Mezinárodní spolupráce v boji proti informační kriminalitě

PRAHA 2009

1 Mezinárodní rozměr boje proti kybernetickým incidentům jako nezbytná podmínka jeho úspěchu

Vzhledem k nadnárodnímu charakteru počítačových sítí (zejména Internetu) závisí situace v oblasti boje proti kybernetickým incidentům velmi silně na mezinárodní spolupráci. Výraznějšího zlepšení situace je možné dosáhnout jen postupem, koordinovaným na mezinárodní úrovni, respektive vycházejícím z mezinárodních úmluv, při kterém by jednotlivé vnitrostátní právní úpravy navazovaly na mezinárodně koordinované úsilí o řešení konkrétních témat.

Navzdory trvání kulturně podmíněných rozdílů v oblasti postihu určitého chování (různá etická měřítka v různých částech světa), existuje snaha o to, aby v globální síti platil alespoň určitý minimální standard, který by byl co možná nejvíce konsensuálně definován. To by umožnilo odstranit nejkřiklavější případy porušování takového standardu a docílit toho, aby se nespolupracující země nebo území ocitly ve stále větší izolaci.

Mezi relativně nejméně zpochybnitelné oblasti toho, co je nazýváno *"nelegálním a škodlivým obsahem na Internetu*" (illegal and harmful content) patří **dětská pornografie, šíření rasové nenávisti a teroristické návody**. Snaha rozšířit takový konsensus na jiné oblasti by však mohla být chápána jako **omezování lidských práv a svobod** (např. co se týče oblasti šíření politické propagandy, byť extrémní).

Spolupráce mezi státy při stíhání pachatelů internetové extremistické kriminality se v současnosti uskutečňuje na základě mezinárodních úmluv, a to zpravidla za splnění podmínky oboustranné trestnosti. Problémy způsobuje rozpor mezi teritoriálním principem autorského práva a globálním charakterem Internetu, stejně jako problémy s vyšetřováním a dokazováním tohoto druhu trestné činnosti. K šíření nelegálního obsahu Internetu totiž dochází z míst (států, území), u nichž není možnost jakéhokoliv zásahu a proto nelze chránit ani zájmy států, které jsou takovým chováním dotčeny.

S touto skutečností souvisí **legislativní** (mezinárodní právo) **a organizační kroky**, o něž je na mezinárodní úrovni (v rámci zainteresovaných mezinárodních organizací) usilováno. Mezi aktuální priority (přinejmenším v rámci euro-americké civilizace) v uvedené oblasti patří:

- Již zmíněná oblast potírání nelegálního obsahu na Internetu.
- Potírání tzv. "nechtěného" obsahu (unwanted content) na Internetu (zejména spam).
- Technologická spolupráce v boji proti kybernetickým incidentům[1].
- Prevence hospodářských dopadů kybernetických incidentů.
- Ochrana kritické infrastruktury před kybernetickými incidenty.

O tom svědčí i následující výčet aktivit mezinárodních organizací, nejvíce relevantních pro Českou republiku.

2 Jednotlivé mezinárodní organizace

2.1 Organizace spojených národů (United Nations, UN, OSN)

Nejaktuálněji se určitým aspektům boje proti kybernetickým incidentům věnuje Rezoluce Rady bezpečnosti OSN č. 1624 ze dne 14. září 2005,[2] která zavazuje členy Organizace k zákazu podněcování páchání aktů terorismu. Její text vyzývá k přijetí nezbytných opatření na vnitrostátní úrovni, jako zejména:

- Zákonem zakázat nabádání a obhajobu terorismu (tzv. incitement), přičemž je zároveň výslovně uvedeno, že taková aktivita nemůže být chápána jako naplňování práva na svobodu vyjadřování.
- Provádět preventivní kroky v uvedené oblasti.
- Zabránit vzniku útočišť (safe havens) pro osoby, důvodně podezřelé z výše uvedených aktivit.
- Provozovat výměnu informací a zkušeností, souvisejících s uvedeným úsilím.

[1] Jakékoli technologické poruchy, dopady přírodních katastrof nebo dopad úmyslných, člověkem způsobených, nežádoucích aktivit.
[2] Její text navazuje na rezoluce č. 1267 (1999) z 15. října 1999; 1373 (2001) z 28. září 2001; 1535 (2004) z 26. března 2004; 1540 (2004) z 28. dubna 2004; 1566 (2004) z 8. října 2004; 1617 (2005) z 29. července 2005 a na deklaraci, navazující na rezoluci 1456 (2003) z 20. ledna 2003, stejně jako na jiné rezoluce OSN, vztahující se k tématu hrozeb pro mezinárodní mír a bezpečnost.

- Podávat Radě bezpečnosti zprávy o způsobu implementace Rezoluce (první zpráva bude požadována do 12 měsíců od přijetí Rezoluce, tedy do září 2006).

Zároveň je třeba zmínit aktivity Organizace v dalších oblastech kybernetické bezpečnosti, jako je zejména boj proti dětské pornografii a pedofilii na Internetu (jehož patrně nejvíce viditelným aspektem je vytváření sítě "Innocence in Danger").

Problematikou se rovněž zabývá Protiteroristický výbor Rady bezpečnosti OSN (Security Council´s Counter-Terrorism Committee).

V rámci systému OSN největší zodpovědnost za praktické aspekty a aplikace mezinárodní kybernetické bezpečnosti připadá na Mezinárodní telekomunikační unii (International Telecommunication Union, ITU), v jejíž kompetenci existuje od r. 2007 „Global Cybersecurity Agenda" (GCA) jako rámec pro mezinárodní spolupráci. V září 2008 ITU a Mezinárodní mnohostranné partnerství proti kybernetickým hrozbám (International Multilateral Partnership Against Cyber-Threats, IMPACT) uzavřeli dohodu o vybudování pobočky GCA v ústředí IMPACT v Cyberjaya v Malajsii.

