního projektu ukázaly, že průzkum byl sám o sobě považován za prospěšný. Komise a ESVČ připraví na základě získaných zkušeností doporučení s cílem určit prioritní opatření v rámci zvyšování účinnosti, strategické komunikace ochrany kritické infrastruktury a kybernetické bezpečnosti.

V budoucnu by průzkum mohly na základě této první zkušenosti využít i další sousední země; i když budou zapotřebí různé specifické úpravy, aby se zohlednily různé vnitrostátní místní situace a specifické hrozby a zamezilo se překrývání s probíhajícími dialogy o otázkách bezpečnosti a boje proti terorismu. V obecném rámci Komise a vysoká představitelka přijaly dne 7. června 2017 společné sdělení „Strategický přístup k odolnosti ve vnější činnosti EU“[34]. Jeho cílem je podpořit partnerské země v jejich úsilí o zvýšení odolnosti proti globálním problémům dneška. Uznává se v něm, že je nutné přejít od zmírňování krize na strukturovanější dlouhodobý přístup ke zranitelným místům, s důrazem na předjímání, prevenci a připravenost.

<u>Kybernetická odolnost pro rozvoj</u>

EU podporuje země mimo Evropu, aby posílila odolnost jejich informačních sítí. Stále narůstající digitalizace má vnitřní bezpečnostní rozměr, který přináší zvláštní úkoly, pokud jde o odolnost systémů informačních sítí, neboť počítačové útoky neznají hranic. EU podporuje třetí země v rozvoji schopností adekvátně předcházet náhodným poruchám a kybernetickým útokům a čelit jim. V návaznosti na pilotní projekt v oblasti kybernetické bezpečnosti v Bývalé jugoslávské republice Makedonii, Kosovu[35] a Moldavské republice dokončený v roce 2016 Komise zahájí nový program na období 2017–2020 zaměřený na posílení kybernetické odolnosti třetích zemí, zejména v Africe a v Asii, ale také na Ukrajině. Jeho cílem je na základě celostního vládního přístupu zvýšit bezpečnost a připravenost kritických informačních infrastruktur a sítí ve třetích zemích a současně zajistit dodržování lidských práv a zásad právního státu.

[34]Společné sdělení Evropskému parlamentu a Radě: Strategický přístup k odolnosti ve vnější činnosti EU, JOIN(2017) 21 final.

[35] Tímto označením nejsou dotčeny postoje k otázce statusu a označení je v souladu s rezolucí Rady bezpečnosti OSN 1244 a se stanoviskem Mezinárodního soudního dvora k vyhlášení nezávislosti Kosova.

Bezpečnost letectví

Civilní letectví zůstává hlavním a symbolickým terčem teroristických útoků, ale mohlo by se stát terčem rovněž v rámci hybridní kampaně. EU sice již vyvinula spolehlivý rámec na ochranu letectví, ale lety ze třetích zemí mohou být zranitelnější. Komise v souladu s rezolucí Rady bezpečnosti OSN 2309 (2016) zintenzivňuje úsilí, aby posílila kapacity ve třetích zemích. V lednu 2017 Komise zahájila nové integrované posouzení rizik s cílem stanovit priority a koordinovat úsilí při budování kapacit vyvíjené na úrovni EU a na úrovni členských států, jakož i ve spolupráci s mezinárodními partnery. V roce 2016 Komise zahájila čtyřletý projekt ochrany civilního letectví v Africe a na Arabském poloostrově v rámci boje s hrozbou terorismu, jíž je vystaveno civilní letectví. Tento projekt se zaměřuje na sdílení odborných znalostí mezi partnerskými státy a odborníky z členských států Evropské konference civilního letectví, odborné vedení, školení a školící akce. Činnosti v rámci tohoto projektu se během roku 2017 dále rozšíří.

c. PŘEDCHÁZENÍ KRIZÍM, JEJICH ŘEŠENÍ A KOORDINOVANÁ OBNOVA

Následky lze sice zmírnit prostřednictvím dlouhodobých politik na vnitrostátní úrovni i na úrovni EU, ale z krátkodobého hlediska je zásadně důležité posílit kapacity členských států a Unie pro prevenci hybridních hrozeb, reakci na ně a zotavení se po nich, a to rychle a koordinovaně. Zásadní je, aby reakce na události vyvolané hybridními hrozbami byla rychlá. V této oblasti se za loňský rok dosáhlo velkého pokroku: v EU je nyní zaveden operační protokol, který stanoví postup pro řešení krize v případě hybridního útoku. V budoucnosti se bude provádět pravidelné monitorování a cvičení.

