1.1.1.

RADA EU **Brusel, 4. září 2013**

13280/13

PROCIV 98
COHAFA 96
COCON 35
JAI 732
COTER 115
TRANS 456
ENER 395
TELECOM 223
ECOFIN 765
PESC 1031

PRŮVODNÍ DOPIS

Od:	Generální tajemník Evropské komise, podepsaný p. Jordi AYET PUIGARNAU, ředitel
Datum přijetí:	28. srpna 2013
Komu:	p. Uwe CORSEPIUS, Generální tajemník Rady EU
Č. dokumentu:	SWD(2013) 318 v konečném znění
Předmět:	PRACOVNÍ DOKUMENT KOMISE o novém přístupu k Evropskému programu na ochranu kritické infrastruktury (EPCIP) Budování bezpečnější Evropské kritické infrastruktury

Delegace v příloze naleznou dokument Komise SWD(2013) 318 v konečném znění.

_____

Příloha: SWD(2013) 318 v konečném znění

EVROPSKÁ
KOMISE

Brusel, 28. 8. 2013
SWD(2013) 318 v konečném znění

PRACOVNÍ DOKUMENT KOMISE

o novém přístupu k Evropskému programu na ochranu kritické infrastruktury
Budování bezpečnější Evropské kritické infrastruktury

PRACOVNÍ DOKUMENT KOMISE
o novém přístupu k Evropskému programu na ochranu kritické infrastruktury

1. SOUVISLOSTI A CÍLE

Tento dokument stanovuje revidované a praktičtější provádění Evropského programu na ochranu kritické infrastruktury (EPCIP).

Nový přístup k EPCIP vychází z komplexního přezkumu EPCIP[1] z roku 2006 a Směrnice Rady 2008/114/EK[2], který byl veden v úzké spolupráci s členskými státy (ČS) EU a se zainteresovanými subjekty.

Přináší úplnou analýzu prvků současného programu a navrhuje přepracovaný přístup ochrany kritické infrastruktury (OKI) EU, založený na praktickém provádění činností v rámci pracovních proudů prevence, připravenosti a odezvy.

OKI spočívá v zabezpečení služeb životně důležitých pro společnost. Kritická infrastruktura představuje „*prostředky, systém nebo jejich část umístěné v ČS, které jsou zásadní pro udržení kritických sociálních funkcí, zdraví, bezpečnosti, ekonomického a sociálního blahobytu lidí a jejichž narušení nebo zničení jako důsledek selhání těchto funkcí*[3] *by mělo vážný dopad na členské státy*".

Jsme schopni minimalizovat důsledky ztrát v oblasti služeb ve společnosti jako celku tím, že se zajistí vysoký stupeň ochrany infrastruktury v EU a zvýší se její odolnost (proti všem hrozbám a nebezpečím). Tyto cíle převažují ve Stockholmském programu[4] a ve Strategii vnitřní bezpečnosti EU[5].

Jedna část našeho nového přístupu se dívá na **vzájemné závislosti[6],** a to mezi aktéry kritických infrastruktur, průmyslu a státu. Hrozby na jednotlivé kritické infrastruktury mohou mít významný dopad na širokou škálu aktérů v mnoha různých infrastrukturách.

Samozřejmě, že účinky těchto vzájemných závislostí nejsou omezeny jenom na jednotlivé země. Mnoho kritických infrastruktur má přeshraniční dimenzi. Navíc u **vzájemné závislosti mezi odvětvími** existuje také mnoho vzájemných závislostí v rámci téhož odvětví, které ale překlenují více evropských zemí. Jedním z takových příkladů je evropská elektrická síť vysokého napětí.

---

1 KOM(2006) 786 v konečném znění

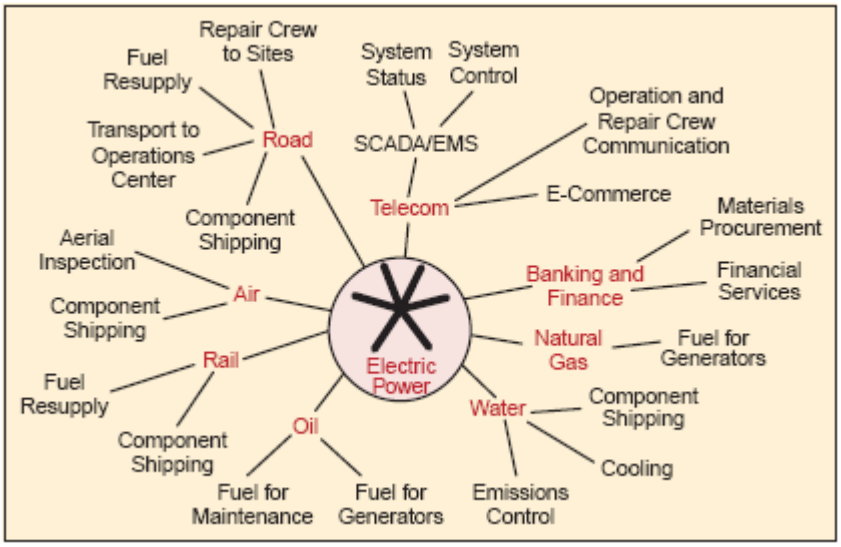
2 Směrnice Rady 2008/114/EK z 8. prosince 2008 o určování a označování EKI a o posouzení potřeby zvýšit jejich ochranu, Úřední věstník EU, L345/75.

3 Idem, čl.2 (a).

4 Závěry Evropské rady z 10/11 prosince 2009 k 'Stockholmskému programu — Otevřená a bezpečná Evropa, která slouží svým občanům a chrání je (2010-2014)'; 17024/09.

5 KOM (2010) 673 v konečném znění. Strategie vnitřní bezpečnosti EU:: pět kroků směrem k bezpečnější Evropě. Cíl 2: Prevence terorismu a předcházení radikalizace a náboru. Cíl 5: zvýšení evropské odolnosti na krize a katastrofy.

