Zahraniční inspirace související s tématem kybernetických hrozeb

PRAHA 2009

Úvod

Jakékoli kroky v domácím bezpečnostním prostředí by bylo více než nezodpovědné konat bez toho, pokud by nebyla nejprve prostudována situace v zahraničí.

Jednotlivé země světa – zejména státy, které jsou nejvíce „internetizovány“ (Korejská republika, USA, Japonsko, některé členské země Evropské unie a další státy) kladou na problematiku prevence a potírání kybernetických hrozeb velký důraz. Takový přístup je třeba chápat do značné míry jako vzor pro Českou republiku. Studovány byly nejen dosavadní výsledky a zkušenosti jednotlivých zemí, ale i jejich podobnost s prostředím České republiky. Není možné bez dalšího srovnávat ambice České republiky s globální supervelmocí typu Spojených států, ale je třeba se spíše zaměřit na přístupy zemí v Evropě.

Informace o situaci v konkrétních zemích světa byly získány v první řadě ze zdrojů, poskytnutých Ministerstvem zahraničních věcí. Další informační zdroje sehrály doplňující úlohu (podklady Ministerstva informatiky, podklady Úřadu pro zahraniční styky a informace, monitoring otevřených zdrojů). Při sledování situace byl zejména kladen důraz na následující prvky:

- Politická podpora pro kroky v oblasti kybernetické bezpečnosti (je tato problematika v dané zemi chápána jako aktuální bezpečnostní priorita nebo nikoli?).
- Spolupráce veřejného, soukromého a akademického sektoru v uvedené oblasti.
- Zaměření subjektů, odpovědných za problematiku kybernetické bezpečnosti v rámci bezpečnostního systému dané země.
- Konkrétní náplň činnosti daných pracovišť (včetně výzkumné činnosti a aspektu komunikace s veřejností a plnění role výstražného střediska při kybernetických incidentech – CSIRT/CERT).
- Zveřejnitelné výsledky práce takového subjektu, způsob jejich distribuce a případně i mediální prezentace.
- Propojení subjektů s jejich zahraničními protějšky.
- Způsob financování vzniku i provozu konkrétního pracoviště (kdo případný subjekt financuje, o jak velké částky se jedná, do jaké míry zde existuje možnost samofinancování).
- Personální nároky, které v rámci pracoviště existují (kolik osob je zde zaměstnáno, jak kvalifikovaný je to personál, jaké jsou nároky na bezpečnostní prověrku takového personálu).

Následují příspěvky věnované jednotlivým sledovaným zemím:

SPOJENÉ STÁTY AMERICKÉ

Důležitým aktérem byla a stále je **Carnegie Mellon University**. Na její půdě již v 90. letech XX. století došlo k vytvoření struktury, přeložitelné jako **„Tým pro reakci na počítačová ohrožení“** (Computer Emergency Response Team Coordination Center, CERT/CC[1]). V jeho rámci byly vytvořeny pracovní skupiny (Botnets, Attribution, Active Defense, Classified Intrusion Sets atd.). Ze strany vládních kruhů je důraz na uvedenou problematiku ve větší míře kladen až v posledních 10 letech:[2]

- 1997: Prezidentská komise použila pojem „rizika v kyberprostoru“ v pololetní veřejné zprávě o své činnosti. Byla zdůrazněna vzájemná propojenost a zranitelnost, související s existencí technologické společnosti.
- 1998: Byla vydána prezidentská směrnice č. 63, navrhující způsoby ochrany státního „kyberprostoru“. Prostor byl věnován zejména obavám z fenoménu Y2K.
- 2000: V platnost vešel **„Národní plán pro ochranu informačních systémů“** (National Plan for Information Systems Protection), který stanovuje základní druhy hrozeb s ohledem na jednotlivé segmenty kritické infrastruktury. Zároveň nastoluje základní otázky, související s rozporem mezi úsilím o ochranu soukromí a občanských práv na straně jedné a efektivní obranou kritické infrastruktury na federální i lokální úrovni na straně druhé.
- 2001 (únor): Byla zveřejněna podrobná Zpráva presidenta Spojených států o stavu aktivit v oblasti ochrany kritické federální infrastruktury. Zároveň došlo k vyčlenění cca 2 miliard dolarů pro investice v oblasti aplikovaného výzkumu, zaměřeného na vyšší bezpečnosti Internetu. Ministerstvo obchodu zahájilo aktivity v oblasti navazování veřejno-soukromých partnerství v řadě sektorů (výroba, obchod, bankovnictví, pojišťovnictví).
- 2001 (říjen, tedy po událostech z 11. září 2001): Tématu se věnuje prezidentské nařízení č. 13231, které označilo bezpečnost kyberprostoru za prioritu bezpečnostní politiky. Byly vyčleněny další finanční prostředky pro zajištění bezpečnosti federální počítačové sítě. Záhy nato byl vydán **„Zákon o informační bezpečnosti“** (Federal Information Security Management Act, FISMA), který se stal rámcem dalších navazujících aktivit.
- 2002: Z iniciativy Bílého domu se v deseti velkoměstech USA konala setkání lokálních politiků, vědců, podnikatelů a finančníků, zaměřená na problematiku bezpečnosti kyberprostoru. Bílý dům vytvořil nové poradní těleso presidenta, Národní poradní radu pro infrastrukturu (National Infrastructure Advisory Council, NIAC)[3], sestávající z odborníků na problematiku kyberprostoru. Další aktivity v oblasti byly spojeny s procesem vytváření Ministerstva vnitřní bezpečnosti.
- 2003 (únor): Byl vydán dokument „**Národní strategie pro bezpečný kyberprostor**“ (National Strategy to Secure Cyberspace)[4]. Zároveň byl zveřejněn jeho prováděcí legislativní rámec, „Zákon o výzkumu a vývoji v oblasti bezpečnosti kyberprostoru“ (Cyber Security Research and Development Act), obsahující zejména odpovídající rozpočtová a personální ustanovení. Specifikem materiálu je vysoce konkrétní výčet úkolů, které jsou rozplánovány (zatím) do horizontu 5 let. Koordinaci bezpečnostního výzkumu a financování aktivit provádí Ministerstvo vnitřní bezpečnosti, které úzce spolupracuje s Ministerstvem energetiky.[5] Očekávání, kladená do implementace Strategie, jsou následující: a) předcházet kybernetickým útokům proti bezpečnosti USA; b) zmírnit zranitelnost země proti kybernetickým útokům; c) minimalizovat škody a usnadnit návrat situace do původního stavu, v případě, že k incidentu přeci jenom dojde.
- 2003 (září): Byl oficiálně vytvořen tzv. US-CERT, a to jako propojení mezi strukturou v rámci Carnegie Mellon University (CERT/CC) a nově vytvořenou součástí Ministerstva pro vnitřní bezpečnost v rámci Ředitelství pro informační analýzu a ochranu infrastruktury (Information Analysis and Infrastructure Protection Directorate): **„Oddělení pro národní kybernetickou bezpečnost“** (National Cyber Security Division, NCSD).[6] US-CERT byl rovněž úzce propojen se subjektem, jménem **„Institut softwarového inženýrství“** (Software Engineering Institute, SEI), což je federální výzkumné a vývojové centrum, financované Ministerstvem obrany. Za účelem

získávání varování a důležitých informací z oblasti kybernetické bezpečnosti byl vytvořen **„Národní systém výstrah souvisejících s kyberprostorem“** (National Cyber Alert System, NCAS), na který se lze napojit prostřednictvím Internetu.[7]

- 2005 (červenec): Ministerstvo pro vnitřní bezpečnost zveřejnilo novou strategii, která by lépe odpovídala aktuálním i budoucím hrozícím rizikům pro bezpečnost Spojených států. V rámci změn uvnitř resortu mimo jiné došlo k vytvoření Ředitelství stálé pohotovosti, jehož součástí se stal i nově zřízený **úsek zabývající se hodnocením a identifikací slabých a zranitelných míst telekomunikačních sítí** (Assistant Secretary for Cyber and Telecommunications), navrhující preventivní opatření a reakce na případné elektronické útoky.
- 2008 (podzim): V USA byly zahájeny diskuse o nutnosti nové **Národní kybernetické bezpečnostní iniciativy** (National Cybersecurity Initiative), která by byla schopná reagovat na nejnovější kybernetické incidenty (Estonsko, Gruzie, akce, přičítané Čínské lidové republice). Koordinátorem příprav je Ministerstvo vnitřní bezpečnosti.

Současný stav by tedy bylo možné charakterizovat následovně: **Nejdůležitějšími subjekty**, aktivními v oblasti kybernetické bezpečnosti USA, jsou **Ministerstvo vnitřní bezpečnosti** (US-CERT, Vědeckovýzkumné centrum pro kybernetickou bezpečnost – Cyber Security R&D Center[8] atd.), **Ministerstvo obrany** (SEI), přičemž u obou subjektů jsou aktivní zástupci a absolventi **Carnegie Mellon University** (CERT/CC, Cyber Security Laboratory). Jedná se o přitom o velmi těsně propojení, konkrétně CERT/CC sídlí v prostorách SEI atd.

Z dalších subjektů stojí za zmínku Institut pro bezpečnostní technologická studia (Institute for Security Technology Studies, ISTS) při Dartmouth College[9].

Celkově je možné konstatovat, že na nejvyšší (federální, ústřední) úrovni se tématu boje proti kybernetickým hrozbám věnuje nejméně několik stovek osob, napojených na tisíce dalších specialistů v řadě subjektů. Přitom je komplexně rozvíjena spolupráce se soukromým sektorem (profesní asociace a sektorové koordinační rady). Finanční náročnost agenty ilustruje nejlépe skutečnost, že problematice „informační bezpečnosti“ je věnováno více než 14 % rozpočtu Ministerstva obrany.

