



EVROPSKÁ KOMISE

V Bruselu dne 26.7.2012
COM(2012) 417 final

**SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, RADĚ A EVROPSKÉMU
HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU**

Bezpečnostní politika v průmyslu

Akční plán pro inovativní a konkurenceschopný bezpečnostní průmysl
{SWD(2012) 233 final}

1. Úvod

Zajištění bezpečnosti je jednou z hlavních starostí každé společnosti. Veškeré oblasti politiky obsahují důležitý prvek bezpečnosti. Bezpečné prostředí je samotným základem každé stabilní společnosti. Konkurenceschopný bezpečnostní průmysl v EU nabízející řešení, která poskytují vyšší míru bezpečnosti, může významně pomoci zvýšit odolnost evropské společnosti.

Bezpečnostní průmysl je odvětvím s velkým potenciálem pro růst a vytváření pracovních míst. Za posledních deset let se hodnota celosvětového bezpečnostního trhu zvýšila téměř na desetinásobek z přibližně 10 miliard EUR na 100 miliard EUR v roce 2011. Četné studie ukazují, že bezpečnostní trh v EU i ve světě bude nadále přesahovat průměrnou míru růstu HDP¹.

S vědomím tohoto výrazného potenciálu pro růst trhu zařadila Komise bezpečnostní průmysl mezi základní části stěžejní iniciativy EU 2020 „*Integrovaná průmyslová politika pro éru globalizace – konkurenceschopnost a udržitelnost v popředí zájmu*“². V tomto dokumentu Komise oznámila zavedení specializované iniciativy pro politiku týkající se bezpečnostního průmyslu.

Tento akční plán je prvním vykročením v rámci zmíněné iniciativy. Cílem je podpořit růst a zvýšit zaměstnanost v bezpečnostním průmyslu EU.

Díky úrovni technického rozvoje patří mnohé ze společností v EU (působících v oblasti bezpečnosti) stále mezi světovou špičku ve většině segmentů odvětví bezpečnosti. Nedávný vývoj a tržní prognózy nicméně naznačují, že tržní podíly evropských společností na světovém trhu budou mít během příštích let sestupnou tendenci. Odhady odvětví i nezávislé studie předpovídají, že současný tržní podíl společností z EU působících v bezpečnostním sektoru by mohl klesnout o jednu pětinu z přibližně 25 % celosvětového trhu v roce 2010 na 20 % do roku 2020, nebudou-li podniknuty kroky ve prospěch zvýšení konkurenceschopnosti bezpečnostního průmyslu EU.

Trhu vévodící společnosti z USA jsou stále na špici v technologiích, navíc mají také prospěch z jednotného právního rámce a silného domácího trhu. To jim dává nejen pevné zázemí, ale rovněž poskytuje přínos v podobě jednoznačně uznávané a odlišitelné americké značky, což se v mezinárodní konkurenci ukázalo jako velká výhoda oproti společnostem z EU.

Absence obdobné „značky EU“ je obzvláště závažná, uvažíme-li, že v budoucnosti budou hlavní odbytiště bezpečnostních technologií nikoli v Evropě, nýbrž v rozvíjejících se zemích v Asii, Jižní Americe a na Blízkém východě.

Asijské země stále rychleji snižují svou ztrátu, kterou v technologiích mají na společnosti z EU. Bez náskoku v technologiích budou společnosti z EU čelit nelítostné konkurenci, zohledníme-li navíc nevýhodu v podobě výrobních nákladů, s níž se firmy z EU často potýkají.

¹ Všechny číselné údaje a studie uvedené v tomto akčním plánu jsou podrobněji popsány v pracovním dokumentu útvarů Komise (dále též „pracovní dokument“), který tento akční plán doprovází.

² KOM(2010) 614 v konečném znění.

Prvořadým cílem Komise je proto vytvořit lépe fungující evropský vnitřní trh bezpečnostních technologií. Příznivé podmínky na vnitřním trhu, posílení hospodářské soutěže a snížení výrobních nákladů využitím úspor z rozsahu jsou rovněž nezbytnými prvky k posílení pozice bezpečnostního průmyslu EU ve zmíněných rozvíjejících se zemích, které představují budoucnost bezpečnostního sektoru. Zvláštní důraz by se měl klást na podporu malých a středních podniků při jejich snaze o vstup na mezinárodní trhy ve třetích zemích.