6 *'Vzájemná závislost: obousměrný vztah mezi dvěma infrastrukturami, jejichž prostřednictvím stát vlastnící infrastrukturu ovlivňuje nebo má vztah se státem vlastnící jiné infrastruktury. '* Steven M. Rinaldi, James P. Peerenboom, Terrence K. Kelly, Identifying, Understanding and Analysing Critical Infrastructure Interdependencies, IEEE Control Systems Magazine, December 2001, p.14



Obr 1[7] - Příklad závislostí u infrastruktury elektrické energie

V této souvislosti se například podíváme, kam až dosáhl vliv v případě současného plánování OKI a jak se může význam vzájemné závislosti zlepšit. Proces přezkumu současného EPCIP[8] vedený v úzké spolupráci s ČS a ostatními zainteresovanými subjekty odhalil, že se nebere dostatečný zřetel na vazby mezi kritickými infrastrukturami v různých odvětvích, dokonce ani přes státní hranice. Abychom mohli získat řádnou ochranu kritických infrastruktur a vybudovat jejich odolnost, potřebujeme pro vyřešení těchto nedostatků nový přístup. Nový přístup se započne se čtyřmi kritickými infrastrukturami evropského rozměru: Eurocontrol, Galileo, elektrická přenosová síť a plynová přenosová síť (Čtyřka). Tato Čtyřka byla vybrána na základě jejich pan-evropského charakteru a také podle jejich vlastního zájmu spolupracovat s Komisí na hledání přístupu k ochraně a odolnosti kritické infrastruktury, který bude brát více v úvahu vzájemné závislosti. Počítá se s tím, že také další významné infrastruktury budou profitovat z procesů a nástrojů, které budou vyvinuty pro práci Čtyřky.

Při práci se Čtyřkou a vytvářením nového přístupu bude mít EU, vedená Komisí, u ČS podpůrnou úlohu při jejich vlastních aktivitách v oblasti ochrany a odolnosti KI a zároveň bude moci v této oblasti usnadňovat spolupráci v rámci EU. Vzhledem k tomu, že mnoho kritických infrastruktur je v soukromém vlastnictví, tak lepší spolupráce zahrnuje podporu rozvoje strukturovaných dialogů se soukromým a veřejným sektorem.

2. NÁVAZNOST NA SOUČASNÝ PROGRAM

Ve své zprávě o EPCIP z 12. prosince 2006 vysvětluje Komise celkový politický přístup a rámec pro aktivity v oblasti ochrany kritických infrastruktur v EU. Tento navrhovaný nový přístup bude vycházet z tohoto rámce a bude zaměřený na své silné stránky a na řešení nedostatků zjištěných během procesu přezkumu. Čtyři hlavní oblasti, na které se EPCIP zaměří, jsou:

- Postup určování a označování evropských kritických infrastruktur a posouzení potřeby zvýšit jejich ochranu (podrobně popsané ve Směrnici Rady 2008/114/ES);

[7] *Totéž.*

[8] Pracovní dokument Komise o přezkumu Evropského programu na ochranu kritické infrastruktury (EPCIP), SWD(2012) 190 v konečném znění

- Opatření pro usnadnění provádění EPCIP zahrnující Akční plán, Informační síť KI (CIWIN), využití skupin odborníků na OKI na úrovni EU, proces výměny informací v oblasti OKI, a určování a analýzu vzájemné závislosti;

- Financování opatření souvisejících s OKI a projektů zaměřených na „prevenci, připravenost a zvládání následků teroristických útoků a jiných rizik spojených s bezpečností“ pro období 2007-2013; a

- Vývoj vnějšího prostředí EPCIP.

2.1. Směrnice Evropské kritické infrastruktury

Směrnice Rady 2008/114/ES[9] vyzývá ČS, aby určily a označily evropské kritické infrastruktury a zhodnotily potřeby pro zlepšení jejich ochrany. Všechny ČS tuto směrnici implementovaly na základě procesu určení a označení evropských kritických infrastruktur v odvětví energetiky a dopravy.

Nicméně evropských kritických infrastruktur bylo označeno méně než 20 a následkem toho bylo vypracováno jen málo nových plánů bezpečnosti provozovatele. Několik jasně kritických infrastruktur evropské dimenze, jako jsou hlavní elektrické distribuční sítě, nebylo zahrnuto. Navzdory zlepšení evropské spolupráce během procesu OKI, namísto vytvoření skutečného evropského fóra pro spolupráci povzbudila tato směrnice především bilaterální zapojení ČS.

Odvětvově zaměřený přístup směrnice rovněž představuje výzvu pro mnoho ČS, protože v praxi není analýza kritičností omezená odvětvovými hranicemi a řídí se spíše přístupem podle „systému“ nebo „služby“ (např. nemocnice, finanční služby).

Na druhou stranu, podle většiny názorů komunity OKI, se v EU zvýšila úroveň spolupráce a všeobecné povědomí o OKI, a to díky různým aktivitám a fórům organizovaným v rámci směrnice (konkrétně v odvětví energetiky a dopravy).

I když se názory na zlepšení bezpečnosti značně liší, vypadá to, že pouhá existence právního nástroje pomohla politikám zaměřených na ochranu národních kritických infrastruktur. V důsledku tohoto nástroje došlo ke konkrétním akcím, jako je vytvoření speciálních národních orgánů, které se zabývají politikami OKI. V odvětví energetiky bylo ve spolupráci s provozovateli dosaženo pokroku při zavádění opatření v oblasti zvládání rizik a ochrany.

Celkem vzato je směrnice Rady 2008/114/ES považována větší částí zainteresovaných subjektů za velmi zásadní. Navíc se očekává, že budou ekonomické a politické náklady pro přijetí a implementaci nového právního nástroje vysoké, především díky krátké době, která uběhla od transpozice a implementace současné směrnice. Většina komunity OKI očekává, že přínos současné směrnice, zejména u zvyšování povědomí, se bude dále zvyšovat.