Ochranu kyberprostoru v USA je charakterizována vytvářením **„Systému celostátní reakce v oblasti bezpečnosti kyberprostoru“** (National Cyberspace Security Response System), který může být popisován jako dělba práce mezi jednotlivými propojenými stupni (levely):

- Level 1 – domácí uživatel, malé podniky: Stroje (počítače) se mohou stát slabým místem systému, případně dokonce braní útočníka, pokud se na ně bez vědomí vlastníka neoprávněně napojí.
- Level 2 – velké podniky (často definované jako části kritické infrastruktury, respektive jako cíle útoku): Odpovědní pracovníci firem musí sledovat aktuální vývoj v oblasti, učit se z vhodných osvědčených postupů a aplikovat je.
- Level 3 – kritická infrastruktura: Pod tímto výrazem se rozumí ne jednotlivé provozy, ale sektory (odvětví), kde je nezbytné sdílení informací, výměna osvědčených řešení a všestranná spolupráce. Některé resorty (za pomoci institucí, respektive agentur, existujících ve struktuře věcně příslušných ministerstev) vytvořily centra pro sdílení a analýzu informací (Information Sharing and Analysis Centers – ISAC-s), která nezbytnou výměnu informací zefektivňují a zrychlují.
- Level 4 – celostátní úroveň: Určité úkoly je třeba řešit celostátně (nikoli lokálně nebo sektorálně). To platí například o Internetu jako takovém, bezpečnosti jeho protokolů a routerů, respektive o strategických investicích do výzkumu a vývoje. Důležité je i stanovení unifikovaných standardů pro výcvik a vzdělávání bezpečnostních odborníků.
- Level 5 – celý svět: Útok na kyberprostor v USA může přijít z opačného konce planety. Stát proto musí pomáhat svým partnerům v oblasti boje proti zločinu (terorismu) všude na světě. I velké továrny a akademická obec by se se svými protějšky, kolegy – a dokonce i konkurenty – měly dělit o získané zkušenosti atd. Pokud se tak nestane, mohou všichni fatálně ztratit.

SPOJENÉ KRÁLOVSTVÍ

Vláda Spojeného království označuje **za národní kritickou infrastrukturu** hodnoty, služby a systémy, které jsou základem ekonomického, politického a společenského života v zemi. Taková infrastruktura je v zemi členěna do **deseti sektorů veřejného života**: komunikace; pohotovostní služby (rychlá lékařská pomoc, hasiči, policie); energetika; finančnictví; potravinářství; vládní a veřejné služby; zdravotnictví; veřejná bezpečnost; doprava a vodní hospodářství. Všechny uvedené oblasti života společnosti jsou vysoce závislé na počítačových a souvisejících technologiích a tím se stávají velmi zranitelnými elektronickým (počítačovým) útokem.[10]

Tělesem, které je v první řadě odpovědné za udržování kybernetické bezpečnosti ve Spojeném království, je **„Středisko pro ochranu národní infrastruktury“** (Centre for the Protection of National Infrastructure, CPNI), které vzniklo transformací „Národního koordinačního centra pro bezpečnost infrastruktury“ (National Infrastructure Security Co-ordination Centre, NISCC), založeného roku 1999. Jedná se o vládní meziresortní instituci, která:[11]

- sleduje rizika, souvisejících s kyberprostorem a navrhuje preventivních kroky proti nim;
- soustřeďuje související informace od jednotlivých ministerstev a dalších subjektů (zejména resorty obrany, vnitra a obchodu, policejní orgány a zpravodajské služby);
- je v kontaktu se širokým spektrem soukromých a polosoukromých společností, které často spravují i oblast veřejných služeb (často se jedná o subjekty, u kterých existuje mezinárodní přesah nebo bývají vlastněné zahraničními majiteli);
- je napojena na klíčové zainteresované domácí akademické instituce;
- koordinuje spolupráci výše uvedených subjektů a je ve styku s obdobnými agenturami v zahraničí.

Práce centra je s ohledem na hlavní předmět jeho činnosti organizována po čtyřech hlavních liniích:[12]

- **Vyhodnocování hrozeb:** vyšetřování, vyhodnocování a eliminace počítačových hrozeb;
- **Osvětová činnost:** vysvětlování a propagace ochrany proti počítačovým útokům (sdílení informací, nabízení odborných rad a *„best practices“*);
- **Preventivní a reaktivní činnost:** varování před aktuálními a novými hrozbami; zmírňování důsledků napadení a napomáhání regeneraci a vylepšení systémů po případném útoku;
- **Výzkumná činnost:** vytváření technologií a metod k ochraně před počítačovými hrozbami.

Rozpočet Centra je odhadován na 10 milionů liber (rok 2006). Personál Centra sestává z cca 85 osob.

V operativní rovině spadá vyšetřování trestné činnosti s prvkem počítačové bezpečnosti pod vládní **Agenturu pro boj se závažnou organizovanou trestnou činností** (Serious Organised Crime Agency, SOCA)[13]. Agentura vznikla roku 2006 a převzala i agendu, kterou v letech 2001 – 2006 řešil **Národní útvar pro boj se zločinem používajícím vyspělých technologií** (National Hi-Tech Crime Unit), který byl součástí Útvaru boje proti organizovanému zločinu (Police Organised Crime Unit).[14]

Dále se tématem boje proti kybernetickým hrozbám zabývají odborná pracoviště (universitní platformy, včetně tzv. think-tanků), jejichž provázanost se státními orgány bývá tradičně vysoká:

- Středisko pro bezpečnostní studia (Centre for Defence Studies, CDS)[15];
- Institut pro bezpečnostní studia spojených služeb království (Royal United Services Institute for Defence Studies)[16];
- Universita Sussex (Science and Technology Policy Research, SPRU)[17];
- Wilton Park[18].

Možné snížení materiálních nákladů na bezpečnostní výzkum – Inspirace ze Spojeného království[19]

V červenci 1998 se Ministerstvo obrany Spojeného království (Ministry of Defence, MOD) začalo zabývat myšlenkou na progresivní snížení nákladů svého chodu. Jednou z kapitol, kde byla potřeba úspor největší, byla oblast technologického výzkumu a vývoje. Od počátku bylo jasné, že se řešení bude hledat v těsné součinnosti s dosud největším spolupracovníkem resortu v oblasti vojenského výzkumu, firmou DERA.

DERA (The Defence Evaluation and Research Agency, Agentura pro obranné vyhodnocování a výzkum) v té době zaměstnávala na 11 500 osob a její roční obrat činil okolo jedné miliardy liber. Pozice firmy v oblasti vědy, výzkumu a výroby z ní činila vedoucí sílu v oboru v zemi a přirozeného spojence ozbrojených sil. Firma byla majitelem několika výzkumných laboratoří a jiných zařízení po celé zemi a zaměstnávala špičkové odborníky ve svém oboru. DERA se postupně stala největším příjemcem vládních grantů pro vojenský výzkum a vývoj. DERA vždy zadání náležitým způsobem splnila.

V září 1998 proto MOD ustanovilo komisi pro analýzu možností úspor, jejímž cílem bylo zajistit, aby státní sféra maximálně profitovala z nastolení „soutěživých mechanismů“ v oboru vojenského výzkumu. Studovány byly možnosti a mantinely případného veřejno-soukromého partnerství, které by spojovalo přednosti státního a soukromého sektoru. Řešeny byly kompetenční spory, financování, případné pojišťování zaměstnanců soukromé firmy z veřejných zdrojů atd.

Dne 24. července 2000 se obě strany rozhodly pro následující řešení: bude zajištěna nezávislost většinové části původní firmy a státní rozpočet ušetří. Byl zahájen proces rozdělování firmy DERA, který skončil 1. července 2001. Počínaje 2. červencem 2001 vznikly místo dosavadního jednoho dva oddělené subjekty:

- QuinetiQ (soukromá firma) zaměstnává 9 000 osob. Personální obsazení firmy závisí zcela na majitelích. Firma je nezávislá na státním rozpočtu. Patenty jsou majetkem firmy. Audit je vnitřní věcí firmy. MOD je odběratelem asi 2 % produkce.
- DstL (částečně soukromá firma) zaměstnává 3 000 osob. MOD může zasahovat do personálního obsazení firmy, nařizovat bezpečnostní prověrky jejího personálu. Firma je napojena na státní rozpočet. Patenty jsou majetkem MOD. MOD je odběratelem 90 % produkce firmy, jako hlavní zákazník disponuje nadstandardními právy. Firma je povinná přijímat kontrolu MOD, aby nedocházelo k nehospodárnému zacházení z penězi státního rozpočtu.

Firma DstL a její subdodavatelé jsou od té doby integrováni do struktury a rozpočtu ministerstva. Asi polovina projektů, které jsou DstL od státu zadány, je jinde nezpeněžitelná a tato skutečnost je podmínkou kontraktu. To firmu omezuje, ačkoli ji plnění úkolů stojí mnoho úsilí a prostředků. Výsledné řešení, „zpolostátnění“ organizace a její dofinancovávání ze státního rozpočtu, je ve výsledku čestným řešením pro obě strany. Ministerstvo obrany je hlavním zákazníkem DstL (na druhou stranu je DstL jediným možným dodavatelem některých zakázek resortu). Zvolená velikost firmy je nezbytná pro zvládnutí řešených úkolů.

- Pro stát je firma nezbytná, aby udržel krok v inovaci technologií pro svou potřebu.
- Tím, že se stát spojí se soutěživým prvkem soukromého sektoru, se ušetří zdroje a zefektivní celý proces.
- Stát tak ihned získá již vyškolené odborníky. Lidské zdroje na takové úrovni by stát nedokázal vytvořit, respektive v žádném případě ne tak rychle a relativně levně.
- Prostředky, které jsou do této činnosti státem vloženy, se vyplatí. Zkrátí se časové prodlevy mezi výzkumem a jeho aplikací ve prospěch státu.

Záměr Ministerstva obrany soustředit všechny tyto kapacity do víceméně jednoho celku by se mohl zdát nebezpečný, ale DERA a DstL za léta spolupráce dokazují že důvěru zaslouží. Výhrady vůči tomuto spojení nejsou ostatně zaměřeny na to, že by firma DstL nebyla dostatečným garantem bezpečnosti dat z prostředí Ministerstva obrany, ale na to, že tento kontrakt je natolik exkluzivní, že vzbuzuje zdání monopolu. Protiargument MOD je následující: V oblasti dílčích dodávek může kterýkoli malý subjekt DstL snadno předčít. Neustálá soutěživost nedovolí ani DstL ustrnout.

SPOLKOVÁ REPUBLIKA NĚMECKO

Klíčovým subjektem v uvedené oblasti je **Spolkový úřad pro bezpečnost v informační technice** (Bundesamt für Sicherheit in der Informationstechnik, BSI).[20]

- Na do té doby roztříštěné aktivity v oblasti bezpečnostních otázek, spojených s moderními technologiemi dohlížela od roku 1986 „Ústřední agentura pro šifrování“ (Zentralstelle für das Chiffrierwesen, ZfCh). Jednalo se spíše o instituci, jejíž hlavní úkoly spočívají v oblasti bezpečnosti systémů, nakládajících s utajovanými skutečnostmi.
- Roku 1987 byla pod vedením spolkového ministra vnitra vytvořena meziresortní komise pro bezpečnost informačních technologií.
- Roku 1989 byla Ústřední agentura pro šifrování přetvořena v „Ústřední agenturu pro bezpečnost informačních technologií“ (Zentralstelle für Sicherheit in der Informationstechnik, ZSI).
- V roce 1990 (17. prosince 1990) byl formou rozšíření výše uvedené Agentury zákonem založen Spolkový úřad pro bezpečnost v informační technice.
- K datu 1. srpna 2001 byl Úřad výrazně organizačně přeskupen a personálně posílen.

