Ochrana kritické infrastruktury Evropské unie

Critical Infrastructure Protection of European Union

Bc. David Kotík

Diplomová práce
2008

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2007/2008

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. David KOTÍK**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Ochrana kritické infrastruktury Evropské unie**

Zásady pro vypracování:

1. **Analýza hrozeb současnosti**
2. **Zhodnocení současného stavu v oblasti KI EU**
3. **Organizace ochrany KI EU**
4. **Analýza opatření v rámci EPCIP**
5. **Důsledky opatření ochrany KI EU pro Českou republiku**

Rozsah práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **K ochraně kritické infrastruktury v ČR, In Sborník 4.mezinárodní konference Crisis management, Bezpečnost Připravenost Ochrana obyvatelstva, 1. vydání, Brno 2006, 349 s. ISBN 8072311418.**
2. **Zelená kniha o Evropském programu na ochranu kritické infrastruktury, Brusel 2005, KOM 2005 576 v konečném znění.**
3. **The European Programme for Critical Infrastructure Protection (EPCIP), Brusel 2006, MEMO/06/477.**

Vedoucí diplomové práce: **doc. Ing. Luděk Lukáš, CSc.**
Ústav elektrotechniky a měření

Datum zadání diplomové práce: **22. února 2008**

Termín odevzdání diplomové práce: **4. června 2008**

Ve Zlíně dne 22. února 2008

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce se zabývá ochranou kritické infrastruktury Evropské unie. Je rozdělena do několika částí, ve kterých jsou popsány současné hrozby, které ohrožují Evropské unii, je zhodnocen současný stav kritické infrastruktury Evropské unie, rozebrána organizace ochrany kritické infrastruktury, jsou vymezeny podpůrná opatření pro EPCIP a definovány důsledky opatření ochrany kritické infrastruktury Evropské unie pro Českou republiku. Jednotlivé oblasti kritické infrastruktury jsou vymezeny v kapitole Organizace ochrany kritické infrastruktury. V závěru je uvedeno celkové zhodnocení dané problematiky. Dále jsou zde obsaženy dvě přílohy, a to Seznam odvětví kritické infrastruktury Evropské unie a Seznam odvětví kritické infrastruktury České republiky.

Klíčová slova: Evropská unie, Evropský program na ochranu kritické infrastruktury, hrozba, kritická infrastruktura, oblasti kritické infrastruktury, ochrana kritické infrastruktury.

ABSTRACT

The thesis deals with a critical infrastructure protection of European Union. It is divided into several sections in which the threats that endanger European Union are described, moreover, there is evaluated the present condition of critical infrastructure of European Union, organization of critical infrastructure protection is analyzed as well. Furthermore, they are defined corroborative measures for EPCIP and consequences of critical infrastructure measure protection of European Union for the Czech Republic. Critical infrastructure sectors are defined in chapter Organization of critical infrastructure protection. The complete classification is listed in the conclusion. Last but not least, there are two attachments – List of critical infrastructure sectors of European Union and List of critical infrastructure sectors in the Czech Republic.

Keywords: European Union, The European Programme for Critical Infrastructure Protection, threat, critical infrastructure, critical infrastructure sectors, critical infrastructure protection.

Na tomto místě bych rád poděkoval doc. Ing. Luďku Lukášovi, CSc., vedoucímu diplomové práce, za cenné připomínky, podnětné rady a odborné vedení konzultací, kterými přispěl k vypracování této diplomové práce. Rád bych také poděkoval své rodině za důležitou morální i finanční pomoc.

Prohlašuji, že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně, dne 4. června 2008

……

Podpis diplomanta

OBSAH

ÚVOD

Evropa nebyla nikdy v dějinách tak bezpečná a svobodná. Podstatné pro tento vývoj bylo vytvoření Evropské unie. Vytvoření změnilo vztahy mezi evropskými státy i životy občanů. Evropské země začaly řešit spory mezi sebou smírně a spolupracovat prostřednictvím společných institucí. Vznik Evropské unie přinesl všem zemím ekonomickou prosperitu i blahobyt pro občany. Občané mohou např. volně cestovat po celé Evropské unii, pracovat ve všech zemích i usazovat se v nich. Avšak příznivá bezpečnostní situace Evropské unie nevládne ve všech regionech světa. Z tohoto důvodu se musí Evropská unie postarat o bezpečnost svých občanů i své ekonomiky. Musí při mimořádných událostech a dalších neštěstích zajistit brzké vyřešení této situace a při ní zajistit občanům nezbytné zásoby po dobu onoho trvání. Proto se začalo mluvit o nezbytných systémech a službách, které musí být zajištěny jak v období míru, tak při vzniku určitého nebezpečí. Tyto nezbytné systémy a služby byly pojmenovány s odstupem času jako kritická infrastruktura.

Do kritické infrastruktury patří vybraná technická infrastruktura území a vybrané služby. Každá část kritické infrastruktury tvoří sama o sobě systém. Každý systém se skládá z prvků, vazeb a toků, z nichž některé tvoří kritická místa, která při narušení způsobují, že systém neplní funkci, k níž je určen, anebo k tomu významně přispívají. Kritická infrastruktura je neodmyslitelnou součástí bezpečnostního systému, ve kterém platí „řetězové“ pravidlo, tj. že bezpečnostní systém bude tak bezpečný, neboli efektivní a akceschopný, jak bezpečný je jeho nejslabší článek. Proto tato oblast začíná být v posledních letech prioritní pro zajištění bezpečnosti v Evropské unii.

Cílem této diplomové práce je analyzovat současné kroky, které učinila Evropská unie pro ochranu kritické infrastruktury. Po přečtení tohoto materiálu by čtenář měl získat ucelené informace o dané problematice. Mojí snahou bylo napsat práci tak, aby byla jasná a srozumitelná všem, kteří se o tuto problematiku zajímají nebo kteří ji budou potřebovat k výkonu svého povolání.

1 HROZBY SOUČASNOSTI

Evropa čelí bezpečnostním hrozbám a problémům neustále. Vypuknutí války na Balkáně všem připomnělo, že válka z našeho kontinentu nevymizela. Během posledního desetiletí se ozbrojené konflikty nevyhnuly žádné z hlavních zeměpisných oblastí světa. Většina konfliktů se přitom odehrávala uvnitř států, ne mezi státy, a většinu obětí tvořili civilisté. Evropské unii však v současné době žádný vojenský konflikt nehrozí. Zárukou míru je už samotná sjednocující se Evropa, fungující na základě spolupráce mezi jednotlivými členskými zeměmi. Tradiční příčiny bojů byly překonány, k vojenským rozbrojům by nemělo v dohledné době dojít ani ze strany států, které vnímají demokratickou Evropskou unii jako svého nepřítele.

Bezpečnost je základní podmínkou rozvoje. Konflikty nejenže ničí infrastrukturu, včetně vnitřní struktury samotné společnosti, ale vedou i k růstu kriminality, odrazují investory a znemožňují normální hospodářskou aktivitu. Naše tradiční pojetí sebeobrany – platné až do konce studené války – vycházelo z hrozby územního napadení a invaze. V případě nových hrozeb bude první obranná linie často v zahraničí. Nové hrozby jsou dynamické. Žádná z nich není čistě vojenská ani jí nelze čelit čistě vojenskými prostředky. Každá vyžaduje kombinaci vícera způsobů zasahování. Nebudeme-li zasahovat proti teroristickým sítím, stanou se postupně ještě nebezpečnějšími. Riziko šíření zbraní hromadného ničení s časem vzrůstá. I eroze státních struktur a organizovaný zločin se šíří, pokud jim nevěnujeme pozornost.

Aby Evropská unie mohla plnit svoji funkci, tj. zabezpečit ochranu zájmů (životy a zdraví občanů, majetek, životní prostředí, existenci lidské společnosti), musí mít fungující kritickou infrastrukturu. To znamená, že za normálních, nestandardních i kritických podmínek musí být v provozu základní prvky, vazby a toky systému, které jsou základem schopnosti státu dosáhnout za každé situace stability a nastartovat další rozvoj. Kritickou infrastrukturou jsou převážně míněny systémy, jejichž zničení nebo omezení funkčnosti by mělo vážné dopady na ekonomickou a společenskou stabilitu, obranyschopnost a bezpečnost státu.

Hrozby mohou vycházet od jednotlivých pachatelů trestných činů, teroristických a kriminálních organizací, ale také z nepřátelských států. Do té míry se stále více překrývá civilní a vojenské ohrožení i vnitřní a vnější bezpečnost. S rostoucím pronikáním nových informačních a komunikačních technologií do všech oblastí života vznikají nové hrozby

nejen pro jednotlivce, ale i pro stát, hospodářství a společnost. Jsou zaměřeny proti infrastruktuře zemí s vyspělou technologií, na které v rostoucím rozsahu závisí všechny funkční oblasti informačního věku.

Běžné rozlišování například mezi válkou a neválkou, mezi veřejnými a soukromými zájmy, válečnými a kriminálními aktivitami nebo politickými a zeměpisnými hranicemi se v kybernetickém boji stále více prolínají. Čím je některá oblast života společnosti závislejší na informačních technologiích, tím závažněji na daný sektor infrastruktury působí nefunkčnost informačních technologií. Tím se dostává problematika kritické infrastruktury z „abstraktní“ oblasti do oblasti zabezpečení života společnosti v sektorech, jako je např. doprava, telekomunikace, zásobování energií, potravinami a pitnou vodou, ale také zabezpečení zdravotnictví, bankovnictví, fungování státní správy atd.

1.1 Definice pojmu hrozba, riziko

1.1.1 Hrozba

- Jakýkoli fenomén, který má potenciální schopnost poškodit chráněné zájmy objektu. Míra hrozby je dána velikostí možné škody a časovou vzdáleností (vyjádřenou obvykle pravděpodobností čili rizikem) možného uplatnění této hrozby; [10]
- Je subjekt, jenž svým působením (činností) může poškodit nebo zničit konkrétní chráněnou hodnotu nebo zájem jiného subjektu;
- Je to jev či událost jako bezprostřední příčina poškození nebo zničení konkrétní chráněné hodnoty nebo zájmu;
- Odvozenou, kvantitativní dimenzi hrozby je riziko.

1.1.2 Riziko

- Možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí. Riziko je vždy odvoditelné a odvozené z konkrétní hrozby. Míru rizika, tedy pravděpodobnost škodlivých následků vyplývajících z hrozby a ze zranitelnosti zájmu, je možnost posoudit na základě tzv. analýzy rizik, která vychází i z posouzení naší připravenosti hrozbám čelit; [10]
- Je možnost vzniku události (jevu) s výsledkem odchylným od předpokládaného cíle, a to s určitou objektivní matematickou nadějí či statistickou pravděpodobností;

- Je to kvantifikovaná nejistota;
- Je odvozenou, kvantitativní dimenzí hrozby, tj. jeho signifikací.

1.2 Hlavní hrozby mající vliv na bezpečnost Evropské unie

V současné době nelze vnímat bezpečnost omezeně, jen v národním, evropském nebo transatlantickém rámci. Její zajištění je možné pouze na celosvětové úrovni. Globální bezpečnost není dosažitelná pouze diplomacií, nebo naopak vojenskou silou, protože její ohrožení dnes ve značné míře spočívá v destabilizaci společnosti a životního prostředí. Evropa čelí novým hrozbám, které jsou různorodější, méně nápadné a hůře předvídatelné. Nejnaléhavější a nejvážnější hrozbou současnosti se stalo propojení extrémního fundamentalismu s terorismem a vlastnictví zbraní hromadného ničení nestabilními státy. Bezpečnostní prostředí ovlivňují globální strategická stabilita i významné regionální hrozby. Strategická stabilita je zajišťována hlavními aktéry mezinárodního společenství (kde patří i EU) a jejich snahou o kooperativní vztahy a řešení problémů diplomatickou cestou. Přesto však existují oblasti, v nichž napětí nebo nestabilita hrozí přerůst v otevřený konflikt. V některých případech hraje roli i vlastnictví či vývoj jaderných zbraní u jedné nebo více zúčastněných stran. [9]

Bezpečnost ohrožují jak hrozby záměrné (zejména terorismus a extremismus, šíření zbraní hromadného ničení, organizovaný zločin a nelegální migrace, narušení komunikačních a informačních systémů, průmyslové a další havárie), tak i nezáměrné, vzniklé bez úmyslného lidského zavinění (přírodní katastrofy, šíření nakažlivých chorob).

1.2.1 Záměrné hrozby

1.2.1.1 Terorismus a extremismus

Definice terorismu dle FBI: „Terorismus je nezákonné použití síly a násilí proti osobám či majetku se záměrem zastrašit nebo donutit vládu, civilní obyvatelstvo či jeho určitou skupinu, a tím dosáhnout politických nebo společenských cílů.“ [35]

Terorismus ohrožuje lidské životy, vede k vysokým nákladům, snaží se oslabit otevřenost a toleranci, které stojí v základech našich společností. Stává se stále větší hrozbou pro celou

Evropu. Teroristická hnutí mají lepší finanční zázemí, jsou propojena elektronickými sítěmi a ochotna použít neomezeného násilí, které způsobí obrovské ztráty na životech.

Nejnovější vlna terorismu je ve svém dosahu globální a je spojena s násilným náboženským extremismem. Její příčiny jsou složité – patří k nim tlak modernizace, kulturní, společenské a politické krize a pocit odcizení, rozšířený mezi mladými lidmi, kteří žijí v jiných než svých domovských společnostech. Nárůst této formy extremismu souvisí s radikalizací mladé generace muslimů, která je nespokojena se svou sociální situací a zavrhuje hodnotový systém demokratického světa. Řešení vidí v islámském fundamentalismu a v návratu k původním muslimským hodnotám. Problematika terorismu úzce souvisí s kontrolou trhu s materiály dvojího užití.

Možným rizikem je v této souvislosti především použití nekonvenčních materiálů (jedovatých chemikálií, patogenních mikroorganismů atd.) k teroristickému útoku. Je též pravděpodobné, že mohou být k teroristickým účelům ve větší míře více zneužívány moderní informační a komunikační technologie. Tento fenomén je i součástí naší vlastní společnosti. Evropa je jak cílem, tak základnou zmíněného typu terorismu. Teroristé se zaměřují na evropské země a také už proti nim zaútočili. Zároveň byly v Anglii, Itálii, Německu, Španělsku a Belgii odhaleny logistické základny buněk al-Kájdy. Koordinovaný evropský postup proti terorismu je tedy nezbytností. [7]

1.2.1.2 Šíření zbraní hromadného ničení, konvenčních zbraní a technologií a zboží dvojího užití a porušování mezinárodních kontrolních a sankčních režimů

Šíření (proliferace) zbraní hromadného ničení je potenciálně největší hrozbou naší bezpečnosti. Díky režimům mezinárodních úmluv a vývozním kontrolám se podařilo šíření ZHN a systémů jejich přenosu zpomalit. Nyní se ale ocitáme na prahu nového a nebezpečného období, kdy hrozí, že zejména země Blízkého východu začnou mezi sebou závodit ve výrobě zbraní tohoto typu. Pokrok v biologických disciplínách může v příštích letech zvýšit účinnost biologických zbraní. Na lehkou váhu nelze brát ani možné útoky s použitím chemických a radiologických materiálů. Šíření raketové technologie je dalším prvkem zvyšujícím nestabilitu a může pro Evropu představovat vzrůstající riziko.

Nejobávanějším z možných scénářů budoucího vývoje je ten, v němž by se teroristickým skupinám podařilo získat ZHN. V takovém případě by malá skupina osob mohla způsobit škodu v rozsahu, jakého byly dříve schopny jen státy a armády.

Vzhledem k možným účinkům představují největší nebezpečí zbraně biologické a jaderné. Při hodnocení pravděpodobnosti útoku, jsou největším nebezpečím zbraně chemické a radiologické. Nebezpečí globálního jaderného konfliktu není vysoké, jeho zdrojem by však mohl být lokální konflikt a jeho následná eskalace. Ve světě stále existuje několik oblastí s možností lokálního použití jaderných zbraní. Proto je potřebné všemi dostupnými prostředky zabránit proliferaci ZHN.

Nárůst ozbrojených konfliktů v nestabilních oblastech bude provázen zvýšenou poptávkou po zbraních a vojenském materiálu. I s ohledem na pravděpodobný růst terorismu bude tedy nabývat na významu celosvětová kontrola obchodu se zbraněmi a zbožím dvojího užití. Pro většinu zemí bude problémem nejen odhalování zbrojních obchodů a transferů ilegálních, ale i kontrola legálních obchodů, a to v rámci dodržování národních legislativ, mezinárodních kontrolních režimů a závazků vůči přijatým rozhodnutím EU a Rady bezpečnosti OSN. [7]

1.2.1.3 Regionální konflikty

Problémy toho druhu, jaké existují v Kašmíru, v oblasti velkých afrických jezer a na Korejském poloostrově, mají na evropské zájmy přímý i nepřímý vliv stejně jako konflikty, které se odehrávají blíže evropskému území, zejména na Blízkém východě. Násilné nebo „zakonzervované“ konflikty, které přetrvávají i těsně za našimi hranicemi, ohrožují regionální stabilitu. Ničí lidské životy a společenskou i hmotnou infrastrukturu, jsou hrozbou pro menšiny a pro základní lidské svobody a práva. Konflikt může vést k extremismu, terorismu a zhroucení státní moci. Otevírá také prostor organizovanému zločinu. Pocit ohrožení může v určité oblasti živit poptávku po ZHN. V mnoha případech bude tím nejpraktičtějším způsobem, jakým se lze vypořádat s často těžko uchopitelnými hrozbami nové doby, řešení starších problémů spojených s regionálními konflikty. [7]

1.2.1.4 Zhroucení státní moci

Špatné vládnutí – korupce, zneužívání moci, slabé instituce a absence standardních mechanismů odpovědnosti – rozkládají spolu s občanskými konflikty státy zevnitř.

V některých případech vedly tyto faktory až ke kolapsu státních institucí. Somálsko, Libérie a Afghánistán pod vládou Talibanu jsou jen nejznámějšími příklady z poslední doby. Selhání základních funkcí státu s sebou přináší zřejmé hrozby, jakými jsou organizovaný zločin nebo terorismus. Rozpady států jsou velice znepokojivým jevem, který oslabuje globální vládnutí a prohlubuje regionální nestabilitu.[1] [9]

1.2.1.5 Organizovaný zločin a nelegální migrace

Evropa patří k územím, na něž se činnost sítí organizovaného zločinu zaměřuje nejčastěji. Tato vnitřní hrozba naší bezpečnosti má ovšem i významnou vnější dimenzi: velkou část činnosti zločineckých gangů totiž představuje pašování drog, žen, ilegálních přistěhovalců a zbraní. Navíc může být organizovaný zločin propojen i s terorismem. Takovéto zločinecké aktivity bývají často typické pro slabé nebo rozkládající se státy. V několika zemích, kde se pěstují drogy, byly příjmy z obchodu s nimi používány k oslabování státních struktur. Příjmy z obchodu s drahými kameny, dřevem a lehkými střelnými zbraněmi živí konflikty na jiných místech světa. Všechny tyto aktivity podkopávají jak základy právního státu, tak společenský řád jako takový. V extrémních případech může organizovaný zločin státní struktury i ovládnout. Novým rozměrem organizovaného zločinu, který si v budoucnu rozhodně zaslouží více pozornosti, pak je nárůst námořního pirátství.

Nebezpečí a celospolečenské riziko projevů organizovaného zločinu spočívá nejen v přímém porušování a ohrožování hodnot chráněných příslušnými trestněprávními normami, ale též v jeho potenciální schopnosti ohrozit instituce demokratického právního státu uplatňováním různých způsobů korupce, vydírání a přímým pronikáním do orgánů veřejné správy. Organizovaný zločin může být využíván skupinami mezinárodního terorismu a naopak i sám je může využívat. [7]

---

[1] V současné době je nejvíce napjatá situace v africkém Čadu, kde povstalci zaútočili na hlavní město Ndjamen a pokusili se o svrhnutí prezidenta. Organizace „Lékaři bez hranic“ informovala, že při bojích padlo na sto lidí a 70 bylo zraněno. Dále ze země uprchlo na 50 tisíc lidí do Kamerunu. Vzhledem k této situaci vydala Rada bezpečnosti OSN nezávislou rezoluci, která vyzývá mezinárodní společenství, aby poskytlo podporu čadské vládě proti vzbouřencům.

1.2.1.6 Závislost na strategických surovinách

Politický i ekonomický vývoj ve světě budou v následujících letech v ještě větší míře ovlivňovat základní energetické suroviny – ropa a zemní plyn. Narůstající poptávka rozvojových ekonomik (Čína, Indie) po energetických surovinách může vést k jejich nedostatku, což donutí vyspělé země urychleně hledat jiné, alternativní zdroje. Ve snaze o kontrolu teritoriálně sporných nalezišť může docházet k lokálním politickým krizím a ozbrojeným konfliktům. EU a Evropa jako celek bude s úbytkem kapacit ložisek uhlovodíkových paliv zvyšovat svou závislost na dovozech.

