KOMISE EVROPSKÝCH SPOLEČENSTVÍ

V Bruselu dne 22.5.2007
KOM(2007) 267 v konečném znění

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, RADĚ A EVROPSKÉMU VÝBORU REGIONŮ

k obecné politice v boji proti počítačové kriminalitě

{SEK(2007) 641}
{SEK(2007) 642}

SDĚLENÍ KOMISE
EVROPSKÉMU PARLAMENTU, RADĚ
A EVROPSKÉMU VÝBORU REGIONŮ

k obecné politice v boji proti počítačové kriminalitě

1. ÚVOD

1.1. Co je počítačová kriminalita?

Bezpečnost informačních systémů, jejichž význam neustále roste, v naší společnosti zahrnuje mnoho prvků, z nichž boj proti počítačové kriminalitě je prvkem klíčovým. Bez existence dohodnuté definice počítačové kriminality se často používají zaměnitelné pojmy „počítačová kriminalita“, „počítačová trestná činnost“, „trestná činnost v oblasti výpočetní techniky“ či „trestná činnost páchaná s využitím špičkové techniky“. Pro účely tohoto sdělení se pod pojmem „počítačová kriminalita“ rozumí „trestné činy spáchané za použití elektronických komunikačních sítí a informačních systémů či trestné činy spáchané proti takovým sítím a systémům“.

V praxi se pojem počítačová kriminalita vztahuje na tři kategorie trestné činnosti. Do první patří **tradiční formy kriminality**, jako například podvod či padělání, ačkoliv v souvislosti s počítačovou kriminalitou se toto týká konkrétně činů spáchaných prostřednictvím elektronických komunikačních sítí a informačních systémů (dále jen elektronické sítě). Do druhé kategorie patří zveřejňování **nezákonného obsahu** prostřednictvím elektronických médií (mj. materiály týkající se pohlavního zneužívání dětí či materiály podněcující k rasové nenávisti). Třetí kategorie zahrnuje **trestné činy postihující výlučně elektronické sítě**, tj. napadení informačních systémů, útoků typu „denial of service“ a hacking. Tyto typy útoků mohou být namířeny rovněž proti klíčovým kritickým infrastrukturám v Evropě a mohou v mnoha oblastech ovlivnit stávající systémy rychlého varování, což může mít katastrofální následky pro celou společnost. Pro všechny kategorie trestných činů je společným prvkem skutečnost, že mohou být páchány velkoplošně a na velkou zeměpisnou vzdálenost mezi trestným činem a jeho oběťmi. Technická hlediska používaných metod vyšetřování jsou tudíž často stejná. Toto sdělení se zaměří na uvedené společné prvky.

1.2. Nejnovější vývoj v oblasti počítačové kriminality

1.2.1. Obecně

V důsledku skutečnosti, že trestné činnosti se neustále vyvíjí a k dispozici je nedostatek spolehlivých informací, je obtížné utvořit si přesnou představu o současné situaci. Lze nicméně rozpoznat některé všeobecné trendy:

- Počet případů počítačové kriminality roste a trestné činy jsou stále důmyslnější a mají stále více mezinárodní charakter[1].

- Jasné náznaky poukazují na rostoucí zapojení skupin organizovaného zločinu do počítačové kriminality.

- Počet případů, které jsou v Evropě stíhány na základě přeshraniční spolupráce v oblasti prosazování právních předpisů však nestoupá.

1.2.2. Tradiční formy trestných činů v oblasti elektronických sítí

Většina trestných činů může být spáchána za použití elektronických sítí a různé druhy podvodů a pokusů o podvod jsou obzvláště běžné a patří k rostoucí formě kriminality v oblasti elektronických sítí. Nástroje jako krádež identity, phishing[2], spamy a škodlivé kódy lze používat k páchání velkoplošných podvodů. Nezákonný vnitrostátní a mezinárodní internetový obchod se rovněž stal rostoucím problémem, včetně obchodu s drogami, ohroženými druhy a zbraněmi.