Zachováním současné směrnice, konsolidací doposud vykonané práce a rozvojem **meziodvětvového přístupu** k EPCIP (popsáno v kapitole 3) můžeme řešit nedostatky současného přístupu a nezbavovat se výhod (aktuálních a potenciálních) současného právního rámce. Prostřednictvím tohoto přístupu můžeme dále podporovat prostředí důvěry a zajišťovat společné cíle včetně pružného zaměření na specifické oblasti, země a odvětví, kde je zapotřebí zlepšení.

[9] Směrnice Rady 2008/114/EK z 8. prosince 2008 o určování a označování EKI a o posouzení potřeby zvýšit jejich ochranu, Úřední věstník EU, L345/75.

Provozovatelé kritických infrastruktur včetně těch, kteří podnikají v energetice a v dopravě, budou navíc spadat pod zvládání rizik a budou u nich platit požadavky na podávání zpráv o nehodách navrhované ve směrnici o bezpečnosti sítí a informací[10].

2.2. CIWIN

Sdělení EPCIP z roku 2006 vyzvalo k vytvoření Informační sítě pro kritickou infrastrukturu (CIWIN). Tento chráněný bezpečnostní a informační systém na internetové bázi je určen k diskusi a pro výměnu informací souvisejících s OKI (studie a/nebo osvědčené postupy) v rámci komunity EU. CIWIN se v prosinci 2012 posunul do provozní fáze a funkční je od ledna 2013. V prvních měsících jeho existence byl zaznamenán pozitivní vývoj, a to včetně nárůstu využívání statistik a vyhrazeného prostoru CIWIN pro národní účely.

Očekává se, že se bude CIWIN dále rozvíjet a že bude sloužit jako důležitý interaktivní nástroj pro vývoj zde popisovaného přístupu EU. Tato role může být naplněna prostřednictvím několika důležitých funkcí CIWIN:

- Síť budeme využívat pro ukázku vývoje vybraných případů pan-evropských kritických infrastruktur a k získání zpětné vazby od uživatelů CIWIN.
- Cílem CIWIN bude nabídnout soubor nástrojů obsahující metodiky posouzení rizik a nástroje pro analýzu rizik (např. šablony).
- CIWIN se může stát hostitelskou platformou pro několik národních oblastí OKI v ČS.
- Tato síť bude obsahovat všechny důležité informace týkající se spolupráce s vybranými třetími zeměmi jako je USA, Kanada a země EFTA.

2.3. Vnější prostředí EPCIP

Komise získala ve svých závěrech z června 2011[11]od Rady mandát pro další rozvoj vnějšího prostředí EPCIP. V závěrech jsou vyzváni jak Komise, tak ČS k pokračování ve spolupráci s třetími zeměmi nejen kvůli výměně osvědčených postupů, ale také aby byly určeny kritické infrastruktury ve třetích zemích, které je mohou potenciálně ovlivňovat a naopak.

ČS daly najevo, že vnější prostředí je pro OKI velmi důležité. Především je považována za prioritu spolupráce se zeměmi EFTA. Aby této spolupráci s EEA dala Komise formální souhlas, tak představila návrh rozhodnutí Rady pro rozšíření použitelnosti směrnice 2008/114/ES na země EEA[12], které vedlo k rozhodnutí společného výboru EEA o určování a označování evropských kritických infrastruktur[13]. Jak Norsko, tak Island nedávno oznámily splnění jejich ústavních požadavků pro platnost tohoto rozhodnutí[14].

---

10 KOM(2013)48

11 Závěry Rady z 9-10. června 2011 o rozvoji vnějšího rozměru Evropského programu na ochranu kritické infrastruktury

12 Návrh pro Rozhodnutí Rady pro pracovní skupinu EFTA o pozici, kterou má převzít EU ve společném výboru EEA týkající se přepracování protokolu 31 do smlouvy EEA, o spolupráci ve speciálních oblastech mimo čtyř svobod (smlouva — dok. 7539/12 EEE 19 AELE 15 PROCIV 40).

13 EEA Rozhodnutí společného výboru 101/2012 (určování a označování EKI).

14 Oznámení z Norska (7/12/2012) a Islandu (4/3/2013) o splnění ústavních požadavků pro rozhodnutí 101/2012 – upravující protokol 31 pro smlouvu EEA – Směrnice Rady 2008/114/EK.

Navržené nařízení ustanovující nástroj stability (IfS)[15] — nástroj vnější spolupráce — umožňuje pomoc při ochraně kritické infrastruktury ve třetích zemích, v oblasti mezinárodní dopravy (letectví a námořní dopravě), v energetických operacích a v distribuční síti, a v elektronicko-informačních a komunikačních sítích (kybernetická bezpečnost).

Pro podporu strategického partnerství mimo Evropu se také ročně konala setkání odborníků EU-US a EU-Kanada, naposledy v květnu 2013. Tyto jednání jsou zaměřené především na potřebu posílit spolupráci, a to cestou výměny informací, osvědčených postupů a informací o OKI, včetně rozvoje bezpečnostního balíčku globální infrastruktury. Jejich účelem je podpora výměny osvědčených postupů, metodik, analýz, získaných zkušeností a jiného užitečného materiálu mezi EU, USA a Kanadou. Při budoucích setkáních se budeme koncentrovat na vybraná témata, jejichž důležitost pro OKI v mezinárodní dimenzi roste. Mezi ně patří: zahraniční vzájemné závislosti; vzájemná propojenost kritické infrastruktury; možnost globálních kaskádovitých efektů; a vzájemné závislosti fyzických a kybernetických infrastruktur.

2.4. Projekty související s OKI

V rámci EU se uskutečnilo více kroků pro vytvoření povědomí o tom, jak lépe ochránit kritické infrastruktury. Pod programem „**Prevence, připravenost a zvládání následků teroristických útoků a jiných rizik spojených s bezpečností“** (CIPS) v období od 2007-2012, který je zaměřený na OKI a krizové řízení[16], jsme nalezli 100 rozličných projektů. Tyto projekty mají velký rozsah, zasahují do všech odvětví včetně analýz kritičností a závislostí.