V mnoha evropských zemích bude v souvislosti s problémem dovozu strategických surovin pravděpodobně přehodnocován přínos a bezpečnost jaderné energetiky při výrobě elektrické energie. Je možné očekávat nejen pozastavení programů postupného odstavování jaderných elektráren, ale dokonce i zahájení výstavby nových. Cílem by měla i nadále být stabilizace spotřeby a udržení, resp. posílení míry diverzifikace dodávek těchto surovin.

Strategickou surovinou se v některých regionech světa stane sladká, resp. pitná voda. Lze očekávat, že již v příští dekádě může dojít k politickým krizím a lokálním ozbrojeným konfliktům vedeným snahou získat kontrolu zdrojů vody, přinejmenším s cílem dosáhnout vyššího podílu jejího čerpání. [9]

1.2.1.7 Narušení komunikačních a informačních systémů

S rozvojem informačních technologií a souvisejícím nárůstem využívání počítačových služeb budou nejspíše stále častěji napadány informační systémy a systémy mající vazbu zejména na státní infrastrukturu. Může docházet k pokusům o narušení řídících systémů kritické infrastruktury (výrobní i nevýrobní systémy, jejichž nefunkčnost by měla vážné dopady na bezpečnost, ekonomiku a zachování nezbytného rozsahu dalších základních funkcí státu v krizových situacích). S rozvojem státní síťové informační infrastruktury budou v daleko větší míře ohroženy systémy provozující např. finanční oblast, oblast sociálního a zdravotního zabezpečení, dodávky plynu, ropy, elektrické energie apod. Při růstu využívání elektronické formy komunikace může docházet k elektronické krádeži dat a jejich zneužití. [9]

1.2.1.8 Průmyslové a další havárie

Navzdory preventivním a ochranným opatřením zůstávají i nadále hrozbou průmyslové havárie ve stacionárních objektech a zařízeních, v nichž je nakládáno s nebezpečnými látkami, přípravky nebo odpady. Hrozbu představuje také nárůst dopravních nehod v silniční dopravě, kterými se zvyšuje i riziko nehod vozidel přepravujících nebezpečné látky na pozemních komunikacích. [9]

1.2.2 Nezáměrné hrozby

1.2.2.1 Přírodní katastrofy, narušování životního prostředí

V důsledku globálních klimatických změn se častěji objevují hrozby v podobě rozsáhlých živelních pohrom, jako jsou např. povodně či jiné klimatické kalamity. Přitom může dojít ke kumulaci jednotlivých hrozeb. Např. dlouhotrvající sucho, kromě rizika nedostatku pitné i užitkové vody a vlivu na její kvalitu, zvyšuje pravděpodobnost rizika rozsáhlých lesních požárů, a to zejména v kombinaci s vichřicemi. Četnost a rozsah účinků živelních pohrom v posledním období svědčí o tom, že riziko jejich vzniku se zvyšuje. [9]

1.2.2.2 Šíření nakažlivých chorob

V blízké budoucnosti lze očekávat zhoršující se zdravotní stav obyvatelstva v některých zemích a oblastech, zejména v souvislosti s šířením AIDS[2] a zvýšeným výskytem dalších nemocí, jako je např. tuberkulóza nebo nemoci přenosné ze zvířat na člověka, např. případy BSE, SARS a ptačí chřipka. [9]

[2] Epidemie AIDS se nejrychleji šíří ve Východní Evropě a Střední Asii. Za poslední dva roky došlo k více než 70% nárůstu počtu HIV pozitivních. Nejrychleji se epidemie šíří na Ukrajině, která vykazuje nejvyšší míru výskytu v regionu – 1,5%. To představuje téměř 370 tisíc HIV pozitivních lidí.

1.3 Strategické cíle Evropské unie

Tyto cíle vycházejí ze schopností EU, tj. myslet globálně a současně jednat lokálně. Evropská unie má tři strategické cíle, které jsou klíčové pro zajišťování její bezpečnosti a prosazování jejích hodnot:

a) Reakce na hrozby

Zvyšování své obranyschopnosti, zabránit šíření ZHN a zabezpečení kontrolních mechanizmů, zvýšit povědomí Evropanů o regionálních konfliktech a humanitárních tragédiích jinde na světě, zasahovat proti teroristickým sítím, organizovanému zločinu, erozi státních struktur. EU by měla být připravena jednat ještě dříve, než vznikne mimořádná událost (krizová situace). Vše musí být zaměřeno do oblasti prevence konfliktů a hrozeb s využitím politických a ekonomických nástrojů (preventivní diplomacie). Při boji s terorismem se předpokládá spolupráce zpravodajských, policejních, soudních, vojenských a jiných složek.

V přístupu k hrozbě globálního terorismu klade EU rozhodující důraz na sedm směrů preventivního působení a to:

- Posilování mezinárodní spolupráce;
- Zamezování přístupu teroristů k finančním a jiným ekonomickým zdrojům;
- Zvyšování připravenosti k prevenci teroristických úderů;
- Zajišťování bezpečnosti mezinárodní dopravy a zlepšování hraniční kontroly;
- Zdokonalování schopností nezbytných pro zvládání důsledků případných teroristických úderů;
- Soustředění pozornosti na ty faktory, které usnadňují nábor do teroristických organizací. Jde zejména o bariéry a vzájemné předsudky mezi různými kulturami a náboženstvími. EU usiluje o jejich překonávání cestou zlepšování dialogu mezi kulturami;
- Preventivní úsilí ve třetích zemích, z nichž se mohou rekrutovat případní teroristé.

b) Posilování bezpečnosti v oblastech sousedících s EU

Strategickým cílem je docílení toho, aby EU obklopovaly jen dobře spravované státy – nejlepší pojistka bezpečnosti, s nimiž bude dobrá spolupráce a udržování korektních vztahů. Strategickou prioritou pro EU je vyřešení arabsko-izraelského konfliktu, rozvíjení vztahů se středomořskými partnery prostřednictvím hospodářské, bezpečnostní a kulturní

spolupráce v rámci barcelonského procesu, rozšiřování styků mezi EU a arabskými státy, začlenění zemí do mezinárodního společenství.

c) Mezinárodní řád založený na účinném systému mnohostranné spolupráce (multilateralismus).

Evropská unie pokročila na cestě ve zvýšení bezpečnosti a to jak ve vyšší účinnosti zahraniční politiky, tak v efektivnosti krizového řízení. Do budoucna se předpokládá, že:

- Evropská unie musí být aktivnější v prosazování svých strategických cílů;
- EU musí být schopná nasadit více sil a prostředků. Z toho vyplývá přeměna armád v pružnější mobilní síly, které budou s to se postavit novým hrozbám s nasazením a účinným použitím všech nezbytných civilních zdrojů;
- Efektivní práce diplomacie, (požadavek zlepšení vzájemného porozumění a komunikace), společné hodnocení hrozeb (požadavek na sdílení zpravodajských informací mezi členskými státy EU a dalšími partnery), rozšíření spektra misí EU (společné odzbrojovací operace, podpora třetích zemí v jejich boji s terorismem či při reformě bezpečnostního sektoru) apod.;
- Musí být jednotnější v postojích a jednáních.

1.4 Počátky kritické infrastruktury

USA a Austrálie patří mezi první státy, které začaly vnímat potenciál a šířku problému kritické infrastruktury. Byly to právě tyto země, které zahájily diskusi o zranitelnosti životní infrastruktury (později označované jako kritické infrastruktury).

Prvním uceleným materiálem, řešící otázky ochrany kritické infrastruktury, byla tzv. „Bílá kniha“. Jednalo se o Směrnici 63[3], kterou vydal v květnu 1998 prezident USA Clinton jako prezidentské rozhodnutí. Bílá kniha pojímá kritickou infrastrukturu jako základní systémy, které mají hmotnou a kybernetickou základnu a mají vliv na funkčnost ekonomiky a státu. Tyto základní systémy zahrnují oblasti:

- Systémy dodávky elektřiny;
- Systémy dodávky vody;

[3] Presidential Decision Directive 63. [27]

- Kanalizační systém;
- Přepravní síť;
- Komunikační a energetické systémy;
- Bankovní a finanční sektor;
- Další sektory závislé na počítačových systémech.

Hlavním záměrem prezidentské směrnice bylo přijetí nezbytných opatření k rychlé eliminaci zranitelnosti, a to z hlediska hmotných a kybernetických útoků na kritickou infrastrukturu. Větší důraz byl v té době přikládán možným útokům na kybernetické systémy.

Důležitým požadavkem „Bílé knihy" je rozšiřování politiky ochrany kritické infrastruktury ke všem zainteresovaným subjektům jak v soukromém, tak ve veřejném sektoru. Politika ochrany kritické infrastruktury stanovila cíle, poskytla koncepci a zdroje, zařadila kritickou infrastrukturu mezi národní životní zájmy a vytvořila novou startovací čáru pro opatření v oblasti vnitřní bezpečnosti.

Po teroristickém útoku na světové obchodní centrum v New Yorku, k němuž došlo 11. září 2001, otázky ochrany kritické infrastruktury eskalují a nabývají nový obsah a rozměr. Již 16. října 2001 vydává prezident USA George W. Bush „Vládní nařízení na ochranu kritické infrastruktury"[4]. Toto nařízení bylo vydáno za účelem zabezpečit ochranu informačních systémů pro kritickou infrastrukturu, včetně nouzové komunikační připravenosti a ochrany hmotných zařízení, které informační systémy podporují. Jako prioritní bylo stanoveno zabezpečení tří vzájemně závislých funkcí: ekonomiky, činnost státu a vedení národní obrany.

Řešení kritické infrastruktury v USA doznalo svého současného vyvrcholení v únoru 2003, a to vydáním národní strategie. Tomuto kroku předcházelo zpracování a vydání v červenci 2002 „Národní strategie vnitřní bezpečnosti"[5].

Mimo jiné tato strategie uvádí definici kritické infrastruktury: „Systémy a zařízení, jak hmotné tak virtuální, které jsou životně důležité pro USA a zneschopnění nebo zničení

[4] Executive Order on Critical Infrastructure Protection.

[5] The National Strategy for Homeland Security.

takových systémů nebo zařízení by mělo vliv na snížení bezpečnosti, národní ekonomické bezpečnosti, národního veřejného zdraví nebo bezpečí, nebo na jakoukoliv jejich kombinaci.“

14. února 2003 pak byla vydána „Národní strategie fyzické ochrany kritické infrastruktury a klíčových zařízení“[6] a „Národní strategie zabezpečení kybernetického prostoru“[7].

„Národní strategie fyzické ochrany kritické infrastruktury a klíčových zařízení“ je v současnosti nejkomplexnějším materiálem, zabývajícím se problematikou kritické infrastruktury. Formuluje politiku státu v této oblasti a při tom zdůrazňuje, že USA musí chránit takovou kritickou infrastrukturu a klíčová zařízení, která by:

- Oslabila schopnost federální vlády vykonávat základní národní bezpečnostní úkoly a zabezpečovat veřejné zdraví a bezpečnost;
- Narušila schopnosti centrálních a místních orgánů při udržování pořádku a zabezpečování základních veřejných služeb;
- Poškodila funkčnost privátního sektoru při zabezpečování řádného chodu ekonomiky a základních služeb;
- Podkopávala veřejnou morálku a důvěru v národní ekonomiku a politické instituce.

Ochrana kritické infrastruktury a klíčových zařízení je v USA považována za jádro vnitřní bezpečnosti. Přijatá strategie je považována jako „systém o systémech“. Úsilí státních orgánu při ochraně kritické infrastruktury a klíčových zařízení zahrnuje vytváření takové politiky a prostředí, které podmiňuje a vyvolává aktivní přístup nejen státní administrativy, ale i soukromého sektoru a občanů USA. [15]

[6] The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets.

[7] The National Strategy to Secure Cyberspace

2 ZHODNOCENÍ SOUČASNÉHO STAVU KRITICKÉ INFRASTRUKTURY EVROPSKÉ UNIE

2.1 Charakteristika Evropské unie

V moderních, demokratických dějinách Evropy se základy myšlenky, že by Evropa měla vytvořit silnější a odolnější celek vůči bezpečnostním i hospodářským rizikům, objevily ve 20. letech minulého století jako reakce na 1. světovou válku. Teprve 2. světová válka a její následky však tuto myšlenku posílily na nutnost. Část evropských politiků viděla jediné řešení v úzkém ekonomickém a později i politickém propojení evropských států, které by napříště znemožnilo růst nového agresora na evropském kontinentě a vznik dalších ozbrojených konfliktů. Dalším motivem pro postupné evropské sjednocování byla snaha po hospodářské obnově Evropy.

Evropská integrace byla započata v 50. letech 20. století vznikem Evropského hospodářského společenství (EHS), Evropského společenství uhlí a oceli (ESUO) a Evropského společenství pro atomovou energii (ESAE = Euratom). Na těchto základech pak mohla vzniknout Evropská unie jako taková. Oproti klasickým mezinárodním společenstvím států spočívá zcela nová charakteristika EU v tom, že se členské země vzdaly části svých suverénních práv ve prospěch Společenství a zároveň je vybavily novými pravomocemi jednat nezávisle na vůli členských zemí. Při vykonávání těchto pravomocí je ES umožněno vydávat vlastní suverénní akty, jež mají stejnou právní sílu jako zákony v jednotlivých státech. O vytvoření ES se nejvíce zasloužil roku 1950 francouzský ministr zahraničí Robert Schuman svou deklarací z 9. května, ve které představil společně s Jeanem Monnetem vypracované plány na spojení evropského uhelného a ocelářského průmyslu. „Schumanův plán“ se stal skutečností, když byla mezi šesti státy (Belgie, Francie, Itálie, Lucembursko, Nizozemsko a Spolková republika Německo) uzavřena zakládací Smlouva Evropského společenství uhlí a oceli (ESUO). V návaznosti na to vytvořily tytéž státy o několik let později Evropské hospodářské společenství (EHS) a Evropské společenství pro atomovou energii (ESAE = Euratom), která začala fungovat vstupem smluv v platnost 1. ledna 1958.

Samotná Evropská unie byla založena Maastrichtskou smlouvou. Tato smlouva byla podepsaná již 7. února 1992 v Maastrichtu, ale kvůli problémům při ratifikaci vstoupila

v platnost až 1. listopadu 1993. Obsahuje vedle řady změn Smlouvy o založení E(H)S a Euratomu také zakládací akt Evropské unie. Takto vzniklá Evropská unie nenahrazuje Evropská společenství, ačkoliv je to tak někdy prezentováno v médiích, nýbrž je společně s novými „politikami a formami spolupráce“ zastřešuje. Tento fakt lze obrazně přirovnat ke stavbě s třemi pilíři, na kterých EU spočívá: Evropská společenství, spolupráce v zahraniční a bezpečnostní politice a vnitrní záležitosti a justice.

2.2 Pilíře Evropské unie

2.2.1 PRVNÍ PILÍŘ: Tři Evropská společenství

První pilíř navazuje na integrační principy, z nichž Unie postupně vznikla. Tento pilíř tvoří tři Evropská společenství (EHS, Euratom a ESUO) prohloubená a rozšířená hospodářskou a měnovou unií. Evropské hospodářské společenství bylo při založení EU přejmenováno na Evropské společenství. Ze Smlouvy o založení EHS se stala Smlouva o založení ES. Tím má být vyjádřen kvalitativní posun EHS od čistě hospodářského společenství k politické unii. První pilíř ztělesňuje jurisdikci Společenství v její nejrozvinutější formě. V rámci ES mohou instituce Společenství v oblastech, v nichž jim byla delegována zákonodárná pravomoc, vytvářet legislativu, která má v členských státech bezprostřední platnost a má přednost před národním právem. Jádro ES tvoří vnitřní trh se svými základními svobodami (volný pohyb zboží, pracovních sil, svoboda usazování, volný pohyb služeb a kapitálu a volný platební styk) a také jeho pravidla hospodářské soutěže.

Mezi politiky, za něž odpovídá Společenství, patří: hospodářská a měnová politika, zemědělská politika, vízová, azylová a přistěhovalecká politika, dopravní politika, daňová politika, politika zaměstnanosti, obchodní politika, sociální a vzdělávací politika a politika zaměřená na mládež, kulturní politika, politika ochrany zdraví a spotřebitele, politika transevropských sítí, průmyslová politika, politika hospodářské a sociální soudržnosti, politika vědy a výzkumu, politika na ochranu životního prostředí a politika rozvojové pomoci.

2.2.2 DRUHÝ PILÍŘ: Společná zahraniční a bezpečnostní politika

Druhým pilířem EU se stala zahraniční a bezpečnostní politika členských zemí. Před uzavřením Smlouvy o EU probíhala politická spolupráce členských státu ES v rámci

„evropské politické spolupráce“ (EPS). Jednalo se o pravidelné konzultace ministrů zahraničí a stálé kontakty jejich úřadů. Cílem EPS bylo přivést členské státy k vzájemnému lepšímu pochopení v oblasti zahraniční politiky, k harmonizaci jejich stanovisek a – do maximální možné míry – ke společnému postupu. Avšak všechna rozhodování musela být přijímána jednomyslně, což způsobovalo rozpory v EU. Proto ve Smlouvě o EU se hlavy států a vlád shodly na tom, že budou krok za krokem rozvíjet společnou zahraniční a bezpečnostní politiku, mezi jejíž cíle patří:

- Zajištění společných hodnot, základních zájmu a nezávislosti EU;
- Posílení bezpečnosti EU a jejích členských státu;
- Zajištění světového míru a posílení mezinárodní bezpečnosti v souladu se zásadami Charty Organizace spojených národu a se zásadami helsinského závěrečného aktu z roku 1975 a Pařížské charty z roku 1990, které v roce 1994 shrnula Organizace pro bezpečnost a spolupráci v Evropě (OBSE);
- Podpora mezinárodní spolupráce;
- Podpora demokracie a vlády zákona a zajištění lidských práv a základních svobod.

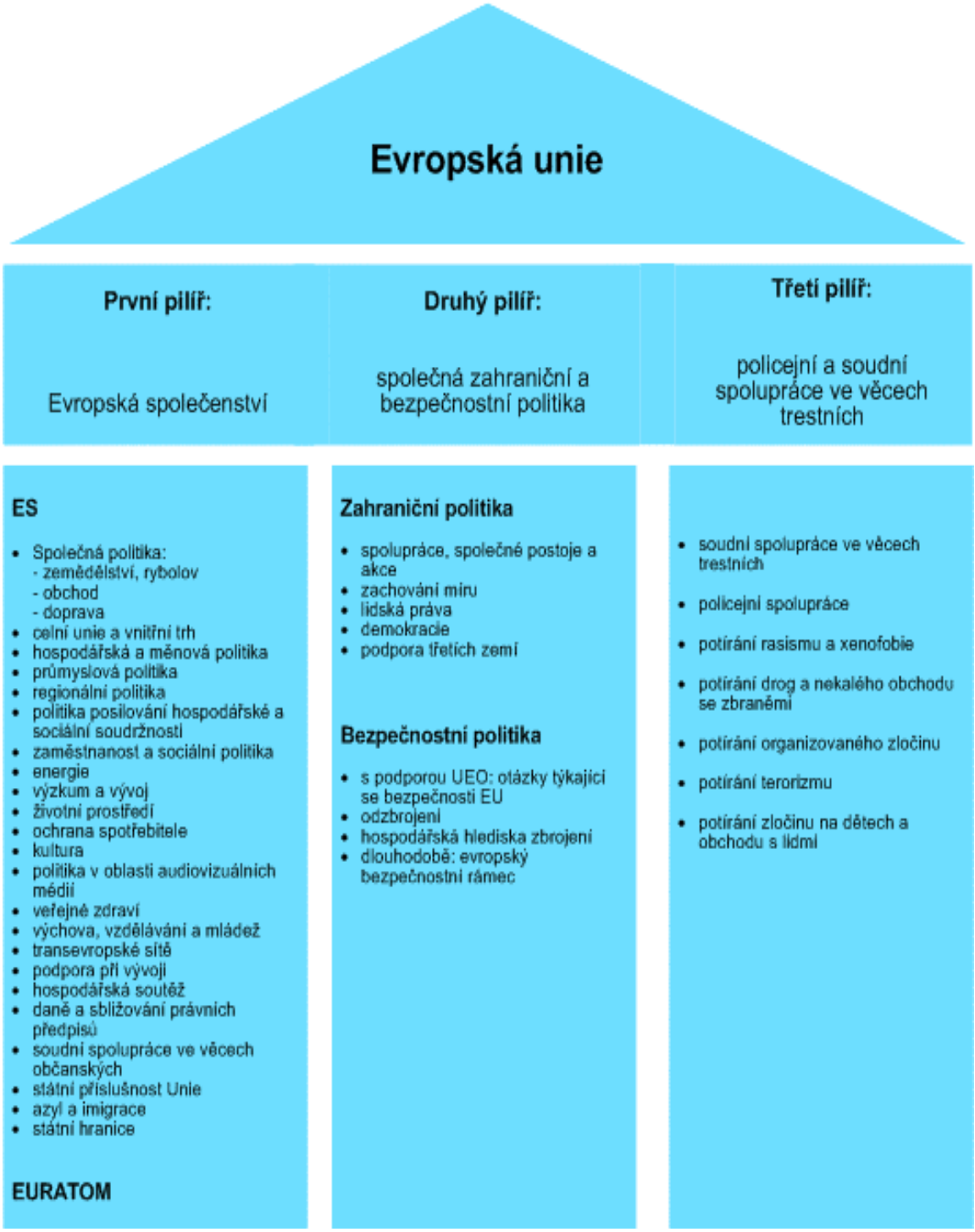
Zahraniční a bezpečnostní politika patří tradičně k těm oblastem, kde si státy svou suverenitu (státní svrchovanost) mimořádně pečlivě střeží. Je velice obtížné definovat společné zájmy v této oblasti také proto, že jen Francie a Velká Británie vlastní atomové zbraně. Další problém spočívá v tom, že ne všichni členové EU jsou současně členy obranných aliancí NATO (Irsko, Rakousko, Finsko a Švédsko) a ZEU (Dánsko, Řecko, Irsko). Rozhodování v oblasti „společné zahraniční a bezpečnostní politiky“ jsou proto v současné době stále ještě přijímána v rámci spolupráce mezi státy. Pro tuto oblast se vytvořil samostatný soubor nástrojů, které nalezneme v Amsterodamské smlouvě a díky němuž získala mezistátní spolupráce jasné obrysy.