1.2.3. Nezákonný obsah

V Evropě roste počet dostupných stránek s nezákonným obsahem, mezi který patří materiál týkající se pohlavního zneužívání dětí, podněcování k teroristickým činům, nezákonné velebení násilí, terorismu, rasismu a xenofobie. Prosazování právních předpisů zaměřených proti takovým stránkám je nepředstavitelně složité, protože vlastníci a správci stránek se často nachází v zemích jiných než cílových a často rovněž mimo EU. Stránky lze velmi rychle uzavřít a zpřístupnit na jiném místě, i mimo území EU, a definice nezákonnosti se mezi jednotlivými státy značně liší.

1.2.4. Trestné činy postihující výlučně elektronické sítě

Stále více dochází k velkoplošným útokům proti informačním systémům či organizacím a jednotlivcům (často prováděným prostřednictvím tzv. sítí botnets[3]). V poslední době byly rovněž pozorovány případy systematických, dobře koordinovaných a velkoplošných přímých útoků proti kritické informační infrastruktuře státu. Sloučené technologie a zrychlené vzájemné napojení informačních systémů, díky čemuž jsou systémy zranitelnější, takové útoky usnadnily. Útoky jsou často dobře organizovány a využívány za účelem vydírání. Lze předpokládat, že stupeň podávání zpráv o útocích je nízký, částečně z toho důvodu, že podnik může být znevýhodněn, pokud se jeho bezpečnostní problémy dostanou na veřejnost.

---

1 Většina informací, které jsou uvedeny v tomto sdělení, týkajících se všeobecných trendů byla převzata ze studie posuzující dopady sdělení o počítačové trestné činnosti, kterou zadala Komise v roce 2006 (Smlouva č. JLS/2006/A1/003).

2 Pojem „phishing“ se používá pro pokusy podvodně získat citlivé informace, například hesla a údaje o platebních kartách, vydáváním se za důvěryhodnou osobu v elektronické komunikaci.

3 Pojem „botnet“ se používá pro soubor napadených počítačů, které spouštějí programy pod společným příkazem.

1.3. Cíle

S ohledem na měnící se prostředí je bezprostředně nutné podniknout na vnitrostátní i evropské úrovni opatření proti všem formám počítačové kriminality, která představuje narůstající významnou hrozbu pro kritické infrastruktury, společnost, obchod i občany. Ochrana jednotlivců proti počítačové kriminalitě je často nepříznivě ovlivněna otázkami souvisejícími s určením příslušné jurisdikce, použitelnými právními předpisy, přeshraničním prosazováním právních předpisů či uznáním a využíváním elektronických důkazů. Převážně přeshraniční charakter počítačové kriminality tyto obtíže zdůrazňuje. S cílem vypořádat se s těmito hrozbami zahajuje Komise obecnou politickou iniciativu a hodlá na evropské a mezinárodní úrovni zlepšit koordinaci v boji proti počítačové kriminalitě.

Cílem je posílit boj proti počítačové kriminalitě na vnitrostátní, evropské a mezinárodní úrovni. Zejména další vývoj specifické politiky EU pokládají již dlouho členské státy a Komise za prvořadý úkol. Iniciativa se zaměří na prosazování právních předpisů a hlediska trestního práva v boji proti počítačové kriminalitě a politika doplní další opatření EU s cílem všeobecně zdokonalit bezpečnost v oblasti počítačové techniky. Politika bude případně zahrnovat: zdokonalenou operativní spolupráci v oblasti prosazování právních předpisů; lepší politickou spolupráci a koordinaci mezi členskými státy; politickou a právní spolupráci se třetími zeměmi; zlepšování obecného povědomí; odbornou přípravu; výzkum; posílený dialog s daným odvětvím a možné legislativní kroky.