Klíčovým cílem tohoto souboru projektů bylo poskytnout odborné znalosti a hlubší pochopení o kritické infrastruktuře na všech úrovních, zavedení OKI do politických priorit a poskytnutí vědeckého základu pro tuto práci. V rámci mezi-odvětví mělo těchto několik příkladů projektů viditelnost v komunitě OKI a dosáhly dobrého výstupu:

- Definice metodiky pro posouzení vzájemné závislosti mezi ICT a výrobou/distribucí elektrické energie[17];
- Manuál osvědčených postupů OKI pro tvůrce politiky[18];
- Zlepšování znalostí o účinné OKI a usnadnění výměny osvědčených postupů[19];
- Sdílení informací ze systémů varování a vyrozumění na národní a evropské úrovni[20];
- Simulace modelů vzájemné závislosti[21] kritické infrastruktury ICT.

Jednou z vlajkových lodí je čtyřletý projekt ERNCIP (Evropská referenční síť pro OKI). Jeho úkolem je *„podporovat vývoj inovativních, kvalifikovaných, účinných a konkurenceschopných bezpečnostních řešení prostřednictvím propojení evropských experimentálních kapacit“.* Pro zajištění tohoto cíle udržuje ERNCIP archiv experimentálních kapacit EU; zde se vytváří síť

15 KOM(2011) 845 v konečném znění.
16 CIPS 2007-2012: 111 přiřknutých projektů (CIP — 70; krizové řízení — 32; kombinované — 9). Celková přiřknutá částka: 45 mil. EUR.
17 JLS/2007/CIPS/019.
18 JLS/2009/CIPS/AG/C1-036.
19 JLS/2008/CIPS/011.
20 JLS/2008/CIPS/016.
21 JLS/2009/CIPS/AG/C2-42.

odborníků z různých oblastí souvisejících s OKI, jako je CBRN, určování výbušnin, kybernetická bezpečnost proti zemětřesení; a ta také přispívá ke standardizačním aktivitám.

Prostřednictvím Sedmého rámcového programu (FP7) programu Bezpečnost bylo až dosud financováno více než 40 projektů souvisejících s OKI. Tyto projekty pokrývaly všechny druhy kritických infrastruktur a všechny typy hrozeb, včetně kybernetických hrozeb[22].

V souvislosti s metodikami **posouzení rizik** a **zvládání rizik** Komise také financovala četné projekty, které pokrývaly všechny odvětví pod programem CIPS. Sem patří: rozvoj metodiky posouzení rizik pro zlepšení bezpečnostní informovanosti v řízení letecké dopravy[23]; vyhodnocení odolnosti vůči hrozbám u řízení kontrolních a datových systémů energetických distribučních sítí[24]; a interaktivní posouzení rizik v oblasti kritické infrastruktury, které vychází z dat systému pozorování Země a systému integrovaných geografických informací[25].

Studie ukazují, že metodiky posouzení rizik pro OKI vycházejí buď 1) z odvětvového přístupu, kde se každé odvětví zpracovává odděleně, a to vlastními metodikami určení a řazení rizik; nebo 2) ze systémového přístupu, kde jsou kritické infrastruktury brány jako propojená síť. Většina prací byla odvětvová, ovšem tyto metodiky ukazují svá omezení tam, kde je zapotřebí řešit problematiku meziodvětvových problémů. Proto bude nyní Komisí podporován **systémový přístup**.

3. VEDENÍ NOVÉHO PŘÍSTUPU K EPCIP

V první fázi by se měl vést praktický přístup se čtyřmi vybranými infrastrukturami evropského rozměru - Eurocontrol, Galileo, elektrická přenosová síť a plynová přenosová síť za účelem optimalizace jejich ochrany a odolnosti.

Tato čtyřka byla vybrána na základě:

- evropského charakteru, díky jejich přeshraniční dimenzi. Tento přeshraniční rozměr mají jak z fyzických důvodů (např. infrastruktury jsou umístěné na území více než jednoho členského státu), tak podle úrovně nabízených služeb (např. narušení služeb v jednom členském státě může mít dopad na několik dalších členských států – domino efekt);

- jejich symboličnosti — vybrané případy pokrývají odvětví dopravy, energetiky a vesmíru; a

- zájmu jejich provozovatelů/vlastníků podílet se na tomto pilotním úkolu a sdílet osvědčené postupy.

EUROCONTROL[26] je určena jako Síťový manažer pro EU ATM (uspořádání letového provozu) síť, která spravuje přibližně 30 000 letů za den. Cíle, úkoly a funkce Síťového

[22] V současnosti probíhá jeden větší ukázkový projekt s EU přispěním ve výši 25 mil. EUR. Jeho cílem je vypracovat soubor nástrojů ke zlepšení bezpečnosti městské dopravy cestou rozvoje balíku modulárních řešení vyhodnocených prostřednictvím demonstrace ve velkých evropských městech.

[23] HOME/2010/CIPS/AG/030.

[24] JLS/2008/CIPS/018.

[25] HOME/2010/CIPS/AG/037.

[26] Viz příloha I.

manažera se řídí dle nařízení Komise (EU) č. 677/2011 ze 7. července 2011, které podává podrobná pravidla pro implementaci funkcí sítě ATM[27].

GALILEO[28] je evropský program pro globální satelitní navigační systém, který je částečně vlastnictvím EU a bude poskytovat velmi důležité služby našim občanům a našemu hospodářství.

Elektrická přenosová síť[29] a **Evropská plynová přenosová síť**[30] jsou sítěmi bez národních hranic, což znamená, že když dojde k poruše jedné části sítě, může se rozšířit do dalších oblastí, a tak mít vliv na několik zemí.

Po určení důležitosti použití systémového přístupu nyní musíme zjistit, jakým způsobem nejlépe umožnit čtyřem infrastrukturám, aby zvážily mezi-odvětvové faktory při posilování svých aktivit pro ochranu kritických infrastruktur.

Prvním stupněm práce se Čtyřkou bude zajistit celkové pochopení jejich opatření OKI, zaznamenat pracovní zaměření prevence, připravenosti a odezvy, včetně zjištění, jak se vzájemné závislosti a kaskádovité efekty objevují v jejich plánování OKI. Potom nastoupí společné činnosti na určení společných faktorů a zvažování cest, jakými lze ochranu KI a opatření odolnosti zlepšit.

