Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření

Současná společnost ve stále větší míře využívá informační systémy a technologie pro nejrůznější oblasti činností. Je možné bez nadsázky říci, že společnost dvacátého prvního století, a především její ekonomika, bude zcela postavena na informačních technologiích (informační společnost, infoekonomika) a na vzájemném propojení informačních systémů do sítí, kdy dominantní roli bude hrát veřejná informační a komunikační síť – internet. Celosvětově jsou ze strany národních a zejména mezinárodních institucí vyvíjeny snahy o urychlení přechodu k informační společnosti (např. Evropská komise připravila koncem roku 1999 projekt *e*Evropa[1]). Na druhé straně zřejmě budou moderní informační technologie v čím dál větší míře využívány k trestné činnosti. Tento materiál si klade za cíl analyzovat současný stav a vývoj trestné činnosti v této oblasti s postižením aktuálních problémů včetně návrhů na řešení. Opírá se přitom o vládní dokument "Státní informační politika – cesta k informační společnosti", jehož obsahem je prezentace cílů a priorit na cestě budování informační společnosti (tento dokument přijala vláda usnesením číslo 525 ze dne 31. května 1999).

Koncepce boje proti trestné činnosti v oblasti informačních technologií především musí vycházet z konkrétních poznatků policejní práce v této oblasti kriminality a dále z informací, pocházejících z nejrůznějších oblastí společenského života, a to jak z domácích, tak i ze zahraničních zdrojů. V rámci resortu Ministerstva vnitra byla této problematice věnována určitá pozornost již od počátku devadesátých let. V posledních dvou letech došlo k velmi výraznému posunu v chápání důležitosti celé problematiky, a to umožnilo jednak zkvalitnit policejní práci a dále věnovat více pozornosti komplexní systematické analýze situace v dané oblasti.

[1] Na základě této iniciativy připravila Evropská komise návrh Akčního plánu pro Evropskou Radu, který stanoví základní úkoly (včetně termínů pro jejich splnění) v oblasti prosazování elektronických technologií, zejména urychlení tvorby vhodného právního prostředí (na evropské úrovni je připravována a diskutována celá řada příslušných legislativních návrhů) a podpora nové infrastruktury a služeb v celé Evropě.

Koncepce byla vypracována se znalostí společného přístupu států zastoupených v Radě Evropy, jak je vyjádřen v doporučení Rady ministrů č. 13 z roku 1995, týkající se problémů trestního práva procesního spojeného s informačními technologiemi, v doporučení Rady ministrů č. 5 z roku 1999, týkající se ochrany soukromí na internetu a zvláště v návrhu (poslední verze č. 25 z 22. 12. 2000) mezinárodní dohody o "kyberzločinu", jejíž definitivní znění má být předloženo k podpisu již do konce tohoto roku. Význačným činem Evropské unie v této oblasti je akční plán *e*Europe 2002, který byl přijat v červnu r. 2000 a který má být splněn do roku 2002. Důležité jsou rovněž aktivity skupiny G-8, a zvláště USA, které byly na shromáždění ministrů spravedlnosti a vnitra ze zemí G-8 ve Washingtonu v roce 1997 shrnuty v deset principů boje s "high-tech" zločinem a v desetibodový akční plán boje proti tomuto typu zločinu. Zásady boje proti organizovaným zločineckým aktivitám v tzv. "kyberprostoru[2]", tedy v oblasti informačních a komunikačních technologií, byly deklarovány v nedávné době na různých mezinárodních fórech, například na Konferenci o strategiích EU a USA v boji proti nadnárodnímu organizovanému zločinu, která se konala v belgickém Gentu v lednu 2001.

Koncepce je také reakcí na úkol, který vyplynul pro ministra vnitra z "Aktualizované koncepce boje proti organizovanému zločinu", kterou schválila vláda České republiky v říjnu roku 2000. Ministru vnitra bylo (na základě harmonogramu úkolů, který tvoří přílohu k příslušnému usnesení vlády) uloženo "průběžně koncepčně řešit potírání organizovaných zločineckých aktivit v oblasti informačních technologií". Předložený materiál je ovšem pojat komplexněji, neboť páchání trestné činnosti v oblasti informační kriminality není omezeno pouze na aktivity organizované.

Základním východiskem koncepce je názor, že přístup státu vůči tomuto typu trestné činnosti má být systémový, vyvážený v odlišném důrazu na jednotlivé aspekty této trestné činnosti podle jejich společenské nebezpečnosti, žádoucím způsobem diversifikovaný podle resortů i v rámci nich a zároveň koordinovaný skrze intenzivní spolupráci všech zúčastněných složek státních organizací, státu s nestátními organizacemi a státu s jinými státy.