2.2.3 TŘETÍ PILÍŘ: Policejní a justiční spolupráce v trestních věcech

Třetí oblastí působení Unie je oblast vnitra, justice a policejní spolupráce. Týká se slaďování postupů soudů a policie včetně boje proti organizovanému zločinu. Cílem spolupráce v oblasti justice a trestních věcí je společným postupem garantovat všem občanům prostor svobody, bezpečnosti a práva, a to prevencí a bojem proti kriminalitě (obzvláště proti terorismu, obchodu s lidmi, ilegálnímu obchodu se zbraněmi a drogami, proti korupci a podvodům), proti rasismu a xenofobii. Již byla provedena první opatření: přijetí směrnice

proti praní peněz a vytvoření evropského policejního úřadu (Europol). V oblasti justiční spolupráce jde navíc také o ulehčení a urychlení spolupráce při soudních procesech, při výkonu rozhodnutí, usnadnění vydávání osob mezi členskými státy, určení minimálních pravidel vztahujících se k základním charakteristikám skutkových podstat trestných činů a dále k trestům na poli organizovaného zločinu, terorismu a obchodu s drogami. Stejně jako v oblasti zahraniční a bezpečnostní politiky neprobíhá spolupráce v této sféře na základě rozhodovacích procedur ES, ale na základě spolupráce jednotlivých státu.

Kritická infrastruktura sehrává významnou roli ve všech třech pilířích Evropské unie. Významnější roli má KI v oblasti prvního pilíře, kde jsou přímo definovány různé politiky, které přímo či nepřímo reprezentují oblasti KI. Zde patří např. hospodářská a měnová politika, politika ochrany zdraví a spotřebitele, dopravní, průmyslová nebo politika vědy a výzkumu. Druhý a třetí pilíř hraje nezastupitelnou roli v oblasti prevence, kdy druhý pilíř EU tvoří společnou zahraniční a bezpečností politiku a třetí policejní a justiční spolupráci v trestních věcech. Důslednou spoluprací preventivní politiky II. a III. pilíře a bezpečnostní politiky pilíře I. se dosáhne účelného výsledku ochrany KI.



Obr. 1: Pilíře EU [14]

2.3 Státy Evropské unie

Členskými státy Evropské unie jsou v první řadě zakládající země, tzn. Belgie, Francie, Itálie, Lucembursko, Německo a Nizozemí. 1. ledna 1973 do Společenství vstoupila Velká Británie, Irsko a Dánsko (nyní bez Grónska, jehož obyvatelstvo se v únoru roku 1985

těsnou většinou v referendu vyslovilo proti setrvání ostrova v ES). V letech 1976 a 1977 požádalo o členství Řecko, Portugalsko a Španělsko. Řecko se stalo členem ES již 1. ledna 1981. Portugalska a Španělska vstoupilo do ES o pět let později, a to 1. ledna 1986 – „první a druhé jižní rozšíření". Po jižním rozšíření následovalo 1. ledna 1995 přistoupení Rakouska, Finska a Švédska do EU. Dnem 1. května 2004 se členy Evropské unie staly také Česká republika, Slovensko, Maďarsko, Polsko, Lotyšsko, Litva, Estonsko, Slovinsko, Kypr a Malta. Zatím poslední rozšíření Evropské unie nastalo 1. ledna 2007 vstupem Rumunska a Bulharska. O přistoupení dalších států, a to Turecka, Chorvatska a Makedonie se právě jedná. Dalšími možnými uchazeči se mohou stát tzv. Západobalkánské země. Tyto země, které byly většinou součástí Jugoslávie, nyní Evropskou unii žádají, aby urychlila jejich hospodářskou obnovu, zlepšila jejich vzájemné vztahy, které poznamenaly etnické a náboženské konflikty, a stabilizovala jejich demokratické orgány. K těmto možným uchazečům patří Albánie, Bosna a Hercegovina, Černá Hora a Srbsko.

2.3.1 Časový harmonogram rozšíření Evropské unie:

- Zakládající státy – Belgie, Francie, Itálie, Lucembursko, Německo a Nizozemí;
- První rozšíření – 1. leden 1973 – Dánsko, Irsko, a Spojené království Velké Británie a Severního Irska;
- Druhé rozšíření („jižní") – 1. leden 1981 – Řecko;
- 1985 – Grónsko se v referendu rozhodlo opustit ES a Euratom;
- Třetí rozšíření („druhé jižní") – 1. leden 1986 – Portugalsko a Španělsko;
- 3. říjen 1990 – sjednocení východního a západního Německa;
- Čtvrté rozšíření („severní") – 1. leden 1995 – Rakousko a dvě severské země Finsko a Švédsko přistupují k EU;
- Páté rozšíření („východní") – 1. květen 2004 – zatím největší rozšíření, Česko, Estonsko, Kypr, Litva, Lotyšsko, Maďarsko, Malta, Polsko, Slovensko a Slovinsko;
- Šesté rozšíření („druhé východní") – 1. leden 2007 – Bulharsko a Rumunsko přistupují k Evropské unii.

2.4 Základní statistické údaje o Evropské unii

Počet členů	27
Počet obyvatel	496 000 000
Procento světové populace	7,5 %
Celková rozloha	4 314 000 km²
Procento světové rozlohy pevniny	2,9 %
HDP na obyvatele	22 600 PPS (standard kupní síly)
Míra nezaměstnanosti	7,9 %
Celkové veřejné výdaje na vzdělání v % HDP	5,17 %
Celkové veřejné výdaje na vědu a výzkum v % HDP	1,92 %

2.5 Evropské instituce

Základním principem fungování Evropské unie je svěřování pravomocí, které byly dříve v kompetenci členských států, na evropské instituce. Hlavními aktéry v institucionálním systému EU je na jedné straně Evropská rada a na straně druhé instituce ES, mezi něž patří Rada Evropské unie, Evropská komise, Evropský parlament, Soudní dvůr ES a Evropský účetní dvůr. Tyto instituce doplňuje ještě Evropská centrální banka, Evropská investiční banka, Hospodářský a sociální výbor a Výbor regionů.

2.5.1 Evropská rada

Evropská rada se schází přibližně třikrát do roka, skládá se z hlav států a předsedů vlád členských států EU, ministrů zahraničí a představitelů Evropské komise. V jejím čele je prezident nebo předseda vlády země, která v daném období předsedá Radě Evropské unie. Rozhoduje o nejzávažnějších politických a ekonomických otázkách a vymezuje směry, kterými se má Unie ubírat. Evropská rada rozhoduje na základě jednomyslnosti.

Maastrichtskou smlouvou se Evropská rada oficiálně stala iniciátorem hlavních politik EU a získala oprávnění rozhodnout v obtížných otázkách, na něž nedokázali najít společnou odpověď ministři, kteří jednali v Radě Evropské unie. Evropská rada rovněž řeší naléhavé mezinárodní problémy v rámci společné zahraniční a bezpečnostní politiky, která umožňuje EU zaujímat jednotný postoj k diplomatickým otázkám.

2.5.2 Rada Evropské unie

Rada Evropské unie (zkráceně pouze „Rada“) je hlavní rozhodující institucí EU a zastupuje zájmy členských států na evropské úrovni. Členské státy EU se každých šest měsíců střídají v předsednictví Rady. Hlavní úkoly předsedající země je organizovat setkání Rady a reprezentovat EU navenek. Každého zasedání Rady se účastní jeden ministr z každé členské země EU. To, který ministr se účastní, závisí na projednávané agendě. Rada Evropské unie je nejvlivnějším orgánem EU. Významné pravomoci má v oblastech 2. a 3. pilíře (např. společná zahraniční politika nebo policejní spolupráce), v oblasti 1. pilíře může rozhodovat pouze na základě návrhu Komise.

Rada rozhoduje buď jednomyslně, kvalifikovanou nebo prostou většinou hlasů. Jednomyslnost je požadována v oblasti 2. a 3. pilíře. Prostou většinou se hlasuje pouze o procedurálních otázkách a některých aspektech společné obchodní politiky. Většina rozhodování se provádí na základě kvalifikované většiny, kdy hlasy členských států mají různou váhu v závislosti na počtu obyvatel.

Německo, Francie, Itálie, Velká Británie	29
Španělsko, Polsko	27
Rumunsko	14
Nizozemsko	13
Belgie, Česká republika, Řecko, Maďarsko, Portugalsko	12
Rakousko, Bulharsko, Švédsko	10
Dánsko, Irsko, Litva, Slovensko, Finsko	7
Kypr, Estonsko, Lotyšsko, Lucembursko, Slovinsko	4
Malta	3
CELKEM	**345**

Tab. 1: Počet hlasů přidělených jednotlivým zemím v Radě [17]

Rada Evropské unie:

- Je legislativním orgánem Evropské unie, v řadě otázek vykonává tuto pravomoc v součinnosti s Evropským parlamentem;
- Koordinuje hospodářskou politiku členských států;

- Uzavírá jménem Evropské unie mezinárodní smlouvy s jedním nebo s více státy a s mezinárodními organizacemi;
- Sdílí s Evropským parlamentem rozpočtové pravomoci;
- Přijímá rozhodnutí nezbytná pro formulování a provádění společné zahraniční a bezpečnostní politiky podle směrnic přijatých Evropskou radou;
- Koordinuje činnost členských států a přijímá opatření v oblasti policejní a soudní spolupráce v trestních věcech. [19]

Slovinsko	leden – červen 2008
Francie	červenec – prosinec 2008
ČR	leden – červen 2009
Švédsko	červenec – prosinec 2009
Španělsko	leden – červen 2010
Belgie	červenec – prosinec 2010
Maďarsko	leden – červen 2011
Polsko	červenec – prosinec 2011
Dánsko	leden – červen 2012
Kypr	červenec – prosinec 2012
Irsko	leden – červen 2013
Litva	červenec – prosinec 2013
Řecko	leden – červen 2014
Itálie	červenec – prosinec 2014
Lotyško	leden – červen 2015
Lucembursko	červenec – prosinec 2015
Nizozemsko	leden – červen 2016
Slovensko	červenec – prosinec 2016
Malta	leden – červen 2017
Velká Británie	červenec – prosinec 2017

Tab. 2: Předsednictví v EU v letech 2008-2017 [18]

2.5.3 Evropská komise

Evropská komise sleduje zájmy Evropské unie jako celku. Největší pravomoci má v oblasti 1. pilíře, má právo iniciovat návrhy zákonů a dohlíží na dodržování přijatých smluv.

V případě jejich neuplatňování může Komise podat u Soudního dvora žalobu na stranu, která neplní své povinnosti, aby ji donutila jednat v souladu s právem EU. Vypracovává také návrh rozpočtu EU a provádí kontrolu jeho plnění. Dále Komise zastupuje EU při mezinárodních jednáních a má právo sjednávat s třetími státy dohody. Má významné pravomoci při přijímání nových členů do Unie a zajišťuje kontakty s nečlenskými státy.

Na základě Smlouvy z Nice má každá země jednoho komisaře, v současnosti je jich 27. Evropská komise rozhoduje na základě prosté většiny hlasů. Jakožto výkonný orgán EU Komise realizuje rozhodnutí Rady. Má širokou pravomoc při řízení společných politik EU, např. v oblasti výzkumu a technologie, pomoci zámořským zemím, regionálního rozvoje. Spravuje také rozpočet těchto politik.

2.5.4 Evropský parlament

Evropský parlament funguje jako kontrolní a poradní orgán Evropské unie. Schvaluje složení Evropské komise a má právo kontrolovat její činnost, podílí se na tvorbě zákonů, vyslovuje souhlas s mezinárodními smlouvami a přijímáním nových členských států. Má pravomoci v oblasti společného rozpočtu EU.

Na základě Smlouvy z Nice má dnes Evropský parlament 785 poslanců, kteří jsou od roku 1979 voleni obyvateli EU na období pěti let. Poslanci mají možnost sdružovat se do poslaneckých klubů na základě politické příslušnosti, nejsou tedy rozsazeni podle národností. Evropský parlament se usnáší prostou většinou.

Parlament se účastní práce na legislativě EU na trojí úrovni:

- Vyslovuje se k návrhům směrnic a nařízení připravených Evropskou komisí, která je následně s přihlédnutím ke stanovisku Parlamentu může příslušným způsobem pozměnit;
- Schvaluje mezinárodní dohody vyjednané Komisí a jakékoli navrhované rozšíření Evropské unie;
- Parlament má stejné pravomoci jako Rada při přijímání legislativy, která se týká významných otázek jako např. volný pohyb pracovních sil, vzdělávání, výzkum, životní prostředí, zdravotnictví atd. Evropský parlament má pravomoc zamítnout předpisy navrhované pro tyto oblasti, pokud absolutní většina jeho poslanců hlasuje proti „společnému postoji“ Rady.

Evropský parlament je také orgánem, který vykonává demokratickou kontrolu nad Unií. Má pravomoc rozpustit Komisi tak, že jí hlasováním vysloví nedůvěru. Parlament rovněž klade Komisi a Radě ústní a písemné dotazy, kterými kontroluje každodenní řízení politik EU. Kromě toho předseda Evropské rady informuje Parlament o rozhodnutích, které Rada přijala. [19]

2.5.5 Evropský soudní dvůr

Jakýkoliv pořádek může být trvale stabilní jen tehdy, pokud existuje nezávislá moc, která na něj dohlíží. K tomu se ještě u společenství států přidává fakt, že jsou společná pravidla – pokud jsou přenechána kontrole národních soudů – v každém státě rozdílně vykládána a aplikována. Jednotná aplikace práva Unie ve všech státech by tak byla zpochybněná. Tyto důvody vedly ke zřízení Soudního dvora EU. ESD se v současné době skládá z 27 soudců a 8 generálních advokátů, kteří jsou jmenováni ve vzájemné shodě vlád členských států na 6 let. Každý členský stát vysílá jednoho soudce. ESD disponuje nejvyšší a současně jedinou soudní mocí ve všech otázkách práva Unie.

Obecné pojetí úlohy Evropského soudního dvora zahrnují tři základní oblasti:

1) Kontrola aplikace práva ES jak při provádění Smluv orgány EU, tak i z hlediska členských států a jednotlivců při plnění povinností uložených jim právem Unie;
2) Výklad práva Unie;
3) Vývoj práva Unie. [14]

2.5.6 Evropský účetní dvůr

Evropský účetní dvůr byl zřízen 22. července 1975 a začal fungovat v říjnu 1977 v Lucemburku. V současné době se skládá z 27 členů, jak plyne ze Smlouvy z Nice po rozšíření EU. Úkolem Účetního dvora je přezkoumávání, zda je s příjmy a výdaji EU nakládáno řádně a v souladu s právními předpisy. Kromě toho dohlíží na správnost finančního řízení. Na rozdíl od některých národních účetních dvorů nedisponuje Evropský účetní dvůr soudní pravomocí k vynucovacímu prosazování svých kontrolních pravomocí nebo k vyšetřování v případě podezření z nezákonné činnosti. Na druhé straně je autonomní ve volbě zkoumaného objektu a v metodě zkoumání. Jeho kontrole mohou být podřízeny i soukromé osoby, např. v otázce, zda byla finanční podpora Unie využita v souladu s předpisy EU.

Hlavní zbraní Evropského účetního dvora je možnost zveřejňování. Výsledky jeho kontrolní činnosti jsou na konci každého rozpočtového roku shrnuty ve výroční zprávě, která je uveřejněna v Úředním listu EU a takto je zpřístupněna evropské veřejnosti. Kromě toho může EUD kdykoliv zaujmout ve zvláštní zprávě stanovisko k určitým otázkám finančního řízení. Toto stanovisko je také zveřejněno v Úředním listu EU.

2.5.7 Další významné instituce a poradní orgány Evropské unie:

Evropská investiční banka;

Evropský investiční fond;

Evropský ombudsman;

Evropská centrální banka;

Hospodářský a sociální výbor;

Výbor regionů.

3 ORGANIZACE OCHRANY KRITICKÉ INFRASTRUKTURY

Ochrana kritické infrastruktury je proces, který při přezkoumání všech možných rizik a hrozeb vede k zajištění funkčnosti vazeb, prvků a toků kritické infrastruktury tak, aby se významným způsobem snížila možnost jejího selhání. V důsledku provázanosti sektorů může selhání kritické infrastruktury v jednom státě ovlivnit více států. Ochrana KI vyžaduje nejen sdílení odpovědností s privátním sektorem a výměnu informací mezi veřejnou správnou a dalšími relevantními organizacemi, ale i spolupráci v rámci celé Evropské unie.

Účinná ochrana vyžaduje komunikaci, koordinaci a spolupráci na národní, evropské i mezinárodní úrovni mezi všemi zúčastněnými subjekty. Na úrovni EU bude zaveden společný rámec na ochranu kritické infrastruktury, který zajistí, že každý členský stát bude poskytovat přiměřenou anebo stejnou úroveň ochrany týkající se vlastní KI. Dále bude zaveden společný rámec na ochranu kritické infrastruktury, kde Komise bude na podporu aktivit členských států poskytovat identifikaci KI, výměnu a šíření nejlepších postupů týkajících se problematiky ochrany KI.

Posílení kritické infrastruktury v EU bude dosaženo zavedením společného rámce EPCIP (společné cíle, metody, např. pro srovnávání, určování vzájemných závislostí), který umožní výměnu nejlepších postupů a kontrolních mechanismů.

Některé z prvků, které by měly být součástí společného rámce:

- Společné principy CIP;
- Společně dohodnuté kódy/standardy;
- Obecné definice, na základě kterých mohou být vytvořeny odvětvově specifické definice;
- Společný seznam odvětví s kritickou infrastrukturou EU;
- Prioritní oblasti CIP;
- Popis odpovědností zúčastněných subjektů;
- Dohodnuté referenční ukazatele;
- Metody pro srovnávání a stanovení prioritních infrastruktur u jednotlivých odvětví. [1]

3.1 Faktory pro určení potenciální kritické infrastruktury a jejich prvků

3.1.1 Rozsah

Ztráta prvku kritické infrastruktury se hodnotí podle velikosti zeměpisné oblasti, která by mohla být jeho ztrátou nebo nedostupností postižena – mezinárodní, vnitrostátní, oblastní, teritoriální nebo místní. [2]

3.1.2 Závažnost

Stupeň dopadu nebo ztráty může být hodnocen jako žádný, minimální, mírný nebo velký. Mezi kritéria, která lze pro hodnocení velikosti použít, patří:

- Veřejný dopad (počet dotčených obyvatel, ztráty na životech, onemocnění, vážné zranění, evakuace);
- Hospodářský dopad (vliv na HDP, závažnost hospodářské ztráty anebo zhoršení kvality výrobků nebo služeb);
- Životní prostředí (dopad na veřejnost a okolní oblast);
- Vzájemná závislost (mezi jinými prvky kritické infrastruktury);
- Politický dopad (důvěra ve schopnost vlády). [2]

3.1.3 Vliv času

Toto kritérium zjišťuje, kdy by mohla mít ztráta prvku vážný dopad (tj. okamžitě, za 24 – 48 hodin, za týden, jindy). [2]

3.2 Organizace ochrany kritické infrastruktury

Organizace Ochrany kritické infrastruktury Evropské unie není ještě přesně definována. Směrnice, která tuto problematiku bude zastřešovat, je ve stavu pozměňovacích návrhů. Proto jsou zde uvedeny všechny stavy, které mohou nastat.