Řešením mnohých z těchto otázek se již zabývalo Evropské fórum pro výzkum a inovace v oblasti bezpečnosti (ESRIF) a navazující sdělení Komise³. V odvětví informačních a komunikačních technologií (IKT) je prosazování bezpečnosti nedílnou součástí zařízení a produktů, které společnosti v tomto oboru nabízejí, a je klíčem k budoucí konkurenceschopnosti. Této věci bude věnovat pozornost i nadcházející evropská strategie pro bezpečnost internetu. V rámci EU však dosud neexistoval jednotný přístup usilující o to, aby byl bezpečnostní průmysl EU konkurenceschopnější a inovativnější.

Studie i stanoviska zúčastněných stran⁴ ukazují, že spíše než na služby se tlak celosvětové konkurence zaměří na výrobu výrobků a technologie, protože tyto oblasti tvoří převážnou většinu vývozního potenciálu odvětví bezpečnosti. Tento akční plán proto nezahrnuje bezpečnostní služby jako takové (např. personál fyzické ostrahy budov), ale pouze ty, které se týkají instalace a údržby bezpečnostních zařízení.

Komise použije všechny dostupné nástroje, aby pro bezpečnostní technologie vytvořila skutečný vnitřní trh, čímž bezpečnostnímu průmyslu EU poskytne pevnou domácí základnu s vyhlídkami na získání podílů na rozvíjejících se trzích.

Komise zajistí, aby veškeré iniciativy ve prospěch rozvoje vnitřního trhu s bezpečnostními technologiemi respektovaly Listinu základních práv, zejména právo na ochranu soukromí a osobních údajů.

2. BEZPEČNOSTNÍ PRŮMYSL A TRH V EU

Hodnota celosvětového bezpečnostního trhu se odhaduje na přibližně 100 miliard EUR (údaj z roku 2011) a toto odvětví celosvětově zaměstnává přibližně 2 miliony osob. Odhadovaná tržní hodnota bezpečnostního trhu EU se pohybuje v rozmezí 26 miliard až 36,5 miliard EUR a počet zaměstnaných osob je přibližně 180 000 (údaje z roku 2011).

V současné době nicméně neexistuje jasná definice bezpečnostního průmyslu a metodické klasifikaci tohoto odvětví brání řada faktorů:

- Na odvětví bezpečnosti se nevztahují hlavní statistické nomenklatury (NACE, Prodcom atd.).
- Výroba zboží souvisejícího s bezpečností se skrývá pod řadou různých kategorií. Statistiky za tyto kategorie nerozlišují, zda má daná činnost souvislost s bezpečností či nikoliv.
- Na evropské úrovni neexistuje zdroj statistických údajů od samotného odvětví.

³ KOM(2009) 691 v konečném znění.

⁴ Viz pracovní dokument útvarů Komise.

- Z hlediska nabídky nemusí být objednavatelé bezpečnostního vybavení a systémů ochotni poskytovat informace o svých výdajích na bezpečnost.

Za účelem odstranění nedostatku údajů o bezpečnostním průmyslu a jeho odbytištích vytvoří Komise empirický základ, díky němuž bude možné o bezpečnostních trzích získat spolehlivější údaje. Důležitým předpokladem pro takový počin je spolupráce s hlavními obchodními sdruženími.

Bezpečnostní průmysl EU lze nicméně rozčlenit zhruba do těchto odvětví⁵:

- bezpečnost letectví,
- bezpečnost námořní dopravy,
- bezpečnost hranic,
- ochrana kritické infrastruktury,
- protiteroristické zpravodajství (včetně kybernetické bezpečnosti a bezpečnosti komunikací),
- krizové řízení / civilní ochrana,
- ochrana fyzické bezpečnosti, a
- ochranné oděvy.