2.2 Evropská unie (European Union, EU)

V rámci EU byla vydána řada dokumentů, souvisejících, alespoň částečně, s problematikou kybernetické bezpečnosti, například (řazeno chronologicky):

- Směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců se zřetelem na zpracování osobních dat a o volném pohybu takových dat.
- Nařízení Evropského parlamentu a Rady 97/66/EC ze dne 15. prosince 1997, vztahující se k nakládání s osobními údaji a k ochraně soukromí v telekomunikačním sektoru.
- Rozhodnutí Evropského parlamentu ze dne 19. května 2000, k legislativní akci proti zločinu za použití vyspělých technologií.
- Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o určitých aspektech služeb informační společnosti, zejména elektronického obchodního styku v rámci vnitřního trhu.
- Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.
- Směrnice Evropského parlamentu a Rady 95/46/ES ve znění nařízení (ES) č. 1882/2003, požadující po členských státech Evropské unie ochranu práv a svobod fyzických osob s ohledem na zpracovávání osobních dat, zejména co se týče jejich práva na soukromí, s cílem zajistit zároveň svobodný tok osobních údajů v rámci Společenství.
- Směrnice 91/250/EC, k právní ochraně počítačových programů, zejména pak stanovisko expertů k tomuto Nařízení "Právní ochrana počítačových programů v Evropě: Průvodce Nařízením Evropského společenství".[3]
- Rozhodnutí Rady ze dne 29. května 2000, o boji s dětskou pornografií na Internetu.
- Doporučení Rady ze dne 25. června 2001, o kontaktních bodech 24-hodinové služby pro boj s kriminalitou za použití vyspělých technologií.
- Rozhodnutí Rady ze dne 28. ledna 2002, ke společnému přístupu v oblasti síťové a informační bezpečnosti.
- Rámcové rozhodnutí Rady 2002/465/JHA ze dne 13 července 2002, o Společných vyšetřovacích týmech.
- Rámcové rozhodnutí Rady 2005/222/JHA ze dne 24. února 2005, o útocích proti informačním systémům.
- Nařízení Evropského parlamentu a Rady ze dne 21. února 2006, o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s ustavením veřejně přístupných elektronických komunikačních služeb (dokument popisuje povinnosti poskytovatelů telekomunikačních služeb, související mimo jiné s tématem boje proti terorismu).

Co se koncepčního rámce zmíněné problematiky týče, je třeba zdůraznit, že již od samého počátku byla v rámci Evropské unie daná agenda chápána do značné míry jako bezpečnostní téma (a tedy většinou jako

[3] Směrnice a její výklad přesně definují rozdíl mezi programem a daty, což je základní rozlišovací hledisko při kvalifikaci trestného činu § 152 trestního zákona: "*Porušování autorského práva, práv souvisejících s právem autorským a práv k databázi*".

součást III. pilíře EU, věcně spadající vždy alespoň částečně do působnosti Rady pro spravedlnost a vnitřní věci). Stranou ale nikdy nezůstaly ani aspekty hospodářské a technické.

Klíčovým dokumentem, v uvedené oblasti je **"Akční plán pro Bezpečnější Internet"** (Safer Internet Action Plan) pro roky 1999 – 2004[4] a na něho navazující materiál "**Bezpečnější Internet plus**" (Safer Internet plus) pro roky 2005 – 2008.

Jedná se o dokumenty, usilující o vytváření rámce co nejširší informační společnosti, která je v souladu s prioritami III. pilíře, tedy určitými aspekty vytváření tzv. "Oblasti svobody, bezpečnosti a spravedlnosti". Cílem konceptu zejména je:

- Zkvalitnit bezpečnost informační infrastruktury z hlediska boje proti zločinu.
- Na unijní úrovni povzbuzovat rozvoj "internetového" průmyslu (Internet industry).
- Zajistit bezpečné používání Internetu a dalších technologií pro dálkový přístup k počítačovým systémům, v boji proti nelegálnímu obsahu na Internetu (se zvláštním důrazem na obsah, který by mohl znamenat újmu dětí a nezletilých).[5]
- Vytvářet bezpečné prostředí (Evropská síť horkých linek, snaha o ustavení samoregulačních mechanismů a etických kodexů providerů, respektive vytváření pomyslných "černých listin" nespolupracujících subjektů) se zvláštním zřetelem na nelegální obsah na Internetu (dětská pornografie, rasistická propagace, teroristická propaganda).
- Úsilí o technické vyvíjení systému pro filtrování a indexování potenciálně nebezpečného obsahu na Internetu (což rozhodně neznamená, že takový obsah je apriori nelegální).
- Iniciovat akce v oblasti zvyšování veřejné bdělosti (co se týče dodržování bezpečnostních pravidel v kyberprostoru).
- Udržet standardy Evropské unie v oblasti ochrany základních lidských práv a svobod.

Rozpracováním uvedeného rámce je **řada dalších dokumentů a aktivit, zaměřených na rozvoj Unijní informační společnosti**:

- **Usnesení Rady Evropské unie k Strategii pro bezpečnou informační společnost**.
- **Akční plán členských zemí eEurope 2002** (přijat v červnu r. 2000 a s jehož splněním se počítalo do roku 2002).
- **Akční plán kandidátských zemí eEurope+ 2003**.
- **Akční plán členských zemí eEurope 2005** (přijat v roce 2002).