Původní text:

Přímou odpovědnost za ochranu kritických infrastruktur v současnosti nesou členské státy a vlastníci či provozovatelé kritických infrastruktur. To by se nemělo měnit. [20]

Pozměňovací návrh č. 1:

Přímou a konečnou odpovědnost za ochranu kritických infrastruktur nesou členské státy a vlastníci či provozovatelé kritických infrastruktur. S ohledem na skutečnost, že vnitrostátní služby znají situaci ve vlastních zemích nejlépe, měl by být u evropské kritické infrastruktury (ECI) uplatňován přístup „zdola nahoru“. [20]

Pozměňovací návrh č. 2:

Přímou odpovědnost za ochranu kritických infrastruktur nesou členské státy a vlastníci či provozovatelé kritických infrastruktur. To se v budoucnosti nesmí měnit. [20]

Pozměňovací návrh č. 3:

Přímou odpovědnost za ochranu kritických infrastruktur v současnosti nesou členské státy a vlastníci či provozovatelé kritických infrastruktur. EU by však měla v této oblasti převzít koordinaci, neboť účinnost opatření jednotlivých členských států v mnoha případech závisí na přeshraniční spolupráci. [20]

Nejreálnější a nejvíce pravděpodobný přístup bude v podobě Pozměňovacího návrhu č. 1, neboť některé země EU (Francie, Německo, Nizozemí) mají již svou kritickou infrastrukturu definovanou. Dále se zde musí brát i skutečnost, že u všech zemí je situace s KI rozdílná, protože každá země má své zvláštní specifika, která jiné země nemají.

3.3 Úrovně ochrany kritické infrastruktury

3.3.1 Kritická infrastruktura na úrovni EU (ECI)

Evropské kritické infrastruktury představují takové zřízené kritické infrastruktury, které jsou nejdůležitější pro Unii, a které by v případě jejich narušení nebo zničení postihly dva nebo více členských států, popř. jeden z členských států, pokud je kritická infrastruktura umístěna v jiném členském státě. To s sebou nese přeshraniční dopady vyplývající ze vzájemných závislostí mezi propojenými infrastrukturami napříč všemi různými odvětvími.

Zavádění ECI:

1) Komise spolu s členskými státy připraví pro identifikaci ECI konkrétní kritéria podle jednotlivých odvětví;

2) Proběhne postupná identifikace a ověřování ECI v jednotlivých odvětvích členskými státy a Komisí. Vzhledem k přeshraničnímu charakteru dané kritické infrastruktury, budou rozhodnutí o jejím označení jako ECI učiněna na evropské úrovni;
3) Členský stát a Komise analyzují nedostatky v bezpečnosti ECI v jednotlivých odvětvích;
4) Členské státy a Komise se s ohledem na vzájemné závislosti dohodnou na prioritních odvětvích/infrastrukturách;
5) Komise a hlavní zainteresované subjekty členských států navrhnou dle potřeby pro každý sektor základní ochranná opatření, která mohou obsahovat standardy;
6) Po přijetí návrhu Radou budou tato opatření zavedena;
7) Pravidelná kontrola bude zajišťována členskými státy a Komisí. Revize (opatření a označení KI) budou prováděny dle potřeby. [1]

3.3.2 Národní kritická infrastruktura (NCI)

S přihlédnutím ke stávajícím pravomocím Unie mají odpovědnost za ochranu vnitrostátních kritických infrastruktur jejich vlastníci, provozovatelé a členské státy.

Za účelem zlepšení ochrany vnitrostátních kritických infrastruktur by měly všechny členské státy vytvořit vnitrostátní program na ochranu kritických infrastruktur. Cílem takových programů by mělo být stanovení přístupu členského státu k ochraně vnitrostátních KI umístěných na jeho území. Tyto programy by se měly zabývat minimálně těmito otázkami:

- Určení a vytvoření vnitrostátních kritických infrastruktur členským státem podle předem definovaných vnitrostátních kritérií. Tato kritéria by měl vytvořit každý členský stát s přihlédnutím minimálně k následujícím kvalitativním a kvantitativním dopadům narušení nebo zničení určité infrastruktury:
    - *Rozsah* – narušení nebo zničení určité kritické infrastruktury bude hodnoceno podle velikosti zeměpisné oblasti, která by mohla být její ztrátou nebo nedostupností postižena.
    - *Závažnost* – důsledky narušení nebo zničení určité kritické infrastruktury budou posuzovány na základě:
        - veřejného dopadu (počet dotčených obyvatel);
        - hospodářského dopadu;
        - dopadu na životní prostředí;

- § politických dopadů;
- § psychologických dopadů;
- § dopadů na veřejné zdraví.

Pokud taková kritéria neexistují, Komise členskému státu na jeho žádost pomůže při jejich rozvoji poskytnutím příslušných metodik;

- Zahájení dialogu s vlastníky, provozovateli kritických infrastruktur;
- Určení vzájemných zeměpisných a odvětvových závislostí;
- Vytváření případných krizových plánů souvisejících s vnitrostátními kritickými infrastrukturami;
- Doporučuje se, aby každý členský stát založil svůj program na ochranu kritické infrastruktury na společném seznamu odvětví kritické infrastruktury vytvořeném pro evropské kritické infrastruktury.

Zavedení obdobných přístupů k ochraně vnitrostátních KI v členských státech by pomohlo zajistit, aby subjekty zainteresované na KI v celé Evropě měly prospěch z toho, že nepodléhají odlišným rámcům vedoucím k dalším nákladům a že není narušen vnitřní trh.

Zavádění NCI

1) Členské státy navrhnou za pomoci EPCIP konkrétní kritéria pro identifikaci NCI;
2) Proběhne postupná identifikace a ověřování NCI členskými státy v jednotlivých odvětvích;
3) Členské státy analyzují možné bezpečnostní nedostatky NCI v jednotlivých odvětvích;
4) Členské státy určí prioritní odvětví, kde je třeba jednat a případně při tom vezmou v úvahu vzájemné závislosti a priority schválené na úrovni EU;
5) V případě potřeby schválí členské státy minimální ochranná opatření pro jednotlivá odvětví;
6) Členské státy zajistí, že vlastníci, provozovatelé v jejich kompetenci provedou nezbytná implementační opatření;
7) Pravidelné monitorování zajistí členské státy. Revize (opatření a označení KI) budou vykonávány dle potřeby. [1]

3.3.3 Privátní sektor – role vlastníků, provozovatelů a uživatelů KI

Označení kritická infrastruktura představuje pro vlastníky a provozovatele dané infrastruktury určitou odpovědnost. Z označení infrastruktury jako ECI nebo NCI vyplývají pro její vlastníky a provozovatele čtyři hlavní povinnosti:

1) Oznámení příslušnému orgánu členského státu, že infrastruktura může být kritická;
2) Určení vedoucího představitele (představitelů) vystupujícího jako styčný úředník pro bezpečnost mezi vlastníky, provozovateli a příslušným orgánem ochran KI v členském státě. Styčný úředník pro bezpečnost se bude podílet na rozvoji bezpečnostních a krizových plánů. Měl by být rovněž hlavním styčným úředníkem s příslušným odvětvovým orgánem v členském státě a podle potřeby i s donucovacími orgány;
3) Zřízení, implementace a aktualizace Operačního plánu pro bezpečnost;
4) Je-li to vyžadováno, účast na vypracování krizového plánu KI s orgány odpovědnými za civilní obranu v příslušném členském státě a s donucovacími orgány. [1]

Ve specifických situacích, ke kterým může u některých infrastruktur docházet, např. u elektrorozvodné nebo informační sítě, nemůžeme předpokládat (z praktického a finančního hlediska), že vlastníci a provozovatelé budou schopni zajistit dostatečnou úroveň bezpečnosti pro celý svůj majetek. Pro takové případy se navrhuje, aby vlastníci a provozovatelé společně s příslušnými orgány identifikovali kritická místa (uzly) fyzické nebo informační sítě, na která by se ochranná opatření měla zaměřit.

3.4 Subjekty ochrany kritické infrastruktury

Při tvorbě různých strategií ochrany KI je důležité si uvědomit, které subjekty jsou do tohoto procesu zavedeny. Na žádného z nich by se nemělo při této tvorbě zapomenout.

Při tvorbě evropské strategie je to Evropská unie, která plní úlohu koordinátora celého procesu ochrany kritické infrastruktury. Plní úlohu hlavního tvůrce ochrany, dále kontrolora a také má funkci represivní, kdy při nedodržení či nesplnění podmínek může ukládat sankce.

Na národní úrovni je to stát, který nám rovněž plní dvě role. Na jedné straně má stát povinnost chránit občany, majetek a životní prostředí. Na druhé straně sám stát je zřizovatelem řady subjektů kritické infrastruktury.

Dalším v pořadí jsou soukromí vlastníci podniků či organizací a provozovatelé – tedy subjekty kritické infrastruktury.

V neposlední řadě je nutno zmínit roli fyzické osoby, které se výpadek funkce subjektů KI významně dotkne.

Především je nutno zdůraznit to, že základem jakýchkoliv strategií k ochraně KI je respektování toho, že podstatná část subjektů KI je v soukromých rukou. To tedy znamená, že bez velmi úzké spolupráce se soukromým sektorem není realizace jakékoliv strategie ochrany KI dost dobře možná. Dále nutno zdůraznit, že žádné násilné vstupy státu cestou stanovení povinností subjektů KI nemusí přinést žádoucí výsledky. Reakce soukromého sektoru bude vždy v oblasti toho, co mi to přinese, respektive kdo to zaplatí. Bude tedy vhodnější volit takový přístup, který umožní soukromé subjekty pro řešení dané problematiky zapojit, ještě lépe, pro řešení nadchnout. Tedy přesvědčit je o tom, že pro jednotlivé subjekty KI je jejich ochrana přínosem. To sice znamená vynaložení určitých prostředků, ale dotčený subjekt tím získává konkurenční výhodu. Ty spočívají v tom, že za krizové situace má subjekt KI minimalizované ztráty a může prakticky bez přerušení výrobní činnosti nabízet své produkty ve prospěch řešení krizové situace.

3.5 Analýza směrnic vydaných Evropskou unií

Ochrana kritické infrastruktury na úrovni Evropské unie je stále v procesu utváření jednotlivých legislativních norem. Zatím chybí konkrétní zákon, dle kterého by ochrana KI EU fungovala. Z toho důvodu se musí pracovat dle více dílčích směrnic a sdělení.

3.5.1 Sdělení Komise Radě a Evropskému parlamentu „Ochrana kritické infrastruktury při boji proti terorismu“

Tento dokument je prvním uceleným materiálem Evropské unie týkající se ochrany KI a má 5 kapitol. První kapitola hovoří o přípravě na celkovou strategii ochrany kritické infrastruktury a obsahuje současný přehled opatření, která Komise provádí v oblasti ochrany KI. Druhá kapitola seznamuje s možnými hrozbami a dopadem na KI EU. Hovoří o útoku na jednu část KI, kdy může či nemusí dojít ke ztrátám na životech. Dalším typem katastrofického selhání infrastruktury by mohl být případ, kdy selhání jedné části infrastruktury vede k selhání jejích dalších částí, což způsobuje rozsáhlý kaskádový efekt. Kaskádové události mohou vést k rozsáhlým škodám, protože způsobují rozsáhlé výpadky veřejných služeb. Takovými případy byli např. výpadky elektrického proudu v Severní Americe a v Evropě, ke kterým došlo v posledních letech. Třetí kapitola vymezuje Evropské

kritické infrastruktury. Zde se hovoří o tom, co je to kritická infrastruktura, stanovuje oblasti KI, faktory pro určování potenciální KI a oblast řízení bezpečnosti. Upozorňuje, že každé odvětví a členský stát si musí v rámci své příslušné oblasti působnosti a v souladu s harmonizovaným postupem Evropské unie určit infrastrukturu, která je pro ně kritická, a organizace nebo osoby odpovědné za bezpečnost. Ochrana KI vyžaduje konzistentní, kooperativní partnerství mezi vlastníky a provozovateli kritických infrastruktur a orgány členských států. Čtvrtá kapitola mluví o dosavadních pokrocích při ochraně KI na úrovni Unie. Tato činnost byla po útocích v Americe a Evropě zintenzívněna a předpokládá se další zlepšení a rozšíření opatření. Poslední kapitola pojednává o zvyšování schopnosti Evropské unie chránit kritické infrastruktury. Zde řadíme Evropský program na ochranu kritických infrastruktur EPCIP, Výstražná informační síť kritické infrastruktury – CIWIN, dosavadní provádění EPCIP a cíle a ukazatele pokroku EPCIP.

3.5.2 Zelená kniha o Evropském programu na ochranu kritické infrastruktury

Prostřednictvím tohoto dokumentu se EU obrací na odborníky i laickou veřejnost. Cílem je snaha o zapojení velkého množství subjektů, které by poskytly konkrétní informace o politikách vhodných pro Evropský program pro ochranu kritické infrastruktury. Zelená kniha má celkem 9 kapitol. V úvodu jsou zmíněny souvislosti, kvůli kterým tento dokument vznikl. Stanoví, že pro účinnou ochranu lidských životů v ohrožení a majetku na území EU před terorismem, přírodními pohromami a nehodami je nezbytné, aby veškerá narušení či manipulace s KI byla, v rámci možností, krátká, málo četná, řiditelná, územně omezená a měla minimální negativní dopad na dobré životní podmínky občanů členských států a celé EU. Zelená kniha předkládá možnosti, kterých může Komise využít, aby splnila požadavek Rady zřídit EPCIP a CIWIN. Dále stanovuje účel a oblast působnosti EPCIP. Hlavním cílem EPCIP by bylo zajistit, aby v rámci celé Evropské unie existovala přiměřená a rovnoměrná úroveň bezpečnostní ochrany KI. Úroveň ochrany by neměla být stejná pro všechny KI, ale měla by být odvozená od dopadu, jež by mohlo způsobit jejich možné selhání. V oblasti působnosti a ochrany předpokládá existenci možných třech oblastí:

a) Stejný přístup pro veškerá ohrožení

Komplexní přístup, který počítá jak s hrozbami úmyslných útoků, tak přírodních pohrom. Zajistil by maximální synergický efekt mezi ochrannými opatřeními, ale bez zvláštního důrazu na terorismus;

b) Stejný přístup pro veškerá ohrožení, ale se zaměřením na terorismus

Pružný přístup, který by zajistil návaznost na další druhy ohrožení, jako je hrozba úmyslných útoků či přírodních pohrom, ale s prioritním zaměřením na terorismus. Pokud je úroveň ochranných opatření u příslušného odvětví přiměřená, zainteresované subjekty by se měly zaměřit na ohrožení, kde jsou stále zranitelné;

c) Přístup zaměřený na terorismus

Přístup orientovaný na terorismus, bez jakékoliv zvláštní pozornosti vůči běžnějším ohrožením.

Přístup, který by se měl uplatnit, zatím není stanoven a vše je ve fázi jednání. V Zelená knize je také uveden návrh základních principů EPCIP. Stanovuje, na jakém společenském rámci EPCIP pracuje, definuje kritickou infrastrukturu na úrovni Evropské unie, na národní úrovni a určuje roli vlastníků, provozovatelů a uživatelů KI. V poslední kapitole zdůrazňuje určitá podpůrná opatření pro EPCIP. Zde seznamuje s projektem CIWIN, možnostmi určitého sladění či normalizaci různých výstražných systémů států, oblastmi financování těchto oblastí a způsoby hodnocení a kontroly implementace EPCIP.

3.5.3 Sdělení Komise o Evropském programu na ochranu kritické infrastruktury

Tento dokument je doposud poslední, který byl přijat Evropskou unií. Dokument už obsahuje zásady, postupy a nástroje navrhnuté s cílem zavést systém EPCIP. Sdělení je složeno z 8 kapitol. Obecným cílem je zlepšit ochranu KI v EU. Ochrana KI bude založena na principu stejného přístupu pro veškerá ohrožení, ovšem s prioritním zaměřením na terorismus. Jsou zde konkretizovány zásady pro provádění EPCIP, kde na rozdíl od Zelené knihy je přidána zásada odvětvového přístupu. Je zde stanoven rámec EPCIP a kontaktní skupina pro ochranu KI. Jsou zde definovány Evropské kritické infrastruktury. Ty představují takové zřízené KI, které jsou nejdůležitější pro Unii a které by v případě narušení nebo zničení postihly dva nebo více členských států, popř. jeden z členských států, pokud je KI umístěna v jiném členském státě. Čtvrtá kapitola pojednává o opatřeních navržených pro usnadnění rozvoje a provádění EPCIP. Zde je popsán Akční plán EPCIP, Výstražná informační síť kritické infrastruktury CIWIN, Skupiny odborníků, Proces sdílení informací o ochraně kritické infrastruktury a Určení vzájemných souvislostí. V páté kapitole je rozebráno téma Národní kritické infrastruktury (NCI). V šesté Krizové plánování se hovoří o tom, že je to klíčový prvek procesu ochrany KI a je důležitý pro minimalizaci

potenciálních dopadů narušení nebo zničení KI. V předposlední kapitole Vnější prostředí je zdůrazněno, že terorismus a další trestné činnosti, přírodní nebezpečí a další důvody nehod nejsou omezeny hranicemi. Na hrozby nelze nahlížet pouze ve vnitrostátních souvislostech. Vnější prostředí ochrany KI musí být při provádění EPCIP zohledněno v plném rozsahu. Aspekt propojenosti a vzájemné závislosti současného hospodářství a společnosti znamená, že dokonce i narušení za hranicemi EU by mohlo mít vážný dopad na Unie a jeho členské státy. Spolupráce zaměřená na zvýšení ochrany KI v rámci EU sníží riziko, že hospodářství EU bude narušeno, čímž se posílí celosvětová hospodářská konkurenceschopnost EU. Poslední kapitola hovoří o Doprovodných finančních opatřeních, kdy z programu Společenství „Prevence, připravenost k obraně proti terorismu a jiným souvisejícím bezpečnostním rizikům a zvládání jejich následků“ pro období 2007-2013 se užijí finanční prostředky pro provádění EPCIP.

3.6 Oblasti kritické infrastruktury Evropské unie

3.6.1 Energetika

Energetika je základním sektorem pro všechny rozvinuté ekonomiky a je hnací silou mnoha procesů společnosti. Je nezbytná pro ekonomiku, obranu i udržení kvality života občanů. Udržitelná, konkurenceschopná a bezpečná energie je jedním ze základů našeho života. Prioritním cílem politiky EU v této oblasti je zabezpečení dodávek energií pro všechny spotřebitele za dostupné ceny při respektování životního prostředí. Evropská unie s více než 450 miliony spotřebitelů představuje druhý největší trh s energií na světě. Jedná-li jako jeden celek, má dostatečnou váhu, aby ochránila a prosadila své zájmy. Evropská unie nedisponuje jen velikostí, ale i škálou politik[8], které může pro nové energetické prostředí použít. Evropa však musí v této oblasti jednat rychle, protože v odvětví energetiky trvá mnoho let, než se inovace začnou používat. Rovněž musí i nadále podporovat rozmanitost typů energií, zemí původu a tranzitních zemí.

[8] Třetí „Energetický balíček“ Evropské komise; Návrh zprávy o strategii pro biomasu a biopaliva (2006/2082(INI)); Nařízení 2003/1228/ES o přeshraniční obchodu s elektrickou energií, které stanovuje pravidla pro přenos elektřiny mezi členskými státy.

Z hlediska výstupu lze energetický sektor rozdělit do dvou skupin:

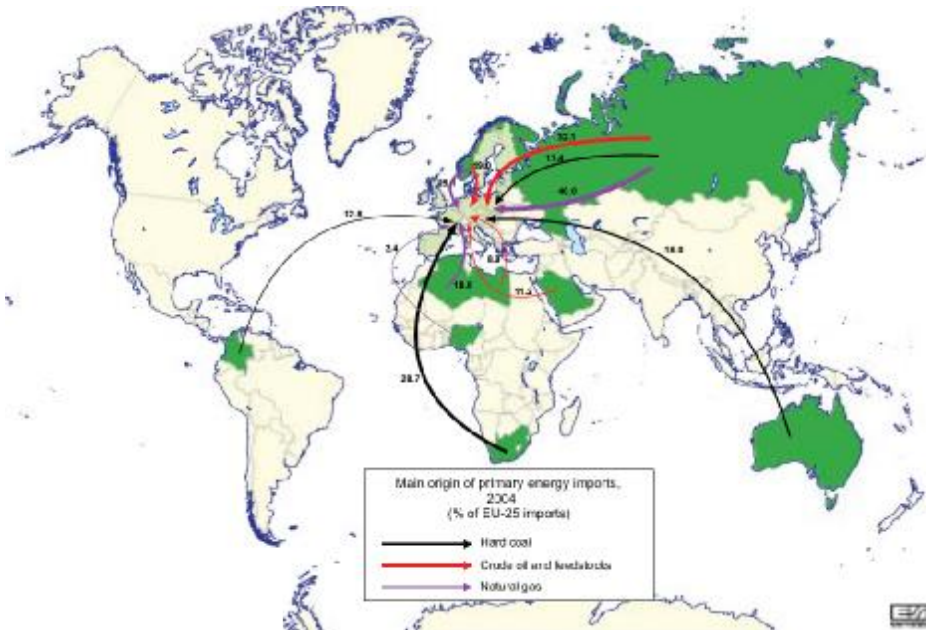
- Produkce ropy a plynu, rafinování, zpracování, skladování a distribuce potrubím;
- Výroba a rozvod elektřiny.