Trh v oblasti bezpečnosti má tři charakteristické znaky:

- 1) **Jedná se o značně roztržštěný trh rozdělený podél státních či dokonce regionálních hranic.** Bezpečnost je jednou z politicky nejcitlivějších oblastí, a proto patří mezi ty, u nichž se členské státy zdráhají vzdát svých národních výsad.
- 2) **Je to institucionální trh.** Z velké části se stále jedná o institucionální trh, tj. kupujícími jsou veřejné orgány. Dokonce i tam, kde má tento trh komerční charakter, se bezpečnostní požadavky stále utvářejí převážně právními předpisy.
- 3) **Má výrazný společenský rozměr.** Bezpečnost je jednou z nejzákladnějších lidských potřeb, zároveň je ovšem vysoce citlivou oblastí. Bezpečnostní opatření a technologie mohou mít dopad na základní práva a často vyvolávají obavy z možného ohrožení soukromí.

3. HLAVNÍ PROBLÉMY, JIMŽ ČELÍ BEZPEČNOSTNÍ PRŮMYSL EU

Tři výše uvedené charakteristické znaky trhu v oblasti bezpečnosti jsou zároveň určujícími faktory třech hlavních problémů, s nimiž se bezpečnostní průmysl EU potýká:

⁵ Tento seznam není vyčerpávající, podrobnější přehled o různých odvětvích a technologiích, které zahrnují, lze nalézt v pracovním dokumentu útvarů Komise.

(1) Roztříštěnost bezpečnostního trhu EU

Hlavní problém představuje značně roztržštěný charakter (např. nedostatek jednotných certifikačních postupů a norem) bezpečnostního trhu EU. Odlišné přístupy v praxi vedly k vytvoření přinejmenším 27 různých bezpečnostních trhů, každý z nich se přitom ještě dělí na velký počet bezpečnostních sektorů.

Tato skutečnost vytváří nejen poměrně unikátní situaci z hlediska vnitřního trhu, ale má rovněž značně negativní dopad na straně nabídky (průmysl) i poptávky (pořizovatelé bezpečnostních technologií z veřejného a soukromého sektoru). Způsobuje velké překážky pro vstup na trh a velmi znesnadňuje, ne-li znemožňuje, úspory z rozsahu. Tato situace má navíc za následek nedostatečnou hospodářskou soutěž mezi dodavateli a neefektivní využití veřejných prostředků.

(2) *Velká vzdálenost mezi výzkumem a trhem*

Při výzkumu a vývoji nových technologií je pro bezpečnostní průmysl v EU mnohdy velmi těžké předem odhadnout, zda půjde daný produkt dobře na odbyt, či alespoň získat určité ujištění, zda vůbec bude na trhu po takovém produktu poptávka. Přestože se jedná o rozšířený problém, s nímž se lze setkat v mnoha průmyslových odvětvích, u bezpečnostního průmyslu je zvláště relevantní, neboť ten se většinou pohybuje na institucionálním trhu.

Vede to k řadě negativních důsledků: kupříkladu se upouští od vědecko-výzkumných koncepcí se slibným potenciálem, což znamená, že určité technologie, které by mohly zlepšit bezpečnost občanů, se vůbec nedostanou na stranu poptávky.

(3) *Společenský rozměr bezpečnostních technologií*

Širší společenské přijetí nových výrobků a technologií je obvyklým problémem pro různá průmyslová odvětví. Bezpečnostní technologie ovšem mají řadu zvláštností, které je od jiných oblastí odlišují. Bezpečnostní technologie se mohou přímo či nepřímo dotýkat základních práv, např. práva na respektování osobního a rodinného života, na ochranu osobních údajů, soukromí nebo lidské důstojnosti.

Problémy související s přijetím bezpečnostních technologií společností přinášejí řadu negativních důsledků. Průmysl riskuje investici do technologií, které veřejnost nakonec nepřijme, a jde tudíž o promarněnou investici. Pro poptávající to znamená, že jsou nuceni pořídit méně kontroverzní výrobek, který však zcela nesplňuje bezpečnostní nároky.

4. ŘEŠENÍ PROBLÉMU

Komise identifikovala řadu zásadních politických opatření, jimiž lze posílit konkurenceschopnost bezpečnostního průmyslu EU, podpořit jeho růst i vytváření pracovních míst. Zásadní politická opatření se týkají těchto oblastí:

- **Odstranění roztržštěnosti trhu** vytvořením unijních/mezinárodních norem, harmonizací postupů EU pro osvědčování/posuzování shody bezpečnostních technologií a lepším využíváním součinností mezi bezpečnostními a obrannými technologiemi.