- Plán zdůrazňuje velkou důležitost bezpečnosti počítačových sítí a boje proti kyberzločinu. Jeho cílem je zvýšit bezpečnost informačních infrastruktur a zajistit, aby orgány činné v trestním řízení měly veškeré přiměřené prostředky k činnosti. Zároveň požaduje plné respektování základních lidských práv a svobod.
- Je zde zmíněna mj. potřeba používání šifrování pomocí veřejného klíče, využívání kvalitních antivirových programů i firewallů, identifikačních prostředků karetních či biometrických, elektronických podpisů apod.
- Plán popisuje i otázky monitoringu komunikace, zajištění dopravovaných dat, anonymního přístupu a užití zdrojů, praktické spolupráce na mezinárodní úrovni, jurisdikce a hodnoty počítačových dat v důkazním řízení.
- Plán se věnuje i otázkám nelegislativních opatření jako je činnost specializovaných jednotek na národní úrovni, speciálního výcviku, zlepšené informace a společná pravidla pro komunikační protokoly. Je zmíněna možná spolupráce na úrovni EU i spolupráce s nestátní sférou.

Česká republika se v roce 2001 připojila k akčnímu plánu eEurope+ 2003, společnému závazku kandidátských států EU v oblasti rozvoje informační společnosti. V následujícím období se Česká republika soustředila na naplňování cílů Akčního plánu eEurope 2005.

[4] Rozhodnutí Evropského parlamentu a Rady č. 276/1999/EC ze dne 25. ledna 1999, ve znění doplněném Rozhodnutím Evropského parlamentu a rady č. 1151/2003/EC ze dne 16. června 2003.
Vyhodnocovací studie (7442/04) v uvedené souvislosti konstatuje, že Akční plán pro roky 1999 – 2004 přispěl ke zlepšení situace, nicméně že další úsilí v uvedené oblasti je nadále více než žádoucí.

[5] Nejnověji viz dokument ze dne 27. února 2008 č. 07241/2008, COM(2008) 106 final, „Proposal for a Decision of the European Parliament and of the Council Establishing a Multiannual Community Programme on Protecting Children Using the Internet and other Communication Technologies".

Další aktivitou Evropské unie v uvedené oblasti bylo zřízení platformy **ENISA** (”The European Network and Information Security Agency”, ”**Evropská agentura pro síťovou a informační bezpečnost**”) v březnu 2004.[6] Úkolem této agentury je:

- Poskytování poradenství a pomoc Komisi a členským státům Evropské unie při vytváření informační bezpečnosti a vedení dialogu se zástupci soukromých průmyslových společností při úsilí o zajištění informační bezpečnosti.
- Sběr a analýza dat souvisejících s bezpečnostními incidenty v Evropě a z toho vyplývajícími bezpečnostními riziky.
- Uplatňování metod analýzy ohrožení pro zvýšení schopností odolávat hrozbám v oblasti informační bezpečnosti.
- Včasné varování a zajištění kooperace mezi různými aktéry na poli informační bezpečnosti, zejména podpora programů veřejno – soukromého partnerství.

V roce 2008 vypracovala agentura rozsáhlou studii, týkající se odolnosti a bezpečnosti sítí elektronických komunikací a informačních systémů. Očekává se, že mandát pro činnost agentury potrvá minimálně do března roku 2011.

Oblasti boje proti kybernetickým incidentům v kontextu boje proti terorismu se v první řadě věnuje klíčový unijní dokument v uvedené oblasti, a to Evropská protiteroristická strategie, respektive **Akční plán Evropské unie pro boj s terorismem**, a to v bodech:[7]

- 1.1.1: Potřeba efektivní akce proti zneužívání Internetu (teroristy).
- 2.2.4: Ochranná opatření proti elektronickým útokům na klíčové počítačové systémy.
- 3.4.4: Ustavení právní rámce pro odstraňování ilegálního materiálu z Internetu.

K tématu ”kybernetického” rozměru agendy boje proti terorismu se rovněž vyjadřuje:

- **Deklarace Evropské rady o boji proti terorismu** ze dne 25. března 2004, navazující na útoky v Madridu. Její text vyzývá ke stanovení pravidel pro uchovávání údajů elektronického provozu.
- **Deklarace související s teroristickými útoky v Londýně**, přijatá dne 13. července 2005. Její text znovu zdůrazňuje potřebu přijetí opatření v oblasti uchovávání údajů elektronického provozu.
- **Rámcové rozhodnutí o boji proti terorismu** ze dne 13. června 2002. Jeho článek 4 výslovně vyzývá k sankcionování (trestnosti) všech forem schvalování a podpory terorismu, včetně vyzývání k teroristickým činům (incitement).
- Dílčím rozpracováním konkrétních úkolů, zakotvených v Akčním plánu je **Strategie Evropské unie pro boj s radikalizací a rekrutováním** (13888/2005), přijatá dne 28. října 2005 po komplikovaných jednáních a v návaznosti na existenci řady dalších dokumentů utajované povahy (zejména to platí pro Návrh Akčního plánu EU pro boj s radikalizací a rekrutováním - Draft EU Action Plan for Combating Radicalisation and Recruitment, ze 4. října 2005; 12165/2005ADD1 – RESTREINT). Strategie obsahuje i úkoly v oblasti prevence a represe, které se vztahují k fenoménu propagandy a obhajoby terorismu, stejně jako k fenoménu tzv. seberadikalizace prostřednictvím propagandy na Internetu.
- **Dokumenty unijního protiteroristického koordinátora ze závěru roku 2007** (15448/2007: Implementace Protiteroristické strategie EU: Podklad k diskusi; Implementation of the EU Counter-Terrorism Strategy – Discussion Paper; 15411/2007: Implementace Strategie a Akčního plánu boje proti terorismu; Implementation of the Strategy and Action Plan to Combat Terrorism). V jejich rámci jsou například zmíněna témata, jako je:

    - Omezování prostoru pro zneužívání výbušnin teroristy. Snahy o hledání možností pro omezování zneužívání Internetu pro umísťování návodů na přípravu improvizovaných zbraní.
    - Celé spektrum úkolů v oblasti ochrany kritické infrastruktury a ochrany před zneužitím chemických, biologických, jaderných a nukleárních látek teroristy.