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**.**

Společný rámec doporučil zavedení mechanismů rychlé reakce na události vyvolané hybridními hrozbami k zajištění koordinace mezi mechanismy reakce EU[36] a systémy včasného varování. Útvary Komise a ESVČ za tímto účelem vydaly operační protokol EU pro boj proti hybridním hrozbám (pravidla EU (EU Playbook))[37], který vymezuje způsoby koordinace, propojování a analýzu zpravodajské činnosti, využívání informací při postupech tvorby politik, cvičení a odborné přípravy a spolupráce s partnerskými organizacemi, zejména s NATO, v případě hybridní hrozby. Podobně i organizace NATO vypracovala pravidla pro posílenou spolupráci mezi NATO a EU při předcházení hybridním hrozbám a boji proti nim v oblastech kybernetické obrany, strategické komunikace, informovanosti o situaci a zvládání krizí. Pravidla EU budou otestována během cvičení na podzim 2017 jako součást paralelního a koordinovaného cvičení Evropské unie, které zahrnuje spolupráci s NATO.

[36] Integrovaná opatření EU pro politickou reakci na krize (opatření IPCR), která schválila Rada, systém Komise ARGUS a CRM služby ESVČ.
[37] Pracovní dokument útvarů Komise (2016) 227 přijatý dne 7. července 2016.

<u>Opatření 20</u>: 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.

Ustanovení čl. 42 odst. 7 SEU hovoří o ozbrojeném napadení na území členského státu, zatímco článek 222 SFEU (doložka solidarity) hovoří o teroristickém útoku nebo přírodní nebo člověkem způsobené pohromě na území členského státu. V případě hybridních útoků je pravděpodobnější, že bude použit druhý zmíněný článek, neboť jde o kombinaci kriminálního a podvratného jednání. Využití doložky solidarity spouští koordinaci na úrovni Rady (Integrovaná opatření pro politickou reakci na krize) a zapojení příslušných orgánů, agentur a subjektů EU, jakož i programů a mechanismů pomoci EU. Způsoby provádění doložky solidarity Unií stanoví rozhodnutí Rady 2014/415/EU. Tyto způsoby použití zůstávají platné a není zapotřebí rozhodnutí Rady revidovat. Pokud by hybridní útok zahrnoval ozbrojené napadení, lze použít i čl. 42 odst. 7. V takovém případě poskytnou pomoc i podporu členské státy i EU. Komise a vysoká představitelka budou nadále posuzovat nejefektivnější způsoby, jak takové útoky řešit.

Přijetí výše zmíněného operačního protokolu EU takové posouzení přímo podporuje a bude prováděno jako součást paralelního a koordinovaného cvičení (PACE) EU v říjnu 2017. Tímto cvičením se otestují různé mechanismy EU i její schopnost jednat s cílem urychlit rozhodování v případě nejasností vyvolaných vlivem hybridních hrozeb.

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

V reakci na pověření integrovat vojenské kapacity na podporu SZBP/SBOP a v návaznosti na seminář s vojenskými odborníky v prosinci 2016 a pokyny pracovní skupiny Vojenského výboru Evropské unie z května 2017 bylo v červenci 2017 dokončeno vojenské doporučení na téma „vojenský příspěvek EU k boji proti hybridním hrozbám v rámci SBOP“, které bude dále rozvinuto v rámci plánu pro realizaci vývoje koncepcí.

d. SPOLUPRÁCE MEZI EU A NATO

<u>Opatření 22</u>: 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.

Na základě společného prohlášení, které podepsali dne 8. července 2016 ve Varšavě předsedové Evropské rady a Evropské komise a generální tajemník NATO, vypracovaly EU a NATO společný soubor 42 návrhů na provádění, který byl následně schválen samostatnými paralelními postupy dne 6. prosince 2016 radami EU i NATO[38]. V červnu 2017 vysoká představitelka a místopředsedkyně a generální tajemník NATO zveřejnili zprávu o celkovém pokroku, kterého se dosáhlo ve věci 42 opatření společného prohlášení. Boj proti hybridním hrozbám představuje jednu ze sedmi oblastí spolupráce stanovených ve společném prohlášení a zahrnuje deset ze čtyřiceti dvou opatření. Zpráva ukazuje, že společné úsilí vyvinuté v

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

loňském roce přineslo výrazné výsledky. Řada konkrétních opatření zaměřených na boj proti hybridním hrozbám již byla zmíněna výše, včetně Evropského střediska pro boj proti hybridním hrozbám, zlepšení informovanosti o situaci, zřízení střediska EU pro hybridní hrozby a jeho spolupráce s nově vytvořeným úsekem NATO pro analýzu hybridních hrozeb a spolupráce mezi týmy pro strategickou komunikaci. Štáby EU a NATO budou poprvé společně nacvičovat reakci na scénář hybridní situace. Očekává se, že toto cvičení prověří provádění více než třetiny společných návrhů. EU letos provede své vlastní souběžné a koordinované cvičení a připravuje se na převzetí vedoucí úlohy v roce 2018.