- **Zmenšení vzdálenosti mezi výzkumem a trhem** uspořádáním programů financování a větším využíváním práv duševního vlastnictví (IPR), a stejně tak plným využíváním zadávání veřejných zakázek v předobchodní fázi (dále též „PCP“) v souvislosti s bezpečnostním výzkumem v rámci Horizontu 2020⁶.
- **Lepší začlenění společenského rozměru** pečlivým posuzováním společenských důsledků, včetně dopadů na základní práva, a vytvořením mechanismů pro otestování společenských dopadů už během výzkumu a vývoje.

4.1. Odstranění roztržičnosti trhu

4.1.1. Normalizace

Normy mají při odstraňování roztržičnosti trhů důležitou úlohu a průmyslu pomáhají dosahovat úspor z rozsahu. Normy mají rovněž prvořadý význam z hlediska poptávky, zejména s ohledem na interoperabilitu technologií pro první odběratele, donucovací orgány atd. Kromě toho jsou normy nezbytné k zajištění jednotné jakosti při poskytování bezpečnostních služeb. Vytvoření norem EU a jejich prosazování na celosvětové úrovni jsou také zásadními předpoklady pro konkurenceschopnost bezpečnostního průmyslu EU ve světě.

V současnosti ovšem v EU existuje jen několik norem v oblasti bezpečnosti. Velkou překážku při vytváření skutečného vnitřního trhu v oblasti bezpečnosti představují rozdílné vnitrostátní normy, což omezuje konkurenceschopnost průmyslu EU. Chce-li EU významněji přispět k vytvoření celosvětových norem, je překonání těchto vnitrostátních rozdílů naprosto nezbytným krokem.

Již ve svém sdělení o strategické vizi pro evropské normy Komise avizovala, že je třeba urychlit práce na standardizaci v oblasti bezpečnosti⁷. V roce 2011 proto Komise pověřila evropské normalizační organizace, aby sestavily podrobný přehled platných mezinárodních, evropských i vnitrostátních norem v oblasti bezpečnosti, a rovněž připravily seznam nedostatků z hlediska normalizace. Výrazné nedostatky byly zjištěny v těchto oblastech:

- chemická, biologická, radiologická a jaderná bezpečnost a výbušniny – minimální normy pro detekci a odběr vzorků, včetně bezpečnosti letectví;
- zabezpečení hranic – společné normy pro technické fungování a interoperabilitu automatizovaných systémů pohraniční kontroly, dále normy pro biometrické identifikátory; a
- krizové řízení / civilní ochrana – normy pro interoperabilitu komunikací a interoperabilitu velení a řízení, včetně organizační interoperability, a rovněž normy pro hromadné vyrozumění obyvatelstva.

Opatření č. 1: Na základě těchto prvotních priorit Komise požádá evropské normalizační organizace, aby sestavily konkrétní a podrobné normalizační plány. Tyto plány by se měly zaměřit na nástroje a technologie příští generace. Pro zdárné provedení bude zásadní zapojení koncových uživatelů i bezpečnostního průmyslu a soudržnost politiky.

⁶ KOM(2011) 809 v konečném znění.

⁷ KOM(2011) 311 v konečném znění.

4.1.2. Postupy pro osvědčování/posuzování shody

Momentálně neexistují systémy osvědčování bezpečnostních technologií platné pro celou EU. Mezi vnitrostátními systémy panují značné rozdíly, což velkou měrou přispívá k roztržitosti trhu v oblasti bezpečnosti. Komise identifikovala oblasti⁸, u nichž by v úvodní fázi dávalo vytvoření unijního systému osvědčování největší smysl; začalo by se v těchto oblastech:

- detekční zařízení bezpečnostní kontroly na letištích, a
- poplachové systémy⁹.

V případě letištních detekčních zařízení existuje celý soubor právních předpisů EU, které stanovují požadavky na vlastnosti těchto zařízení¹⁰. Tento soubor předpisů nicméně neobsahuje požadovaný mechanismus posuzování shody, díky němuž by se osvědčení detekčního zařízení vydané jedním členským státem uznávalo ve všech ostatních členských státech. Nedostatek harmonizovaných norem a právně závazného posuzování shody letištních detekčních zařízení na úrovni EU má za následek roztržitost vnitřního trhu.