I. Prevence

Začneme převzetím do té doby nashromážděných pracovních výsledků, provedeme aktualizaci vývoje bezpečnostních opatření a vývoje vzájemné závislosti s jinými odvětvími (ICT, vodní hospodářství, atd.). Tyto činnosti vytvoří základnu, ze které se bude vycházet.

Práce se Čtyřkou budou pokračovat založením nástrojů pro **posouzení rizik a zvládání rizik**, využitím výsledků současného výzkumu a inovačních aktivit prováděných v rámci FP7 zejména programu Životního prostředí (zahrnující klimatické změny). Tyto aktivity souvisejí především se skupinou pro pozorování Země (GEO) – jako je Iniciativa supersítě – a s vývojem metodik posouzení nebezpečných rizik pro události s nízkou pravděpodobností – vysokými následky, které mohou být využity v budoucnu v „zátěžových testech“ u kritických infrastruktur.

Co se týče odvětví ICT, Strategie kybernetické bezpečnosti – Otevřeného a bezpečného kybernetického prostoru[31] – určuje kroky, které dále přispějí ke kybernetické odolnosti a bezpečnosti infrastruktur z EPCIP. Návrhy strategií obsahují koordinované ochranné mechanismy, kvalitnější připravenost a zapojení soukromého sektoru.

Tam, kde to bude třeba, budeme mezi Čtyřkou sdílet informace za účelem určení příležitostí k posílení existujících plánů ochrany. Budeme podporovat dialog mezi provozovateli kritických infrastruktur a aktéry, na kterých jsou závislí; budeme podporovat výměnu osvědčených postupů a tvorbu scénářů cvičení, směrnic a doporučení. Budeme zkoumat, kde nástroje jako analýzy nabízené např. Střediskem EU pro analýzu zpravodajských informací

---

27 Nařízení Komise (EU) č. 677/2011 ze 7. července 2011, které přináší podrobná pravidla pro implementaci funkčností sítě uspořádání letového provozu (ATM) a upravuje nařízení (EU) č. 691/2010, Úřední věstník EU, L 185/1.

28 Viz příloha II.

29 Viz příloha III.

30 Viz příloha IV.

31 JOIN (2013) 1.

(INTCEN) a vývoj metodik pro zátěžové testy mohou hrát roli při zlepšování účinnosti existujících opatření. Také při práci se Čtyřkou zvážíme, zda by bylo užitečné mít lepší spojení s posouzením rizik a řídícími aktivitami prováděnými v rámci Mechanismu civilní ochrany Unie [32].

Ve všech těchto uvedených aktivitách bude mít Komise podpůrnou úlohu, bude vytvářet směrnice, metodické nástroje a jiné pomocné nástroje pro celkové posouzení závislostí a kritičností.

II. Připravenost

Připravujeme také podporovat rozvoj strategií pro připravenost vycházejících z kontingenčního plánování, zátěžových testů, zvyšování povědomí, odborné přípravy, společných kurzů, cvičení a výměnných programů. Vytváření podobného systému lze také podporovat prostřednictvím informování o nehodách, které mohou být podporovány jako prostředek pro zlepšení úrovně znalostí o výkonu kritických infrastruktur během nehody (např. rozsah kaskádovitého efektu, celkový dopad, atd.). Se Čtyřkou budeme pokračovat na získání obrazu o tom, co je využitelné na evropské úrovni.

Budeme také prosazovat a usnadňovat dialog mezi provozovateli kritických infrastruktur a jejich účastníky, na kterých jsou závislí. Cílem je **u členských států a jiných aktérů závislých na kritické infrastruktuře** zvýšit **povědomí o tom, jak se mohou v rámci odezvy připravit na události, které mohou zasáhnout evropskou kritickou infrastrukturu**. Členské státy a jiní aktéři mohou dobrovolně sdílet informace o nehodách souvisejících se Čtyřkou, které je mohou postihnout. Tím, že tento dialog proběhne, tak také můžeme zlepšit celkovou úroveň připravenosti.

Dále budeme zkoumat možnost propojení sítě odborné přípravy civilní ochrany, která je plánovaná v návrhu nového Mechanismu civilní ochrany Unie, a to s odpovídajícím souborem aktivit odborné přípravy v oblasti kritických infrastruktur. Pro podtrhnutí komplementarity opatření EU pro připravenost se plánují společná cvičení s relevantními odvětvími nebo s Mechanismem civilní ochrany.

III. Odezva

Usnadněním dialogu v rámci připravenosti tak může Komise pomoci označeným aktérům, aby se zamyslely nad jejich odezvou na různé události. Našim cílem je posílit spojení mezi komunitou kritické infrastruktury a systémy včasného varování, protože nástroje včasného varování na přírodní katastrofy mohou ukázat na potenciální hrozby vůči kritickým infrastrukturám. Taky chceme, aby lidé začali uvažovat o mechanismech průběžné komunikace v době, kdy není obnovená funkčnost mezi Čtyřkou a dalšími aktéry, kteří na ní závisí.

Vzhledem k tomu, že se současný Mechanismus civilní ochrany Unie zaměřuje pouze na bezprostřední odezvu nějaké události, budeme zkoumat, jak by mechanismus dále mohl napomáhat využitím odborníků na obnovu, kteří by byli rozesíláni na požádání členských států a pomohli by s dlouhodobou obnovou kritických služeb. Se Čtyřkou se bude pracovat na tom, zda by bylo užitečné pro ochranu kritických infrastruktur, kdyby se v rámci mechanismu

[32] 2007/779/EK, Euratom: Rozhodnutí Rady z 8. listopadu 2007 o vytvoření Mechanismus civilní ochrany Společenství (přepracovaná verze).

vytvořily specifické moduly pro OKI, nebo případně se do existujících modulů zahrnuly požadované expertízy na OKI.