Úřad je organizačně koncipován jako složka v rámci Spolkového ministerstva vnitra. Cílem, který vedl k vytvoření Úřadu, je ve všeobecném smyslu slova „ochrana informací a komunikace“ v rámci Spolkové republiky. Mezi klíčové činnosti Úřadu patří:

- Informování státních i soukromých subjektů, stejně jako nejširší veřejnosti o hrozících rizicích a aktuálním bezpečnostním vývoji, v kybernetickém prostředí (včetně funkce CERT-DE).
- Poradenství pro libovolné zainteresované subjekty.
- Vědecko-výzkumné aktivity (hardware a software).
- Úkoly v oblasti e-governmentu (elektronizace úřední agendy).
- Certifikace systémů (s důrazem na oblast nakládání s utajovanými skutečnostmi).
  Provozování vazeb mezinárodní spolupráce se svými protějšky v zahraničí.

Služby Úřadu jsou určeny jak federálním orgánům, tak orgánům spolkových zemí, soukromým firmám a nejširší veřejnosti.

Roku 2005 celkový rozpočet Úřadu činil bezmála 52 milionů eur (z toho 20 milionů na mzdy). Na konci roku 2005 BSI zaměstnávala cca 450 osob (převažují technické obory, ale je zde uplatnění i pro absolventy oborů přírodní vědy, právo, hospodářství, sociální vědy).

Mezi principy fungování Úřadu jsou vyzdvihovány týmová práce, průhlednost, nezávislost, schopnost rychlé reakce, pružnost, orientace na zákazníka, sdílení informací a celoživotní vzdělávání personálu.

Není bez zajímavosti, že Úřad byl roku 2005 ohodnocen jako v pořadí 8. ze 150 institucí v zemi, zabývajících se informačními technologiemi, co se týče atraktivity pro nové absolventy (IT-Absolventenbarometer). Podobných výsledků dosáhly soukromé firmy jako Siemens, IBM nebo Microsoft).

V průběhu roku 2006 byla, za metodického vedení Úřadu, zahájena iniciativa Německa po linii Evropské unie, nazvaná „**Check the Web**“. Jejím cílem je posílení spolupráce mezi jednotlivými zeměmi Unie, která by zabránila duplikaci konkrétních aktivit, zaměřených na boj proti kybernetickým ohrožením.[21]

NIZOZEMÍ

Základním dokumentem, který se v rámci Nizozemí věnuje problematice kybernetické bezpečnosti, je **„Strategie pro boj proti zneužívání Internetu pro extremistické a teroristické účely“** (Strategy for Combating the Use of the Internet for Radical and Terrorist Purposes). V jejím rámci je konstatováno, že klíčovým fenoménem dneška je geometrický růst výskytu „diskusních fór“ extremistů, které jim umožňují plánovat akce bez toho, aby se fyzicky scházeli nebo ohrozili svou anonymitu. Zároveň roste počet internetových stránek v holandštině, obsahujících „radikální“ rétoriku, jejichž autoři jsou zpravidla imigranti z muslimských zemí, kteří již holandštinu ovládají lépe, než jakýkoli jiný jazyk.[22] Vedle stránek, naplňujících konkrétní skutkové podstaty trestního zákona existuje řada příspěvků, které jsou sice z bezpečnostního hlediska „nežádoucí“, ale jejichž zveřejňování a šíření nelze podle platného práva omezovat.

Strategie je v první řadě zaměřena na zneužití Internetu jako prostředku pro výměnu a šíření nežádoucích informací (včetně propagandy). Přitom se trvale zvyšuje důraz na problematiku prevence zneužití Internetu jako zbraně (například útoky na sítě a subjekty v rámci kritické infrastruktury státu).

Současné politické a expertní diskuse se již zabývají praktickými aspekty takových kroků, jako je zneprovoznění domácích a filtrování zahraničních internetových stránek, stejně jako postihy autorů konkrétních příspěvků a správců sítí. Toto téma bylo přitom ještě donedávna v Nizozemí „tabu“. Totéž platí o snahách o tzv. samoregulaci poskytovatelů prostoru na Internetu (providerů). Oficiální materiály vlády tak: „vybízí providery aby byli více proaktivní a více odpovědní s ohledem na služby, které poskytují“.

Z praktických kroků je třeba uvést v roce 2006 zřízení **Národního hlásného střediska pro kybernetický zločin** (Meldpunt, Nationel Cybercrime Reporting Centre).[23]

Jedná se o středisko, spravované policejními složkami, kterému kdokoliv může nahlásit svá zjištění o aktivitách v kyberprostoru, které považuje za jakkoli závadné.

Policisté dále rozhodnou, zda případ spadá do jejich kompetence, případně jej předají dalším subjektům (státní zastupitelství, zpravodajské služby).

Vedle uvedené policejní platformy existují v Nizozemí i dva nevládní projekty, v obou případech do značné míry financované granty Ministerstva spravedlnosti.

- **Horká linka proti diskriminaci v rámci Internetu** (Meldpunt Discriminatie Internet, MDI), je zaměřená na boj proti „diskriminujícímu“ obsahu na Internetu (diskriminace žen, národností atd.).
- **Horká linka pro nahlašování dětské pornografie** (Meldpunt Kinderporno op het Internet, MKI), soustřeďující podněty od osob, které zaznamenaly výskyt dětské pornografie.

Po linii Evropské unie (spolupráce s tzv. třetími zeměmi) je Nizozemí aktivní zejména s ohledem na Maroko (odkud pochází několik desítek tisíc imigrantů v Nizozemí, a to zejména těch, kteří jsou nejvíce náchylní k radikalizaci či k rekrutování do teroristických struktur). V průběhu roku 2006 proběhl v Maroku terénní výzkum, podpořený vládou Maroka, zaměřený proti zneužívání Internetu k teroristickým účelům.

ITÁLIE

V Itálii spadá problematika boje s informační kriminalitou do kompetence zvláštní policejní složky, tzv. **Policie pošt a komunikací** (Polizia Postale e delle Comunicazioni, „poštovní policie“).[24] Ředitelství poštovní policie je zařazeno do tzv. Odboru veřejné bezpečnosti (Dipartimento di Pubblica Sicurezza), což je jeden z odborů (sekcí) italského Ministerstva vnitra, v jeho čele stojí generální ředitel pro otázky veřejné bezpečnosti, jenž je současně ředitelem italské státní policie.

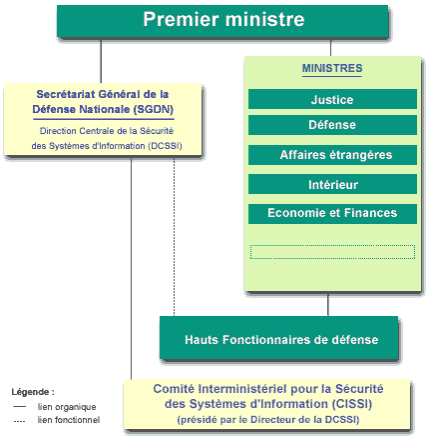
Složka byla vytvořena zákonem z roku 1981 (o reformě státní policie). Dalšími právními normami, jež upravují její statut a činnost, jsou dekret ministra vnitra z 31. března 1998 a následně meziministerský dekret z 19. ledna 1999, kterým byla tato policejní složka označena za ústřední orgán státu pro bezpečnost a zákonnost telekomunikačních služeb.

- Úkolem Složky je sledovat dodržování zákonů v oblasti telekomunikací a využívání informatických technologií a bránit jejich zneužití k nelegální činnosti. Poštovní policie provádí (zejména prostřednictví své internetové stránky) aktivní osvětovou činnost, zejména v oblasti boje s internetovou pedofilií. Nelegální činnost na Internetu mohou občané poštovní policii hlásit přímo prostřednictvím elektronické pošty („komisařství on line“).
- Složka se člení na centrální službu (ředitelství) se sídlem v Římě, dále pobočky v Neapoli, přičleněné k Úřadu pro garanci telekomunikací, 19 regionálních oddělení a 77 oddělení v provinciích, jež zajišťují rovnoměrné pokrytí celého území Itálie. Centrální služba složka je členěna následujícím způsobem:

    - sekce koordinace;
    - sekce pro boj proti útokům na informatické systémy;
    - složena ze skupiny expertů – vyšetřovatelů a specializovaných techniků (tito experti se nevěnují pouze vyšetřování, ale i studiu nových technik zásahů do sítí, zejména prostřednictvím sledování specializovaných chatů);
    - sekce pro ochranu copyrightu;
    - zaměřena na boj proti šíření nelegálního softwaru, proti zneužívání telefonní sítě k podvodným (zejména mezinárodním) telefonním hovorům, na ochranu rozhlasového vysílání respektive proti nelegálnímu/pirátskému audiovisuálnímu vysílání;
    - sekce pro boj s pedofilií na Internetu;
    - sekce pro potlačování nelegální činnosti spojené s elektronickým obchodem.

- V rámci poštovní policie působí celkem 2 000 osob, a to zejména vysoce kvalifikovaných specialistů a techniků, ale i nezbytného administrativního personálu. Velká pozornost je věnována i průběžnému vzdělávání personálu (doplňující kurzy, tématické semináře a konference doma i v zahraničí, stáže u zahraničních kolegů atd.).
- Vzhledem k tomu, že se jedná o plně státní složku, je činnost poštovní policie financována z prostředků státního rozpočtu.
- Určité servisní funkce pro poštovní policii vykonává tzv. Vědecký poradní výbor, který sdružuje universitní odborníky v oblasti informačních a komunikačních technologií, kteří bezpečnostním složkám (údajně zdarma) poskytují odbornou pomoc a specializované konzultace.