U poplachových systémů již určité evropské výkonové normy existují. Kromě toho má odvětví svůj vlastní certifikační mechanismus CertAlarm. Potíž tohoto systému ovšem spočívá v tom, že je v soukromých rukou a že orgány členských států nemají povinnost přijímat osvědčení, která jsou podle něj vydána.

V budoucnosti by produkty osvědčené podle certifikačního systému EU mohly dostávat „bezpečnostní označení EU“, po vzoru označení CE používaného pro bezpečnost výrobků. Jak navrhlo Evropské fórum pro výzkum a inovace v oblasti bezpečnosti (ESRIF), takové označení by mohlo být „pečetí kvality“ u bezpečnostních produktů (vyrobených a validovaných v EU).

Konzervativní odhady udávají, že u těchto dvou kategorií produktů by roční úspory odvětví, co se týče zkoušení a osvědčování, mohly dosáhnout až 29 milionů EUR.

Harmonizace certifikačních postupů u detekčních a poplašných systémů na letištích by měla mít rovněž pozitivní vliv na utváření zřetelnější evropské identity těchto technologií, tj. případné „obchodní značky EU“. Tato značka by měla přispět k posílení konkurenceschopnosti společností z EU ve světě, vůči jejich konkurentům z USA a Číny.

⁸ Podrobnosti ke zdůvodnění a kritériím pro výběr cílových oblastí lze nalézt v pracovním dokumentu útvarů Komise.

⁹ Je třeba poznamenat, že poplachové systémy jsou velmi důležitým segmentem, s tržním objemem ve výši 4,5 miliardy EUR, neboli 50 % trhu v oblasti fyzické bezpečnosti.

¹⁰ Viz nařízení (ES) č. 300/2008, (ES) č. 272/2009 a (EU) č. 185/2010.

Opatření č. 2: Po důkladné analýze posouzení dopadů a konzultaci se zúčastněnými stranami Komise předloží dva legislativní návrhy: první by zaváděl jednotný certifikační systém EU pro letištní detekční zařízení; druhým by se zřizoval jednotný certifikační systém EU pro poplachové systémy. Cílem je, aby byly certifikační systémy vzájemně uznatelné.

Období provádění: od poloviny roku 2012 do konce roku 2014

4.1.3. Využití synergií mezi bezpečnostními a obrannými technologiemi

Lze jasně rozlišovat mezi (civilním) bezpečnostním trhem a (vojenským) obranným trhem. Nicméně samotnou existenci těchto dvou oddělených trhů lze považovat za roztržičnost. Tato roztržičnost je do jisté míry přirozená, neboť průmyslové základny zásobující tyto dva trhy nejsou zcela totožné, liší se koncoví uživatelé i oblasti použití, a tudíž i požadavky. Tato roztržičnost je nicméně pocíťována v úvodních fázích procesu, tj. na úrovni výzkumu a vývoje a rozvoje schopností, tak v dalších fázích, konkrétně při normalizaci. Někdy to vede ke zbytečnému překrývání úsilí v oblasti výzkumu a vývoje a nemožnosti využít úspor z rozsahu kvůli lišícím se normám na těchto dvou trzích.

S Evropskou obrannou agenturou (EDA) se prostřednictvím *evropské rámcové spolupráce* v současnosti hledají součinnosti mezi civilní a vojenskou oblastí, pokud jde o výzkum a vývoj. V rámci této spolupráce probíhá koordinace mezi tématem „Bezpečnost“ sedmého rámcového programu a činnostmi EDA na poli obranného výzkumu. Smyslem je tento výzkum synchronizovat, aby se zamezilo zdvojení činností a naopak se využilo možných synergií. Komise hodlá v rámci Horizontu 2020 v této spolupráci pokračovat a rozšířit ji.

Zatímco v ještě ranější fázi by spolupráce směřující k synchronizovanějšímu plánování schopností byla užitečná, Komise se domnívá, že vzhledem k tomu, že do oblasti civilní bezpečnosti vstupuje tak velký počet veřejných orgánů, není v současné době možné ustavit společné plánování schopností s obranným sektorem, v němž je obvykle pouze jeden subjekt za každý členský stát, totiž ministerstvo obrany.