4. CESTA VPŘED

Komise bude nadále rozvíjet ochranu a odolnost již existujících opatření a hledat, jak jejich využití zlepšit. Kromě toho se tento nový přístup také snaží rozšířit dialog mezi kritickými infrastrukturami a těmi všemi aktéry napříč Evropou, kteří by byly postiženy jakoukoliv událostí ovlivňující jejich funkčnost. Tato aktivita bude prováděná v rámci aktivit prevence, připravenosti a odezvy, a to po označení relevantních pan-Evropských kritických infrastruktur. Komise si ponechá svou roli usnadňovat a podporovat činnost kritických infrastruktur, členských států a průmyslu a nabízet služby, které tito aktéři mohou využít pro zlepšení OKI napříč Evropou.

Také je důležité, aby paralelně s tímto novým přístupem členské státy a soukromý sektor pokračovaly a snažily se označit evropské kritické infrastruktury – vycházely z jejich dosud provedené práce a výsledků již dokončených projektů. CIWIN bude i nadále podpůrným nástrojem v tomto procesu.

V rámci tohoto nového přístupu začne okamžitě pilotní fáze, ta stanoví plán a vytýčí úkoly, které se mají dokončit do druhé poloviny roku 2014. Po uplynutí této doby bude Komise zpětně informovat o dosažených výsledcích a další cestě vpřed. Vedením této akce je pověřeno DG HOME s vědeckou podporou Společného výzkumného střediska (JRC), a to společně se čtyřmi vybranými kritickými infrastrukturami a přidruženými generálními ředitelstvími (např. DG MOVE, DG ENTR, DG RTD, DG ENER a DG ECHO).

Členské státy a další zainteresované subjekty (jako jsou společnosti provozovatelů) budou vyzváni k aktivní účasti na všech stupních pilotní fáze. Jejich technická vstupní data budou mít velkou cenu, když budou úspěšně dokončená. Přínos bude trojnásobný: hlubší pochopení toho, jak jsou aktéři v členských státech (jak z veřejného tak ze soukromého sektoru) závislí na Čtyřce; lepší přístup k nástrojům a k osvědčeným postupům identifikovaných Komisí během tohoto procesu; a příležitost přispět do diskusí o tom, jak mohou kritické infrastruktury nejlépe využívat výhod ze struktur EU s cílem zlepšit jejich ochranu i po skončení pilotní fáze.

Tento přístup nabízí příležitost vytvořit v Evropě více kohezní plánování OKI. Tím, že budeme mluvit k některým evropským kritickým infrastrukturám o tom, co dělají správně a jak by se mohly učit jedna od druhé, pomůžeme jim, aby si zabezpečily optimální plán OKI. Přimějeme-li odvětví, aby mezi sebou komunikovaly, a do tohoto dialogu zapojíme i členské státy, tak můžeme rozšiřovat jejich osvědčené postupy a napomoci jejich využívání i v jiných kritických infrastrukturách po Evropě. Hledáním možnosti zapojení struktur EU můžeme zlepšit schopnost odezvy na nějakou událost.

Po pilotní fázi očekáváme, že se bude situace vyvíjet následovně:

- Uplatnění pracovních proudů v těchto čtyřech pan-evropských kritických infrastrukturách by mělo poskytnout nutné indikátory, podle nichž se bude vypracovávat **přístup EU k OKI**. Přístup bude vycházet ze získaných výsledků a z nedostatků zjištěných při práci se Čtyřkou a bude se snažit poskytnout užitečné nástroje pro zvýšení ochrany a odolnosti, počítaje v to opatření pro **posílení zmírnění rizika, připravenosti a odezvy.**

- Dalším krokem může být **implementace tohoto přístupu v regionech**, kde mají členské státy zájem o vzájemnou spolupráci. Příklady by mohly zahrnovat koncepci odolnosti pro celkovou kritickou infrastrukturu dopravy v okolí Baltského moře a program pro řetězce kritičnosti v Podunají.

- Činnosti prováděné v souladu s tímto novým přístupem by se měly porovnat s časovým harmonogramem nového víceletého finančního rámce 2014-2020 a propojit se s jeho klíčovými prioritami. Namísto financování velkého počtu rozličných projektů by se mělo spustit několik velkých přeshraničních strategických projektů

- EU bude v této souvislosti hrát **podpůrnou úlohu**, pomáhat rozvoji politiky OKI a vzrůstající spolupráci mezi komunitami OKI, jakož i rozdělování finančních prostředků na podporu klíčových politických cílů nastíněných v tomto dokumentu.

Nový přístup EU bude takto podporovat vývoj OKI na všech úrovních (od místní a národní až po evropskou a mezinárodní), vytvářet Evropu bezpečnější a lépe připravenou na hrozby na jejich kritické infrastruktury a zlepšovat celkovou odolnost proti potenciálním poruchám.

PŘÍLOHY: VYBRANÁ PAN-EVROPSKÁ KRITICKÁ INFRASTRUKTURA

Příloha I. EUROCONTROL

V kontextu rozvoje a fungování Jednotného Evropského nebe, byla určena agentura EUROCONTROL jako Síťový manažer ATM sítě pro EU. To předpokládalo vytvoření kooperujících opatření pro konzultace a rozhodovací proces se všemi zúčastněnými hráči ve vzdušných dopravních operacích (např. národní dopravní poskytovatelé služeb, uživatelé vzdušného prostoru, letiště, kompetentní národní úřady a vojenské úřady a servisní zásobovací úroveň). Důležitá operační aktivita Síťového manažera je koordinace Managementu vzdušného dopravního toku s organizacemi Vzdušného dopravního řízení v Evropě.

Ve spojení s tímto, je jeden z úkolů Síťového manažera zajišťovat podporu pro síť krizového řízení: Evropská letecká krizová koordinační buňka (EACCC), zahrnující stálé reprezentanty všech ATM zainteresovaných subjektů a různé EU instituce stejně tak, jako kontaktní body v korespondujících strukturách v Členských státech; byla formálně založena k zmírňování potenciálních síťových krizí. Je využívána k pravidelnému setkávání, k simulaci možných scénářů nepříznivě ovlivňující letectví a které mohou být deklarovány jako síťové krizové události a k organizaci ad hoc setkání s kontaktními body v členských státech. Síťový manažer, ve spojení se členy EACCC, je odpovědný za aktivaci a deaktivaci EACCC, koordinování řízení odpovědi na síťové krize, monitorování implementace kontingenčních plánů a navrhování procedur, jestliže neexistují kontingenční plány.