FRANCIE



Boji proti konkrétním aspektům kybernetických ohrožení se ve Francii věnuje několik desítek subjektů.[25] Každé ministerstvo zodpovídá za ochranu svých vlastních sítí a kritických infrastruktur. Technickou stránku koordinace celého procesu zajišťuje **Ústřední služba pro bezpečnost informačních systémů** (Service Central pour la Sécurité des Systemes ďlnformation – SCSSI).[26] Vzhledem k růstu významu SCSSI se dokonce zvažuje její institucionální osamostatnění s vlastním rozpočtem a početnějším personálem. Počet pracovníků SCSSI se odhaduje na cca 100 osob.[27]

Hlavní roli v uvedené oblasti ve Francii sehrává armáda, konkrétně **Generální sekretariát národní obrany** (Secrétariat Général de la Défense Nationale – SGDN).[28]

V současnosti údajně nejméně polovina případů, jimiž se SGDN zabývá, obsahuje ve větší či menší míře aspekt bezpečnosti informačního systému Francie.

V květnu 1999 byla sekce SGDN, nazvaná „Obrana a stát“ reorganizována a nahrazena sekcí **„Ochrana a bezpečnost státu“**.[29] V rámci této sekce od července 2001 existuje **„Oddělení pro bezpečnost ústředních informačních systémů“** (Direction centrale de la sécurité des systèmes d'information, DCSSI)[30]. To sehrává ústřední roli při kontrole bezpečnostních systémů v rámci státní služby ve Francii, jejichž instalování probíhalo souběžně s napojením státní správy na Internet. DCSSI provozuje i CERT-FR (CERTA). Formální zastřešení celé agendy spadá pod **Meziministerský výbor pro bezpečnost informačních systémů** (Comité Interministériel pour la Sécurité des Systemes ďlnformation, CISSI), v jejímž čele stojí ředitel DCSSI.

Počínaje rokem 2001 probíhá ve Francii řada celonárodních cvičení ke zvýšení kvalifikace hlavních operátorů vládních sítí (minimálně tři ročně).

ŠPANĚLSKO

Oblast kybernetických hrozeb zatím nepatří mezi výslovné priority bezpečnostní politiky ve Španělsku. V zemi v současnosti neexistuje žádný subjekt, který by byl přímo odpovědný za problematiku kybernetické bezpečnosti v celé její šíři. Problematikou kybernetických hrozeb se zabývá jeden policejní útvar v rámci policejního Vysokého komisařství pro informace. Tento Útvar zaměstnává pouze 4 osoby, jeho finanční zdroje pocházejí z rozpočtu Policie. Vládu Útvar o své činnosti informuje na její vyžádání, popř. z vlastní iniciativy, nejedná se však o periodickou činnost. Útvar přímo nespolupracuje s žádnou z dalších bezpečnostních složek státu, činí tak pouze v případě žádosti jedné ze stran, ty jsou však sporadické.[31]

RAKOUSKO

Rakousko neprovozuje žádnou platformu, kterou by bylo možné označit za středisko pro boj s kybernetickými hrozbami.

- Daná problematika je řešena oddělením v rámci spolkové kriminální policie, které se zabývá všemi formami počítačových deliktů: stahováním peněz z účtů klientů bank a spořitelen počínaje a dětskou pornografii konče.[32]
- Podle §7 zákona o informační bezpečnosti (Informationssicherheitgesetz – InfoSIG) je každé spolkové ministerstvo povinno zřídit nejméně dvě systemizovaná místa pro bezpečnostní techniky v oblasti informačních technologií.
- Byla rovněž vytvořena příručka, věnovaná problematice bezpečnosti informačních technologií, kterou jsou povinna se řídit všechna pracoviště Spolkového ministerstva vnitra (BM.I). V rámci struktury Ministerstva působí i „**Tým bezpečnostního managementu**“ (Sicherheitsmanagement-team) jehož úkolem je – mimo jiné – analýza rizik i vypracování a realizace návrhů, zamřených na ochranu informačních a komunikačních technologií v rámci resortu.

Pro úplnost je třeba dodat, že právní řád (Trestní zákoník) Rakouska již v současnosti obsahuje konkrétní skutkové podstaty trestných činů, které lze výkladem aplikovat i na kybernetické prostředí:

- §12: výzva ke konkrétnímu zločinu (incitement);
- §15: příprava trestného činu;
- §282: výzva ke zločinu, obecně (pobuřování, výzvy, zaměřené proti určitým skupinám obyvatelstva);
- §283: schvalování trestných činů (agitace).

IRSKO

V Irsku neexistuje specializovaný subjekt zabývající se kybernetickými hrozbami, respektive jejich potíráním. Téma obecně spadá do kompetence Ministerstva spravedlnosti (v jehož rámci jsou systemizovány věcně příslušné policejní a zpravodajské složky, které se danou problematikou rámcově zabývají).[33] CERT-IE, vybudovaný na akademické půdě, se zaměřuje zejména na zvyšování „počítačové gramotnosti“ mezi nejširší veřejností (s cílem napomoci budování „hospodářství, založeného na znalostech“ – knowledge based economy).[34]

DÁNSKO

V zemi neexistuje samostatný subjekt zabývající se kybernetickými hrozbami. Zástupci ústředních státních orgánů se pravidelně scházejí se zástupci průmyslového odvětví k dané problematice.[35] CERT-DK byl vytvořen roku 1991, jako jeden z prvních CERT ve světě (bezprostředně inspirován vzorem z USA).

DK•CERT

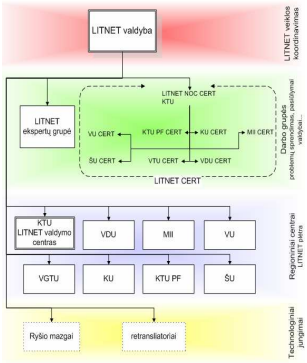
Platforma je přidruženou agenturou Státního střediska pro výzkum v oblasti informačních technologií, financovanou Ministerstvem vzdělávání.

ŠVÉDSKO

Ve Švédsku není zřízeno samostatné centrum pro boj s kybernetickými hrozbami. Je však možné, že některé nedávné kybernetické incidenty (on-line sbírky pro financování kurdských bojových skupin v Iráku; útoky na webové stránky některých domácích politických stran; hospodářská špionáž v síti koncernu Ericsson nebo snahy o napadení vojenských serverů atd.) tuto situaci změní (viz určité vize, obsažené ve Strategii pro bezpečnost Internetu, která byla ve Švédsku zveřejněna v červenci 2006). Zatím nicméně v uvedené oblasti sehrávají klíčovou roli následující subjekty:

- **Švédská bezpečnostní služba** (Säkerhetspolisen – SÄPO)[36], která je součástí státní policie a do jejíž působnosti náleží ochrana ústavního pořádku, včetně boje proti terorismu na domácí půdě a zajišťování mezi-agenturní spolupráce s dalšími bezpečnostními orgány (v rámci Ministerstva obrany). V rámci SÄPO se tématu boje proti kybernetickým hrozbám věnuje Ochranná bezpečnostní jednotka (Protective Security Unit).[37] Tato větev řeší incidenty, které mohou ohrozit národní bezpečnost.
- **Policejní jednotka S-BIT** v rámci Národního úřadu trestního vyšetřování Policejního prezídia. Po této linii se řeší apriori kriminální případy (bez politického podtextu).
- Určité úkoly v dané oblasti plní i CERT-SE (SITIC)[38], tedy těleso, stojící na základech akademického sektoru, stejně jako konkrétní soukromé i polostátní subjekty (operátoři, provideři, asociace výrobců).

LITVA



V právním řádu Litvy existuje celé spektrum ustanovení, zaměřených na boj proti kyberzločinu (zákaz propagace rasové, národnostní či náboženské diskriminace, výzvy k protiprávnímu jednání v rámci Internetu atd.).

V Litvě zatím neexistuje subjekt, který by se zabýval speciálně kybernetickými hrozbami. Výhledově není žádná změna v této oblasti plánována (a to i s ohledem na skutečnost, že v zemi nebyly údajně zaznamenány žádné závažné kybernetické incidenty).[39] CERT v zemi provozuje akademická platforma **LITNET**[40]. Problematika boje proti kybernetickým ohrožením v rámci Litvy nyní rámcově spadá zejména do působnosti následujících subjektů:

- **Státní bezpečnostní úřad** (Valstybės Saugumo Departamentas, VSD; State Security Department, SSD),[41] jehož hlavním úkolem je „ochrana suverenity Litvy a jejího ústavního systému“. To v praxi obnáší velmi široké spektrum činností (rozvědná a kontrarozvědná činnost, ochrana utajovaných skutečností, ochrana základů národní ekonomiky a strategických objektů, socio-politická analýza a prognóza bezpečnostního vývoje státu, analýza veřejných informací, vyšetřování případů genocidy a implementace lustračního zákona). Úřad konkrétně zmiňuje svůj zájem na sledování internetových diskusních fór v litevštině, aby zamezil jejich zneužívání ze strany terorismu nebo organizovaného zločinu.
- **Policejní speciální jednotka pro boj s kybernetickou trestnou činností** (Cybercrime Unit)[42]. Jednotka vznikla roku 2001 a je integrální součástí státní policie. V současnosti je náplň činnosti Jednotky zaměřena na implementaci mezinárodní Úmluvy o kyberzločinu, ke které se Litva připojila roku 2003 (s účinkem od ledna 2004). Jednotka působí v oblasti prevence, vyšetřování a odhalování trestných činů, které byly naplánovány a spáchány pomocí Internetu nebo v uzavřených sítích (Intranetu).

ESTONSKO

Otázky kybernetických hrozeb respektive boje proti kybernetickému terorismu v Estonsku dílčím způsobem řeší několik orgánů státní správy (respektive dalších organizací).[43]

- **Bezpečnostní policejní sbor** (Security Police Board, SPB), což je přidružená (zpravodajská) agentura, podřízená ministru vnitra. Sbor se zabývá především sběrem informací, prováděním bezpečnostních a průzkumných operací, hodnocením informací a rizik, předběžným vyšetřováním a dalšími podobnými aktivitami. Úkolem Sboru je i předcházet teroristickým útokům v Estonsku a přispívat v mezinárodním měřítku protiteroristickým aktivitám.
- **Estonské středisko informatiky** (Estonian Informatics Centre) se zabývá mimo jiné zvyšováním povědomí o kybernetických hrozbách a je odpovědné za fungování CERT-EE[44]. Středisko se zabývá bezpečnostními incidenty v počítačových sítích v Estonsku, provádí preventivní opatření k zamezení takovým incidentům a přispívá k povědomí veřejnosti o otázkách bezpečnosti v rámci Internetu. Středisko zabezpečuje podporu a pomoc systémovým a síťovým administrátorům, organizacím a providerům Internetu, přičemž úzce spolupracuje s dalšími subjekty v rámci veřejného i soukromého sektoru.
- Organizace „**Look at World Foundation**“ je nadací, která se zaměřuje na širokou veřejnost s informacemi o bezpečném používání Internetu (provozuje internetový portál k tématu bezpečnostních aspektů používání informačních technologií).