3.6.1.1 Produkce ropy a plynu, rafinování, zpracování, skladování a distribuce potrubím

Přírodní zásoby ropy a zemního plynu jsou v EU omezeny. Takřka všechny státy EU musí tyto suroviny dovážet. Jediné významnější naleziště ropy a plynu v západní Evropě – Severní moře – bude již brzy vyčerpáno. Proto bude Evropská unie muset tyto výpadky nahradit a nejvýznamnější alternativu představuje Rusko, jakožto největší producent a exportér zemního plynu a druhý největší producent a exportér ropy na světě.

Otázku rafinování, zpracování, skladování ropy a plynu řeší jednotlivé členské státy individuálně. Evropská unie však vydává různé Sdělení či Směrnice, které musí státy dodržovat. Posledním významnějším materiálem je Směrnice Rady 2006/67/ES, kterou se členským státům ukládá povinnost udržovat minimální zásoby ropy nebo ropných produktů.

Distribuce potrubím je vzhledem k vzdálenostem, na které se dnes ropa a zemní plny přepravuje nejnáročnějším článkem řetězce. Evropa je dnes protkána hustou sítí dálkových plynovodů a ropovodů. Ty jsou vedeny nejen po souši, ale mohou být také položeny na mořském dně. Kvalita potrubních cest musí být neustále kontrolována a případné závady neodkladně odstraněny, aby nedocházelo k ekologickým katastrofám. Tuto kontrolu je však nutno vykonávat od počátku, tj. od produkce, rafinování, zpracování i skladování těchto látek.



Obr. 2: Hlavní oblasti dovážených primárních energií do EU

3.6.1.2 Výroba a rozvod elektřiny

Takřka každá činnost vyžaduje elektřinu. Elektřina je také nutná k výrobě jiných forem energie, jako je např. proces rafinování ropy apod. Elektrický systém EU je silně propojený, mnohauzlový a distribuční. Fyzicky je možné tento systém dělit na tři části:

- Distribuce;
- Řízení;
- Komunikace.

Výrobní prvky KI zahrnují především elektrárny na fosilní paliva, přehrady a jaderné elektrárny. Pro výrobu elektrické energie je důležité zajistit plynulý přísun surovin, ze kterých se bude elektrická energie vyrábět. Vstupní suroviny mohou být často samy o sobě nebezpečné. Pro případ výpadku je nutné mít k dispozici dostatečnou záložní kapacitu, která by byla tento výpadek schopna pokrýt.

Mezi opatření ochrany tohoto sektoru lze zařadit například identifikace nutných zásob surovin pro zajištění plynulosti výroby elektrické energie. Bezpečnost jednotlivých zařízení je dnes řešena individuálně – pro každé zařízení. Toto by se mělo v rámci EU sjednotit. Dále bezpečnostní řešení obvykle ignorují fakt, že tato zařízení jsou zapojena do většího celku energetické soustavy státu. Plánování ochranu bude z tohoto důvodu nutné přehodnotit a více zohlednit národní a především evropské měřítko.

3.6.2 Jaderný průmysl

Jaderný průmysl a jaderné elektrárny jsou v Evropské unii velice diskutovaná témata. Ke konci ledna 2005 bylo ve světě v provozu 443 komerčních jaderných bloků, dalších 31 jaderných bloků je rozestavěno. Tyto reaktory dodávají 15 % světové elektřiny. Kromě toho 56 států provozuje celkem 284 výzkumných reaktorů pro vědecké účely. Dalších 220 jaderných elektráren pohání vojenská a námořní plavidla. Na celém světě je dále 28 jaderných reaktorů ve výstavbě a dalších 35 je pevně naplánováno. V rámci EU je v provozu celkem 152 jaderných reaktorů v 15 členských státech (Belgie, Bulharsko, Česká republika, Finsko, Francie, Litva, Maďarsko, Německo, Nizozemí, Rumunsko, Slovensko, Slovinsko, Spojené království Velké Británie a Severního Irska, Španělsko, Švédsko).

Jaderná energie je v EU nejvýznamnějším zdrojem, následuje uhlí (30 %), plyn (18 %) a ropa (6 %). Obnovitelné zdroje poskytují 14 % energie. [25]

Z hlediska výstupu se jaderný sektor dělí pouze na jednu skupinu:

- Produkce a skladování/zpracování jaderných látek.

V celé Evropské unii vznikne asi 40 000 m^3 radioaktivního odpadu za rok. Naprostá většina tohoto radioaktivního odpadu pochází z každodenního provozu jaderných elektráren a dalších jaderných zařízení a je klasifikován jako nízce radioaktivní a krátkodobý. Vyhořelé jaderné palivo produkuje přibližně 500 m^3 vysoce radioaktivního odpadu ročně, ve formě buďto ozářeného jaderného paliva nebo vitrifikovaného odpadu[9]. Celkem byly dosud uloženy v povrchových nebo podpovrchových úložištích asi 2 milióny m^3 takových odpadů. V případě vysoce radioaktivního a dlouhodobého odpadu sice existuje řada stupňů strategie řízení, ale žádná země dosud nezavedla navrhované konečné řešení. Ve výběru lokality

[9] Vitrifikace – uskladnění radioaktivních odpadů zatavením do skla. Při tomto procesu je radioaktivní materiál přidán do sklářského kmene a výsledná homogenní sklovina je převedena do ocelových kontejnerů určených pro uskladnění v hlubinném úložišti.

došlo k významnému pokroku ve Finsku[10], Švédsku a Francii. Ve většině zemí je však výběr lokality ústředním bodem, který zneškodnění odpadu zpožďuje.

Ve výzkumných programech se vyvíjejí doplňkové techniky nakládání s odpadem, které jsou v zásadě zaměřeny na snižování buďto objemu, anebo dlouhodobé složky. I když by nabízely možnost snížit dlouhodobou toxicitu takových odpadů, nikdy nemohou úplně odstranit potřebu jejich izolace od životního prostředí. Tento přístup „koncentrace a uzavření" umožňuje minimalizovat dopady na životní prostředí. Klíčem k zajištění pokroku je příznivější postoj veřejnosti a její zapojení do rozhodovacího procesu. Bezpečnost je rovněž v centru pozornosti výzkumné činnosti Unie (Euratomu) v různých oblastech.

Pokud jde o provoz stávajících jaderných zařízení v Evropě, uznává se vysoká úroveň jaderné bezpečnosti. Udržení této úrovně a její možné zvýšení jsou předmětem koordinované a dlouhodobé vývojové a výzkumné činnosti. Nezastupitelnou úlohu při tomto úsilí má rámcový program Euroatomu pro výzkum[11].

3.6.3 Informační a komunikační technologie, (I.C.T.)

V souvislosti s neustálým rozvojem informačních a komunikačních technologií se často hovoří o informační infrastruktuře jako takové (počítačové vybavení, software, Internet apod.). Ta se v současné době vyvíjí enormní rychlostí – rozšiřování Internetu, neustálé zvyšování rychlosti přenosu dat, užívání mobilních telefonů, přechod analogového na digitální TV vysílání, používání GPS navigací apod. A v návaznosti na to, s rozvojem internetového bankovnictví, on-line přístupů k různým datům, řízení technologických procesů prostřednictvím Internetu, stahování legálních her, filmů či hudby je nutné tuto oblast neustále bezpečnostně rozvíjet a chránit.

---

[10] Ve Finsku bylo úložiště vybráno se souhlasem místního obyvatelstva a schváleno finským parlamentem. Finské právo vylučuje možnost vývozu nebo dovozu jaderného odpadu z Finska či do něj.

[11] Nařízení Rady (Euratom) č. 1908/2006, ze dne 19. prosince 2006, kterým se stanoví pravidla pro účast podniků, výzkumných středisek a vysokých škol na akcích v rámci Sedmého rámcového programu Evropského společenství pro atomovou energii a pro šíření výsledků výzkumu (2007–2011).

Z hlediska výstupu se informační a komunikační sektor rozděluje na osm skupin:

- Ochrana informačních systémů a sítí;
- Automatizace přístrojů a kontrolních systémů (SCADA atd.);
- Internet;
- Poskytování pevných telekomunikačních sítí;
- Poskytování mobilních telekomunikačních sítí;
- Radiová komunikace a navigace;
- Satelitní komunikace;
- Vysílání (televizní a rozhlasové).

Informační a komunikační sektor je specifický vysokou mírou inovací a také vysokou mírou konkurence. Tyto dva faktory způsobují, že celý sektor je velmi dynamický. Konvergence technologií způsobuje pozvolný přechod od využívání klasických telefonů k moderním datovým službám. Objevují se také úplně nové technologie, jako jsou např. bezdrátové sítě apod.

Mezi vlivy mající význam z hlediska bezpečnosti můžeme zařadit povětrnostní a klimatické vlivy nebo i činnost člověka jako je neúmyslné přeseknutí kabelu nebo hrozby, které plynou od tzv. „insider tradingu“[12]. Výpadek telekomunikací může snadno způsobit kaskádový efekt selhání navazujících sektorů a tak zvýšit celkové následky tohoto výpadku.

V první řadě je nutné definovat minimální úroveň zabezpečení, kterou by ICT systémy měly mít zabudovanou. Tato minimální úroveň může být prosazována Generálním ředitelstvím pro komunikaci Evropské komise a také prostřednictvím různých Sdělení[13]. Mezi opatření, která je možná realizovat v rámci tohoto sektoru, je možnost přizpůsobit systémy tak, aby byly schopné ve větší míře přesměrovat svůj provoz. Význam výpadku jednoho prvku by se pak zmenšil, protože celkový provoz by byl přesměrován přes jiná zařízení.

[12] Zneužívání důvěrných či neveřejných informací.

[13] Sdělení Komise Radě, Evropskému parlamentu, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: i2010 – První výroční zpráva o evropské informační společnosti (SEC (2006) 604).

Vzhledem k dynamičnosti tohoto sektoru bude nutné pečlivě zkoumat rizika, kterým jsou nynější systémy vystaveny a slabiny, které by mohly být zneužity při případném útoku. Informační a komunikační infrastruktura má také význam nadnárodní – mezinárodní, z tohoto důvodu při ochraně bude nutné koordinovat úsilí s klíčovými spojenci a obchodními partnery.

3.6.4 Voda

Voda je pro přežití a vývoj lidské společnosti nepostradatelná. Je nezbytná pro lidský život a potřebná pro mnoho průmyslových činností a postupů. Vodní politika EU se zabývá některými významnými tlaky, jako je znečištění způsobené vypouštěním domácích odpadních vod, živnými látkami ze zemědělství, průmyslovými emisemi a vypouštěním nebezpečných látek. V případech, kdy byly během posledních 10 až 30 letech provedeny investice, došlo z velké části k vyřešení těchto problémů s vodou. U deseti členských států, které přistoupily v roce 2004, a u dvou, které přistoupily v roce 2007, podléhá úplné provádění investičně náročných nařízení zaměřených na kontrolu bodových zdrojů přechodnému období, které ve většině případů potrvá do roku 2015.

Nejaktuálnější opatření týkající se ochrany vody jsou Sdělení s názvem „Směrem k udržitelnému vodnímu hospodářství v Evropské unii – První etapa provádění rámcové směrnice o vodě 2000/60/ES“ a Sdělení s názvem „Řešení problému nedostatku vody a sucha v Evropské unii“. První Sdělení shrnuje opatření, která členské státy doposud v této oblasti učinily. Druhé vymezuje sérii strategických možností s cílem spustit debatu o způsobech, jak se přizpůsobit nedostatku vody.

Z hlediska výstupu lze sektor vody rozdělit do tří skupin:

- Zásobování pitnou vodou;
- Kontrola kvality vody;
- Těsnění a kontrola množství vody.

V této oblasti je důležité shromáždit informace o základních hrozbách, které je možné použít pro hodnocení zabezpečení jednotlivých systémů. Vzhledem k obrovské rozsáhlosti je nesmírně obtížné zjistit včas vypuštění toxických látek do těchto systémů. Z tohoto

pohledu je nejvíce nebezpečná kontaminace zdrojů pitné vody. Pro tento sektor nelze vyloučit ani kybernetický útok[14], který by vedl buď přímo k vyřazení systému, nebo jeho ovládnutí útočníkem. Zde nelze pominout ani návaznost na další sektory KI, zejména chemický průmysl.

Základními předpoklady zajištění bezpečnosti v tomto sektoru je zjištění zranitelností a jejich hodnocení. Teprve na základě takové analýzy je možné efektivně zvýšit bezpečnost, zajistit dostatečnou jakost vody a dostatečné množství pro občany EU.

3.6.5 Potraviny

Důvěra spotřebitelů v bezpečnost potravin a v potraviny vůbec byla v posledních letech několikrát otřesena vlivem zdravotních krizí souvisejících s potravinami. V reakci na tento problém má Evropská unie vypracovanou rozsáhlou strategii, aby obnovila důvěru lidí v bezpečnost potravin „od jejich produkce až po jejich konzumaci“. Strategie je založena na kombinaci přísných norem týkajících se potravin, zdraví a dobrých životních podmínek zvířat a zdraví rostlin. Tyto normy platí jak pro potraviny z produkce EU, tak pro dovoz.

Strategie má tři hlavní pilíře:

- Právní předpisy týkající se bezpečnosti potravin a krmiv;
- Rozhodování na základě spolehlivých vědeckých poznatků;
- Prosazování práva a kontrola.

Vedle obecných právních předpisů pro potraviny a krmiva přijala EU i předpisy zaměřené na konkrétní otázky bezpečnosti potravin, např. používání pesticidů, doplňků stravy, barviv, antibiotik a hormonů při výrobě potravin, přidávání vitaminů a minerálních a podobných látek do potravin a používání výrobků, které jsou s potravinami ve styku, např. obalů, a na konkrétní potraviny, např. maso, želatinu a mléčné výrobky. Přísná pravidla platí také pro uvádění plodin a potravin obsahujících geneticky modifikované organismy na trh, jejich označování a sledování. [28]

---

[14] V Austrálii byl zaznamenán úspěšný průnik do počítačové sítě chemičky. Hackerovi se podařilo získat kontrolu nad výpustí, kterou zneužil k vypuštění několika tun nebezpečných látek do přilehlého potoka.

Z hlediska výstupu má sektor potraviny pouze jednu skupinu:

- Zásobování potravinami a zajištění bezpečnosti potravin.

V této oblasti je velmi důležitý psychologický efekt útoku na potraviny. Jíst musíme všichni a veřejnost je tak obzvláště citlivá na zprávy o jídlu. Negativní zprávy mohou lehce vést ke kompletní změně stravovacích návyků, což může přinést danému sektoru zemědělství existenční problémy. Zajištění a udržení kvality uskladněných výrobků přitom vzhledem k naprosté decentralizaci v rámci sektoru nesmírně obtížné a nejspíše i nemožné. Je proto nutné vypracovat nové metody detekce, které by případnou kontaminaci odhalily ještě před tím, než se daný výrobek dostane na stůl spotřebitele. Současné metody detekce jsou zaměřeny na známé lidské patogeny[15], ale nejsou schopny detekovat mutaci. Pro zlepšení detekčních schopností bude nutné v EU rozšířit počet laboratoří s kvalifikovaným personálem. Dále se začínají zavádět systémy sledování pohybu zvířat tak, aby v případě nákazy mohlo být velmi rychle odhaleno ohnisko nákazy a předešlo se tak nárůstu škod.

3.6.6 Ochrana zdraví

Dobré zdraví je něco, co chceme všichni – pro sebe, pro své děti. Hraje důležitou roli při dlouhodobém ekonomickém růstu a udržitelném rozvoji. Existuje čím dál více důkazů, z nichž plyne, že náklady na udržení zdraví v případě dobrého zdravotního stavu nejsou příliš vysoké, oproti nákladům v případě dlouhodobě špatného zdravotního stavu (na zdravotní péči, léky, nemocenskou dovolenou, sníženou produktivitu, invaliditu nebo předčasné odchody do důchodu)[16].

Tento sektor hraje důležitou úlohu při zdolávání následků teroristických útoků. Jeho fungování určí, jak vážné budou následky útoku, alespoň co se týče celkových ztrát

---

[15] Patogen = biologický faktor (organismus), který může zapříčinit onemocnění hostitele.

[16] Příklad: celkové roční finanční zatížení při onemocnění plic v Evropě se odhaduje na 102 miliard eur, což je číslo srovnatelné s HDP Irska. Chronické onemocnění plic je nejdražší respirační onemocnění v Evropě, s odhadovanými ročními náklady ve výši 38,7 miliard eur, z toho 74 %, (28,6 miliard eur) představuje náklady z důvodu ztracených pracovních dnů. Nepřímé náklady související se ztrátou produktivity jsou téměř třikrát větší než náklady na přímou lékařskou péči. European Lung White Book, European Respiratory Society (ERS) and the European Lung Foundation (ELF), listopad 2003.

na životech. Ochrana tohoto sektoru je velmi problematická. Většina nemocnic z titulu své funkce je veřejně přístupná. To velmi ztěžuje identifikaci případných hrozeb. Zavedení řízeného vstupu přitom není možné, protože by toto opatření šlo proti účelu zdravotního zařízení – poskytnout neodkladnou zdravotní péči.

Z hlediska výstupu lze sektor ochrany zdraví rozdělit do tří skupin:

- Lékařská a nemocniční péče;
- Léky, séra, očkovací látky a léčiva;
- Biologické laboratoře a biologičtí činitelé.

Hlavní odpovědnost za zdravotní péči v Evropské unii nesou jednotlivé členské státy, avšak mnoho otázek v oblasti veřejného zdraví se řeší na úrovni EU. Ta pro řešení tohoto problému zavedla Strategii EU pro zdraví, která se zaměřuje především na posílení spolupráce a koordinace členských států, podporu vzájemné výměny informací a znalostí a na pomoc při vytváření vnitrostátních právních předpisů. Za tímto účelem EU vyvíjí ucelený zdravotnický informační systém, který má v celé EU poskytovat přístup ke spolehlivým a aktuálním informacím o hlavních tématech souvisejících se zdravím, a tedy i základ pro společnou analýzu faktorů ovlivňujících veřejné zdraví. EU rovněž chce rozšířit schopnost rychlé reakce na ohrožení zdraví. Dalším cílem je zajištění bezpečnosti pacientů a kvality zdravotní péče, usnadnění přeshraniční zdravotní péče, jakož i mobility zdravotnických odborníků a pacientů.

EU v návaznosti na problematiku ochrany zdraví vydala Evropský akční plán pro zdraví a životní prostředí pro období 2004-2010[17]. Akční plán je navržen tak, aby poskytoval EU vědecky podložené informace potřebné k tomu, aby pomohly 27 členským státům EU snížit nepříznivé dopady některých ekologických faktorů na zdraví a podpořil lepší spolupráci mezi účastníky v oblasti životního prostředí, zdraví a výzkumu. Při identifikaci navrhovaných akcí bere Akční plán v úvahu také zájmy jiných institucí a je navržen tak,

[17] Sdělení Komise Radě, Evropskému parlamentu, Evropskému hospodářskému a sociálnímu výboru „Evropský akční plán pro zdraví a životní prostředí pro období 2004-2010“; v Bruselu dne 9. 6. 2004 KOM(2004)416 v konečném znění.

aby byl přizpůsoben stávajícím akcím na regionální, vnitrostátní, evropské a mezinárodní úrovni, zejména procesu celoevropského zdraví a životního prostředí WHO.

Z hlediska opatření, která jsou možná provést ke zlepšení ochrany tohoto sektoru, můžeme zařadit např. ustanovení důvěryhodných zástupců veřejnosti – speciálně proškolených odborníků z různých oblastí, kteří budou veřejnost informovat o aktuální situaci a způsobu, jakým se občané mají chovat. Dále pro případ mimořádné události přijímat ustanovení, které by usnadnilo přeshraniční spolupráci mezi nemocnicemi.

3.6.7 Finanční sektor

Finanční sektor hraje v hospodářství Evropské unie klíčovou úlohu. Sektor finančních služeb představuje v EU více než 6% jejího HDP a poskytuje základní finanční produkty průmyslu, zejména investiční kapitál, a jednotlivým spotřebitelům, např. hypotéky, penze a pojištění. Finanční služby již zahrnují 2,5% zaměstnanosti v Unii a existuje zde značný potenciál z hlediska vytváření pracovních příležitostí. Výkonné odvětví finančních služeb zvyšuje konkurenceschopnost hospodářství jako celku tím, že napomáhá optimálnímu umisťování finančního kapitálu.

Poslední výzkumy Evropské komise ukazují významný přínos, který integrace finančních trhů bude znamenat pro podniky, investory i spotřebitele. Podniky budou mít přístup k levnějším financím – integrace akciového trhu sníží cenu investování prostřednictvím akcií o 0,5% a očekává se, že bude následovat snížení nákladů na financování společností pomocí dluhopisů o 0,4 %. Investoři budou těžit z vyšších výnosů z úspor, které budou zohledňovat rizika. Na základě těchto analýz přijala Komise Akční plán pro jednotný finanční trh.