Fungování EUROCONTROL jako Síťového manažera a EACCC může být jedním ze subjektů pro dlouhodobou případovou studii, vedenou HOME ve spojení s dalšími dotčenými službami, s cílem identifikovat nejlepší postupy v aplikování opatření pro prevenci-připravenost a pracovní proudy odezvy zmíněné výše, a vedoucí k rozvoji strategií zmírňující riziko, atd., které by také mohly přispět k lepší ochraně dalších kritických infrastruktur a sektorů.

Jeho komplexní infrastruktura, předmět několika scénářů na hrozby, včetně kybernetických hrozeb, kde přerušení jeho služeb může mít významný dopad na evropské hospodářství, a vzájemné závislosti mezi různými subsystémy vedoucí k různým kaskádovitým efektům, vytvářejí také zajímavý případ pro studii.

Některé nedávné krizové situace také plně zdůvodňují potřebu EACCC a získané zkušenosti z této práce budou také užitečné. To zahrnuje:

- útoky 9/11 2001, kdy, od okamžiku, kdy EUROCONTROL obdržel informaci, že vzdušný prostor USA je uzavřen, trvalo pouze pár minut k výstraze všem evropským leteckým operátorům a letištím k zabránění odletů letů směřujících do USA;

- krize oblaku vulkanického popela, od 15. do 21. dubna 2010, vedla ke zrušení 100 000 letů v Evropě (54% všech letů), s dopadem na světové hospodářství ve výši zhruba 3 mld. EUR. Je odhadováno, že 10 milionů pasažérů uvízlo na letištích po dobu 6 dní. EUROCONTROL hrál klíčovou roli v komunikaci, sdílení informací a zvyšování povědomí; a

- silné sněžení v prosinci 2010, kdy tisíce letů bylo zrušeno napříč Evropou, mnoho dalších zpoždění a tisíce pasažérů uvízlých na letištích na několik dní.

(Navrhovaná studie by neměla ovlivnit regulační rámec řídící ATM Síťového manažera, ani úkoly, nástroje nebo procesy, které již existují.)

Příloha II. GALILEO

Vesmírný systém umožňující široké spektrum aplikací, které hrají fundamentální roli v našem každodenním životě, jsou kritické pro klíčové oblasti hospodářství, a pomáhají zajistit naší bezpečnost. S rostoucí závislostí na vesmírných službách, se stává schopnost chránit vesmírnou infrastrukturu nezbytnou pro naši společnost.

Jakékoliv odstavení byť jen části vesmírné infrastruktury může mít závažné následky pro dobré fungování hospodářských aktivit a naší občanské jistoty a bezpečnosti, a může poškodit zajištění záchranných služeb. Toto platí především pro Galileo – Evropský globální družicový polohový systém (GNSS) – který je první vesmírnou infrastrukturou vlastněnou EU. Větší selhání, ať již náhodné či úmyslné, této GNSS infrastruktury dopadne na uživatele, ale také ovlivní mnoho dalších kritických infrastruktur, ve kterých jsou GNSS služby již hluboce integrovány: dopravu, telekomunikace, obchod a bankovní aktivity závislé na načasování podle GNSS signálů, navigace a bezpečnostní transakce.

Galileo, jako další vesmírné infrastruktury, čelí specifickým hrozbám pro signál a pro satelity. GNSS signály mohou být předmětem mnoha hrozeb na radiových frekvencích jako je interference, neautorizovaný přístup, zneužití, úmyslné rušení, falzifikace a kybernetické útoky. Systém Galileo podstoupil specifické bezpečnostní procesy ke zmírnění indukovaných rizik. Dále jedna ze služeb Galilea, Veřejná regulovaná služba (PRS) byla speciálně vyvinuta k podpoře členských států EU a vládou autorizovaných uživatelů pro citlivé aplikace, které vyžadují efektivní řízení přístupu a neomezené a nepřerušované internetové spojení.

Dále se stal vážnou hrozbou pro udržitelnost vesmírných aktivit včetně operací satelitního modelu Galileo, vesmírného segmentu Copernicus nebo přispívajícím národním veřejným a komerčním satelitům vzrůstající počet vesmírných trosek. V zájmu zmírnění rizika kolize je nezbytné identifikovat a monitorovat satelity a vesmírné trosky, katalogizovat jejich pozice, a sledovat jejich pohyb (trajektorii) když je identifikováno potenciální riziko kolize tak, že satelitní operátoři mohou být varováni, aby odklonily jejich satelity. Tato aktivity je známa jako dozor a sledování (SST), a většinou je dnes založena na pozemních senzorech, jako jsou teleskopy a radary. V současnosti není na evropské úrovni žádná SST kapacita; satelitní a vypouštěcí operátoři jsou závislý na datech USA pro antikolizní varování. Komise navrhuje podpůrný program pro vesmírný dozor EU a sledování (SST). Cílem tohoto programu je podpořit členské státy ve spolupráci a síťování jejich SST kapacit a zajištění antikolizní výstražné služby na evropské úrovni.

Příloha III. Evropská elektrická přenosová síť

Výpadky elektřiny na rozsáhlém území v minulých letech ukázaly, že jediný incident ovlivňující důležitý prvek sítě, může ovlivnit dodávku na celém kontinentě. Hrozby (způsobené člověkem) mají také stejný cíl a způsob provedení přes hranice států, zatímco jednotlivý útočníci nebo koordinované akce mohou útočit na sítě v regionálním, evropském nebo mezinárodním měřítku, jako je to v případě kybernetických útoků.