Co se týče spolupráce v koncové části procesu, Komise se domnívá, že v oblastech, kde jsou technologie stejné a též oblasti jejich použití jsou velmi podobné, by se mělo aktivně usilovat o vývoj „hybridních norem“, tj. norem vztahujících se jak na civilní, tak na obranné bezpečnostní technologie. Komise se zabývá celou řadou slibných oblastí pro takové „hybridní normy“, včetně softwarových rádií a některých technologických požadavků na bezpilotní letecké prostředky (např. technologie pro detekci a vyhnutí se jinému vzdušnému objektu, požadavky na letovou způsobilost). Jen u samotných softwarových rádií se odhaduje, že by hybridní normy mohly vést k celkovému nárůstu prodeje ve výši jedné miliardy EUR.

Opatření č. 3: Komise má v úmyslu vydat v úzké spolupráci s Evropskou obrannou agenturou evropským normalizačním organizacím mandáty pro vypracování „hybridních norem“. Brzy bude vydán první mandát pro softwarová rádia.

Období provádění: od poloviny roku 2012

4.2. Zkrácení vzdálenosti mezi výzkumem a trhem

4.2.1. Uspořádání programů financování, využití potenciálu práv duševního vlastnictví

Návrh Komise pro Horizont 2020 zakládá úzkou vazbu s několika oblastmi politiky, zejména s vnitřními věcmi. Horizont 2020 za tímto účelem předpokládá specifická pravidla týkající se práv duševního vlastnictví v oblasti bezpečnostního výzkumu, což by Komisi a členským státům nejen umožnilo přístup k předním projektům v bezpečnostním výzkumu, ale rovněž dalo možnost tento náskok za spravedlivých a přiměřených podmínek využít při následném zadávání zakázek¹¹.

To by mělo vést k bezprostřednějšímu a rychlejšímu využívání výsledků bezpečnostního výzkumu v EU ze strany vnitrostátních orgánů a k užší spolupráci s většinou veřejných koncových uživatelů, čímž by došlo k výraznému skoku v úsilí o zmenšení vzdálenosti mezi výzkumem a trhem v oblasti bezpečnosti.

Kromě toho obě složky Fondu pro vnitřní bezpečnost navržené na příští finanční období, které se týkají vnějších hranic a víz, resp. policejní spolupráce, prevence a potírání trestné činnosti a krizového řízení, počítají s tím, aby bylo možné v rámci Unii financovaných opatření testovat a ověřovat výsledky pocházející z projektů bezpečnostního výzkumu v EU¹².

K účinnému využívání této možnosti jsou nezbytným prvkem specifická pravidla týkající se práv duševního vlastnictví v oblasti bezpečnostního výzkumu, která Komisi umožní tato práva spravedlivým a přiměřeným způsobem používat, aby bylo možné výsledků bezpečnostního výzkumu využívat při navazujícím testování a ověřování.

Půjde-li o kapacity Unie a bude-li to přiměřené, zváží Komise posílit tato testovací a ověřovací opatření přímo nákupem prototypů pro EU.

Opatření č. 4: Komise plně využije nová pravidla týkající se práv duševního vlastnictví v oblasti bezpečnostního výzkumu uvedená v Horizontu 2020¹³, a to zejména ve formě možnosti uvedené ve dvou zvláštních programech Fondu pro vnitřní bezpečnost, tj. testovat a ověřovat výsledky pocházející z projektů bezpečnostního výzkumu v EU.

Období provádění: od začátku roku 2014

4.2.2. Zadávání veřejných zakázek v předobchodní fázi

Zadávání veřejných zakázek v předobchodní fázi¹⁴ je užitečným prostředkem pro překonání vzdálenosti mezi výzkumem a trhem. Komise jeho význam vyzdvihla již ve svém sdělení Unie inovací¹⁵, zejména v oblastech s institucionálním trhem nebo tam, kde trh do značné míry závisí na legislativě, neboť zadávání veřejných zakázek na inovační výrobky a služby je v době rozpočtových omezení zásadní pro zlepšení kvality a efektivity veřejných služeb. Nakupováním nových technologií by uživatelé z řad veřejného sektoru nakonec mohli díky

¹¹ KOM(2011) 810 v konečném znění.

¹² KOM(2011) 750 a 753 v konečném znění.