Evropská centrální banka jako významná instituce Evropské unie se k této problematice také vyjadřuje. I když je jejím úkolem spravovat euro – jednotnou měnu EU a odpovídat za definování a provádění hospodářské a měnové politiky EU, byla požádána Radou

Evropské unie, aby vyjádřila Stanovisko k Návrhu směrnice Rady o určování a označování evropské kritické infrastruktury a o posouzení potřeby zvýšit její ochranu[18].

Z hlediska výstupu se finanční sektor rozděluje do dvou oblastí:

- Infrastruktury a systémy zúčtování a vypořádání obchodů s cennými papíry;
- Regulované trhy.

V dnešní době se již drtivá většina platebních operací provádí elektronicky, ačkoliv k fyzickému převozu peněz stále dochází[19]. Finanční instituce mají nejmodernější informační technologie. Jejich fungování je přímo závislé na všeobecné důvěře v jejich schopnost zajistit deklarované služby zákazníkům. Podkopání této důvěry může mít za následek prudký odliv klientů těchto institucí ke konkurenci a finanční problémy až krach pro postiženou společnost.

Vzhledem k vysoké provázanosti bankovního sektoru s telekomunikačním sektorem je nutno podchytit rizika plynoucí právě z tohoto propojení. V rámci zvýšení bezpečnosti by měly být zavedeny procesy výměny informací napříč celým sektorem. Dále je důležitá osvěta samotných uživatelů finančního sektoru. Ti jsou v poslední době terčem nepřeberného množství internetových útoků[20].

3.6.8 Doprava

Dopravní politika EU se snaží dosáhnout toho, aby dopravní systémy splňovaly hospodářské a sociální potřeby společnosti, ale i potřeby v oblasti životního prostředí. Účinné dopravní systémy jsou nezbytné pro zajištění evropské prosperity a mají významný

---

[18] Evropská centrální banka vydala v návaznosti na to Stanovisko Evropské centrální banky ze dne 13. dubna 2007 k návrhu směrnice Rady o určování a označování evropské kritické infrastruktury a o posouzení potřeby zvýšit její ochranu (CON/2007/11).

[19] V dnešní době se většinou jedná o převoz finanční hotovosti z hypermarketů a nákupních center.

[20] Zde se hovoří hlavně o phishingu – podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) od obětí útoku. Jejím principem je rozesílání e-mailových zpráv, které se tváří jako oficiální žádost banky či jiné podobné instituce a vyzývají adresáta k zadání jeho údajů na odkazovanou stránku.

dopad na hospodářský růst, sociální rozvoj a životní prostředí. Objem přepravy zboží a cestujících na dlouhé vzdálenosti se zvýšil díky odstranění překážek přeshraničního obchodu a cestování. Po rozšíření EU v roce 2004 se tento jev zrychlil a nyní dochází ke značnému nárůstu. Z veškerého zboží přepravovaného v EU se 44 % přepravuje po silnicích. Námořní přeprava na kratší vzdálenosti je zastoupena 39 %, železniční přeprava 10 % a vnitrozemská vodní přeprava 3 %. Nerovnováha je ještě zřetelnější u přepravy cestujících, kde na silniční připadá 81 %, na železniční přepravu pouze 6 % a na leteckou přepravu 8 %. Přechod od přepravy zboží a cestujících po silnicích k méně znečišťujícím způsobům dopravy bude hlavním faktorem jakékoli udržitelné dopravní politiky. Dalším hlediskem bude schopnost integrovat různé způsoby dopravy kombinováním prvků silnice-železnice, moře-železnice nebo železnice-vzduch.

Z hlediska výstupu lze sektor dopravy rozdělit do pěti oblastí:

- Silniční doprava;
- Železniční doprava;
- Letecká doprava;
- Vnitrozemská vodní doprava;
- Zámořská a příbřežní námořní doprava.

3.6.8.1 Silniční doprava

Silniční doprava je nejvytíženější oblastí dopravní infrastruktury. Lze na ni překonávat krátké i dlouhé vzdálenosti, těžko dostupná místa a je schopna přepravovat jak jednotlivce (jednotlivé zásilky), tak organizovanou početnou skupinu osob (nákladů). Z hlediska flexibility je tento druh přepravy taky neomezen, a to hlavně v oblasti individuální dopravy – lidé a materiály nejsou vázáni jízdními řády apod. Sektor silniční dopravy podobně jako další dopravní sektory je výrazně propojen s dalšími sektory KI. Z tohoto důvodu je nutná spolupráce i s ostatními sektory při řízení unikátních rizik vyplývající s této propojenosti.

Z hlediska zabezpečení jsou kritickými místy tzv. „úzká hrdla“, ve kterých dochází k zahušťování dopravy. Těmito „úzkými hrdly“ mohou být zejména tunely, mosty, hraniční přechody, ale i částečné uzavírky, apod. Zajištění bezpečnosti v těchto místech je hodně problematické. Do oblasti opatření bychom mohli zařadit vývoj vodítek a standardních kritérií pro identifikaci a zkoumání chování „úzkých hrdel“ s možností systémových opatření

k jejich zprůchodnění, resp. eliminace dopravních zácep. Při výstavbě nových staveb, jako jsou tunely, mosty apod., je možné nasadit technologie, které zajistí, že infrastruktura se stane odolnější vůči případným teroristickým útokům.

3.6.8.2 Železniční doprava

Železnice je jedním z nejstarších způsobů masové přepravy lidí a nákladu. Vstupní body do těchto prostor – nádraží – se přitom liší svým návrhem, strukturou, velikostí i účelem pro jaký jsou provozována (nákladní, překladiště mezi jednotlivými druhy dopravy, osobní a jakékoliv kombinace). Tyto faktory komplikují ochranu infrastruktury jako celku. Rozsáhlost sítě znemožňuje ochranu jako celku. Chránit lze tedy pouze kritické uzly, nikoliv celé tratě. Železnice a další druhy dopravy, jsou do určité míry komplementární – do určité míry lze nahradit jeden druh dopravy jiným s tím, že se budou lišit náklady přepravy. Jako největší riziko tohoto sektoru byly identifikovány nebezpečné látky, resp. jejich přeprava. Základní opatření pro zvýšení bezpečnosti se pak odvíjejí od rozhodování týkajících se přepravy a v případě nehody a odstranění následků úniku nebezpečných látek. Jedná se tedy o vyvinutí nejrůznějších systémů pro podporu rozhodování.

3.6.8.3 Letecká doprava

Leteckou dopravu z hlediska infrastruktury můžeme dělit na dvě části a to:
1) Letiště a další podpůrná pracoviště;
2) Letecká kontrola, komunikace a IS potřebný k provozu.

Letecká doprava je specifická tím, že má tisíce vstupních bodů na i mimo území EU. Toto specifikum činí kontrolu velmi obtížnou. Letecká doprava v EU ročně přepraví řádově miliony cestujících. Automatizované detekční systémy jsou přitom velmi nákladné a velmi objemné. Letiště přitom mají pouze omezenou kapacitu, do které je nutné tato detekční zařízení umístit. Tato zařízení navíc nejsou schopna detekovat plnou škálu hrozeb, kterým je vystavena moderní letecká přeprava. Čas, který je možné vyčlenit na detekci je přitom značně omezený a to také z důvodu, že hlavní výhodou letecké dopravy je její rychlost.

Mezi opatření, která jsou možná v tomto sektoru realizovat, můžeme zařadit snahy o identifikaci zranitelností tohoto sektoru a hrozeb, kterými je reálně ohrožen. Na základě toho bude možné zlepšit bezpečnost vstupních bodů. Velmi důležitou oblastí je zlepšení

schopností detekčních systémů tak, aby bylo možné rychle a spolehlivě monitorovat přepravovaný náklad. To ovšem vyžadovat zavádění nových technologií detekce.

3.6.8.4 Vnitrozemská vodní doprava

Vnitrozemská vodní doprava sehrává v hospodářském růstu a růstu životní úrovně obyvatel Evropské unie významnou úlohu. Na tento druh dopravy by měla EU klást v evropské dopravní a přepravní politice větší důraz. Pro rozvoj tohoto sektoru je nejdůležitější podmínkou spolehlivost vodní sítě a dostupnost vnitrozemských přístavů. V této oblasti jsou značné možnosti rozšiřování přepravy.

Jako jeho největší riziko lze identifikovat teroristický útok na lodě přepravující nebezpečnou látku[21]. To, že by to mohlo způsobit zastavení vnitrozemské dopravy na určitou dobu, není problém. Dalo by se to nahradit jinými způsoby přepravy. Daleko větším problémem by se stala kontaminace vody, která by ohrozila faunu a flóru podél vodních cest.

3.6.8.5 Zámořská příbřežní námořní doprava

Mezi základní bezpečnostní problémy můžeme zařadit v dnešní době omezené inspekční schopnosti – omezené ve smyslu technologickém i fyzickém. Inspektorů je málo a jejich vybavení má daleko k ideálnímu stavu.

Námořní doprava jako taková se navíc s větší části řídí mezinárodními úmluvami a mezinárodními autoritami, jako je International Maritime Organization. Vyjednávání na mezinárodní úrovni je náročné z hlediska času i zdrojů. Vyjednáváním se navíc obvykle dosáhne pouze kompromisu – nikoliv optimálního stavu z hlediska vyjednávaného parametru. V současné době také chybí technologie pro zajištění bezpečnosti vstupních bodů, kterých je prakticky neomezené množství. Jedná se o systémy detekce narušení hranic po vodě. Problémem pro výzkum a vývoj bude také konstrukční řešení lodí odolných vůči teroristickým útokům.

---

[21] K dnešnímu dni je po řekách, kanálech a menších vodních cestách přepravováno asi 17% nebezpečných látek

3.6.9 Chemický průmysl

Chemické látky a přípravky poskytují moderní společnosti přínosy, na kterých si tato společnost tvoří určitou závislost či je na ni závislá (např. v potravinářském průmyslu, ve zdravotnictví, textilním a automobilovém průmyslu atd.). Celosvětová produkce chemických látek a přípravků se zvýšila z 1 milionu tun v roce 1930 na dnešních 400 milionů tun. Nyní máme okolo 100 000 různých sloučenin, které jsou registrovány na trhu EU. Hodnota celosvětové produkce chemických látek se odhadovala na 1300 mld. eur, z čehož 31 % připadalo na chemický průmysl EU.

Na druhé straně však určité chemické látky a přípravky způsobily vážné škody na zdraví lidí, které měly za následek předčasná úmrtí a škody na životním prostředí. Mezi mnohými jinými je to azbest, známý pro svou schopnost vyvolávat rakovinu plic, či benzen způsobující leukémii. Ačkoliv byly tyto chemické látky posléze naprosto zakázány či podřízeny přísné kontrole, nebyla tato opatření přijata dříve, než došlo ke škodám, protože informace o negativním vlivu těchto chemických látek a přípravků nebyla k dispozici v době jejich masového nasazení.

Uvedené příklady odhalují slabost současné politiky EU v oblasti chemických látek. Politika EU musí zajistit vysokou úroveň ochrany veřejného zdraví a životního prostředí jak pro nynější, tak i příští generace. Dále v oblasti chemických látek by měla poskytovat motivující impulsy pro technickou inovaci a vývoj bezpečnějších chemických látek a přípravků. [32]

Z hlediska výstupu se sektor chemického průmyslu rozděluje do dvou oblastí:

- Produkce a skladování/zpracování chemických látek;
- Potrubí pro přepravu nebezpečných látek (chemických látek).

Jedním z významných problémů, které jsou typické pro tento sektor je zajištění stability dodávek výrobků chemického průmyslu, které jsou využívány dalšími sektory KI (např. chloramin pro čističky odpadních vod apod.). Schopnost průmyslu chránit kontinuitu přísunu svých surovin je také důležitá. Bezpečnost chemického průmyslu byla zvyšována tradičně poté, co nastala havárie velkého rozsahu. To znamená, že některé prvky ochrany byly navrženy i před desítkami let a řada z nich se od té doby nezměnila. Pro ochranu před dnešními hrozbami již nemusí proto být úplně efektivní.

Evropská unie by se měla zaměřit na důslednou kontrolu chemických látek, které jsou dováženy do EU. O všech by měla mít přehled a měla by mít informace o jejich vlastnostech

a možnostech použití[22]. Všechny tyto látky by neměli ohrožovat veřejné zdraví a neměli by být nebezpečné pro životní prostředí[23]. Do budoucna bude nutné revidovat legislativní prostředí týkající se chemického průmyslu a zejména distribuce pesticidů a dalších vysoce toxických látek, které by bylo možné zneužít pro provedení teroristických útoků. V neposlední řadě je potřeba důsledná analýza látek, která chce být používaná na evropském trhu. Tato důsledná kontrola by měla zamezit případům látek poškozující zdraví či životního prostředí, jako byl již zmiňovaný azbest či benzen.

3.6.10 Vesmír

Vesmírné technologie dnes zasahují do všech oblastí našeho života. Telekomunikace, bankovnictví a navigační systémy jsou řízeny z družic, které obíhají kolem naší zeměkoule. Jejich prostřednictvím je dnes možné řídit záchranné operace při přírodních katastrofách, předvídat klimatické změny, podporovat zemědělství. Vojenské družice mohou dohlížet na pašování drog nebo zbraní, monitorovat pohyb teroristických organizací a podporovat zásahy v krizových oblastech. Bezpochybné přínosy ovšem zastiňuje i skutečnost, že se na oběžné dráze již dlouhou dobu vede boj o to, kdo ovládne vesmír vojensky. Hospodářský objem tohoto odvětví se odhaduje na 90 miliard euro, každoročně vzrůstá asi o 7 procent. Největší podniky se nacházejí ve Francii, v Německu a v Itálii. V oblasti civilního využívání vesmírných technologií hraje významnou roli Evropská kosmická agentura ESA[24], která investuje okolo 6 miliard euro ročně do civilního využívání vesmírných technologií. EU navíc poskytne v období 2007-2013 1,4 miliardy euro na vesmírné projekty v rámci Sedmého rámcového programu pro vědu a výzkum Mezivládní organizaci pro využití

---

[22] V EU již začal fungovat systém kontroly chemických látek – REACH (systém pro registraci, posouzení a autorizace chemických látek).

[23] Bílá kniha – Strategie budoucí politiky v oblasti chemických látek a přípravků (KOM(2001)88)

[24] Mezivládní organizace pro využití vesmíru. V současnosti má 17 členských států (Belgie, Dánsko, Finsko, Francie, Německo, Rakousko, Řecko, Irsko, Itálie, Lucembursko, Nizozemsko, Norsko, Portugalsko, Španělsko, Švédsko, Švýcarsko a Velká Británie. Česko, Maďarsko, Polsko a Rumunsko mají podepsanou s ESA smlouvu o spolupráci PECS (trvání pět let), která jim umožňuje zapojení se do většiny programů a je předstupněm k plnému členství).

vesmíru. V současnosti má 17 členských států (Belgie, Dánsko, Finsko, Francie, Německo, Rakousko, Řecko, Irsko, Itálie, Lucembursko, Nizozemsko, Norsko, Portugalsko, Španělsko, Švédsko, Švýcarsko a Velká Británie. Česko, Maďarsko, Polsko a Rumunsko mají podepsanou s ESA smlouvu o spolupráci, která jim umožňuje zapojení se do většiny programů a je předstupněm k plnému členství). Evropská unie klade velký důraz na svůj vesmírný program. V tomto ohledu se zaměřuje hlavně na projekt „Galileo“[25], který bude na rozdíl od amerického systému GPS čistě pod civilní správou.

Z hlediska výstupu se vesmírný sektor dělí pouze na jednu skupinu:

- Vesmír.

V této oblasti je důležité si uvědomit, že nám vesmír nabízí nepřeberné možnosti pro zajištění bezpečnosti v Evropě v případech, jako jsou např. přírodní a humanitární katastrofy, může pomáhat při řešení vojenských krizí a při boji se zločinem. Na druhou stranu je nutno zmínit i nebezpečí toho, aby při neustálém dobývání vesmíru se z něj nestalo bojiště a vznikla další tzv. „studená válka“. Ta by však neměla pouze dva účastníky (USA, bývalé SSSR), ale více (USA, EU, Rusko, Čína, Japonsko, Indie).

3.6.11 Výzkumná zařízení

Výzkum, technika, vzdělávání a inovace představují významný způsob, jak dlouhodobě a udržitelně vytvářet pracovní příležitosti. Jsou klíčem k hospodářskému růstu, konkurenceschopnosti, zdraví i kvalitě života a životního prostředí. Evropa musí začít více investovat do výzkumu a výzkumných zařízení. Evropská unie má v plánu investovat ke konci roku 2010 do výzkumu 3 % svého HDP. Evropa však potřebuje více výzkumných pracovníků, aby mohla zintenzívnit a zkvalitnit svůj výzkum. EU navrhla Sedmý rámcový program[26], který chce povzbudit více lidí k nastoupení a rozvoji profesní dráhy ve výzkumu a chce znovu přitáhnout do Evropy špičkové talentované výzkumné pracovníky. Finanční

[25] Evropský navigační systém Galileo je civilní družicový navigační systém, který by se měl stát alternativou k americkému navigačnímu systému GPS a ruskému navigačnímu systému GLONASS.

[26] ROZHODNUTÍ EVROPSKÉHO PARLAMENTU A RADY o sedmém rámcovém programu Evropského společenství pro výzkum, technický rozvoj a demonstrace (2007 až 2013)(KOM(2005)119)

podpora na evropské úrovni nabízí příležitosti k posílení prvotřídního a účinného výzkumu, čehož nelze dosáhnout pouze na vnitrostátní úrovni. Proto je nutná spolupráce jak v rámci EU, tak také v rámci celého světa. Specifické programy Sedmého rámcového programu představují další upevnění Evropského výzkumného prostoru, čímž lze zasáhnout do nových oblastí výzkumu a také novými prostředky.

Sedmý rámcový program EU je důležitým nástrojem, který napomáhá EU v posílení vlivu v oblasti vědy a výzkumu. Je rozdělen do čtyř specifických programů, které odpovídají čtyřem hlavním cílům evropské výzkumné politiky:

- Program „Spolupráce“[27], jehož cílem je podpořit projekty mezinárodní spolupráce uvnitř EU i mimo ni v rámci souboru tematických oblastí (zdraví; výživa, zemědělství a biotechnologie; informační a komunikační technologie; nanovědy a nanotechnologie, materiály a nové výrobní technologie; energie; životní prostředí; doprava; sociálně-ekonomické a humanitní vědy; vesmír a bezpečnost). Tato témata odpovídají hlavním znalostním a technologickým oblastem, v nichž je třeba podpořit a rozvinout výzkum, aby se čelilo výzvám, s nimiž se Evropa potýká v oblasti sociální, hospodářské, veřejného zdraví, životního prostředí a průmyslu;
- Program „Myšlenky“[28], jehož cílem je podpora vědecké elity v celé Evropě. Návrhem programu je založit Evropskou radu pro výzkum, která bude novým důležitým článkem evropského výzkumu a zároveň logickým vývojem evropské výzkumné politiky. Ta se zcela ztotožňuje s cíli evropského výzkumného prostoru a zviditelňuje „hraniční výzkum“ prováděný v Evropě s cílem přilákat talentované a mladé vědce;

[27] Rozhodnutí Rady o specifickém programu s názvem Spolupráce, kterým se provádí sedmý rámcový program (2007-13) Evropského společenství pro výzkum, technický rozvoj a demonstrace (KOM(2005)440).

[28] Rozhodnutí Rady o specifickém programu Myšlenky, kterým se provádí sedmý rámcový program (2007 až 2013) Evropského společenství pro výzkum, technický rozvoj a demonstrace (KOM(2005)441).

- Program „Lidé“[29], jehož cílem je podpořit Evropany, aby zahájili vědeckou kariéru a pokračovali v ní, nabádat vědce, aby zůstali v Evropě, a přilákat do Evropy nejvyhlášenější vědce;
- Program „Kapacity“[30], jehož cílem je rozvíjet inovační a výzkumné prostředky v Evropské unii (nové výzkumné infrastruktury, podpora malým a středním podnikům, rozvoj „znalostních oblastí“, liberalizaci výzkumného potenciálu v regionech) a zlepšit postavení vědy ve společnosti.

Programy sedmého rámcového programu jsou navrženy tak, aby se ve spojení s nezbytným vnitrostátním a soukromým úsilím zaměřily na hlavní slabiny, pokud jde o úroveň, kvalitu a dopad evropského výzkumu. Šíření a předávání znalostí je klíčovou přidanou hodnotou evropských výzkumných akcí a budou přijata opatření pro zvýšení využívání jejich výsledků průmyslem, tvůrci politik a společností.

Z hlediska výstupu lze sektor výzkumná zařízení rozdělit do jedné skupiny:

- Výzkumná zařízení.