[6] Česká republika je v Agentuře odpovídajícím způsobem zastoupena.
[7] Study on Legal Issues Relevant to Combating Criminal Activities Perpetrated through Electronic Communications: Executive Summary of Final Recommendations, Brussels; Luxembourg 2000).

- Větší zapojování nestátních provozovatelů sítí kritické infrastruktury do procesů vytváření bezpečnostních plánů a jejich napojování na kanály pro komunikaci s bezpečnostními složkami.
- Zintezívnění aktivit v oblasti národního i unijního bezpečnostního výzkumu.

Důležitou aktivitou v uvedené oblasti je projekt "**Check the Web**" (Projekt pro spolupráci v rámci Evropské unie proti využívání Internetu teroristy, Project on European Union Cooperation against a Terrorist Use of the Internet).[8] Zahájení projektu souvisí se skutečností, že Německo označilo boj proti terorismu a extremismu na Internetu za jednu z priorit svého budoucího předsednictví Unie.

Je konstatováno, že **je bezmála nemožné, aby jeden každý členský stát Unie samostatně monitoroval všechny podezřelé a potenciálně nebezpečné aktivity, ke kterým v rámci Internetu dochází.**[9] **Proto je více než žádoucí sdílet takové břemeno v rámci všech členských států Unie.** Projekt je proto chápán jako nástroj pro vytvoření funkční dělby práce v uvedené oblasti, která by následně usnadnila postup proti nelegálnímu obsahu na Internetu. Velkou úlohu by v tomto projektu měl hrát Europol. Prioritami projektu aktuálně je:

- Dosažení lepší úrovně jazykových a technických dovedností, nutných k porozumění získaným údajům.
- Vytvoření prostředí pružné analytické spolupráce mezi zainteresovanými zeměmi (např. dělba práce při provádění analýz konkrétních internetových stránek a chatových fór).
- Přenos výsledků, dosažených na úrovni jednotlivých zemí, pro potřeby Europolu, jehož cestou by byly využitelné v rámci celé Unie.
- Důrazně potírat publikování návodů na výrobu improvizovaných zbraní.

Projekt obsahuje řadu dílčích kroků, jejich splnění je v určitém časovém horizontu navrhováno. Prvním krokem v uvedené oblasti by mělo být stanovení kontaktní sítě (členské státy oznámí kontaktní body, odpovědné za navazující komunikaci a koordinaci konkrétních aktivit (prvotní vzájemné informování o technických prostředcích a metodách, nejlépe prostřednictvím uspořádání semináře za účasti zainteresovaných expertů; stanovení harmonogramu dalších pravidelných setkání technických expertů). Dále je plánována výměna informací o aktuálním personálním a technickém vybavení zainteresovaných složek v jednotlivých zemích Unie, respektive zjištění regionálních či tematických priorit jednotlivých zemí v uvedené oblasti.

Dalším cílem projektu je společný postup proti nelegálnímu obsahu na Internetu. Jedním z kroků této části projektu je výměna informací o aktuálních zákonných možnostech jednotlivých členských států při zamezení či blokování internetových stránek s nelegálním obsahem. Předpokládá se rovněž zintenzívnění spolupráce s poskytovateli internetových služeb (providery) v jednotlivých zemích.

Celou řadu návrhů v oblasti informační kriminality přineslo Předsednictví Francie (II. pololetí 2008). Jejich základem je zejména snaha o vytvoření unijní platformy pro nahlašování (a potírání) nežádoucího obsahu na Internetu.[10]

Některými aspekty problematiky se zabývá i Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006, o **uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí** a o změně směrnice 2002/58/ES (která bude účinná od 1. ledna 2009).

Stranou pozornosti nestojí ani **vazba mezi ohrožením ze strany terorismu a hospodářským rozvojem Unie**. Generální ředitelství pro trh (DG MARKT) a jeho expertní pracovní skupina k problematice elektronického obchodu (e-Commerce Expert Group) od přelomu let 2005 a 2006 důrazně vyzývají k přijetí náležitých opatření, zaměřených proti násilné radikalizaci a rekrutování do teroristických skupin

[8] Proposals of the German Delegation Regarding EU Co-Operation to Prevent Terrorist Use of the Internet ("Check the Web"), 18. květen 2006 (9496/2006).
[9] Přitom se výslovně předpokládá, že radikální postup proti terorismu přispěje rovněž i k boji proti zneužívání Internetu k distribuci xenofobních materiálů a dětské pornografie.
[10] Sumarizací tohoto úsilí je dokument „Draft Council Conclusions on a Concerted Work Strategy and Practical Measures against Cybercrime" (15569/2008) z 11. listopadu 2008.

prostřednictvím Internetu. Přitom je poukazováno na nástroje, které pro takový boj mohou vyplývat z existence vnitřního trhu.

Členské státy Unie totiž mohou, v případě, že si to žádá určitý veřejný zájem, k omezení určité internetové služby (odstranění určitého obsahu) provozování z území jiného členského státu užít sankce či zahájit vyšetřování. Jako zmíněný veřejný zájem je přitom výslovně uveden například boj proti jakémukoli podněcování k nenávisti na základě rasy, pohlaví, náboženství nebo národnosti, a činy, neslučující se s lidskou důstojností.

Určitým aspektům zajišťování kybernetické bezpečnosti se věnuje i projekt CI2RCO "**Koordinace výzkumu v oblasti kritické informační infrastruktury**", zahájený v březnu 2005. Jeho hlavním cílem je vytvořit a koordinovat unijní úkoly s cílem zabezpečení evropského koordinovaného přístupu ve výzkumu a vývoji v oblasti ochrany kritické informační infrastruktury (CIIP). V této souvislosti je mapován potenciál existujících organizací, které se příslušnou problematikou zabývají (dosavadní výsledky jejich činnosti, zdroje jejich financování atd.). Na základě zjištěných skutečností bude navrženo vytvoření "Unijní sítě pro výzkum a vývoj", která bude sloužit pro:

- Vytvoření vazeb mezi jejími jednotlivými zainteresovanými institucemi.
- Uspořádání pracovních setkání zástupců těchto institucí, s cílem iniciovat a podporovat výměnu informací a výsledků prací.
- Zajistit podporu činností ustavením internetového portálu, na kterém budou sdíleny získané výstupy.