LOTYŠSKO

V Lotyšsku se bojem proti informační kriminalitě zabývá zejména státní policie, konkrétně **Samostatné oddělení pro boj proti kybernetické kriminalitě** v rámci Správy ekonomické policie.[45]

- Oddělení v plném rozsahu provádí funkce procesní i operativní vyšetřování (výzvědnou službu), ale jen ve spojení s vyšetřování konkrétní trestné činnosti (tedy nikoli proaktivně).
- Oddělení je systemizováno pro 7 osob, u kterých je předepsána bezpečnostní prověrka. Stav oddělení však není zpravidla naplněn (v polovině roku 2006 zde sloužili jen 3 policisté).
- Oddělení na vyžádání poskytuje konzultace pro další policejní součásti.
- Výsledky činnosti Oddělení jsou dle potřeby prezentovány policejním odborem public relations.

SLOVINSKO

Ve Slovinsku neexistuje samostatný institut pro boj s kybernetickými hrozbami. V rámci Ministerstva vnitra se touto problematikou zabývá policejní útvar, odpovědný za kriminalistickou analýzu a boj proti informační kriminalitě.[46] CERT v zemi provozuje akademická platforma **Akademická a výzkumná síť Slovinska** (Akademska in Raziskovalna Mreža Slovenije, ARNES).[47]

Jeden ze subjektů, sdružených v ARNES (Fakulta sociální věd, Fakulteta za družbene vede) provozuje kampaň „Klikej bezpečně“ (Drukaj varno), zaměřenou na propagaci náležitého chování v rámci kyberprostoru.

ŘECKO

Tématem boje proti kybernetickým ohrožením se zabývá Ministerstvo veřejného pořádku. V rámci policejních složek je problematika řešena obecně v rámci **Ředitelství pro veřejnou bezpečnost**, které řídí činnost operačních útvarů policie na národní úrovni. Ředitelství tvoří 4 oddělení – oddělení zločinů, oddělení hospodářské kriminality, drogové oddělení a analytické oddělení.[48]

Oddělení hospodářské kriminality se mj. zabývá také kriminalitou, při které jsou využívány elektronické prostředky. Na základě ustanovení trestního zákona č. 100/2004 byla zřízena v rámci ředitelství pro bezpečnost **v Athénách** (pro širší oblast Attiky) **a v Soluni** (pro Makedonii) **oddělení pro elektronickou kriminalitu,** která jsou kompetentní pouze v daných krajích. Zmíněná oddělení monitorují internetovou síť a informují nadřízené složky.

Výše uvedená oddělení disponují pro tento účel odpovídajícím personálním, materiálním i technickým vybavením. V oddělení pro elektronickou kriminalitu ředitelství pro bezpečnost v Athénách pracuje konkrétně 18 policistů, ve stejném oddělení v Soluni 6 policistů.

Výsledky činnosti zmíněných oddělení jsou součástí celkové zprávy o stavu organizovaného zločinu v zemi. Zpráva je vydávána vždy v květnu a je předkládána parlamentu. Zpráva je povinně zasílána rovněž Europolu.

KYPR

Na Kypru neexistuje žádná instituce, která by se plně zaměřovala na boj s kybernetickými hrozbami. Dané definici se nejvíce blíží **Zvláštní tým pro terorismus**, vytvořený v rámci Policie Kyperské republiky. V současné době se zvažuje vytvoření samostatného týmu pro kybernetické trestné činy. Posouzením potřebnosti takto specializovaného útvaru Policie byla pověřena Policejní akademie ve spolupráci s dalšími akademickými subjekty v zemi.[49]

POLSKO

Oblast kybernetické bezpečnosti (tzv. bezpečnost komunikační infrastruktury) byla v Polsku jako výslovná priorita národní bezpečnosti stanovena roku 2000. Do roku 2002 trvaly o tématu odborné diskuse v relativně velmi úzkém kruhu specialistů. V roce 2002 byla z rozhodnutí premiéra vytvořena pracovní skupina, která se zabývala definicí a tvorbou terminologie, určením rozsahu kritické infrastruktury, analýzou situace a poté i tvorbou návrhů na její řešení.

Toto rozhodnutí bylo součástí plánu práce **Agentury vnitřní bezpečnosti** (Agentura Bezpieczenstwa Wewnetrznego, ABW – polská kontrarozvědka, plnící navíc úkoly, obdobné Národní bezpečnostní úřad v České republice[50]) na rok 2003. Od roku 2004 je zástupce ABW (**Oddělení telekomunikační bezpečnosti**, Departament Bezpieczenstwa Teleinformatycznego, DBTI) místem koordinujícím všechny aktivity v uvedené oblasti a jeho zástupce stojí v čele týmu pro ochranu národní kritické informační a telekomunikační infrastruktury (tým **KSOKITI**)[51]. V současnosti existují v Polsku dva prvky systému, které jsou v pokročilém stádiu rozvoje:

- Dohledový systém Arakis (Agregace, analýza a klasifikace incidentů na síti), zprovozněný na podzim 2006, který plní roli systému včasného varování (EWS) v případě kybernetických incidentů. Systém je doplněn řídícím systémem, umožňujícím reagovat na případné změny v datovém toku přenášeném síťovou infrastrukturou. Jedná se o komplexní řešení, vyvinuté domácími specialisty z ABW, v úzké spolupráci s akademickým a soukromým sektorem, napojeným na tzv. CERT (Systém výstrahy při ohrožení kyberprostoru, Centrum Emergency Response Team). Základem systému Arakis je síť senzorů, které jsou umístěny na klíčových rozhraních síťové architektury, které nepřetržitě hlídají její provoz.
- Ve fázi ukončení projektu a počátku konstrukčních prací je vznik Technického a koordinačního centra v rámci kontrarozvědky (ABW). Tento projekt je uskutečňován v úzké spolupráci s NATO. Těleso bude plnit roli ve vnitrostátní výměně informací a mezinárodní komunikaci s obdobnými tělesy v rámci zemí NATO i Evropské unie (Evropská agentura pro síťovou a informační bezpečnost; European Network and Information Security Agency, ENISA). S uvedením Centra do plného provozu se počítá v prvním pololetí roku 2007.
- Na projektech se dohromady podílí asi 30 expertů „na plný úvazek“. Část je z ABW a část z akademické sféry. Jejich bezpečnostní prověrky jsou většinou na úrovni TAJNÉ a PŘÍSNĚ TAJNÉ. Externě je do aktivity zapojeno několik stovek lidí. Jedná se zejména o vysoce specializované vysokoškolsky vzdělané lidi (převažuje vzdělání technického směru: specialisté na operační systémy, síťové protokoly a další).

Projekty jsou financovány ze státního rozpočtu (rozpočtu ABW). S projektem je spojeno i využívání dalších součástí ABW, jako jsou výzkumné laboratoře, aktivní v oblasti kryptografie a možného využití (boje proti zneužití) elektromagnetického záření na počítačové systémy.

S komerčními aktivitami (placené služby pro komerční firmy) se výhledově počítá po vybudování celého systému. Samofinancování zatím neexistuje, neboť není co prodávat a také není jasné jak. Roční rozpočet se pohybuje v tomto období (náběh projektů) kolem 2 milionů eur za rok, pro běžný provoz se počítá s asi 1,5 milionu eur ročně. Ani samofinancování, ani komerční aktivity nejsou zatím provozovány a vše je řízeno přímo zpravodajskou službou. Se zveřejňování věcí patřících do oblasti veřejné služby (výstrahy, nastavení, doporučení, incidenty) nenastal zatím žádný závažnější problém. Obě základní domény: utajovaná (vládní síť) a neutajovaná (Internet) jsou na fyzické úrovni striktně odděleny.

Hlavním subjektem, který v Polsku provozuje CERT, jsou správci tzv. **Vzdělávací a akademické počítačové sítě** (Naukowa i Akademiczna Siet Komputerowa, NASK).

Jedná se o akademické pracoviště, které začalo se zaváděním Internetu v Polsku. Celý projekt je také dobře zapojen do mezinárodní spolupráce. Vedoucí představitelé NASK jsou rovněž velmi aktivní ve vedení ENISA.

MAĎARSKO

V Maďarsku v současnosti působí (na základě požadavku Ministerstva informatiky a komunikací) dva „konkurenční“ týmy, plnící úkoly CERT (CERT-EK, Hun-CERT):[52]

- NIIF-CSIRT. Relativně méně důležitý tým, spojený se sítí NIIF/HUNGARNET, propojující nejdůležitější akademická pracoviště v zemi (university, výzkumné ústavy a některé nevládní instituce). Tým se zabývá pouze incidenty v síti HUNGARNET.[53]
- CERT-Hungary. Jedná se o tým, sloužící nejširší veřejnosti, stejně jako plnící konkrétní zadání vlády. Platforma je označováno za „Středisko informační bezpečnosti země“ a „vědomostní základnu pro experty, působící v oblasti informačních technologií“.[54]

    - Platformu provozuje Nadace Tivadara Puskáse (Theodore Puskás Foundation), fungující z pověření (a financovaná prostřednictvím) Ministerstva informatiky a komunikací, od 1. září 2006 pak z pověření Kabinetu premiéra. V rámci platformy působí i zástupce Ministerstva spravedlnosti (které v Maďarsku plní i funkci resortu vnitra, včetně vedení policejních složek), který je v kontaktu s orgány činnými v trestním řízení. Platforma je na základě dohody o spolupráci spojena i se zpravodajskými službami.
    - Dle systemizace má CERT 10 pracovníků s vysokoškolským a universitním vzděláním a bezpečnostní prověrkou na stupeň DŮVĚRNÉ a TAJNÉ.
    - Výsledky práce platformy jsou prezentované v informační síti vlády, avšak nejsou dostupné veřejnosti. Na veřejné síti je publikováno pouze pozadí konkrétních incidentů, ale i to zpravidla bez větších podrobností jejich dopadu.
    - Nadace Tivadara Puskáse jako taková neprovádí výzkumnou činnost v oblasti informačních a komunikačních technologií. O to větší důraz je Nadací kladen na výchovně-vzdělávací činnost (včetně tématu bezpečného chování v rámci kyberprostoru) zaměřenou na nejširší veřejnost.