Politika v oblasti boje proti počítačové kriminalitě a jejího stíhání bude vytyčena a prováděna způsobem, který plně dodržuje základní práva, zejména právo na svobodu projevu, respektování soukromého a rodinného života a ochranu osobních údajů. U jakéhokoliv legislativního opatření podniknutého v souvislosti s touto politikou bude nejdříve prozkoumáno, zda je slučitelné s uvedenými právy, zejména s Listinou základních práv Evropské unie. Je třeba rovněž poznamenat, že všechny uvedené politické iniciativy budou prováděny za naprostého zohlednění článků 12 až 15 tzv. směrnice o elektronickém obchodování[4] v případech, na které se tento právní nástroj vztahuje.

Cíl tohoto sdělení lze rozdělit do třech hlavních operačních směrů, které lze následovně shrnout:

- zdokonalit a usnadnit koordinaci a spolupráci mezi jednotkami boje proti počítačové kriminalitě, dalšími příslušnými orgány a odborníky v Evropské unii

- v koordinaci s členskými státy, příslušnými organizacemi EU a mezinárodními organizacemi a dalšími zúčastněnými stranami vypracovat ucelený politický rámec EU v boji proti počítačové kriminalitě

- zlepšit obecné povědomí o nákladech a nebezpečích vyplývajících z počítačové kriminality

[4] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (Úřední věstník C 178, 17.7.2000, s. 1).

2. STÁVAJÍCÍ PRÁVNÍ NÁSTROJE V BOJI PROTI POČÍTAČOVÉ KRIMINALITĚ

2.1. Stávající nástroje a opatření na úrovni EU

Stávající sdělení o politice v oblasti počítačové kriminality konsoliduje a rozvíjí sdělení z roku 2001 o vytvoření bezpečnější informační společnosti zlepšením bezpečnosti informačních infrastruktur a bojem proti počítačové kriminalitě[5] (dále jen: sdělení z roku 2001). Sdělení z roku 2001 navrhovalo vhodná podstatná a procedurální právní ustanovení pro boj s vnitrostátními i nadnárodními trestnými činnostmi. Na základě uvedeného sdělení následovalo několik důležitých návrhů. K nim patří zejména návrh vedoucí k rámcovému rozhodnutí 2005/222/SVV o útocích proti informačním systémům[6]. V této souvislosti je třeba poznamenat, že byly přijaty další, všeobecnější právní předpisy vztahující se rovněž na hlediska boje proti počítačové kriminalitě, jako například rámcové rozhodnutí 2001/413/SVV o potírání podvodů a padělání bezhotovostních platebních prostředků[7].

Rámcové rozhodnutí 2004/68/SVV o boji proti pohlavnímu vykořisťování dětí a dětské pornografii[8] je dobrým příkladem konkrétního zájmu, který Komise vyvíjí **při ochraně dětí**, zejména ve vztahu v boji proti všem formám materiálu týkajícího se pohlavního zneužívání dětí, který je zveřejňován za použití informačních systémů. Tuto horizontální prioritu bude Komise i nadále sledovat.

S cílem vypořádat se s úlohami, které stojí před informační společností, vypracovalo Evropské společenství přístup pro bezpečnost sítí a informací rozložený do třech úrovní: zvláštní opatření pro bezpečnost sítí a informací, regulační rámec pro elektronické komunikace a boj proti počítačové kriminalitě. I když lze tyto tři aspekty do jisté míry rozvíjet samostatně, řada vzájemných závislostí vyžaduje úzkou koordinaci. V související oblasti bezpečnosti sítí a informací bylo v roce 2001 vedle sdělení o počítačové kriminalitě přijato i sdělení Komise o bezpečnosti sítí a informací: Návrh na politický přístup EU[9]. Směrnice o ochraně soukromí v odvětví elektronických komunikací 2002/58/ES stanoví povinnost poskytovatelů veřejně dostupných služeb elektronické komunikace zaručit bezpečnost svých služeb. Stanoví rovněž opatření proti spamu a spywaru. Od té doby byla prostřednictvím řady opatření vypracována politika bezpečnosti sítí a informací, naposledy ve sdělení o strategii pro bezpečnou informační společnost[10], které stanoví oživenou strategii a poskytuje rámec pro další rozvoj a vytříbení soudržného přístupu k bezpečnosti sítí a informací, ve sdělení o boji proti spamu a špionážnímu a škodlivému softwaru[11] a prostřednictvím zřízení Evropské agentury pro bezpečnost sítí a informací v roce 2004[12]. Hlavním cílem Evropské agentury pro bezpečnost sítí a informací je zajistit odbornost s cílem podněcovat spolupráci mezi veřejným a soukromým sektorem a poskytovat pomoc Komisi a členským státům. **Výsledky výzkumu** v oblasti technologií určených pro zabezpečení informačních systémů budou rovněž hrát důležitou úlohu v boji proti počítačové kriminalitě. Informační a komunikační technologie, jakož i bezpečnost, jsou tudíž zmíněny jako cíle v sedmém rámcovém programu pro výzkum