Pokud jde o odolnost, personál EU a NATO provádí vzájemné informování, a to i o mechanismu EU pro integrovanou politickou reakci na krize. Pravidelné kontakty mezi personálem NATO a EU, a to i na pracovních seminářích a shromážděních NATO či při účasti na schůzích řídícího výboru Evropské obranné agentury, umožňují výměny informací o základních požadavcích NATO na vnitrostátní odolnost. Další jednání mezi Komisí a NATO o posilování odolnosti se plánují na podzim. Příští zpráva o pokroku týkající se spolupráce mezi EU a NATO navrhne možnosti rozšíření spolupráce mezi oběma organizacemi.

3. ZÁVĚR

Společný rámec nastiňuje opatření, která mají pomoci v boji proti hybridním hrozbám a posílit odolnost na úrovni EU i členských států, jakož i u našich partnerů. Komise a vysoká představitelka v úzké spolupráci s členskými státy a partnery dosahují výsledků ve všech oblastech, je ale nezbytné, aby toto úsilí nepolevovalo, neboť hybridní hrozby se nadále a nepřetržitě vyvíjejí. Za boj proti hybridním hrozbám, pokud jde o vnitrostátní bezpečnost a zachování práva a pořádku, nesou primární odpovědnost členské státy. Odolnost členských států a kolektivní úsilí o ochranu před hybridními hrozbami je třeba chápat jako vzájemně provázané a korespondující prvky téhož celkového úsilí. Členské státy se proto vyzývají k tomu, aby průzkumy hybridních rizik provedly co nejrychleji, neboť poskytnou cenné informace o míře zranitelnosti a připravenosti v celé Evropě. Mělo by se maximálně využít výrazného pokroku pro zvýšení povědomí o potenciálu střediska EU pro hybridní hrozby. Vysoká představitelka vyzývá členské státy, aby podpořily činnost pracovních skupin StratCom v zájmu účinnějšího boje proti nárůstu hybridních hrozeb. EU bude plně podporovat Evropské středisko pro boj proti hybridním hrozbám pod vedením Finska.

Jedinečná síla EU spočívá v pomoci členským státům a partnerům při zvyšování odolnosti s využitím širokého rejstříku existujících nástrojů a programů. V oblasti opatření, která mají posilovat odolnost, se dosáhlo značného pokroku, např. pokud jde o dopravu, energetiku, kybernetickou bezpečnost, kritickou infrastrukturu, ochranu finančního systému před nezákonným využíváním či boj proti násilnému extremismu a radikalizaci. Opatření EU na zvyšování odolnosti budou pokračovat, neboť povaha hybridních hrozeb se neustále vyvíjí. EU zejména vypracuje ukazatele ke zlepšení ochrany a odolnosti kritické infrastruktury proti hybridním hrozbám v příslušných odvětvích.

Evropský obranný fond může společně s členskými státy spolufinancovat i prioritní kapacity na posílení odolnosti vůči hybridním hrozbám. Nové platformy pro boj proti hybridním hrozbám v celé EU poskytne připravovaný balíček týkající se kybernetické bezpečnosti, jakož i meziodvětvová opatření zaměřená na provádění směrnice o bezpečnosti sítí a informací.

Komise a vysoká představitelka vyzývají členské státy a zúčastněné strany, aby se v případě nutnosti rychle dohodly a zajistily rychlé a efektivní provedení řady opatření na posílení

odolnosti nastíněných v tomto sdělení. EU bude využívat a prohlubovat již nyní přínosnou spolupráci s NATO.

Unie je i nadále odhodlána využít k řešení složitého problému hybridních hrozeb veškeré příslušné nástroje EU. Prioritou pro Unii jakožto silnějšího a pohotovějšího subjektu zajišťujícího spolu se svými hlavními partnery bezpečnost zůstává podpora úsilí členských států.