- Vedle výše uvedených subjektů působí určité kapacity na informační bezpečnost i v rámci **Národního zpravodajského úřadu** (Nemzetbiztonsági Hivatal, NBH, odbor boje proti terorismu a extremismu, oddělení operativního vyšetřování)[55] a **Výzkumného institutu pro počítače a automatizaci** Maďarské akademie věd (Számítástechnikai és Automatizálási Kutató Intézet, SZTAKI)[56].

SLOVENSKO

Na Slovensku podle dostupných informací neexistuje subjekt, který by bylo možné označit za těleso, plně se věnující problematice kybernetické bezpečnosti. Děje se tak navzdory skutečnosti, že v dubnu 2006 došlo k závažnému útoku proti **Národnému bezpečnostnému úradu Slovenska**. Uvedená skutečnost získala velký mediální ohlas a vedla v listopadu 2006 k výměně ředitele Úřadu.[57]

Výše uvedený incident byl podle všeho „pomstou“ hackerů za policejní akci, zaměřenou na skupinu kolem kontroverzního serveru **onyx.sk**. Útočníci zkopírovali 36 000 e-mailů z internetové části sítě Úřadu a nakonec zablokovali servery Úřadu opakovanými žádostmi o připojení od vnějších počítačů (jedná se o způsob útoku, zvaný „DOS“, Denial of Service). Je ovšem otázkou, zda se hackerům podařilo proniknout i do utajovaných částí databáze.[58]

RUMUNSKO

Ačkoli Bezpečnostní rada schválila rezoluci k podpoře ochrany kritické infrastruktury (obsahující výslovné zmínky o nutnosti zvýšení obecného povědomí o informační bezpečnosti a vytvoření platformy typu CERT), zůstává klíčová iniciativa v dané oblasti v rámci policejních složek.[59]

V rámci Generálního inspektorátu policie existuje specializovaná organizační složka: Sekce pro boj s organizovaným zločinem. V jejím rámci působí od roku 2003 **Oddělení pro boj s informačním zločinem** (Serviciul de Combatere a Criminalității Informatice, SCCI).[60]

- SCCI se (po řadě reorganizací) v současnosti skládá z pěti referátů, zabývajících se následujícími oblastmi:[61]
    - útoky proti informačním systémům;
    - zpronevěry v elektronickém obchodu;
    - zpronevěry pomocí kreditních karet;
    - dětská pornografie;
    - technické aspekty problematiky (odposlechy, uchovávání údajů z informačních systémů).
- V rámci SCCI působí 20 pracovníků, absolventů Rumunské policejní akademie. Kromě bezpečnostních kriterií (prověrky) musí splňovat i další požadavky (znalosti v oblasti informatiky a jazykové schopnosti – preferována je angličtina a francouzština).
- SCCI rovněž koordinuje příslušné teritoriální útvary (27 regionálních středisek s 27 pracovníky a 14 nadregionálních středisek – s celkem se 14 pracovníky).
- Financování SCCI probíhá z rozpočtu policejního Generálního inspektorátu. **V rámci tzv. „programů pomoci pro prevenci informačního zločinu“ se na chodu SCCI mohou finančně podílet soukromé společnosti, zainteresované například na řešení konkrétního incidentu**. SCCI však ze své iniciativy neprovozuje žádné komerční aktivity.
- SCCI spolupracuje s dalšími policejními a zpravodajskými útvary, stejně jako se soukromým úsekem.
- SCCI neprovádí žádnou činnost v oblasti výzkumu, vzdělávání ani veřejné osvěty.

TURECKO

Klíčovou roli při zajišťování kybernetické bezpečnosti Turecka sehrávají ozbrojené síly (včetně aspektu financováním laboratoří k testování a auditu informačních technologií). CERT v Turecku dodnes slouží takřka výlučně k monitorování incidentů v rámci vojenské infrastruktury (a jeho provoz je rovněž financován z armádního rozpočtu).

Aktivnější roli v „civilním“ rozměru ochrany kyberprostoru v Turecku sehrává Národní výzkumný institut pro elektroniku a šifrování (National Research Institute of Electronics and Cryptology, TUBITAK)[62].

Důvody pro důraz na danou problematiku úzce souvisí s aktivitami kurdských skupin (ze strany Turecka označovaných za teroristické) navazující na formálně zaniklé struktury jako PKK, respektive KONGRA-GEL. „Kurdské“ subjekty provozují desítky internetových presentací, přičemž často se jedná o stránky různým způsobem „zakamuflované“. Pravidlem jsou časté změny adres, respektive providerů internetových služeb. Konkrétní stránky přitom obsahují vedle politických proklamací i velmi konkrétní návody, např. co se týče přípravy improvizovaných zbraní.

Právní řád Turecka přitom pamatuje na řadu aspektů, souvisejících s možným zneužitím Internetu pro kriminální, respektive teroristické účely:

- Trestní zákon (§243 a 244).
- Trestní řád (zákon č. 5271).
- Zákon o boji proti terorismu (zákon č. 5532 a 3713).
- Zákon o tisku (zákon č. 5187).
- V Turecku se rovněž připravuje zvláštní zákon, věnovaný ryze tématu „kybernetického zločinu“.

ARMÉNIE

Dokument **„Národní strategie bezpečnosti kybernetického prostoru“** obsahuje pět klíčových priorit země v oblasti zvyšování kybernetické bezpečnosti (včetně dotvoření dosud ne zcela plnohodnotně fungujícího subjektu typu CERT, AmCERT)[63].

Klíčovou roli v daném kontextu sehrává akademický sektor, Arménská naučno-vzdělávací síťová asociace (Армянская Научно-Образовательная Сетевая Ассоциация, APEHA)[64], založená roku 2000 a Internetová společnost Arménie (Internet Society of Armenia)[65]. Národní strategie vedle toho výslovně klade důraz na oblast vzdělávání státních zaměstnanců i širší veřejnosti o základech náležitého chování v rámci kyberprostoru.[66]

JAPONSKO

Kybernetickými hrozbami a bojem proti nim se v Japonsku zabývá více subjektů (Národní policejní agentura, Ministerstvo obrany, Ministerstvo vnitra a komunikací, Ministerstvo hospodářství, obchodu a průmyslu). Teprve v roce 2005 byly aktivity těchto subjektů podřízeny nově vytvořenému **Japonskému institutu pro kybernetickou bezpečnost** (Japan/National Cyber Security Institute, JP-NCSI, JSCI, NSCI).[67] Institut je organizační složkou japonského úřadu vlády. Do jeho čela je jmenován ředitel, který zároveň vykonává funkci zástupce (náměstka) vedoucího úřadu vlády. Jsou mu přímo podřízeni dva zástupci a jeden poradce pro informační bezpečnost. Hlavním posláním Institutu je vytvářet závazný strategicko-teoretický rámec pro práci policie a dalších informačně bezpečnostních složek. Institut se skládá z pěti oddělení:

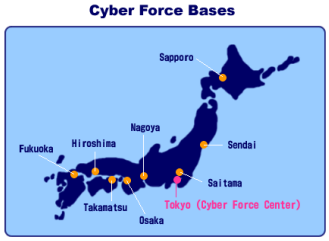
- oddělení rozvoje základních strategií;
- oddělení pro informační bezpečnost ve státní správě;
- oddělení rozvoje schopnosti adekvátní reakce;
- oddělení ochrany důležité informační infrastruktury;
- oddělení mezinárodní strategie.

- Se zpravodajskými službami Institut komunikuje přes Ministerstvo obrany, jehož jsou všechny zpravodajské služby v Japonsku součástí. Institutu nepřísluší žádné výkonné pravomoci.
- Institut je financován z prostředků Úřadu vlády, tedy ze státního rozpočtu. Konkrétní objem prostředků není zveřejňován. Samofinancování (komerční aktivity) Institutu není možné.
- Institut zaměstnává zhruba 60 osob. Jedná se nejčastěji o absolventy technických oborů a právníky. Žádná zvláštní bezpečnostní prověrka personálu není požadována. Většina pracovníků je vybírána po mnohaleté praxi na ostatních státních úřadech (při nástupu na každý státní úřad se každý pracovník podrobí zkoušce zaměřené na vědomosti a inteligenci). Institut ale může zaměstnat i odborníky ze soukromé sféry, kteří žádnou zkouškou ani prověrkou neprošli.
- Institut prezentuje veškeré zveřejňované informace na svém internetovém portálu (v japonštině).
- Konkrétní úspěšné akce nebo mimořádné události jsou prezentovány během tiskových konferencí.
- Institut nedisponuje žádným vzdělávacím střediskem. Jeho výzkumné aktivity se soustřeďují na vývoj operačního systému pro e-government. Osvěta veřejnosti probíhá pomocí Internetu, respektive prostřednictvím ad-hoc tiskových konferencí.

Operativní a vzdělávací rozměr problematiky spadá do působnosti tzv. **„Kybernetické policie“** (High-Tech Crime Technology Division, Cyber-Police, @police).[68]

Jedná se o součást Informační a komunikační kanceláře Národní policejní agentury (Info-Communications Bureau), která vznikla roku 1999 a navazuje na někdejší Útvar (později odbor) zaměřený na prevenci trestné činnosti, spáchané za použití moderních technologií (High-tech Crime Prevention Unit, High-tech Crime Prevention Department), vytvořený na počátku 90. let XX. století.

Roku 1999 bylo rovněž vytvořeno policejní technologické centrum, které mimo jiné sehrává roli technické podpory pro policejní sbory v jednotlivých prefekturách. „Kybernetická policie“ je rovněž připravena personálně podpořit prefekturní útvary při vyšetřování složitějších případů, souvisejících s kybernetickým prostředím (respektive se zapojit do případů, zasahujících do více prefektur). S tím souvisí i vytvoření mobilního týmu, připraveného k zásahu na jakémkoli místě Japonska (Cyber Force).



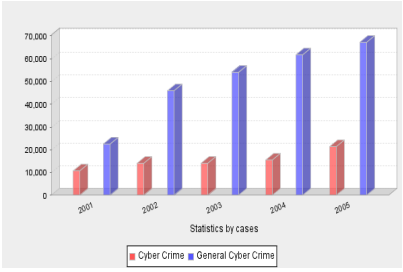
KOREJSKÁ REPUBLIKA

V Korejské republice existují dvě státní instituce zabývající se kybernetickými hrozbami.[69]

Hlavní z nich je Centrum reakce na kybernetický terorismus (CTRC) v rámci Národní policejní agentury.[70]

Jedná se o integrální součást policie. CTRC podléhá generálnímu komisaři a generálnímu řediteli úřadu vyšetřování Národní policejní agentury. Vyšetřování jednotlivých případů probíhá podobně jako u ostatních trestných činů.