[2] Kyberprostorem je nazýváno vzájemné propojení jednotlivých dílčích subjektů do celosvětové informační sítě.

Negativní jevy v oblasti zneužívání informačních technologií jsou velmi často umožněny nepřipraveností společnosti na stále intenzivnější propojení běžných aktivit s novými technikami. Jejich nástup vytváří komunikační mechanismy, které si jejich uživatelé velmi rychle osvojují a dokáží je používat, aniž by si ovšem uvědomovali s nimi spojená rizika. Je proto zapotřebí vytvořit prostředí pro vzájemnou osvětu a informační výměnu mezi subjekty, získávajícími poznatky o jednotlivých bezpečnostních aspektech, spojených s používáním nových technologií. Je úlohou státních orgánů vytvářet stabilní a bezpečné prostředí, které dává občanům oprávněně pocit právní jistoty při využívání moderních informačních a komunikačních prostředků. K získaným poznatkům o jednotlivých obecných i konkrétních bezpečnostních rizicích by měla mít bezprostřední přístup i veřejnost. K tomuto úkolu je třeba přistoupit aktivně, tedy průběžně provádět preventivně cílenou informační kampaň ve spolupráci všech odpovědných resortů a za účinné participace dalších zainteresovaných subjektů. Navržena je proto řada konkrétních informačních opatření.

Boj proti negativním jevům v oblasti informačních technologií není záležitostí pouze ústředních správních úřadů. Existuje celá řada subjektů (jednotlivců, skupin, komerčních i nekomerčních institucí), které jsou na úspěchu této činnosti značně zainteresovány, jsou v oblasti informačních technologií kvalifikovány a mohou proto státní administrativě výrazně pomoci. Proto jsou také navržena opatření k daleko většímu zapojení zástupců mimoexekutivní sféry (především odborné veřejnosti) již do diskuse k tomuto tématu.

Kromě preventivních opatření je ovšem nezbytné zajistit podmínky pro další kvantitativní a zejména kvalitativní rozvoj struktur přímo participujících na potírání informační kriminality – především orgánů činných v trestním řízení. Stěžejní roli zde budou hrát specializované složky Policie České republiky, které musí být souběžně se zkvalitňováním své práce personálně a materiálně posilovány. Zároveň by také měly být odborně školeny justiční orgány, jako nedílná součást řetězce orgánů činných v trestním řízení. Navrhuje se tedy zařazení této problematiky do vzdělávacích programů, připravovaných jednotlivými zainteresovanými součástmi resortu Ministerstva vnitra.

Všechna uvedená opatření vycházejí z přesvědčení, že s dalším rozvojem moderní techniky bude intenzita nezákonných činností souvisejících s jejím zneužíváním narůstat. Je to dáno charakterem a atraktivností nového informačního a komunikačního prostředí, rozdílným přístupem jednotlivých států k potřebě jeho regulace a k boji s kriminalitou, která s ním souvisí, v neposlední míře také omezenými možnostmi státních orgánů dostatečně reagovat na jevy způsobené novým technologickým pokrokem. Možnosti státních orgánů nejsou neomezené, proto je třeba stanovit jednoznačné priority, a těm věnovat největší pozornost. Některá navrhovaná řešení reagují na dlouhodobě se vyskytující problémy, které se již delší dobu nedaří zainteresovaným ministerstvům konsensuálně řešit. Z kvalitativní, ale i kvantitativní analýzy těchto forem kriminality vyplývá jejich zjevná společenská nebezpečnost, neboť zde neexistuje jen nebezpečí materiálních škod u jednotlivých subjektů, ale také nebezpečí následků v podobě obavy z nestabilního a nekontrolovaného prostředí informační a komunikační dimenze společnosti, která může vést ke zbrždění rozvoje moderní společnosti. Vzhledem ke stále výraznějšímu provázání informačních a komunikačních technologií s jednotlivými oblastmi lidských aktivit může nejistota těchto struktur vést až k destabilizaci společensko-ekonomického systému jako takového.

O realizaci dále rozpracovaných opatření bude v rámci zprávy o bezpečnostní situaci pravidelně informována vláda.

Harmonogram opatření

A. Oblast legislativní

1. Projednat v rámci meziresortní komise pro potírání nelegálního jednání proti právům k duševnímu vlastnictví při ministerstvu průmyslu a obchodu návrh věcného záměru novely zákona o neperiodických publikacích, která by reagovala na situaci v oblasti digitálních nosičů informací, zejména stanovením povinnosti jednoznačné identifikace těchto nosičů jejich výrobcem nebo výrobcem rozmnoženiny.