Z účastníků projektu se předpokládá vytvoření Rady, která bude v rámci Evropské unie koordinovat projekty v oblasti vědy a výzkumu, zajišťovat výměnu informací mezi řešiteli z prostoru zemí Evropské unie a připravovat zprávy a návrhy pro Komisi Evropské unie. Projekt je prozatím koncipován na 2 roky.[11]

Patrně nejnověji se v rámci Europské unie daným tématem zabývá dokument **"Zelená kniha o detekčních technologiích při práci donucovacích, celních a jiných bezpečnostních orgánů"** (13183/2006), ze dne 25. září 2006.

Nedílnou součástí agendy Evropské unie v oblasti zvyšování bezpečnosti kyberprostoru, je i zajišťování určitých finančních prostředků, alespoň částečně využitelné v souvislosti v bojem proti kybernetickým incientům.

- V první řadě je třeba zmínit **přípravný program PASR (Preparatory Action for Security Research, Přípravná akce pro bezpečnostní výzkum), řízený poradním výborem ESRAB** (European Security Research Advisory Board, Poradní platforma pro evropský bezpečnostní výzkum), jenž se však soustředil spíše na problematiku bezpečnosti infrastruktury a některé další, spíše pro výrobní průmysl zajímavé aspekty. V rámci přípravy **VII. rámcového programu výzkumu** (který v letech 2007 – 2013 na PASR naváže) však vznikla zvláštní sekce "Bezpečnost a prostor" (Security and Space), jejímž úkolem je zajištění vývoje technologií a získání znalostí nutných pro zajištění bezpečnosti občanů před hrozbami zahrnujícími terorismus, organizovaný zločin, a další. Zájem o tuto část je ze strany členských zemí značný. Upřesňování této oblasti rámcového programu stále ještě probíhá, avšak je již téměř před dokončením. Pro roky 2007 – 2013 se pro **"Bezpečnost a prostor"** předběžně počítá s prostředky o objemu 3,96 miliardy eur. Z toho cca 550 milionů eur bude s největší pravděpodobností určeno na bezpečnostní výzkum v oblasti informačních a komunikačních technologií. **Předběžně se přepokládá, že uvedená suma by byla rozdělena na více než 100 "středních" (tříletých) projektů o objemu cca 5 milionů eur, jejichž spolufinancování ze strany koordinující členské země by nemělo přesáhnout 25 % (tedy cca 1,3 milionu eur na 3 roky).** Existuje tedy **reálná možnost získání minimálně jednoho takového grantu (koordinačního úkolu) pro Českou republiku**. Je považováno za nanejvýš potřebné, aby se takový projekt týkal právě oblasti boje proti kybernetickým hrozbám. Pokud ovšem nedojde k rychlému vnitrostátnímu rozhodnutí o podpoře takového úsilí, může být získání prostředků z unijního rozpočtu pro uvedený záměr značně zkomplikováno.

[11] Vedoucím projektu je společnost Fraunhofer Gesellschaft zur Foerderung der Angewandten Forschung e.V., která těsně spolupracuje s firmami IABG (Industrieanlagen Betriebsgesellschaft mbH), respektive Cityplan spol. s r. o.

- Určité využitelné prostředky obsahuje i Rámcový program AGIS pro policejní a soudní spolupráci pro roky 2003 až 2007. Jeho celkový rozpočet činí 65 milionů eur. Zatím byly realizovány programy STOP a STOP II (oba roku 2000) a další aktivity, věnované zejména boji proti dětské pornografii.
- Určité prostředky z rozpočtu "Akčního plánu Bezpečnější Internet" obdržel i "Preventivní akční program evropského společenství pro boj s násilím na dětech, mladých lidech a ženách" (DAPHNE), rovněž s důrazem na identifikování obětí dětské pornografie.

Z výše uvedených skutečností je zřejmé, že **vzájemně se prolínající priority Evropské unie v uvedené oblasti je možné určitým způsobem plošně zobecnit**:

- Aktivity v oblasti sběru a analýzy dat o kybernetických incidentech a možných ohroženích z nich plynoucích.
- Boj proti škodlivému (harmful) obsahu na Internetu. Hledání koordinovaného postoje k nežádoucímu (unwanted, spam) obsahu na Internetu.
- Aktivity v oblasti ochrany zákazníka.
- Hledání technických řešení v oblasti filtrování a indexování potenciálně nebezpečného obsahu na Internetu (což rozhodně neznamená, že takový obsah je apriori nelegální).
- **Úsilí o zvýšení spolupráce mezi nejvíce zainteresovanými aktéry v oblasti boje proti kybernetickým hrozbám**, a to jak z hlediska spolupráce subjektů napříč zeměmi EU, tak **zejména co se týče rozvoje spolupráce veřejných a soukromých subjektů (tzv. PPP =** Public Private Partnership**), zapojení nevládního neziskového sektoru** (zejména v oblasti boje proti xenofobii a dětské pornografii) **a zapojení akademické obce (zejména co se týče ústavů, kde je prováděn aplikovaný výzkum).** Výzkumné studie jsou žádány v řadě oblastí, např. co se týče studií modu operandi zločinců; nových technických řešení v boji proti kybernetickým incidentům a, v neposlední řadě, nezávislého pohledu na celou problematiku.
- Boj proti porušování autorských práv.
- Snaha o vývoj v oblasti samoregulace (etické kodexy providerů atd.).
- Trvalé vytváření mechanismů, jejichž prostřednictvím je možné oznamovat nelegální obsah na Internetu (horké linky).
- Provádění osvětové činnosti, zaměřené na veřejnost (školy, rodiny, mládež atd.), s cílem zvýšit její bdělost před nástrahami ze strany kybernetických incidentů.
- Dosažení pokroku v oblasti samoregulace (vytvořit a šířit etické kodexy pro poskytovatele internetových služeb).
- Podchytit celou problematiku statisticky (tématu se věnuje i systém Eurobarometer, kladoucí veřejnosti otázky po jejích hlavních požadavcích v oblasti ochrany kyberprostoru).