V dnešní době je důležité si uvědomit, že sektor výzkumu je důležitým nástrojem pro udržení konkurenceschopnosti EU ve všech sektorech lidské činnosti. Ať už se jedná o dopravu, energetiku, informační a komunikační technologie, zdraví, materiální technologie či ochranu životního prostředí. Proto by měla EU začít výrazněji dotovat tuto oblast a upravovat legislativní stránku pro větší konkurenci a lepší možnosti. V neposlední řadě by se měla EU snažit o to, aby neodcházeli její špičkoví vědci mimo EU a naopak se snažit „přetáhnout“ špičkové výzkumné pracovníky s oblastí mimo EU sem. To by mělo za následek zvýšení vlivu EU v oblasti vědy a výzkumu a také hospodářskému růstu a konkurenceschopnosti Evropské unie vůči okolním státům.

[29] Rozhodnutí Rady o specifickém programu Lidé, kterým se provádí sedmý rámcový program (2007 až 2013) Evropského společenství pro výzkum, technický rozvoj a demonstrace (KOM(2005)442).

[30] Rozhodnutí Rady o specifickém programu Kapacity, kterým se provádí sedmý rámcový program (2007 až 2013) Evropského společenství pro výzkum, technický rozvoj a demonstrace (KOM(2005)443).

4 PODPŮRNÁ OPATŘENÍ PRO EPCIP

Nedávné krize, ať už způsobené člověkem (teroristické útoky v New Yorku v roce 2001, v Madridu v roce 2004 a v Londýně v roce 2005) nebo přírodního charakteru (vlny tsunami v Indickém oceánu v prosinci 2004), stejně jako předvídatelná ohrožení lidského zdraví (pandemie chřipky), zdůraznily potřebu posílit nástroje zajišťující účinné a koordinované řízení závažných krizí, které vyžadují opatření na úrovni Evropské unie. Ačkoli hlavní odpovědnost při reakci na mimořádnou situaci nesou členské státy, EU má rovněž svoji úlohu. V případě krize by měla zasáhnout v oblastech své působnosti a podporovat úsilí členských států. Dále spolupráce v rámci Komise usnadní vzájemnou pomoc v případě závažné pohromy na území EU a napomůže členským státům při plnění solidárních závazků vůči třetím zemím. Komise musí veřejnosti a médiím poskytnout dostatečně včas a prostřednictvím vhodných informačních kanálů úplné a ucelené informace týkající se podniknutých opatření a vyvíjeného úsilí. Tím přispěje k účinnější komunikaci s občany.

Sdílení informací, interní koordinace, posilování výstražných systémů řízených Komisí a dostupnost vhodných rozhodovacích procesů pro případ krize jsou základními prvky připravenosti a plánování reakce. Vždy při mimořádné události by mělo být vytvořeno Ústřední krizové centrum, které by sdružilo zástupce všech příslušných útvarů Komise. Toto krizové centrum by koordinovalo úsilí směřující k vyhodnocení nejlepších proveditelných variant reakce a k rozhodnutí o vhodných zásahových opatřeních. Komise potvrzuje potřebu zavést systém pro flexibilní spolupráci na úrovni EU. Vylepšená spolupráce na politické úrovni by EU umožnila maximálně využít dostupné technické expertizy a odborníky na různá témata. Komise pak bude hrát strategickou roli, která by byla přínosná tím, že by usnadňovala práci členským státům a zajistila by důslednost a soudržnost jejich akcí.

4.1 Evropský program na ochranu kritické infrastruktury (The European Programme for Critical Infrastructure Protection) – EPCIP

Hlavním cílem EPCIP je zajistit ochranu kritické infrastruktury Evropské unie, specifikovat vhodné politiky, dle kterých pak bude Komise a členské státy postupovat. Udává relevantní požadavky na ochranu KI EU a říká, že EU, její hospodářství a také bezpečnost je závislé

na fungující KI. Zničení či poškození klíčových prvků by pak mohlo způsobit ztráty na životech, majetku a mohlo by mít negativní vliv na fungování EU.

Hlavním důvodem vydání tohoto dokumentu je fakt, že nám dává jasné odpovědi na 20 základních otázek ochrany KI zahrnutých v tomto dokumentu. Vezmeme-li k porovnání Zelenou knihu, tak ta definuje určité problémy a nejasnosti a formou určitých specifických otázek nabádá zainteresované subjekty (členské státy, vlastníky/provozovatele), aby na tyto problémy reagovaly a formou spoluúčasti je i řešily. EPCIP nám již udává jasné formulace problému, dává nám odpovědi na konkrétní otázky a tím přispívá k pochopení problému ochrany kritické infrastruktury Evropské unie. [4]

4.1.1 Zásadní otázky, které jsou v řešení EPCIP:

Jaká je podstata problému, který chceme řešit?

Na úrovni EU bychom se měli soustředit pouze na ty KI, které mají pro EU význam. EPCIP se bude využívat po celou dobu na stanovování zranitelných míst KI a přípravu návrhů, jak této zranitelnosti předcházet. Klíčové aktivity a specifická ochranná opatření budou použita na ECI a podobný přístup bude zaveden i u NCI.

Proč potřebuje EU úrovňové řešení?

Při rostoucím počtu členských států si každý připraví svůj vlastní přístup k ochraně KI a ten jim Komise a Vysoký představitel CIP schválí, nebo budou mít možnost použít přístup EU. Každá rozdílnost systémů členských států zvětšuje šanci, že různé navenek neslučitelné přístupy ochrany KI mohou být slučitelné. Tím pádem mohou být slabá místa odstraněna.

Může být přijat princip subsidiarity?

Ano. Každý členský stát může pojímat otázky bezpečnosti a její standardy různě. Členské státy a jejich soudní systém neustále chrání svou NCI. Pro bezpečnost v EU je rozhodující, aby byly chráněny nejdůležitější KI, které mají přeshraniční charakterů. Proto u těch KI, co bude mít označení ECI se stanoví minimální ochranná opatření, která musí být dodržena.

Může být přijat princip proporcionality?

Ano. Návrh nemůže stanovit přesně, co je nutné udělat, aby se zlepšila ochrana KI v Evropě. Musí se stanovit minimální opatření potřební k ochraně KI. Následně je důležité určit nejrizikovější oblasti, které je nutno chránit.

Jaký typ infrastruktury by se měl přijmout?

Aktivity Komise budou v zájmu ECI – kritická infrastruktura bude definována, jestliže zničení nebo přerušení bude výrazně ovlivňovat chod dvou a více států EU nebo jednoho státu, který je mimo EU. NCI budou pod odpovědností vlastníků a jednotlivých členských států. Komise bude členské státy v tomto úsilí podporovat. EPCIP bude taky zahrnovat možnost pro členské státy, aby si určovali svou vlastní KI.

Proč dva nebo více členských států a ne tři nebo více?

Jakmile událost postihne dva členské státy, tak je rozměr přeshraniční. To je důležité si uvědomit. Proto když jeden členský stát chrání svou KI nedostatečně, tak to může ohrozit druhý stát, který tím může utrpět ztrátu. Z tohoto důvodu dva a více.

Měla by být ECI stejná jako NCI?

Ne, ale může být podobná. Jestliže bude KI označena jako ECI, je pravděpodobné, že v daném členském státě bude také NCI, nicméně opačně to samozřejmě neplatí. To, co může být pro jeden členský stát NCI, nemusí mít přeshraniční vliv, a tudíž to nebude ECI.

Proč je užíván přístup ke všem rizikům a ne jen k terorismu?

Když zvažujeme vážnost dopadu události, je jedno, co to způsobí. Kdybychom se zaměřili pouze na to, jakou hrozbou je pro nás přirozené neštěstí, průmyslová havárie nebo kriminální čin, je pravděpodobně, že bychom se zaměřili pouze na terorismus. Avšak je důležité zaměřit se na povahu hrozby, zvážit všechny detaily a ochránit obyvatele EU.

Který přístup vezme Komise v úvahu?

Směrnici o identifikaci a označení ECI a hodnocení zvýšit její ochranu, a Sdělení o Evropském programu na ochranu kritické infrastruktury.

Jaké záležitosti budou ve Sdělení EPCIP?

Klíčové prvky EPCIP, které budou v návrhu Sdělení:

- Navržené Směrnice stanoví postup pro identifikaci a označení ECI;
- Opatření, které usnadní realizaci EPCIP včetně Akčního plánu, Výstražné informační sítě kritické infrastruktury CIWIN, užití Skupiny odborníků, Proces sdílení informací o ochraně kritické infrastruktury a Určení vzájemných souvislostí;
- Opatření, které mohou používat jednotlivé členské státy pro svou NCI;
- Identifikace potřeb ohledně zlepšení mimořádného plánování;

- Zahraniční vliv;
- Doprovodné financování z programu EU „Prevence, připravenost a schopnost reakce na terorismus a jiná blízká bezpečnostní rizika“ (výhled pro rok 2007-2013).

Jak se bude ECI identifikovat a určovat?

Jsou zde popsány jednotlivé kroky na identifikaci ECI. Nejdříve se vytipují kritéria pro identifikaci KI, pak určí jednotlivé státy KI, která odpovídá těmto kritérium a oznámí to Komisi. Po tomto procesu Komise připraví seznam prvků ECI.

Jak budou jednotlivé sektory identifikovány?

Komise stanoví jednotlivé sektory, a ty bude každoročně kontrolovat.

Jaké jsou sektory KI?

Viz. Oblasti kritické infrastruktury Evropské unie

Jaké závazky stanoví Směrnice ECI vlastníkům/provozovatelům?

Směrnice ECI prosazuje dvě hlavní povinnosti pro vlastníky/provozovatele KI. Vlastník/provozovatel musí uvést do praxe Operační bezpečnostní plán a mít v podniku Bezpečnostního styčného úředníka, který zajistí výměnu informací mezi ECI a NCI.

Jaký by byl přínos pro vlastníky/provozovatele ECI při plnění závazků Směrnic ECI?

Cena by byla rozdílná u jednotlivých členských států. Bude záviset na tom, v jakém stádiu vývoje budou mít jednotlivé státy provedenou ochranu KI. Když budou mít vlastníci zavedený Operační bezpečnostní plán a určeného Bezpečnostního styčného důstojníka, tak jejich náklady budou nízké nebo žádné. Kdyby museli tyto dva závazky zavádět do praxe, jejich náklady mohou podstatně vzrůst.

Jak se bude postupovat v oblastech, kde už bezpečnostní opatření existují?

Každý sektor kritické infrastruktury si může specifikovat další požadavky, které budou následně posuzovány. Velký důraz se bude klást na to, aby nedocházelo ke zdvojování opatření.

Proč by měla být Směrnice zahrnuta jako specifický sektor OSP závazku pro jediný oblastní sektor?

Protože DG TREN si vyžádal výjimku během mezioborových konzultací. Směrnice 2005/65/EC Evropskému parlamentu a Radě na zvýšení oblastní bezpečnosti se zavázala vytvořit Oblastní bezpečnostní plán.

Který závazek vytvořený Operačním bezpečnostním plánem by měl být uskutečněn?
Vlastník musí splnit určité kritéria, aby mohl užívat označení ECI. Proces označení může trvat určitou dobu. Když bude mít vlastník splněny všechny kritéria, Operační bezpečnostní plán bude mít platný minimálně jeden rok, bude moci užívat označení ECI.

Jak ECI směrnice zlepší ochranu?
Směrnice ECI vedou k procesu identifikace mezer bezpečnosti. Členské státy by měli zasílat Komisi typy bezpečnostních mezer pro identifikaci v sektorech. Na základě těchto informací navrhne Komise další ochranná opatření.

Jaké ochranné opatření EPCIP navrhne?
EPCIP nenavrhne žádná konkrétní opatření. Směrnice ECI stanoví postupy, jak vést k identifikaci mezer ochrany. Jakmile budou takové mezery poznány, Komise může navrhnout závazná nebo nezávazná opatření.

4.1.2 Zásady spolupráce v rámci EPCIP

- *Subsidiarita* – úsilí Komise v oblasti ochrany kritické infrastruktury se bude zaměřovat na infrastrukturu, která je kritická spíše z evropského než vnitrostátního či regionálního pohledu. Ačkoli se Komise zaměří na ECI, může v případě potřeby a s přihlédnutím ke stávajícím pravomocím Unie a dostupným zdrojům poskytnout podporu členským státům v souvislosti s vnitrostátními KI.
- *Doplňkovost* – Komise se vyvaruje zdvojování stávajícího úsilí, na úrovni EU i vnitrostátní či regionální úrovni, pokud je toto úsilí při ochraně KI prokazatelně efektivní. EPCIP bude tedy navazovat na existující odvětvová opatření a doplňovat je;
- *Důvěrnost* – jak na úrovni EU, tak na úrovni členských států budou informace o ochraně KI utajovány a přístup k nim bude povolen jen v případech potřeby. Sdílení informací o KI bude probíhat v prostředí důvěry a bezpečnosti;
- *Spolupráce zainteresovaných subjektů* – všechny příslušné zainteresované subjekty se v rámci svých možností zapojí do rozvoje a provádění EPCIP. To bude zahrnovat vlastníky, provozovatele KI označených jako ECI a také státní či další příslušné orgány;
- *Proporcionalita* – opatření budou navržena pouze tam, kde byla na základě analýzy stávajících nedostatků v oblasti bezpečnosti zjištěna jejich potřebnost, a tato opatření budou úměrná úrovni a druhu daného ohrožení;

- *Odvětvový přístup* – jelikož u různých odvětvích existují odlišné zkušenosti, odborné znalosti a požadavky týkající se ochrany KI, bude EPCIP rozvíjen podle odvětví a prováděn podle dohodnutého seznamu odvětví ochrany kritické infrastruktury.

4.2 Akční plán EPCIP

Komise zřídila Evropský program pro ochranu kritické infrastruktury, který by měl zajistit, aby v rámci EU existovala přiměřená a rovnoměrná úroveň bezpečnosti ochrany kritické infrastruktury, co nejméně možností selhání a rychlá, vyzkoušená nápravná opatření. Úroveň ochrany by měla být odvozena od dopadu, jenž by mohl způsobit jejich možné selhání. EPCIP by měl co nejvíce minimalizovat veškeré negativní dopady, které mohou mít vliv na zvýšené investice na ochranu a také na konkurenceschopnost příslušného odvětví. Ochrana KI bude založena na sblížení všech rizik. Pokud bude měřitelná úroveň ochrany konkrétního sektoru KI dostatečná, budou zainteresované subjekty věnovat své úsilí hrozbám, vůči kterým jsou stále zranitelné.

EPCIP bude průběžným procesem a pravidelné přezkoumání bude probíhat formou Akčního plánu EPCIP. Akční plán EPCIP stanoví akce, kterých bude třeba realizovat, a příslušné termíny. Akční plán bude pravidelně aktualizován na základě dosaženého pokroku.

Akční plán EPCIP člení činnosti související s ochranou KI do tří pracovních oblastí:

- Pracovní oblast 1, která se bude zabývat strategickými aspekty EPCIP a rozvojem opatření horizontálně použitelných na veškerou práci v oblasti ochrany KI;
- Pracovní oblast 2 zabývající se ECI bude prováděna na úrovni odvětví;
- Pracovní oblast 3, která bude podporovat členské státy v jejich činnostech týkajících se vnitrostátních KI. [3]

Akční plán EPCIP bude proveden při zohlednění specifik jednotlivých odvětví a při současném zapojení dalších zainteresovaných subjektů.

4.3 Výstražná informační síť kritické infrastruktury CIWIN

Výstražná informační síť kritické infrastruktury CIWIN bude založena na bezpečné výměně informací o společných hrozbách a zranitelných místech. Bude poskytovat vhodná opatření a strategie pro snížení rizik a na podporu ochrany KI a doplňovat existující sítě. Měla by také poskytnout platformu pro výměnu rychlých výstrah propojenou se systémem

Komise ARGUS. Tento systém bude logistickým rozhraním zajišťující rychlý tok informací mezi stávajícími systémy rychlé výměny informací, jehož cílem bude dosažení maximální ochrany a bezpečnosti, včetně sítě donucovacích orgánů. Velký důraz bude kladen na to, aby v rámci sítě CIWIN nedocházelo k duplicitám. Jednotlivé členské státy by měly zajistit, aby byly příslušné informace předávány všem příslušným vládním útvarům a agenturám, včetně útvarů pohotovostních služeb. Dále budou informovány příslušné orgány průmyslových odvětví, které budou informovat dotčené vlastníky a provozovatele kritické infrastruktury prostřednictvím sítě kontaktů vytvořených v rámci členských států.

Za pomoci EPCIP bude zřízeno trvalé fórum, v jehož rámci by bylo možné vyvážit na jedné straně omezení daná hospodářskou soutěží, odpovědností a citlivostí informací a na druhé straně výhody bezpečnějších KI. V rámci tohoto procesu bude úzce konzultován průmysl. Tento přístup pomůže poskytovat více informací o konkrétních hrozbách partnerům, které jim umožní přijmout opatření zaměřená na řešení jejich možných následků. [22]

4.4 Systém rychlého varování ARGUS

Systém rychlého varování ARGUS bude sestávat z interní komunikační sítě a zvláštního koordinačního procesu, který bude aktivován v případě závažné víceodvětvové krize. Interní komunikační síť bude realizována prostřednictvím sítě přenosu dat. Bude využívat stávajících databází a interních technologií přenosu zpráv a bude podporována dalšími komunikačními prostředky (SMS, telefon). Účastníci sítě ji budou využívat ke sdílení příslušných informací v reálném čase o nastávajících a probíhajících krizích a ke koordinaci vhodné reakce. Informace přenesené prostřednictvím systému ARGUS budou přístupné všem účastníkům a budou uloženy a zaznamenány. Systém bude aktualizován na základě získaných zkušeností a technologického pokroku.

Všeobecný systém rychlého varování ARGUS usiluje o:

- Poskytnutí interní platformy umožňující generálním ředitelstvím a útvarům Komise vyměňovat si v reálném čase příslušné informace o vznikajících víceodvětvových krizích nebo o předvídatelných anebo bezprostředních ohroženích;
- Zpřístupnění vhodného procesu koordinace, který bude aktivován v případě mimořádné krize. Takový proces by umožnil Komisi přijmout rozhodnutí a řídit rychlou,

koordinovanou a soudržnou reakci v oblastech její působnosti a ve spolupráci s ostatními orgány a založenou na všech příslušných informacích;

- Poskytnutí kontextu pro účinnou komunikaci s občany a pro podání vyrovnaného, soudržného a úplného obrázku o úsilí vynaloženém Komisí. [21]

Zásady systému ARGUS jsou následující:

- Zásada subsidiarity;
- Systém bude respektovat zvláštní charakteristiky, kompetence a odbornou způsobilost stávajících systémů rychlého varování Komise, které budou nadále plnit své aktuální funkce v souladu s jejich zvláštními postupy;
- ARGUS bude fungovat v případě víceodvětvové krize, která bude vyžadovat opatření na úrovni Unie, ať již bude postihovat občany, majetek nebo zájmy členských států či třetích zemí;
- Komunikační síť bude vyhrazena pro interní použití v rámci Komise a bude propojovat různé systémy rychlého varování, generální ředitelství a útvary Komise. Členské státy budou napojeny prostřednictvím systémů rychlého varování a jejich zvláštních sítí. Tato koordinace zajistí úplnou a konsolidovanou databázi příslušných ověřených informací;
- ARGUS bude využívat stávající technologii a infrastrukturu spravovanou generálním ředitelstvím pro informatiku;
- Systém bude přezkoumán nejpozději rok po vstupu v platnost odpovídajícího rozhodnutí Komise s ohledem na získané zkušenosti a technologický pokrok, aby bylo zajištěno propojení a koordinace stávajících specializovaných sítí;
- Systém bude fungovat v rámci stávajících zdrojů a prostředků útvarů Komise;
- Co se týče externí komunikace, tak ta bude zajištěna na nejvhodnější geografické úrovni a prostřednictvím vhodných nástrojů k dosažení a plnému informování veřejnosti (tisková konference, tiskové komuniké, internet). [21]

4.5 Skupiny odborníků

Dialog se zainteresovanými subjekty je pro zlepšení ochrany kritických infrastruktur v EU rozhodující. Pokud je zapotřebí specifických odborných znalostí, může Komise zřizovat skupiny odborníků na ochranu KI na úrovni EU, které se budou zabývat jasně definovanými otázkami a usnadní dialog mezi veřejným a soukromým sektorem v oblasti ochrany KI.

Skupiny odborníků budou EPCIP podporovat tím, že svým poradním hlasem usnadní výměnu názorů na otázky související s ochranou KI. Tyto skupiny odborníků představují dobrovolný mechanismus, ve kterém se mísí veřejné a soukromé zdroje k dosažení cíle nebo skupiny cílů, které jsou považovány za vzájemně prospěšné jak pro občany, tak pro soukromý sektor. Skupina odborníků na úrovni EU bude mít jasně stanovený cíl, časový rámec cíle, kterého má být dosaženo, a jasně stanovené členstvo.