   Odpovídá: odbor bezpečnostní politiky ve spolupráci s odborem legislativy, koordinace předpisů a kompatibility s právem Evropských společenství a s Policejním prezidiem
   Doporučeno spolupracovat s ministrem kultury a s ministrem průmyslu a obchodu
   Termín: 31. 12. 2001

2. Projednat a navrhnout novelizaci ustanovení § 240 trestního zákona ve vztahu k ochraně zasílaných informací elektronickou poštou.

   Odpovídá: odbor bezpečnostní politiky ve spolupráci s odborem legislativy, koordinace předpisů a kompatibility s právem Evropských společenství
   Doporučeno spolupracovat s ministrem kultury, úřadem pro veřejné informační systémy a s ministrem průmyslu a obchodu
   Termín: 31. 12. 2001

B. Oblast organizační

3. Zajistit podmínky pro další rozvoj struktur přímo participujících na potírání informační kriminality. Rozšiřovat a podporovat spolupráci se zpravodajskými službami a s nevládními subjekty zabývajícími se problematikou, související s informační kriminalitou. Dohodnout s těmito subjekty způsob, formu a rozsah spolupráce. Průběžně personálně a materiálně posilovat specializované složky Policie České republiky. Každoročně vypracovat podrobnou zprávu o činnosti pro potřeby resortu. Pravidelně informovat veřejnost o výsledcích práce.

   Odpovídá: Policejním prezidium ve spolupráci s Úřadem vyšetřování pro ČR, odborem komunikačních a informačních služeb a odborem bezpečnostní politiky

Termín: průběžně s kontrolním termínem vždy k 31. 12. (poprvé 31. 12. 2001)

4. Ustanovit kontaktní místo, které by bylo dosažitelné 24 hodin denně a které by zajistilo včasnou a efektivní komunikaci se zahraničními partnery při nadnárodních případech informační kriminality. Vytvořit mechanismy pro zajištění bezprostředního přijetí požadavků vzájemné pomoci v naléhavých a důležitých případech a včasných odpovědí na ně pomocí rychlých a dostatečně spolehlivých prostředků komunikace.

   Odpovídá: Policejním prezidium ve spolupráci s odborem komunikačních a informačních služeb
   Termín: 30. 12. 2001

5. Iniciovat meziresortní jednání s Úřadem pro veřejné informační systémy s cílem vypracovat principy plánu ochrany státních a některých strategicky důležitých nestátních informačních systémů – analogii Národního plánu pro ochranu informačních systémů v USA.

   Odpovídá: odbor komunikačních a informačních služeb ve spolupráci s Policejním prezidiem, odborem bezpečnostní politiky, odborem koncepcí a organizace a odborem informatizace veřejné správy
   Doporučeno spolupracovat s ministrem vlády a předsedou Rady vlády pro státní informační politiku a s ředitelem Národního bezpečnostního úřadu
   Termín: 30. 6. 2002

6. Připravit dohodu mezi Ministerstvem vnitra a Ministerstvem průmyslu a obchodu o spolupráci při provádění živnostenských a jiných kontrol (s důrazem na dodržování autorských práv jednotlivými podnikateli).

   Odpovídá: Policejním prezidium ve spolupráci s odborem bezpečnostní politiky
   Doporučeno spolupracovat s ministrem průmyslu a obchodu
   Termín: 30. 12. 2001

7. Vypracovat projekt hlásného systému pro trestnou činnost v oblasti informačních technologií. Iniciovat vznik a podporovat činnost skupiny typu CERT (Central Emergency Response Team) jako nevládního sdružení kvalifikovaných odborníků informujících ostatní profesionály o bezpečnostních problémech a reagujících na probíhající útoky.

   Odpovídá: odbor bezpečnostní politiky ve spolupráci s odborem komunikačních a informačních služeb, odborem koncepcí a organizace, Policejním prezidiem a Úřadem vyšetřování

Doporučeno spolupracovat s předsedou Úřadu pro veřejné informační systémy, s ministrem vlády a předsedou Rady vlády pro státní informační politiku, ministrem spravedlnosti, ministrem kultury, ministrem školství, mládeže a tělovýchovy a s ředitelem Národního bezpečnostního úřadu
Termín: 30. 6. 2002

8. Vytvořit pracovní skupinu k řešení problémů spojených s bojem proti informační kriminalitě za účasti odborníků mimoexekutivní sféry.