- Pod CTRC spadají útvary pro vyšetřování kybernetického zločinu, které jsou součástí policejních jednotek ve 14 provinciích a 233 obcích.
- CTRC je financováno ze zdrojů Národní policejní agentury. Jeho roční rozpočet činí přibližně 3 miliony USD.
- CTRC nerealizuje žádné komerční aktivity.
- CTRC vedle policistů ve služebním poměru zaměstnává také výzkumníky. Celkový počet CTRC zaměstnanců je 63.



V rámci CTRC působí tým pro administrativu a spolupráci, vyšetřovací týmy, tým pro politiku vyšetřování, technický a asistenční tým. CTRC vydává tiskové zprávy pro domácí média, zejména v době, kdy kulminuje konkrétní ohrožení nebo jiný mediálně vděčný případ. Existuje spolupráce CTRC s Institutem pro národní bezpečnost a vyšetřování zločinů, příslušníci CTRC v rámci Institut provozují přednášky a provozují další výměnu zkušeností.

Dalším subjektem je Centrum pro vyšetřování internetového zločinu v rámci Kanceláře nejvyššího státního zástupce.[71] Vedle toho mohou mít podobné útvary zřizovat i velké soukromé společnosti.

UKRAJINA

Subjektem, který se v rámci Ukrajiny věnuje dané problematice, je tzv. **„Centrum pro výzkum počítačového zločinu“** (Computer Crime Research Center, CCRC) v rámci Národní university v Záporoží.[72]

Dle aktuálních informací se daný subjekt potýká se závažnými komplikacemi co se týče jeho financování (platforma je do značné míry závislá na sponzorování od akademických a vládních kruhů USA, Norska a Korejské republiky), respektive v souvislosti se skutečností, že špičkoví počítačoví experti z Ukrajiny hledají mnohem lépe ohodnocené působení jinde ve světě.

ZÁVĚR

Výše uvedený přehled neobsahuje všechny země, které by mohly být z uvedeného hlediska zajímavé (například Kanada, Austrálie, Nový Zéland, Izrael, Belgie, Lucembursko, Portugalsko, Finsko, Norsko, Švýcarsko, Ruská federace, Čínská lidová republika – aktuálně proslulá kontroverzními snahami o „progresivní filtrování“ Internetu, Čínská republika – Taiwan, ale i tak exotická lokalita, jako třeba Brazílie[73]). U sledovaných zemí se nepodařilo ve všech případech získat zcela srovnatelné informace. Navzdory konstatovaným slabinám je však možné dospět k následovaným obecným skutečnostem:

- V řadě zemí stála u zrodu snah o bezpečnější kybeprostor akademická pracoviště. Nezřídka se jednalo o vysoké školy, které byly aktivní už při samotném zavádění Internetu do konkrétní země. Akademické subjekty před 15 – 20 lety vlastně „investovaly“ své prostředky a personální kapacity do péče o rozvoj technologie, u které nebylo zřejmé, jakým způsobem se rozvine. Aktuální bezpečnostní úsilí je proto bez zapojení akademického sektoru (nebo alespoň absolventů konkrétních universit) v řadě zemí de facto nemyslitelné.
- V některých zemích hrají v dané oblasti hlavní (nebo důležitou) roli ozbrojené síly (Francie, Spojené státy, Turecko, Polsko – zde přinejmenším prostřednictvím grantů NATO).
- V řadě zemí existuje určitý „uzlový bod“, odpovědný za aktivity v oblasti kybernetické bezpečnosti. Pokud nevyvíjí komplexnější činnost (vědeckovýzkumné aktivity, osvěta pro nejširší veřejnost), pak alespoň určité incidenty či zjištění „třídí“ na oblast, zajímavou pro policejní složky (útoky na internetové bankovnictví, zakázané formy pornografie) a na oblast, kde sehrávají větší roli zpravodajské služby (extremistická a teroristická propaganda, snaha o snížení obranyschopnosti státu atd.).
- Silný impuls pro investování do bezpečnosti informačních a komunikačních technologií přinesl často konkrétní incident, případně kampaň okolo fenoménu Y2K, nebo, v poslední vlně, aktuální fáze tzv. „celosvětového protiteroristického úsilí“.

O to více je překvapivé, že stále nemalý počet zemí Organizace pro hospodářskou spolupráci a rozvoj, tedy nejrozvinutějších států světa, téma kybernetických ohrožení, de facto ignorují, nebo se mu věnují jen okrajově (prakticky jen vyčleněním části úvazku několika osob v rámci policejních složek).

[1] Řada autorů je ale toho názoru, že pojem CERT není zkratka, ale umělé slovo, vzniklé v komunitě počítačových nadšenců, kterému byl až později přisoudil konkrétní význam.

[2] Do 11. září 2001 nebyly přímo v USA škody, způsobené terorismem velké, respektive informační kriminalita se nechápala jako politicky motivovaná aktivita. Významnější byl v tomto ohledu boj proti zločincům se zištnými úmysly (případy neoprávněného čerpání z cizích bankovních kont).
Hillas, K., M., Dopad událostí 11. září v systému vnitřní bezpečnosti Spojených států; in: Ustavení systému komplexního řízení bezpečnosti České republiky, BOOSS, Český Krumlov 2002, str. 39-41.
http://www.dhs.gov/interweb/assetlibrary/dhsorgchart.htm
http://www.dhs.gov/index.shtm
http://www.first.gov/topics/government_performs.shtml (tato adresa uvádí výčet činností, jimiž se jednotlivé resorty zapojují do boje proti terorismu; dále se zde nachází rady pro občana, instituce, firmy atd., jak se bránit proti terorismu a chovat se v kritických situacích a nechybí ani kontakty na místní koordinátory protiteroristických opatření v jednotlivých státech Unie)
http://www.ready.gov (stránka, zaměřená na rady občanům, rodinám a firmám, nejen s ohledem na ohrožení terorismem)
http://www.us-cert.gov/
http://www.useu.be/issues/cyb0107.html (Cupp, S., L., President Clinton Announces New Plan To Fight Cyber-Terrorism, 7. I. 2000.; Ross, W., S.; Cupp, S., L., Clinton Holds Meeting on Ways to Make the Internet Safer, 15. I. 2000.)

[3] NIAC je v praxi strukturou, úzce spojenou s Národní bezpečnostní službou (National Security Agency, NSA, tzv. „Velké ucho“), aktivní v oblasti celosvětového monitoringu elektronického provozu. V mezinárodní soutěži, kterou NIAC vypsal na přelomu let 2005 – 2006 k tématu rozpoznávání jazyka se v některých kategoriích umístil na předních pozicích tým z České republiky, Fakulta informačních technologií Vysokého učení technického v Brně. I to dokazuje, že příslušné kapacity světové úrovně Česká republika nepostrádá, musí ale dbát na to, aby nedaly přednost důstojněji ohodnocenému angažmá v zahraničí. Více viz: Čechová, Š., Mladí čeští vědci slaví úspěch na mezinárodní scéně; in: ČRo 1 – Radiožurnál, 10. VII. 2006.
Bednářová, Š., VÚT v Brně uspělo s programem na rozeznávání hlasu; in: ČT 24, 10. VII. 2006.
Fila, M.; Malý, P., VÚT v Brně uspělo s programem na rozeznání hlasu; in: ČT 1, 10. VII. 2006.
„Kdopak to mluví?“, to vědí v Brně; in: LN, 12. VII. 2006.
Petrucha, D., Vědci z Brna vyvinuli program na rozpoznávání identity mluvčího; in: ČTK, 10. VII. 2006.
Počítač pozná, jakou řečí mluvíte; in: Hospodářské noviny, 23. II. 2006.
Program nejlépe na světě pozná, kdo volá; in: Rovnost - Brněnský deník, 11. VII. 2006.
Poznají hlas člověka v telefonu mezi desetitisíci volajících; in: Právo, 11. VII. 2006.
Špión z brněnské techniky; in: HN, 5. VI. 2006, str. 17, 21.

[4] http://www.whitehouse.gov/pcipb/

[5] Systémy „Digital Control Systems“ (DCS) a „Supervisory Control and Data Acquisition Systems“ (SCADA) za posledních 20 let řada zavedla společností. Systémy slouží ke kontrole klíčových procesů a funkcí kyberprostoru, jíž bylo do té doby třeba vykonávat ručně. DCS a SCADA slouží ve vodohospodářství, dopravě, energetice, zdravotnictví atd. DCS/SCADA používají Internet k přenosu dat více, než sítě pro potřeby domácností. Podíl Internetu na celkovém objemu přenosu řídících informací mezi stroji stoupá a stále bude stoupat. Takto přenesené informace jsou tudíž náchylnější ke zneužití. **Kolaps řídících systémů by znamenal pro „nekybernetické“ části kritické infrastruktury řady zemí nedozírné následky.** Úspěšný útočník by mohl převzít kontrolu nad klíčovými a vzájemně propojenými součástmi kritické infrastruktury (přehrady, vodovody, energetika, klimatizace v tunelech, letecká doprava a doprava vůbec, družicové systémy, v neposlední řadě i armáda atd.), a touto cestou buď vydírat konkrétní oběť, nebo způsobit ztráty na životech a na majetku. Zřejmý je zvláště dopad takového útoku na finanční sektor (nefungují bankomaty a bezhotovostní platby, klesne důvěra v bankovní služby, burzy, pojišťovnictví atd.). Kybernetický útok může vyvolat i exploze nebo uvolnění nebezpečných látek. Kybernetický útok velkého rozsahu by zároveň zpravidla omezil možnost využívat telefonní síť, včetně služeb tísňového volání.

[6] http://www.cmu.edu/cmnews/extra/030915_cyberpartner.html (článek k tématu propojení CERT/CC a Ministerstva pro vnitřní bezpečnost)

[7] http://www.us-cert.gov

[8] http://www.cyber.st.dhs.gov

[9] http://www.ists.dartmouth.edu

[10] Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, 31. VII. 2006; Miko, R., Velvyslanectví České republiky Londýn, 22.VIII. 2006 (č. j.: 744/2006-Londýn).
Morris, S., The Future of Netcrime Now, 2004, studie, věnovaná přehledu situace Spojeného království v oblasti počítačových hrozeb.