---

5 KOM(2000) 890, 26.1.2001.
6 Úř. věst. L 69, 16.3.2005, s. 67.
7 Úř. věst. L 149, 2.6.2001, s. 1.
8 Úř. věst. L 13, 20.1.2004, s. 44.
9 KOM(2001) 298.
10 KOM(2006) 251.
11 KOM(2006) 688.
12 Nařízení 460/2004 o zřízení Evropské agentury pro bezpečnost sítí a informací, (Úř. věst. L 77, 13.3.2004, s. 1).

EU, který bude probíhat v letech 2007-2013[13]. Přezkum regulačního rámce pro elektronické komunikace by mohl vést ke změnám posilujícím účinnost ustanovení týkajících se bezpečnosti uvedených ve směrnici o ochraně soukromí v odvětví elektronických komunikací a směrnici o univerzální službě 2002/22/ES[14].

2.2. Stávající mezinárodní nástroje

V důsledku globální povahy informačních sítí nemůže být žádná politika v oblasti počítačové kriminality účinná, pokud jsou snahy vyvíjeny pouze v rámci EU. Pachatelé mohou nejen zaútočit na informační systémy z jednoho členského státu do druhého či dopouštět se přeshraničních trestných činů v rámci EU, ale mohou rovněž snadno páchat trestné činy, které nespadají do jurisdikce EU. Komise se proto aktivně účastnila mezinárodních diskusí a struktur spolupráce, mj. v rámci skupiny G8 Lyon-Řím pro boj proti trestné činnosti páchané s využitím špičkové techniky a v rámci projektů řízených Interpolem. Komise pozorně sleduje zejména činnost sítě pro nepřetržité kontakty v oblasti trestné činnosti páchané s využitím špičkové techniky (síť 24/7)[15], jejímiž členy je značný počet států na celém světě, včetně členských států EU. Síť G8 je mechanismem usnadňujícím kontakty mezi zúčastněnými státy, přičemž zahrnuje kontaktní body fungující nepřetržitě 24 hodin denně pro případy, na něž se vztahují elektronické důkazy a případy vyžadující naléhavou pomoc ze strany zahraničních orgánů činných v trestním řízení.

Lze se domnívat, že hlavním evropským a mezinárodním nástrojem v této oblasti je Úmluva Rady Evropy o počítačové trestné činnosti z roku 2001[16]. Úmluva, která byla přijata a vstoupila v platnost v roce 2004, obsahuje společné definice různých druhů počítačové trestné činnosti a stanoví základy pro fungování soudní spolupráce mezi smluvními státy. Byla podepsána mnoha státy, včetně Spojených států amerických a jiných neevropských států, a všemi členskými státy. Řada členských států však úmluvu či dodatečný protokol k úmluvě pojednávající o činech rasové a xenofobní povahy spáchaných prostřednictvím počítačových systémů ještě neratifikovala. Vzhledem k smluvenému významu úmluvy vyzve Komise členské státy a příslušné třetí země, aby úmluvu ratifikovaly a zvážily možnost, aby se Evropské společenství stalo stranou úmluvy.