Agenda kybernetické bezpečnosti přitom v rámci Evropské unie začíná ve stále větší míře prolínat ze III. do II. pilíře. Například Evropské radě byla ve dnech 11.-12. prosince 2008 předložena „Zpráva o provádění Evropské bezpečnostní strategie – Zajišťování bezpečnosti v měnícím se světě" (zpráva generálního tajemníka, vysokého představitele), ve které je pasáž týkající se počítačové bezpečnosti (*Moderní ekonomiky se velkou měrou opírají o klíčové infrastruktury, včetně dopravy, komunikací a dodávek energie, ale také o internet. Na internetovou trestnou činnost se zaměřuje strategie pro bezpečnou informační společnost, přijatá v roce 2006. Útoky proti soukromým či vládním počítačovým systémům v členských státech EU však daly tomuto problému nový rozměr jakožto potenciální nové ekonomické, politické a vojenské zbrani. V této oblasti je zapotřebí další práce s cílem prozkoumat komplexní přístup EU, zvýšit informovanost a posílit mezinárodní spolupráci*.)

Přitom všem je třeba opakovaně zdůraznit, že **Evropská unie jako celek v oblasti ochrany kyberprostoru zaostává za Spojenými státy americkými a toto zpoždění se trvale prohlubuje**. Děje se tak i proto, že **Unie usiluje o "vlastní cestu" v oblasti boje proti terorismu, která by kladla větší důraz na ochranu lidských práv, než například postup USA**. Ještě na samém konci XX. století v rámci Evropského parlamentu například probíhaly debaty o nutnosti monitorování systému Echelon, provozovaném Národním bezpečnostním úřadem USA.

Takové kroky, nejenže znamenají fatální snížení efektivity příslušných protiopatření, ale podepisují se i na ochotě federální vlády, Kongresu i občanů USA sdílet s unijními strukturami určité klíčové informace (a technologie). **Nikdo nemůže zaručit, že USA v budoucnu z jakýchkoli důvodů nepřestanou velkoryse sdílet se zeměmi Evropy své technologicko-organizační výsledky v uvedené oblasti. Zároveň je zřejmé,**

že se bude prohlubovat technologickou závislost Evropské unie na USA, co se sdílení informací v oblasti kybernetických hrozeb týče. Případné ochlazení vztahů USA – Evropská unie by tak pro Unii znamenalo nemalé komplikace ve snaze držet krok se světovými trendy.

Ani u prostředků z rozpočtu Evropské unie nelze propadat přílišnému optimismu. Zejména s ohledem na pozici České republiky jako "nového" členského státu Unie je zřejmé, že daleko nejsnazší je získat prostředky na nákup zařízení (s ohledem na dynamiku odvětví de facto již v okamžiku sériové výroby překonaných) z jiných ("starých") členských zemí Unie (a tím je finančně podpořit), než najít prostředky na vlastní aplikovaný výzkum (který by v konečném důsledku podpořil Českou republiku a její hospodářství či akademickou obec).

Pro Českou republiku je taková možnost důrazným důvodem k tomu, aby své aktivity v oblasti ochrany kyberprostoru nevázala pouze na Evropskou unii, ale usilovala jak o přímou bilaterální spolupráci s jinými zeměmi světa (USA, ale i Japonsko, Korejská republika atd.), a usilovala i o vlastní aplikovaný výzkum.

2.3 Rada Evropy (Council of Europe, CoE)

Rada Evropy začala projevovat zájem o řešení problematiky informační kriminality již koncem osmdesátých let minulého století. V roce 1989 publikovala studii, obsahující doporučení pro úpravy a vytváření nových zákonů jednotlivých států, určených ke kriminalizaci určitých činů, spáchaných prostřednictvím počítačových sítí (Doporučení č. 9 / 1989). Roku 1995 následovala další studie, obsahující principy, týkající se trestněprávního postupu souvisejícího s informačními technologiemi (Doporučení č. 13 / 1995). V roce 1997 byla ustavena Komise expertů na zločin v kyberprostoru. Výsledkem její činnosti byla Úmluva o kyberzločinu (Convention on Cybercrime, ETS 185), otevřená k přístupu dne 9. února 2005.[12] K Úmluvě mohou přistoupit i země, které nejsou členy Rady Evropy. Česká republika Úmluvu zatím nepodepsala, s tímto krokem se počítá po implementaci konkrétních skutkových podstat, v souvislosti s probíhající rekodifikací trestního práva hmotného.

Úmluva je prvním mezinárodněprávním instrumentem, určeným speciálně pro řešení problémů spojených s mezinárodním charakterem počítačového zločinu. Její text požaduje, aby signatářské země kriminalizovaly určitá jednání, které je možné zařadit do oblasti počítačového zločinu, a aby tyto země přijaly procesní normy, umožňující takovou trestnou činnost postihovat. Prostřednictvím Úmluvy je kriminalizován také návod a napomáhání k takovým typům zločinů. Řešena je rovněž otázka odpovědnosti právnických osob. V Úmluvě jsou uvedeny i principy a konkrétní způsoby vzájemné pomoci mezi jednotlivými státy při vyšetřování informační kriminality, včetně otázek vydávání osob, způsobů předávání zajištěných dat, způsobů předávání požadavků a vytváření bodů pro nepřetržitý kontakt

Vedle Úmluvy se tématu kybernetických incidentů věnují i další dokumenty Rady Evropy:

- Dodatkový protokol o kriminalizaci činů rasistické a xenofobní povahy, spáchaným prostřednictvím počítačového systému (Additional Protocol Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Commited through Computer Systems, ETS 189).
- Doporučení Rady ministrů č. 13 z roku 1995, týkající se problémů trestního práva procesního, spojeného s informačními technologiemi.
- Doporučení Rady ministrů č. 5 z roku 1999, týkající se ochrany soukromí na Internetu.