Odpovídá: odbor bezpečnostní politiky
Termín: 30. 9. 2001

C. Oblast vzdělávání, výzkumu a mediálního působení

9. Vypracovat projekt vzdělávání a doškolování orgánů činných v trestním řízení s důrazem na objasňování problematiky trestné činnosti v oblasti informačních technologií. Za uvedeným účelem připravit návrhy výukových materiálů.

Odpovídá: odbor vzdělávání a správy policejního školství ve spolupráci s Policejní akademií, Policejním prezidiem a Úřadem vyšetřování pro ČR
Doporučeno spolupracovat s ministrem spravedlnosti, s ministrem školství, mládeže a tělovýchovy a s úřadem pro veřejné informační systémy
Termín: průběžně s kontrolním termínem vždy k 31. 12. (poprvé 31. 12. 2001)

10. Pro potřeby škol v resortu MV vypracovat nebo zajistit vypracování pedagogických materiálů, objasňujících problematiku kriminality v oblasti informačních technologií. Podporovat začleňování výuky této problematiky do učebních plánů.

Odpovídá: odbor vzdělávání a správy policejního školství ve spolupráci s Policejní akademií a odborem přípravy pracovníků ve veřejné správě
Doporučeno spolupracovat s ministrem školství, mládeže a tělovýchovy
Termín: průběžně s kontrolním termínem vždy k 31. 12. (poprvé 31. 12. 2001)

11. Vyvíjet a zavádět forenzní standardy pro vyhledávání a ověřování elektronických dat při kriminálním vyšetřování a trestním řízení.

Odpovídá: Kriminalistický ústav
Doporučeno spolupracovat s ministrem spravedlnosti

Termín: průběžně s kontrolním termínem vždy k 30. 6. (poprvé 30. 6. 2002)

12. Podporovat (např. formou grantu nebo ocenění) nezávislou výzkumnou, publicistickou a dokumentaristickou činnost zabývající se negativními jevy v souvislosti s informačními technologiemi. Provádět osvětu a propagaci boje proti kriminalitě v oblasti informačních technologií.

    Odpovídá: odbor koncepcí a organizace ve spolupráci s odborem bezpečnostní politiky, odborem tisku a public relations, Policejní akademií, Policejním prezidiem a odborem prevence kriminality
    Doporučeno spolupracovat s ministrem spravedlnosti, ministrem kultury, ministrem školství, mládeže a tělovýchovy a s ministrem vlády a předsedou Rady vlády pro státní informační politiku
    Termín: průběžně s kontrolním termínem vždy k 30. 6. (poprvé 30. 6. 2002)

D. Oblast mezinárodní spolupráce

13. Sledovat aktivity mezinárodních a nadnárodních organizací v oblasti boje proti trestné činnosti v oblasti informačních technologií. Aktivně se zúčastňovat akcí týkajících se boje proti těmto formám trestné činnosti pořádaných těmito a dalšími organizacemi.

    Odpovídá: odbor mezinárodní spolupráce a evropské integrace ve spolupráci s odborem bezpečnostní politiky a Policejním prezidiem
    Doporučeno spolupracovat s ministrem zahraničních věcí a ministrem spravedlnosti
    Termín: průběžně s kontrolním termínem vždy k 30. 6. (poprvé 30. 6. 2002)

14. Připravit podmínky pro realizaci mezinárodních úmluv a dalších relevantních aktů mezinárodního společenství (s důrazem na přípravu vstupu České republiky do Evropské unie) v oblasti mezinárodní spolupráce v boji proti informační kriminalitě. Provést analýzu dopadů realizace mezinárodních úmluv v oblasti boje proti informační kriminalitě na stávající právní normy

    Odpovídá: odbor mezinárodní spolupráce a evropské integrace ve spolupráci s odborem legislativy, koordinace předpisů a kompatibility s právem Evropských společenství, odborem bezpečnostní politiky a Policejním prezídiem
    Doporučeno spolupracovat s místopředsedou vlády a ministrem zahraničních věcí a s ministrem spravedlnosti
    Termín: průběžně s kontrolním termínem vždy k 30. 6. (poprvé 30. 6. 2002)

E. Oblast koordinační a kontrolní

15. Koordinovat a kontrolovat plnění úkolů uvedených v tomto harmonogramu. V rámci zprávy o bezpečnostní situaci zajistit pravidelné informování Vlády České republiky.

    Odpovídá: odbor bezpečnostní politiky
    Termín: průběžně