---

13 Evropská unie podpořila řadu příslušných - a úspěšných - výzkumných projektů již v rámci šestého rámcového programu pro výzkum a technologický vývoj.

14 KOM(2006) 334, SEK(2006) 816, SEK(2006) 817.

15 Viz článek 35 Úmluvy Rady Evropy o počítačové trestné činnosti.

16 http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

3. DALŠÍ VÝVOJ ZVLÁŠTNÍCH NÁSTROJŮ V BOJI PROTI POČÍTAČOVÉ KRIMINALITĚ

3.1. Posílení operativní spolupráce při prosazování právních předpisů a úsilí v oblasti odborné přípravy na úrovni EU

Nedostatek okamžitých struktur pro **přeshraniční operativní spolupráci** či jejich nedostatečné využívání zůstává hlavní slabou stránkou v prostoru svobody, bezpečnosti a práva. Tradiční vzájemná pomoc v naléhavých případech počítačové kriminality byla pomalá a neúčinná a nové struktury spolupráce nebyly dosud dostatečně vypracovány. I když vnitrostátní soudní orgány a orgány činné v trestním řízení v Evropě úzce spolupracují prostřednictvím agentur Europol, Eurojust a jiných struktur, i nadále je zjevně zapotřebí posílit a ujasnit odpovědnosti. Konzultace provedené Komisí naznačují, že tyto klíčové kanály nejsou používány optimálním způsobem. Koordinovanější evropský přístup musí být operativní a strategický a rovněž musí zahrnovat výměnu informací a osvědčených postupů.

V blízké budoucnosti bude Komise klást zvláštní důraz na potřeby **odborného vzdělávání**. Je známým faktem, že v důsledku rozvoje technologií je zapotřebí, aby se orgánům činným v trestním řízení a soudním orgánům dostávalo neustálé odborné přípravy v otázkách počítačové kriminality. Plánuje se proto posílená a lépe koordinovaná finanční podpora ze strany EU určená na mnohonárodní programy odborné přípravy. Komise bude rovněž v úzké spolupráci s členskými státy a jinými příslušnými orgány, jako je například Europol, Eurojust, Evropská policejní akademie (CEPOL) a Evropská síť pro vzdělávání právníků (EJNT), pracovat na tom, aby na úrovni dosáhla koordinace a propojení všech příslušných programů odborné přípravy.

Komise v roce 2007 zorganizuje v Evropě **setkání** odborníků činných v trestním řízení z členských států, jakož i z Europolu, Evropské policejní akademie a Evropské sítě pro vzdělávání právníků, za účelem projednání zlepšení strategické a operativní spolupráce, jakož i odborného vzdělávání v oblasti počítačové kriminality. Projednávat se bude mj. vytvoření stálého kontaktního bodu EU pro výměnu informací a vytvoření platformy EU pro odborné vzdělávání v oblasti počítačové kriminality. Toto setkání bude prvním z řady jednání plánovaných do blízké budoucnosti.

3.2. Posílení dialogu s daným odvětvím

Soukromý i veřejný sektor mají zájem na společném vypracování metod určujících škody vzniklé v důsledku trestné činnosti a metod zabraňujících těmto škodám. Společná účast soukromého a veřejného sektoru, založená na vzájemné důvěře a společném cíli snížit škody, se jeví jako účinný způsob posílení bezpečnosti, rovněž v boji proti počítačové kriminalitě. Soukromě-veřejná hlediska politiky Komise v oblasti počítačové kriminality budou včas zařazena do plánované globální politiky EU v oblasti dialogu mezi veřejným a soukromým sektorem, která bude zahrnovat celou oblast evropské bezpečnosti. Tuto politiku urychlí zejména evropské fórum pro výzkum bezpečnosti a inovace, které Komise hodlá v dohledné době vytvořit a které přeskupí příslušné zúčastněné strany z veřejného a soukromého sektoru.