Téma boje proti informační kriminalitě je pravidelně důležitým bodem jednání Výboru expertů Rady Evropy proti terorismu (CODEXTER).[13]

2.4 Interpol

Využití mezinárodní policejní struktury Interpol (podobně jako v případě Europolu jako struktury Evropské unie) v oblasti boje s informační kriminalitou je relativně všestranné (prioritou je boj proti počítačovým podvodům a jiné hospodářské a finanční kriminalitě; vytváření hlásného a informačního systému o

[12] Struktura Úmluvy je zmíněna v kapitole 2.1.
[13] http://www.coe.int/t/e/legal_affairs/legal_co-operation/fight_against_terrorism/4_theme_files/cyberterrorism%20database.asp

organizované a informační („počítačové“) kriminalitě; harmonizace právních předpisů v oblasti trestního práva hmotného a procesního atd.).

2.5 Organizace pro bezpečnost a spolupráci v Evropě (Organisation for Security and Cooperation in Europe, OBSE, OSCE)

V uvedeném kontextu je klíčové rozhodnutí Rady ministrů Organizace č. 3 / 2004 ”O boji proti používání Internetu pro účely terorismu” (Ministerial Council Decision on Combating the Use of the Internet for Terrorist Purposes), které vzešlo ze zasedání v Sofii dne 7. prosince 2004 a které navazuje na závěry Konference, kterou stejná organizace pořádala ve dnech 15. - 16. července 2004 v Paříži k tématu souvislosti mezi zločiny z nenávisti a rasistickou, xenofobní a antisemitskou propagandou na Internetu (Meeting on the Relationship Between Racist, Xenophobic and Anti-Semitic Propaganda on the Internet and Hate Crimes).

Obsahem konference bylo zejména téma oprávněnosti převodu odpovědnosti za obsah internetových stránek z vlád na poskytovatele jednotlivých stránek. Jednotlivé země byly vyzvány k tomu, aby legislativní cestou označily to, co považují za ilegální. Co nebude možné označit právně za ilegální, by mělo být interpretováno jako využívání svobody slova. Důležitá. je také prevence, kde se nabízí prostor ve vzdělávání a zvyšování obecného povědomí o ohrožení ze strany terorismu, souvisejícím se zneužitím Internetu. V návaznosti na dosavadní vývoj byl ve dnech 13. - 14. října 2005 ve Vídni uspořádán expertní dvoudenní worskhop k tématu výměny relevantních informací mezi členskými státy Organizace, věnovaný zároveň problematice identifikace možných strategií k potírání teroristické hrozby při zajištění dodržování lidských práv.

2.6 Organizace pro hospodářskou spolupráci a rozvoj (Organisation for Economic Cooperation and Development, OECD)

Organizace, respektive její Výbor pro informační, počítačovou a komunikační politiku (Committee for Information, Computer and Communication Policy) vydal v roce 2002 dokument ”Přehled: Bezpečnost informačních systémů a sítí: Směrem ke kultuře bezpečnosti” (Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security). Jeho text doporučuje, aby členské země Organizace:

- Zřídily nové nebo posílily existující zásady, praktiky, opatření a postupy pro tuto tématiku prostřednictvím přijetí a provádění tzv. ”kultury bezpečnosti”.
- Koordinovaly postupy a spolupracovaly na národní i mezinárodní úrovni (i mezi nečleny Organizace).
- Šířily tuto ideu ve veřejném i soukromém sektoru (včetně vládních a jiných organizací i individuálních uživatelů).
- Jednou za pět let podaly zprávu o plnění ”Přehledu” (popis toho, jak je konkrétní zemí naplňována mezinárodní spolupráce v oblastech, vztahujících se k bezpečnosti informačních systémů a sítí).

2.7 Severoatlantická obranná aliance (North Atlantic Treaty Organisation, NATO)

Kybernetická obrana se stala součástí Defence Capability Initiative a následně i Prague Capability Commitments (rok 2002). V roce 2002 bylo uloženo výboru NC3B (NATO Consultation, Command and Control Board), aby v rámci aliance prosadil adekvátní kybernetickou obranu. V rámci NATO se problematikou kybernetické obrany zabývá dále NATO Office of Security (NOS), který koordinuje dosahování schopnosti NATO Computer Incident Response Capability (NCIRC).

Kybernetickými incidenty se v rámci NATO zabývá např. Výbor pro plánování civilních komunikací (Civil Communications Planning Committee, CCPC), a to v dokumentu EAPC(CCPC)D(2006)0002 ze dne 2. února 2006: ”Civilní nouzové plánování: Následky, související s kybernetickými útoky a informačními zbraněmi na kritickou civilní komunikační infrastrukturu a služby; Civilní nouzové plánování: Následky ustavení Týmu pro civilní počítačové bezpečnostní incidenty” (”Civil Emergency Planning: Consequences Regarding Cyber Attacks/Info Warfare on Critical Civil Communications Infrastructure and Services and CEP Consequences of the Establishment of Civil Computer Security Incident Response Teams (cCSIRTs)”).

V letech 2007-2009 vyhotovila pracovní skupina pro telekomunikace (Working Group for Telecommunications) Civil Communication Planning Committee NATO mimo jiné i studii zabývající se problematikou tzv. cyber attack/defense a ochrany sítí elektronických komunikací a informačních systémů.