¹³ Přijetí těchto pravidel nicméně ještě podléhá schválení Radou a Evropským parlamentem.

¹⁴ Zadáváním veřejných zakázek v předobchodní fázi se zde rozumí přístup k pořizování služeb z oblasti výzkumu a vývoje, při němž práva duševního vlastnictví nenáleží (výhradně) veřejnému zadavateli. Viz KOM(2007) 799 v konečném znění.

¹⁵ KOM(2010) 546 v konečném znění.

zadávání veřejných zakázek v předobchodní fázi hrát významnější roli v inovačním cyklu. Pořizovatelé by měli být „tahouny změn“.

V oblasti bezpečnosti však zatím tohoto způsobu zadávání veřejných zakázek využilo jen málo členských států. Na úrovni EU bylo v rámci tématu „Bezpečnost“ sedmého rámcového programu při výběrovém řízení z roku 2011 zavedeno předprovozní validační schéma fungující jako předchůdce případného budoucího režimu zadávání veřejných zakázek v předobchodní fázi.

Součástí Horizontu 2020 je zvláštní nástroj pro zadávání veřejných zakázek v předobchodní fázi, jenž by měl podstatně pomoci s řešením praktických potíží při používání tohoto způsobu zadávání zakázek.

Na základě zkušeností USA s programem inovací a výzkumu pro malé podniky (SBIR)¹⁶ lze předběžně předpokládat, že 1% zvýšení ročního tempa růstu podporou výzkumu a vývoje pomocí režimu zadávání veřejných zakázek v předobchodní fázi by odvětví bezpečnosti do roku 2020 přineslo dodatečné tržby ve výši dvou miliard EUR.¹⁷

Opatření č. 5: Komise hodlá plně využít nástroj pro zadávání veřejných zakázek v předobchodní fázi stanovený v Horizontu 2020 a vyčlenit významnou část z rozpočtu pro bezpečnostní výzkum právě na tento nástroj. Tento nový přístup k financování by měl výzkum přiblížit trhu tím, že již od zahájení výzkumného projektu povede k propojení průmyslu, veřejných orgánů a konečných uživatelů. Komise míní, že ochrana hranic a bezpečnost letectví jsou nejslibnějšími oblastmi pro využití zadávání veřejných zakázek v předobchodní fázi.

Komise bude také nabádat členské státy, aby na své úrovni rovněž zahájily obdobné iniciativy, a to v souladu s příslušnými právními předpisy EU pro zadávání veřejných zakázek.

Období provádění: od začátku roku 2014

4.2.3. Přístup k zahraničním veřejným zakázkám

Přístup k veřejným zakázkám v EU je tradičně velmi otevřený. Ne vždy tomu ovšem odpovídá podobný stupeň otevřenosti ze strany našich obchodních partnerů. V celosvětovém měřítku je pouze čtvrtina veřejných zakázek přístupná mezinárodní konkurenci.

Komise navrhla nařízení¹⁸, jež má pomoci zpřístupnit veřejné zakázky v celosvětovém měřítku a zajistit, aby k nim evropské podniky měly spravedlivý přístup. Toto nařízení má poskytnout řadu nástrojů, které zajistí dosažení těchto cílů.

Opatření č. 6: Komise beze zbytku využije veškerých dostupných nástrojů, aby svému bezpečnostnímu průmyslu zajistila spravedlivý přístup na mezinárodní trhy s veřejnými

¹⁶ Zkratka SBIR znamená „Small Business Innovation and Research“ (inovace a výzkum pro malé podniky), jedná se o americký program na podporu inovací v malých a středních podnicích pomocí režimu PCP.

¹⁷ Viz pracovní dokument útvarů Komise.

¹⁸ COM(2012) 124 final.

zakázkami. Vzhledem k citlivosti bezpečnostních technologií se bude věnovat nejvyšší pozornost příslušným vývozním předpisům.

Období provádění: od konce roku 2013

4.2.4. Omezení odpovědnosti vůči třetím stranám

K překonání vzdálenosti mezi výzkumem a trhem a zejména ve snaze zajistit, aby hrozba odpovědnosti neodrazovala bezpečnostní průmysl od vývoje, zavádění a komercializace technologií a služeb, které by mohly zachraňovat lidské životy, přijaly USA po 11. září 2001 zákon o bezpečnosti USA. Zákon o bezpečnosti USA zavádí omezení právní odpovědnosti v případě dodavatelů protiteroristických technologií a služeb. Na trzích třetích zemí by tato právní úprava mohla poskytnout trhu vévodícím společnostem z USA konkurenční výhodu vůči jejich protějškům z EU.