Rozvoj moderních informačních technologií a elektronickým komunikačních systémů je z velké míry kontrolován soukromými subjekty. Soukromé společnosti provádějí hodnocení hrozeb, vypracovávají programy pro boj proti kriminalitě a technická řešení zabraňující trestné činnosti. Odvětví projevilo velmi pozitivní přístup při pomoci veřejným orgánům v boji proti počítačové kriminalitě, zejména v úsilí zaměřeném proti dětské pornografii[17] a jiným druhům nezákonného obsahu na internetu.

Další otázka se týká zjevného nedostatku výměny informací, odborných znalostí a osvědčených postupů mezi veřejným a soukromým sektorem. Z důvodu ochrany obchodních modelů a tajemství se subjekty ze soukromého sektoru často zdráhají – nebo nejsou jasně zákonně povinny – hlásit orgánům činným v trestním řízení případy trestné činnosti nebo poskytovat příslušné informace o těchto případech. Takových informací však může být zapotřebí, pokud mají veřejné orgány vytyčit účinnou a vhodnou politiku zaměřenou proti kriminalitě. Budou rovněž zváženy možnosti zdokonalení výměny informací mezi sektory s ohledem na stávající pravidla o ochraně osobních údajů.

Komise již hraje důležitou úlohu v různých veřejně-soukromých strukturách zabývajících se bojem proti počítačové kriminalitě, jako je například skupina odborníků pro předcházení podvodům[18]. Komise je přesvědčena, že účinná všeobecná politika v boji proti počítačové kriminalitě musí rovněž zahrnovat strategii pro spolupráci mezi subjekty veřejného a soukromého sektoru, včetně organizací občanské společnosti.

Pro dosažení širší veřejně-soukromé spolupráce v této oblasti zorganizuje Komise v roce 2007 konferenci pro odborníky činné v trestním řízení a zástupce soukromého sektoru, zejména poskytovatele internetových služeb, aby mohlo být projednáno, jak zlepšit veřejně-soukromou operativní spolupráci v Evropě[19]. Konference se bude zabývat všemi otázkami považovanými za důležité pro oba sektory, ale především:

- zlepšením operativní spolupráce v boji proti nezákonným činnostem a nezákonnému obsahu na internetu, zejména v oblastech terorismu, materiálů týkajících se pohlavního zneužívání dětí a jiných nezákonných činností, které jsou obzvláště citlivé z hlediska ochrany dětí

- vypracováním veřejně-soukromých dohod, jejichž cílem je v rámci EU zablokovat stránky s nezákonným obsahem, zejména s materiálem týkajícím se pohlavního zneužívání dětí

- vytyčením evropského modelu pro sdílení potřebných a relevantních informací v rámci soukromého a veřejného sektoru, přičemž je třeba vytvořit atmosféru vzájemné důvěry a zohlednit zájmy všech stran

- zřízením sítě kontaktních bodů v oblasti prosazování právních předpisů v soukromém i veřejném sektoru

---

17 Nedávným případem spolupráce v této oblasti je spolupráce mezi orgány činnými v trestním řízení a společnostmi vydávajícími kreditní karty, kdy tyto společnosti pomohly policii vypátrat osoby kupující na internetu dětskou pornografii.

18 Viz http://ec.europa.eu/internal_market/payments/fraud/index_en.htm.

19 Konferenci by bylo možné považovat za pokračování fóra EU uvedeného v oddílu 6.4 sdělení o počítačové kriminalitě.

3.3. Právní předpisy

Všeobecná harmonizace definicí trestné činnosti a vnitrostátních trestních právních předpisů v oblasti počítačové kriminality zatím není vhodná v důsledku různorodosti trestných činů, na které se vztahuje toto sdělení. Jelikož účinná spolupráce mezi orgány činnými v trestním řízení často závisí na existenci alespoň částečně harmonizovaných definicí trestné činnosti, zůstává harmonizace právních předpisů členských států i nadále dlouhodobým cílem[20]. S ohledem na některé klíčové definice trestných činů byl již podniknut důležitý krok v podobě rámcového rozhodnutí o útocích proti informačním systémům. Jak je uvedeno výše, objevily se následně nové hrozby a Komise pozorně sleduje vývoj s ohledem na skutečnost, že je důležité neustále vyhodnocovat potřebu dodatečných právních předpisů. Sledování vyvíjejících se hrozeb je úzce koordinováno s evropským programem na ochranu kritické infrastruktury.