2.8 Skupina osmi průmyslově vyspělých států světa (G8, Group 8, Lyonská skupina)

Ministři spravedlnosti a vnitřních věcí zemí Skupiny přijali v prosinci roku 1997 na summitu ve Washingtonu deset principů, které byly následně podepsány na summitu Skupiny v Birminghamu v květnu 1998. Dokument shrnuje cíle zúčastněných států v boji s "high-tech" zločinem ("high-tech" zločin se zde obsahově kryje s pojmem zločin v "kyberprostoru"):

- Nesmí existovat bezpečné útočiště pro ty, kteří zneužívají informační technologie.
- Vyšetřování a trestní řízení v oblasti "high-tech" zločinu musí být koordinováno mezi všemi zúčastněnými státy bez ohledu na to, kde se škoda stala.
- Orgány prosazující právo je třeba k potírání "high-tech" zločinu dostatečně vyškolit a vybavit.
- Právní systémy musí chránit důvěrnost, integritu a dosažitelnost dat a systémů před neoprávněným narušením a zajistit, aby jejich vážné zneužití bylo trestáno.
- Právní systémy by měly zajistit uchovávání dat z telekomunikačního provozu dat a rychlý přístup k nim, což je jedním ze základních předpokladů pro úspěšné vyšetření této trestné činnosti.
- Vzájemná spolupráce vlád musí zajistit včasný sběr a výměnu důkazů v případech zahrnujících "high-tech" zločin.
- Přeshraniční přístup orgánů prosazování práva k veřejně dostupným informacím nesmí být podmíněn povolením od státu, na jehož území jsou data fyzicky umístěna.
- Pro vyhledávání a ověřování elektronických dat při kriminálním vyšetřování a trestním řízení musí být vyvinuty a používány příslušné forensní standardy.
- Informační a komunikační systémy je třeba pokud možno navrhovat tak, aby přispívaly k obraně proti zneužití sítí, k detekci takového zneužití a měly by usnadnit vystopování zločinců a sběr důkazů.
- Veškeré aktivity v této oblasti je třeba koordinovat s činností ostatních relevantních mezinárodních fór, aby se zabránilo zdvojování konkrétních aktivit.

Principy byly následně konkretizovány v Akčním plánu pro potírání "high-tech" zločinu. Příslušné orgány zainteresovaných zemí jsou povinné:

- Využít vybudovanou síť odborného personálu, aby byla zajištěna včasná a efektivní odpověď na nadnárodní případy informační kriminality a ustanovit styčná místa, která budou dosažitelná 24 hodin denně.
- Přijmout odpovídající opatření k zajištění dostatečných kapacit orgánů prosazování práva. Tyto orgány musí být připraveny potírat "high-tech" zločin a vzájemně spolupracovat s příslušnými orgány jiných států.
- Provést revizi právních systémů tak, aby touto cestou bylo dostatečně kriminalizováno zneužití telekomunikačních a počítačových systémů, a dále podporováno odhalování "high-tech" zločinu.
- Při vyjednávání dohod a ujednání o vzájemné pomoci brát v úvahu otázky spojené s "high-tech" zločinem. Pokračovat ve zkoumání a rozvíjení prakticky proveditelných řešení, které se týkají zachování důkazů před vydáním soudního rozhodnutí, přeshraničních prohlídek a prohledávání dat v počítačích, v případech, kdy není známo umístění těchto dat.
- Vyvinout urychlené postupy pro získání provozních dat ze všech komunikačních prostředků v řetězci komunikace, studovat způsoby urychleného mezinárodního předávání těchto dat.
- Spolupracovat s průmyslovými odvětvími tak, aby bylo zajištěno, že nové technologie usnadní boj s "high-tech" zločinem.
- Vytvořit mechanismy pro zajištění bezprostředního přijetí požadavků vzájemné pomoci v naléhavých a důležitých případech a včasných odpovědí na ně pomocí rychlých a dostatečně spolehlivých prostředků komunikace (i prostřednictvím hlasu, faxu nebo elektronické pošty, s případným dodatečným písemným potvrzením).
- Podpořit organizace, zabývající se tvorbou mezinárodně uznávaných standardů v oblasti telekomunikačních a informačních technologií, aby trvale poskytovaly veřejnému i privátnímu sektoru standardy technologií bezpečné telekomunikace a zpracování dat.
- Vyvinout a použít kompatibilní forensní standardy pro vyhledávání a ověřování elektronických dat při kriminálním vyšetřování a trestním řízení.

Česká republika (zejména prostřednictvím odboru informační kriminality Policejního prezídia) daný vývoj intenzívně sleduje.

2.9 Aktivity související s Mezinárodní asociací internetových horkých linek[14]

Přední světové finanční subjekty (bankovní a úvěrové instituce) a představitelé internetového průmyslu (provideři, poskytovatelé internetových služeb) se spojili s Mezinárodním střediskem pro pohřešované a zneužívané děti (ICMEC) a jeho sesterskou organizací, Národním střediskem pro pohřešované a zneužívané děti (NCMEC), aby společně bojovali proti dětské pornografii. Cílem iniciativy je vymýtit dětskou pornografii. Koalice navázala spolupráci s Mezinárodní asociací internetových horkých linek (International Association of Internet Hotlines (INHOPE). Jejím výsledkem je kampaň, apelující na nejširší veřejnost v konkrétních zemích. Na "horké linky" INHOPE je možné hlásit informace o výskytu internetových stránek s dětskou pornografií. V České republice od 1. dubna 2007 existuje horká linka ve správě nevládní organizace Naše dítě (http://www.internethotline.cz/), která se stala součástí sítě INHOPE od 25. října 2007.

[14] Zástupci finančního a internetového průmyslu bojují proti dětské pornografii; in: ČTK, 17. III. 2006.
http://www.icmec.org; http://www.missingkids.com