[11] http://www.cpni.gov.uk/methodsofattack/electronicattacks/electronic.aspx (podsekce stránek CPNI, věnovaná kybernetickým ohrožením)

[12] http://www.niscc.gov.uk

[13] http://en.wikipedia.org/wiki/serious_organised_crime_agency (encyklopedie Wikipedia k tématu SOCA)

[14] http://en.wikipedia.org/wiki/national_hi-tech_crime_unit (encyklopedie Wikipedia k tématu NHTCU)

[15] http://www.da.mod.uk/rcds

[16] http://www.rusi.org

[17] http://www.sussex.ac.uk/spru

[18] http://www.wiltonpark.org.uk

[19] http://en.wikipedia.org/wiki/dstl

[20] http://www.bsi.de/ (styčnou osobou byl jmenován pan Hansjürgen Hoeffen)

[21] Česká republika je do projektu odpovídajícím způsobem zapojena. Nelze vyloučit, že se v této fázi jedná o jedinou „novou“ členskou zemi Evropské unie, která je v projektu aktivní.

[22] National contributions to be taken into account in the preparation of the independent report on the use of the Internet for terrorist purposes and cyberterrorism; CODEXTER (2006) 38 prov, 3. X. 2006.

[23] http://www.meldpuntcybercrime.nl

[24] Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, 31. VII. 2006; Rubešová, A., Velvyslanectví České republiky Řím, 21. VIII. 2006 (č. j.: 1296/2006 Řím).
http://www.poliziadistato.it/pds/informatica/index.htm
[25] http://fiweb.9online.fr/secuforces.htm (přehled orgánů, zapojených ve Francii do problematiky boje proti kybernetickým ohrožením)
[26] http://www.ssi.gouv.fr (presentace SCSSI)
[27] SGDN in growing security role; in: Intelligence Newsletter, 4. XI. 1999, č. 369, str. 4-5.
Bulletin ÚZSI, ZSI-622/OA-99
[28] http://www.premier-ministre.gouv.fr/acteurs/premier_ministre_195/secretariat_generale_defense_nationale_328/
[29] V rámci SGDN byly ustaveny i ad hoc pracovní skupiny, jako například k tématu Y2K.
[30] http://www.ssi.gouv.fr/fr/dcssi/ (presentace DCSSI)
[31] Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, 31. VII. 2006; Bařinová, S., Velvyslanectví České republiky Madrid, 9. VIII. 2006 (č. j.: 1735/2006-Madrid).
[32] Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, 31. VII. 2006; Všetečková, N., Velvyslanectví České republiky Vídeň, 10. VIII. 2006 (č. j.: 4687/2006).
http://www.bmi.gv.at/publikationen/
National contributions to be taken into account in the preparation of the independent report on the use of the Internet for terrorist purposes and cyberterrorism; CODEXTER (2006) 38 prov, 3. X. 2006.
[33] Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, 31. VII. 2006; Vítek, M., Velvyslanectví České republiky Dublin, 4. VIII. 2006 (č. j.: 1384/2006-Dub).
[34] http://www.cert.ie
[35] Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, 31. VII. 2006; Prouza, D., Velvyslanectví České republiky Kodaň, 8. VIII. 2006 (č. j.: 677/2006 Kodaň).
[36] http://www.securityservice.se (presentace SÄPO)
[37] Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, 31. VII. 2006; Chatardová, M., Velvyslanectví České republiky ve Švédském království, 22. VIII. 2006 (č. j.: 1205/06).
http://www.sakerhetspolisen.se
http://fhs.se
[38] http://www.sitic.se/ (presentace CERT-SE)
[39] Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, 31. VII. 2006; Pospíšilová, M., Velvyslanectví České republiky v Litvě, Vilnius, 18. VIII. 2006 (č. j. 999/2006 – Vilnius)
http://www.cyberpolice.lt
http://www.vsd.lt
National contributions to be taken into account in the preparation of the independent report on the use of the Internet for terrorist purposes and cyberterrorism; CODEXTER (2006) 38 prov, 3. X. 2006.
[40] http://www.litnet.lt
[41] http://www.vsd.lt/default.asp (presentace VSD)
[42] http://www.cyberpolice.lt/ (presentace Kybernetické policie Litvy)
[43] Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, 31. VII. 2006; Zastupitelský úřad České republiky Tallinn, 21. VIII. 2006 (č. j.: 933/2006-TALL)
http://www.ria.ee
http://www.arvutikaitse.ee (portál IT Security, jen v estonském jazyce)
http://www.kapo.ee/eng_terrorism.html
http://www.kapo.ee
[44] http://www.ria.ee/
[45] Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, Zastupitelský úřad České republiky v Rize, 31. VII. 2006 (č.j.: 432/2006).
[46] Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, 31. VII. 2006; Pořízová, V., Velvyslanectví České republiky Lublaň, 7. VIII. 2006 (č. j.: 1794/2006-Lub).
[47] http://www.cert.si/
[48] Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, 31. VII. 2006; Mottlová, h., Zastupitelský úřad České republiky v Athénách, 21. VIII. 2006 (č. j.: 5523/2006-Ath).
[49] Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, 31. VII. 2006; Zastupitelský úřad České republiky Nikósie, 17. VIII. 2006 (č. j.811 /2006-Nico).
[50] Národní bezpečnostní úřad v České republice ostatně s platformou udržuje úzké styky (kontaktní osobou je zástupce ředitele Úřadu, Ing. Jaroslav Šmíd)
[51] Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, 31. VII. 2006; Posolda, V., Velvyslanectví České republiky Varšava, 10. VIII. 2006 (č. j.: 6778/2006).
http://www.abw.gov.pl/
Kotajná, L., Zpráva z pracovní cesty: „Cyber Security Dimensions of Critical Infrastructure Protection“, Marshall Center, München, 24. – 28. X. 2005. (http://www.marshallcenter.org - podsložka „conferences“)
http://www.nask.pl (ústřední doménový správce v Polsku)
http://www.cert.pl (CERT – polština, angličtina)
[52] Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, 31. VII. 2006; Opělová, M., Velvyslanectví České republiky Budapešť, 22. VIII. 2006 (č. j.: 6997/2006)
Kotajná, L., Zpráva z pracovní cesty: „Cyber Security Dimensions of Critical Infrastructure Protection“, Marshall Center, München, 24. – 28. X. 2005. (http://www.marshallcenter.org - podsložka „conferences“)
http://www.ihm.hu (Ministerstvo hospodářství a dopravy – maďarština a angličtina)
http://www.neti.hu (Ministerstvo informatiky a komunikace)
http://www.neti.hu/pta.php (nadace Tivadara Puskáse)

http://www.cert-hungary.hu (jeden z CERT, působících v Maďarsku, presentace v maďarštině, angličtině a němčině)
http://www.cert.hu (jeden z CERT, působících v Maďarsku, presentace v maďarštině a angličtině)
[53] http://csirt.niif.hu/
[54] http://www.cert-hungary.hu
[55] http://www.nbh.hu
[56] http://www.sztaki.hu/
[57] Tento krok je ale třeba spíše vnímat jako součást mocenskopolitických změn na Slovensku, než jako krok, zajišťující větší důraz na problematiku kybernetické bezpečnosti (zmíněný incident sehrál roli vhodné záminky). Nový ředitel Úradu František Blanárik zastupuje L'udovú stranu - Hnutie za demokratické Slovensko (LS-HZDS) vystřídal Aurela Ugora, nominovaného nyní opoziční stranou Aliancia nového občana (ANO).
Více viz: Hackeři pronikli do počítačů slovenského bezpečnostního úřadu; in: ČTK, 26. IV. 2006.
Nový předseda slovenského NBÚ dostal pověření od parlamentu; in: ČTK, 14. IX. 2006.
Slovenský bezpečnostní úřad se stal kořistí hackerů; in: HN, 26. IV. 2006.
Slovenští hackeři odpojili od netu bezpečnostní úřad; in: Právo, 24. VII. 2006.
Slovenští piráti odřízli tajnou policii od internetu; in: Rovnost - Brněnský deník, 24. VII. 2006.
http://www.nbusr.sk/ (internetová presentace Národného bezpečnostného úradu Slovenska, e-mail: info@nbusr.sk)
[58] Není bez zajímavosti, že „mluvčí" hackerů se nechal slyšet, že právě Úrad, v rozporu se všemi doporučeními, používal pro přihlášení svého personálu do vnější sítě tak „primitivní" heslo jako „nbusr123".
[59] http://www.legi-internet.ro (právní a organizační úprava boje proti kybernetickému zločinu v Rumunsku)
[60] Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, 31. VII. 2006; Velvyslanectví České republiky Bukurešť, 2. VIII. 2006 (č. j.: 779/2006 TIC); 22. VIII. 2006 (č. j.: 779/1/2006 TIC).
http://2003.informatia.ro
[61] Experti SCCI se v poslední době zaměřovali na přestupkovou činnost občanů Rumunska v zahraničí, a to na způsoby zasílání peněžitých částek do Rumunska.
[62] National contributions to be taken into account in the preparation of the independent report on the use of the Internet for terrorist purposes and cyberterrorism; CODEXTER (2006) 38 prov, 3. X. 2006.
http://www.sciam.com/turkey/7.cfm
[63] http://www.cert.am (CERT Armenia)
[64] http://www.arena.am (platforma ARENA)
[65] http://www.isoc.am/
[66] Kotajná, L., Zpráva z pracovní cesty: „Cyber Security Dimensions of Critical Infrastructure Protection", Marshall Center, München, 24. – 28. X. 2005. (http://www.marshallcenter.org - podsložka „conferences")
[67] Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, 31. VII. 2006; Kašička, P., Velvyslanectví České republiky Tokio, 18. VIII. 2006 (č. j.: 1049/2006-Toky)
http://www.jpncsi.com
[68] http://www.cyberpolice.go.jp
[69] Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, 31. VII. 2006; Čech, M., Velvyslanectví České republiky Soul, 21. VIII. 2006 (č. j.: 770/2006-Soul)
[70] http://www.ctrc.go.kr/index.jsp (internetová presentace CTRC - oddělení pro mezinárodní spolupráci CRTC cooperation@npa.go.kr, pan Kim Tae Kyun)
[71] http://www.spo.go.kr (Kancelář nejvyššího státního zástupce, Centrum pro vyšetřování internetového zločinu)
[72] http://cybercrime.zp.ua/ (Universita Záporoží)
[73] http://www.dpf.gov.br