Cílené právní předpisy proti počítačové kriminalitě by však měly být zváženy i nyní. Konkrétní otázka, která možná bude vyžadovat právní předpisy, se týká situace, kdy je počítačová kriminalita páchána ve spojení s **krádeží identity**. Pod pojmem „krádež identity" se všeobecně rozumí používání osobních identifikačních informací, např. číslo kreditní karty, jako nástroj ke spáchání jiných trestných činů. Ve většině členských států by byl pachatel pravděpodobně stíhán spíše za podvod či jiný možný trestný čin, než za krádež identity; přičemž podvod je považován za závažnější trestný čin. Krádež identity není jako taková v členských státech zákonně považována za trestný čin. Je často snadnější dokázat trestný čin krádeže identity, než trestný čin podvodu, takže by spolupráci v oblasti prosazování právních předpisů na úrovni EU prospělo, kdyby byla krádež identity zákonně považována za trestný čin ve všech členských státech. Komise v roce 2007 zahájí konzultace s cílem určit, zda jsou právní předpisy na odpovídající úrovni.

3.4. Vypracování statistických údajů

Panuje všeobecná shoda, že stávající stav informací týkajících se trestných činů je značně nepřiměřený a že je zejména zapotřebí pokroku v porovnávání údajů mezi členskými státy. Ambiciózní pětiletý plán pro řešení tohoto problému byl vytyčen ve sdělení Komise o *rozvoji komplexní a soudržné strategie EU k mapování trestné činnosti a trestního soudnictví: Akční plán EU na období let 2006 – 2010* ze dne 7. srpna 2006[21]. Skupina odborníků ustanovená podle tohoto akčního plánu by byla vhodným fórem pro rozvoj příslušných ukazatelů rozsahu počítačové kriminality.

4. DALŠÍ POSTUP

Komise bude nyní pracovat na obecné politice v boji proti počítačové kriminalitě. Vzhledem k omezeným pravomocem Komise v oblasti trestního práva může tato politika pouze doplňovat kroky podniknuté členskými státy a jinými orgány. Nejdůležitější opatření – z nichž každé bude využívat jednoho, několika či všech nástrojů uvedených v kapitole 3 – budou rovněž podporována prostřednictvím finančního programu „Předcházení trestné činnosti a boj proti ní".

---

[20] Tento dlouhodobý cíl byl již uveden na straně 3 sdělení z roku 2001.

[21] KOM(2006) 437, 7.8.2006.

4.1. Boj proti počítačové kriminalitě všeobecně

- zavést posílenou operativní spolupráci mezi orgány činnými v trestním řízení a soudními orgány členských států; toto opatření bude zahájeno uspořádáním tematického setkání odborníků v roce 2007 a může zahrnovat zřízení ústředního kontaktního bodu EU pro počítačovou kriminalitu

- zvýšit finanční podporu na iniciativy určené pro lepší odbornou přípravu orgánů činných v trestním řízení a soudních orgánů v souvislosti s projednáváním případů počítačové kriminality a podniknout kroky ke koordinaci veškerého mnohonárodního úsilí vyvinutého v této oblasti při vypracování platformy EU na poli odborné přípravy

- prosazovat silnější angažovanost členských států a všech veřejných orgánů při přijímání účinných opatření proti počítačové kriminalitě a přidělit dostatečné zdroje na boj proti ní