Rozsáhlé přerušení dodávky elektřiny se vyskytlo na severoněmecké přenosové síti 4. listopadu 2006 a kromě Německa bylo cítit na většině kontinentu včetně Rakouska, Belgie, Francie, Slovinska a Španělska. Ačkoli akce přijaté přenosovými systémovými operátory (TSOs) fungují preventivně proti výpadku elektřiny, tento případ je považován v Evropě za jeden z nejhorších a nejrozsáhlejších přerušení v minulosti. Důsledky byly zásadní ve smyslu přerušení dodávek elektřiny na průmyslové i domácí úrovni (více než 15 milionů domácností), také služby závislé na elektřině, jako je doprava, byly ovlivněny (např. stovky vlakových spojů byly zrušeny nebo zpožděny).

Tato výzva ke koordinovanému ochrannému mechanismu zahrnuje všechny operátory a jejich oborové orgány. Rizika spojená s výše zmíněnými hrozbami mohou být řádně zacílena odezvou na systémové úrovni, protože integrity a funkcionalita celého systému je ovlivněna. Odvětví (především ENTSO-E) již investovalo do CIP opatření a vyjádřilo silnou podporu přístupu EU, který odpovídá požadavkům opatření vnitřního trhu. Síťové kódy nabízejí citlivý rámec k posílení včlenění společných ochranných metodik pro operátory evropské sítě. Komise může podporovat tento proces během následujících let zajištěním nástrojů a metod CIP.

Kromě toho vývoj směrem k „chytrým sítím“ volá po rozšíření synergií mezi sektorem informačních a komunikačních technologií (ICT) a sektorem energetiky. Více než jindy jsou průmysl a investoři znepokojeni hrozbami kybernetické bezpečnosti. Komise proto iniciovala akci pod vedením Operační skupiny chytrých sítí, kde zainteresované subjekty z energetických a ICT sektorů v současnosti vytvářejí rámec pro hodnocení kybernetické bezpečnosti. Tento rámec zahrnuje hodnocení dostupných metodik pro spolehlivou síť, sdílení analýz zranitelnosti a hrozeb pro chytré sítě a chytré měřící systémy, stejně tak jako identifikaci nejlepších dostupných technik pro chytré měřící systémy.

Příloha IV. Evropská plynová přenosová síť

Fyzické hrozby (sahající od terorismu k bojkotům a stávkám), ničivé přírodní události (zemětřesení, povodně, období mrazu, silné bouře) a obchodní spory, které ovlivňují tuto síť, ji mohou oslabit a ohrozit evropský bezpečný přístup k plynu.

Ilustrativním příkladem vlivů přerušení plynové sítě je případ plynovodu Družba v roce 2009. Tento plynovod, který každý den dopravuje do Evropy skoro 300 miliónů kubických metrů ruského plynu, procházející Ukrajinou, začal počátkem ledna omezovat svůj průtok až do úplného zastavení. Jeho přerušení mělo významný dopad na mnoho členských států, zejména ty, které závisejí výhradně na této dopravní cestě, byly ponechány domovy bez plynu pro topení a vynuceno zastavení produkce v některých průmyslových odvětvích. Dodávky plynu byly plně obnoveny 21. ledna 2009. Toto přerušení bylo nejvážnějším svého druhu v Evropě v nedávné historii: na bezprecedentní období dvou týdnů byla Evropa odstřihnuta od 30% svého celkového dovozu plynu, ekvivalent 20% její dodávky plynu.

Potřeba koordinace na evropské úrovni je tedy jasná a je rozpoznaná Evropskou plynovou infrastrukturou (GIE), reprezentující evropské operátory v oboru. GIE vyjádřila svou podporu programu EPCIP a navrhla rozvoj společné metodologie pro posouzení rizik/hrozeb pro infrastrukturu plynového sektoru v Evropě, berouce v potaz přístup pro všechna rizika. Toto bude v souladu s koordinací prevence a odezvy implementované v plynovém sektoru Nařízením 994/2010, zejména příprava národního posouzení rizik a preventivní akce a pohotovostní plány vytvořené na základě posouzení rizik.

Příloha V. Plán

Akce 1 – Návrh přístupu EU pro ochranu a zvýšení odolnosti Evropské kritické infrastruktury	***Výkonný činitel***	***Časový rámec***
Detailní hodnocení a analýzy procesů a metodologií užitých ve vybraných případech	DG HOME (vedoucí), JRC (podpora) a vybrané zainteresované subjekty	Počátek v druhé polovině 2013
Odsouhlasit kritičnosti a vzájemné závislosti vybraných případů. Odsouhlasit koncepty, definice a metodologii pro posouzení rizik a zvládání rizik KI.	DG HOME (vedoucí), JRC (podpora) a vybrané zainteresované subjekty	Počátek v druhé polovině 2013
Odsouhlasit pohotovostní opatření jako jsou kontingenční plánování, zátěžové testy, zvyšování povědomí, programy odborné přípravy, společné kurzy, cvičení a/nebo výměnné programy.	DG HOME (vedoucí), JRC (podpora) a vybrané zainteresované subjekty	Počátek v druhé polovině 2013
Prozkoumat možnosti pro vytvoření týmů specialistů EU na obnovu KI velkého významu, k pomoci s dlouhodobou obnovou kritických služeb a k využití na vyžádání členských států.	DG HOME a DG ECHO	Počátek v druhé polovině 2013
Hodnocení dosažených výsledků a identifikování nedostatků.	DG HOME (vedoucí) a JRC (podpora)	První polovina 2014
Diskutovat a schválit přístup EU s členskými státy a zainteresovanými subjekty	DG HOME, členské státy a KI operátoři	První polovina 2014
Akce 2 – Rozšiřování implementace přístupu EU	***Výkonný činitel***	***Časový rámec***
Identifikovat a vybrat další možné pan-evropské infrastruktury pro implementaci vytvořeného přístupu.	DG HOME, členské státy a KI operátoři	Druhá polovina 2014
Implementovat na vybrané pan-evropské infrastruktury. Pokračovat ve sdílení a šíření vybraného přístupu do regionů, s projekty pokrývajícími Euro-regiony nebo	DG HOME (vedoucí). JRC (podpora), KI operátoři a členské státy	Druhá polovina 2014

zahrnující skupinu členských států.		
Připojit fondy ISF k realizaci přístupu vytvořeného EU.	Komise	Počínaje 2014

-+