Konkrétní funkce skupin odborníků se mohou v jednotlivých odvětvích KI lišit v závislosti na jedinečných vlastnostech odvětví. Tyto funkce mohou zahrnovat následující úkoly:

- Pomoci při určování zranitelných míst, vzájemných závislostí a osvědčených postupů v odvětví;
- Pomoci při rozvoji opatření ke snížení anebo odstranění hlavních zranitelných míst a při rozvoji metriky plnění;
- Usnadnit sdílení informací o ochraně kritické infrastruktury, školení a budování důvěry;
- Vytvořit a prosazovat „obchodní případy", které ostatním v daném odvětví ukáží hodnotu účasti na plánech a iniciativách týkajících se ochrany KI;
- Poskytnout odborné znalosti v konkrétním odvětví a poradenství v oblastech jako výzkum a vývoj. [3]

4.6 Proces sdílení informací o ochraně kritické infrastruktury

Proces sdílení informací o ochraně kritické infrastruktury mezi příslušnými zainteresovanými subjekty vyžaduje vztah důvěry v tom smyslu, aby nedošlo ke zveřejnění vlastnických, citlivých nebo osobních informací sdílených dobrovolně a aby byly citlivé údaje dostatečně chráněny. Je nutné dbát na dodržování práva na soukromí.

Zainteresované subjekty přijmou vhodná opatření k ochraně informací týkajících se záležitostí, jako jsou bezpečnost KI a chráněných systémů, studie vzájemných závislostí a posuzování zranitelnosti, ohrožení a rizik souvisejících s ochranou KI. Takové informace budou použity pouze pro účel ochrany kritické infrastruktury. Veškerý personál pracující s utajenými informacemi bude prověřen na příslušný stupeň utajení od členského státu, jehož je státním příslušníkem.

V procesu výměny informací o ochraně kritické infrastruktury lze navíc rozpoznat, že určité informace o ochraně KI, i když nejsou utajené, mohou být přesto citlivé, a proto vyžadují zvláštní přístup.

Výměna informací o ochraně kritické infrastruktury umožní:

- Lepší a přesnější informace o vzájemných závislostech, ohroženích, zranitelnosti, mimořádných bezpečnostních událostech, protiopatřeních a osvědčených postupech k ochraně KI a jejich pochopení;
- Zvýšené povědomí o otázkách KI;
- Dialog zúčastněných stran;
- Lépe zaměřené školení, výzkum a vývoj. [3]

5 DŮSLEDKY OPATŘENÍ OCHRANY KRITICKÉ INFRASTRUKTURY EVROPSKÉ UNIE PRO ČESKOU REPUBLIKU

Oblast ochrany kritické infrastruktury České republiky se vyvíjí dlouhodobě. V jejich začátcích se vyvíjela nesystematicky, v poslední době je však její činnost systematická a cíleně řízená. Nejprve se jednalo o připravenost proti jaderným haváriím, popřípadě ochraně po použití zbraní hromadného ničení. Následně k tomu přibylo ohrožení živelními pohromami.

Česká republika přistoupila k ochraně kritické infrastruktury deklarováním základních funkcí státu za krizových situací. ČR určila práva, povinnosti a postupy orgánů veřejné správy, kterými stát udržuje za krizových situací kontrolu nad fungováním společnosti a zajišťováním základních potřeb obyvatelstva. Odpovědnost za problematiku kritické infrastruktury v České republice řeší Výbor pro civilní nouzové plánování. Hlavním koordinátorem spojeným s ochranou kritické infrastruktury se následně stalo Ministerstvo vnitra České republiky, respektive Generální ředitelství Hasičského záchranného sboru České republiky.

V dané oblasti provedla Česká republika řadu kroků, které posunují tuto problematiku vpřed. Má definovanou svou národní kritickou infrastrukturu, do které spadá 10 oblastí, které jsou dále rozděleny do 42 podoblastí produktů nebo služeb. Dále ČR přijala Usnesení Vlády České republiky ze dne 25. února 2008 č. 170 o Harmonogramu dalšího postupu zpracování dokumentů Komplexní strategie České republiky k řešení problematiky kritické infrastruktury a Národního programu ochrany kritické infrastruktury. V oblasti vzdělávání má rovněž řadu kapacit na tuto problematiku, které jsou schopny tuto oblast zastřešit. Orgány veřejné správy by následně celý proces řídili, vydávali metodické pokyny a doporučení a zajišťovali kontrolu naplnění požadovaných opatření. Velice významným faktorem při všech aktivitách spojených s ochranou kritické infrastruktury je nutnost navázání a udržení důvěry mezi soukromým a veřejným sektorem, založený na výměně informací o způsobech zajištění ochrany.

Důsledky opatření ochrany kritické infrastruktury Evropské unie pro Českou republiky by měly vycházet z legislativy Evropské unie. Jelikož Evropská unie doposud tuto legislativu neschválila a nevypadá to, že by tak brzy učinila, snaží se tuto problematiku řešit

ČR sama. V případě přijetí závazného dokumentu na tuto problematiku Evropskou unií by měla ČR tuto skutečnost respektovat a stávající materiály dodržovat.

ZÁVĚR

Pojem kritická infrastruktura je poměrně neznámý a problematika ochrany kritické infrastruktury je relativně mladým odvětvím. O této problematice se začalo významněji hovořit po teroristických útocích na New York a Washington. Tyto útoky všem jasně ukázaly, jak obtížné je zabezpečení oblasti surovinami a službami při neobvyklých, mimořádných situacích. Zdůraznily, že obyvatelstvo je stále více závislé na infrastruktuře, bez které by již nemohlo existovat. Proto ochrana kritické infrastruktury nabývá stále více na významu.

Tato práce má za cíl analyzovat a zhodnotit současný stav ochrany kritické infrastruktury Evropské unie. Je v ní objasněno, co je to kritická infrastruktura, oblasti kritické infrastruktury a základní nástroje Evropské unie k účinné ochraně. Je zde však také zdůrazněno, že Evropská unie nemá ještě dopracovanou legislativu k ochraně kritické infrastruktury. Proto jednotlivé státy postupují samostatně a nesystematicky, což může v konečném důsledku znamenat ztrátu finančních prostředků. Na druhou stranu však při harmonizaci jednotlivých typů ochrany může docházek k nacházení zranitelným míst v jednotlivých oblastech a tím k lepší ochraně kritické infrastruktury.

ZÁVĚR V ANGLIČTINĚ

The term critical infrastructure is relatively unknown and problems of critical infrastructure protection are relatively young branch. These problems have been significantly discussed after the terrorist attacks in New York and Washington. These attacks clearly indicated how difficult is the indemnity of an area by raw materials and service at uncommon, emergency situation. This fact has emphasized that population is so much dependent on infrastructure and without that it can not exist anymore. For that reason the relevance of the critical infrastructure protection has been still increasing.

The thesis is aimed on introducing readers with present state of the critical infrastructure protection of European Union. There is clarified what the critical infrastructure is, moreover, the sectors of critical infrastructure and basic instruments of European Union for effective protection are explained as well. There is also emphasized that EU has not yet finished the whole legislature for critical infrastructure protection. For that reason the particular states progress individually and unsystematically and in the final effect it can mean the loss of finances. On the other hand, the harmonization process of the particular types of protection may lead to finding vulnerable points in particular sectors and this phenomena would result in better protection of critical infrastructure.

SEZNAM POUŽITÉ LITERATURY

[1] *Zelená kniha o Evropském programu na ochranu kritické infrastruktury* [online]. Komise evropských společenství. V Bruselu dne 17. 11. 2005 KOM(2005) 576 v konečném znění, s. 26. [cit. 2007-10-15]. Dostupný z WWW: <http://eur-lex.europa.eu/LexUriServ/site/cs/com/2005/com2005_0576cs01.pdf>.

[2] *Sdělení Komise Radě a Evropskému parlamentu - Ochrana kritické infrastruktury při boji proti terorismu* [online]. Komise evropských společenství. V Bruselu dne 20. 10. 2004 KOM(2004) 701 v konečném znění, s. 17. [cit. 2007-10-15]. Dostupný z WWW: <http://www.europarl.europa.eu/meetdocs/2004_2009/ documents/com/com_com(2004)0701_/com_com(2004)0701_cs.pdf>.

[3] *Sdělení Komise o Evropském programu na ochranu kritické infrastruktury* [online]. Komise evropských společenství. V Bruselu dne 12. 12. 2006 KOM(2006) 786 v konečném znění, s. 13. [cit. 2007-10-15]. Dostupný z WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:CS:PDF>.

[4] *The European Programme for Critical Infrastructure Protection (EPCIP)* [online]. V Bruselu dne 12. 12. 2006 MEMO/06/477, s. 9. [cit. 2007-10-15]. Dostupný z WWW: <http://europa.eu/rapid/pressReleasesAction.do? reference=MEMO/06/477&format=HTML&aged=0&language=EN>.

[5] WEISS, Tomáš. *Nové bezpečnostní hrozby a aktivity Evropské unie v oblasti soft a hard security* [online]. Institut pro evropskou politiku EUROPEUM. Březen 2005, s. 13. [cit. 2007-11-01]. Dostupný z WWW: <http://www.europeum.org/doc/arch_eur/tweiss_soft_a_hard_security.pdf>.

[6] Weiss, Tomáš. *Evropská bezpečnostní strategie ve světle Národní bezpečnostní strategie USA* [online]. Institut pro evropskou politiku EUROPEUM. Září 2004. [cit. 2007-11-01]. Dostupný z www: <http://www.integrace.cz/integrace/clanek.asp?id=825>.

[7] *Bezpečná Evropa v lepším světě: Evropská bezpečnostní strategie* [online]. Středisko bezpečnostní politiky CESES FSV UK, Praha 2007. 9 s. [cit. 2007-11-05]. Dostupný z www: <http://www.ceses.cuni.cz/CESES-76-version1-evropska_bezpecnostni_strategie.pdf>.

[8] *A Secure Europe in a Better World : European Security Strategy* [online]. Brussels : High Representative for CSFP, 12. 12. 2003. 15 s. [cit. 2007-11-04]. Dostupný z WWW: <http://ue.eu.int/uedocs/cmsUpload/78367.pdf>.

[9] *Zpráva o stavu zajištění bezpečnosti České republiky* [online]. Praha: Úřad vlády České republiky, 2006. 65 s. Bezpečnostní rada státu. [cit. 2007-11-13]. Dostupný z WWW: <http://www.vlada.cz/assets/cs/rvk/brs/zprava_o_stavu_zajisteni_bezpecnosti_CR.pdf>. ISBN 80-86734-91-9.

[10] *Výkladový slovník krizového řízení a obrany státu* [online]. [cit. 2007-11-01]. Dostupný z www:<http://www.mvcr.cz/udalosti/slovnik/index_odbor_info.html>.

[11] ANTUŠÁK, Emil. *Přehled základních pojmů krizového managementu*. Praha 2001, Vysoká škola ekonomická, Institut krizového managementu, 52 s.

[12] CHVÁLOVÁ, Olga. *Evropská budoucnost je i budoucnost česká* [online]. Humanea. Praha 2005, s. 164. [cit. 2008-01-21]. Dostupný z WWW: <http://www.euroskop.cz/admin/gallery/2/635a9d0d615fda210c62b1c89e7d9b8e.pdf>.

[13] HAD, Miloslav, STACH, Stanislav, URBAN, Luděk. *Česká republika v Evropské unii: členství, přínosy a výzvy*. Český institut pro integraci EU, Praha 2005. s. 182.

[14] *[ABC] práva Evropských společenství.* Informační centrum Evropské unie, Praha 2004, s. 116. ISBN 80-239-2561-X.

[15] KRULÍK, Oldřich. *Fyzická ochrana kritické infrastruktury a klíčových aktivit* [online]. MVČR. Únor 2006, s. 26. [cit. 2008-01-21]. Dostupný z WWW: <http://www.mvcr.cz/rs_atlantic/data/files/insp_usa_infra.pdf>.

[16] www.cs.wikipedia.org

[17] www.euroskop.cz

[18] http://europa.eu/abc/12lessons/index_cs.htm

[19] *Evropská unie pro studenty*. Radim Perlín. 1. vyd. Praha: Institut evropské demokracie, listopad 2005. 36 s.

[20] *Zpráva o návrhu směrnice Rady o určování a označování evropské kritické infrastruktury a o posouzení potřeby zvýšit její ochranu* [online]. Výbor pro občanské svobody, spravedlnost a vnitřní věci. V Bruselu dne 2. 7. 2007 A6-0270/2007 v konečném znění, s. 59. [cit. 2007-11-04]. Dostupný z WWW:

<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2007-0270+0+DOC+PDF+V0//CS>.

[21] *Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: Předpisy Komise o všeobecném systému rychlého varování „ARGUS“* [online]. Komise evropských společenství. V Bruselu dne 23. 12. 2005 KOM(2005) 662 v konečném znění, s. 4. [cit. 2008-02-17]Dostupný z WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0662:FIN:CS:PDF>.

[22] *Ochrana obyvatelstva 2007 : Ochrana kritické infrastruktury*. Doc. Dr. Ing. Michail Šenovský. 2007. vyd. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2007. 456 s. ISBN 80-86634-51.

[23] *K ochraně kritické infrastruktury v ČR, In Sborník 4. mezinárodní konference „Crisis management“, Bezpečnost – Připravenost – Ochrana obyvatelstva.* 1. vydání, Brno 2006, 349 s. ISBN 80–7231–141–8.

[24] http://ec.europa.eu/energy/index_en.html

[25] *Sdělení komise Radě a Evropskému parlamentu - Jaderný ukázkový program Předložen podle čl. 40 Smlouvy o Euratomu ke stanovisku Evropskému hospodářskému a sociálnímu výboru* [online]. Komise evropských společenství. V Bruselu dne 10. 1. 2007 KOM(2007) 844 v konečném znění, s. 24. [cit. 2008-03-27]. Dostupný z WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0844:FIN:CS:PDF>.

[26] http://www.energetika-eu.cz/

[27] *Presidental Decision Directive 63*. Washington, D.C., 22 May 1998.

[28] http://europa.eu/pol/food/index_cs.htm

[29] http://ec.europa.eu/health-eu/index_cs.htm

[30] *Akční plán finančních služeb* [online]. www.Bankovnictví.ihned.cz, 2003. [cit. 2008-03-14]. Dostupné z WWW: <http://bankovnictvi.ihned.cz/3-12650640-direktivu-900000_d-64>.

[31] http://europa.eu/pol/trans/index_cs.htm

[32] *Bílá kniha – Strategie budoucí politiky v oblasti chemických látek a přípravků* [online]. Komise evropských společenství. V Bruselu dne 27. 2. 2001 KOM(2001) 88 v konečném znění, s. 29. [cit. 2008-03-21].

Dostupný z WWW: <http://www.uef.cz/dokumenty/dokumenty/dokument28.pdf>

[33] *Vesmír – bojiště hospodářských a vojenských zájmů* [online]. Evropský parlament, Bezpečnost a obrana 07. 05. 2007. [cit. 2008-03-14]. Dostupné z WWW: <http://www.europarl.europa.eu/news/public/story_page/031-6347-122-05-18-903-20070507STO06304-2007-02-05-2007/default_cs.htm>.

[34] *Návrh rozhodnutí Rady o specifickém programu Myšlenky, kterým se provádí sedmý rámcový program (2007 až 2013) Evropského společenství pro výzkum, technický rozvoj a demonstrace* [online]. Komise evropských společenství. V Bruselu dne 21. 9. 2005 KOM(2005) 441 v konečném znění, s. 36. [cit. 2008-03-23]. Dostupný z WWW: <http://www.europarl.europa.eu/meetdocs/2004_2009/documents/com/com_com(2005)0441_/com_com(2005)0441_cs.pdf>.

[35] http://denver.fbi.gov/nfip.htm

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AIDS	Acguired Immunodeficiency Syndrome
ARGUS	A General Rapid Alert System
BSE	Bovinní spongiformní encefalopatie
CIP	Critical Infrastructure Protection
CIWIN	The Critical Infrastructure Warning Information Network
ČR	Česká republika
ECI	Eupopean Critical Infrastructure
EHS	Evropské hospodářské společenství
EPCIP	The European Programme for Critical Infrastructure Protection
EPS	Evropská politická spolupráce
ES	Evropské společenství
ESAE	Evropské společenství pro atomovou energie
ESD	Evropský soudní dvůr
ESUO	Evropské společenství uhlí a oceli
EU	Evropská unie
FBI	Federal Bureau of Investigation
GNSS	Global Navigation Satellite System
HDP	Hrubý domácí produkt
KI	Kritická infrastruktura
KOM	Komise
NATO	North Atlantic Treaty Organization
NCI	National Critical Infrastructure
OBSE	Organizace pro bezpečnost a spolupráci v Evropě
OSN	Organizace spojených národů

SARS	Severe Acute Respiratory Syndrome
USA	The United States of America
WHO	World Health Organization
ZEU	Západoevropská unie
ZHN	Zbraně hromadného ničení

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: SEZNAM OBLASTÍ KRITICKÉ INFRASTRUKTURY EVROPSKÉ UNIE

Odvětví		Pododvětví	
I	Energetika	1	Produkce ropy a plynu, rafinování, zpracování, skladování a distribuce potrubím
		2	Výroba a rozvod elektřiny
II	Jaderný průmysl	3	Produkce a skladování/zpracování jaderných látek
III	Informační a komunikační technologie, (I.C.T.)	4	Ochrana informačních systémů a sítí
		5	Automatizace přístrojů a kontrolních systémů (SCADA atd.)
		6	Internet
		7	Poskytování pevných telekomunikačních sítí
		8	Poskytování mobilních telekomunikačních sítí
		9	Radiová komunikace a navigace
		10	Satelitní komunikace
		11	Vysílání
IV	Voda	12	Zásobování pitnou vodou
		13	Kontrola kvality vody
		14	Těsnění a kontrola množství vody
V	Potraviny	15	Zásobování potravinami a zajištění bezpečnosti potravin
VI	Ochrana zdraví	16	Lékařská a nemocniční péče
		17	Léky, séra, očkovací látky a léčiva
		18	Biologické laboratoře a biologičtí činitelé
VII	Finanční	19	Infrastruktury a systémy zúčtování a vypořádání obchodů s cennými papíry
		20	Regulované trhy
VIII	Doprava	21	Silniční doprava
		22	Železniční doprava
		23	Letecká doprava
		24	Vnitrozemská vodní doprava
		25	Zámořská a přibřežní námořní doprava
IX	Chemický průmysl	26	Produkce a skladování/zpracování chemických látek
		27	Potrubí pro přepravu nebezpečných látek (chemických látek)
X	Vesmír	28	Vesmír
XI	Výzkumná zařízení	29	Výzkumná zařízení

PŘÍLOHA P II: SEZNAM OBLASTÍ KRITICKÉ INFRASTRUKTURY ČESKÉ REPUBLIKY

Oblast	Produkty nebo služby
1 Energetika	1.1. Elektřina
	1.2. Plyn
	1.3. Tepelná energie
	1.4. Ropa a ropné produkty
2 Vodní hospodářství	2.1. Zásobování pitnou a užitkovou vodou
	2.2. Zabezpečení a správa objemu povrchových vod a podzemních zdrojů vody
	2.3. Systém odpadních vod
3 Potravinářství a zemědělství	3.1. Produkce potravin
	3.2. Péče o potraviny
	3.3. Zemědělská výroba
4 Zdravotní péče	4.1. Přednemocniční neodkladná péče
	4.2. Nemocniční péče
	4.3. Ochrana veřejného zdraví
	4.4. Výroba, skladování a distribuce léčiv a zdravotnických prostředků
5 Doprava	5.1. Silniční
	5.2. Železniční
	5.3. Letecká
	5.4. Vnitrozemská vodní
6 Komunikační a informační systémy	6.1. Služby pevných telekomunikačních sítí
	6.2. Služby mobilních telekomunikačních sítí
	6.3. Radiová komunikace a navigace
	6.4. Satelitní komunikace
	6.5. Televizní a rádiové vysílání
	6.6. Přístup k internetu a k datovým službám
	6.7. Poštovní a kurýrní služby
7 Bankovní a finanční sektor	7.1. Správa veřejných financí
	7.2. Bankovnictví
	7.3. Pojišťovnictví
	7.4. Kapitálový trh
8 Nouzové služby (Záchranné služby)	8.1. Hasičský záchranný sbor ČR a příslušné jednotky požární ochrany
	8.2. Policie (vnitřní bezpečnost a veřejný pořádek)
	8.3. Armáda ČR
	8.4. Radiační monitorování vč. doporučení ochranných opatření
	8.5. Předpovědní, varovná a hlásná služba
9 Veřejná správa	9.1. Sociální ochrana a zaměstnanost (soc. zabezpečení, státní soc. podpora, soc. pomoc)
	9.2. Diplomacie
	9.3. Výkon justice a vězeňství
	9.4. Státní správa a samospráva
10 Výroba nebezpečných látek, skladování, přeprava	10.1. Výroba a skladování nebezpečných látek
	10.2. Doprava a přeprava nebezpečného zboží
	10.3. Biologické materiály
	10.4. Radioaktivní materiály