- podporovat výzkum prospěšný v boji proti počítačové kriminalitě

- zorganizovat alespoň jednu velkou konferenci (v roce 2007) za účasti orgánů činných v trestním řízení a soukromých subjektů, zejména s cílem zahájit spolupráci v boji proti nezákonným internetovým činnostem v oblasti elektronických sítí a zaměřených proti těmto sítím, podporovat účinnější výměnu informací neosobní povahy a sledovat závěry učiněné na dané konferenci prostřednictvím konkrétních projektů veřejně-soukromé spolupráce

- vyvinout úsilí v oblasti veřejně-soukromých činností a účastnit se těchto činností zaměřených na zvyšování povědomí – zejména mezi spotřebiteli – o nákladech a nebezpečích vyplývajících z počítačové kriminality a zároveň nesnižovat důvěru spotřebitelů a uživatelů zdůrazňováním negativních hledisek bezpečnosti

- aktivně se podílet na celosvětové mezinárodní spolupráci v boji proti počítačové kriminalitě a podporovat ji

- zahájit mezinárodní projekty, které jsou v souladu s politikou Komise v této oblasti, např. projekty, které pořádá skupina G8 a které jsou v souladu se Strategickými dokumenty o zemích a regionech (s ohledem na spolupráci s třetími zeměmi), přispívat k těmto projektům a podporovat je

- podniknout konkrétní kroky při podpoře všech členských států a příslušných třetích zemí v ratifikaci Úmluvy Rady Evropy o počítačové trestné činnosti a jejího dodatečného protokolu a zvážení možnosti, aby se Společenství stalo stranou úmluvy

- prošetřit společně s členskými státy fenomén koordinovaných a velkoplošných útoků proti informačním infrastrukturám členských států s ohledem na jejich prevenci a boj proti nim, včetně koordinace reakcí a sdílení informací a osvědčených postupů

4.2. Boj proti tradičním formám trestných činů v oblasti elektronických sítí

- zahájit podrobnou analýzu s cílem připravit návrh zvláštních právních předpisů EU zaměřených proti krádeži identity

- podporovat rozvoj technických metod a postupů v boji proti podvodu a nezákonnému obchodu na internetu, rovněž prostřednictvím projektů veřejně-soukromé spolupráce

- pokračovat v činnosti – a dále ji rozvíjet – v konkrétně vytyčených oblastech, jako například v činnosti skupiny odborníků pro předcházení podvodům při boji proti podvodům v oblasti bezhotovostních platebních prostředků v elektronických sítích

4.3. Nezákonný obsah

- i nadále rozvíjet opatření proti specifickému nezákonnému obsahu, především s ohledem na materiál týkající se pohlavního zneužívání dětí a materiál podněcující k rasové nenávisti, a to zejména prováděním rámcového rozhodnutí o boji proti pohlavnímu vykořisťování dětí

- vyzvat členské státy, aby přidělily dostatečné finanční zdroje na posílení činnosti orgánů činných v trestním řízení, přičemž zvláštní pozornost bude věnována identifikaci materiálu týkajícího se obětí pohlavního zneužívání, který je rozšiřován online

- zahájit a podporovat činnost zaměřenou proti nezákonnému obsahu, který může nezletilé podněcovat k násilnému a jinak závažnému nezákonnému chování, mj. proti některým druhům velmi násilných internetových videoher

- zahájit a podporovat dialog vedený mezi členskými státy a se třetími zeměmi o technických metodách v boji proti nezákonnému obsahu, jakož i o postupech uzavírání nezákonných internetových stránek, rovněž s ohledem na možné vypracování formálních dohod se sousedními a jinými zeměmi v této otázce

- na úrovni EU vypracovat dobrovolné dohody a úmluvy mezi veřejnými orgány a soukromými subjekty, zejména poskytovateli internetových služeb, o postupech při zablokování a uzavírání nezákonných internetových stránek

4.4. Další postup

Řada opatření zaměřených na zlepšení struktur spolupráce v EU byla v tomto sdělení vytyčena jako další kroky. Komise bude nyní pracovat na těchto opatřeních, zhodnotí postup při provádění činností a podá zprávu Radě a Parlamentu.