Je evidentní, že zákon o bezpečnosti USA vznikl ve specifickém americkém právním kontextu, v němž se nezřídka používá koncept skupinové žaloby. Přestože se neuvažuje o tom, že by se v Evropě zavedl protějšek zákona o bezpečnosti USA, je nicméně třeba lépe pochopit a prostudovat, do jaké míry odrazují otázky související s odpovědností průmysl od uvádění slibných technologií a služeb na trh.

Mezi zúčastněnými stranami z řad průmyslu nepanuje na toto téma obecnější shoda a je nejprve nutné provést důkladnou právní analýzu, pokud jde o slučitelnost s právními předpisy členských států či EU.

Opatření č. 7: Komise vyhlásila výběrové řízení na zpracování rozsáhlé studie, která poskytne analýzu právních a hospodářských důsledků omezení odpovědnosti vůči třetím stranám. Studie se bude zabývat i alternativami k omezení odpovědnosti vůči třetím stranám v podobě, v jaké je upraveno v zákoně o bezpečnosti USA, např. myšlenkou odvětvového fondu vytvořeného na základě dobrovolnosti, doporučením Komise atd. Tato studie vezme náležitě v úvahu důsledky související se základními právy.

Období provádění: od roku 2012 do poloviny 2013

4.3. Lepší začlenění společenského rozměru

4.3.1. Kontrola společenských dopadů během výzkumu a vývoje

Lepší začlenění společenského rozměru do činností bezpečnostního průmyslu by pomohlo zmenšit nejistotu, co se týče přijetí společností. Mělo by to umožnit efektivní využití investic do výzkumu a vývoje a poptávající straně umožnit nakupovat produkty, které beze zbytku odpovídají jejím bezpečnostním nárokům a zároveň jsou akceptovány ve společnosti.

Komise tudíž zastává názor, že ke společenským důsledkům i dopadům na základní práva by se mělo přihlížet ještě před zahájením výzkumu a vývoje a v jeho průběhu, a to formou zapojení společnosti. Společenským problémům by se tak bylo možné věnovat již v rané fázi procesu.

Komise již podnikla řadu kroků s cílem zařadit společenský rozměr mezi hlavní body tématu Bezpečnost v rámci sedmého rámcového programu. Vzhledem k Horizontu 2020 je však třeba

již nyní konsolidovat toto úsilí, zapojit společnost do výzkumu a inovací a systematictěji provádět ověřování společenského dopadu.

Komise zapojí společnost a ve vhodných případech zařadí testování společenského dopadu mezi povinné prvky všech svých budoucích projektů bezpečnostního výzkumu¹⁹. Komise bude zvláště ověřovat společenský dopad nových technologií ve všech svých výše uvedených režimech zadávání veřejných zakázek v předobchodní fázi, budou-li souviset s bezpečností.

4.3.2. Ochrana soukromí již od návrhu (*privacy by design*) a standardní nastavení ochrany soukromí (*privacy by default*)

Je velice obtížné převést společenská hlediska do technologických požadavků, navíc to ještě dále komplikuje široká škála bezpečnostních produktů na trhu. Společenské otázky související s bezpečností se navíc mezi členskými státy značně liší.

Vzhledem k tomu Komise za nejlepší způsob, jak dále postupovat, považuje začlenit do vývojové fáze koncepty ochrany soukromí již od návrhu (*privacy by design*) a standardního nastavení ochrany soukromí (*privacy by default*)²⁰. Za tímto účelem by hospodářský subjekt, který si přeje, aby byl jeho výrobní postup uznán auditem za vyhovující z hlediska ochrany soukromí již od návrhu, musel splnit soubor požadavků stanovených příslušnou normou EU. Tato norma bude dobrovolná. Komise je však přesvědčena, že se vytvoří silný vzájemný tlak na to, aby se společnosti řídily takovou normou, jejíž hodnota by se postupně měla uznávat podobně jako například norma pro management ISO 9000.²¹

Opatření č. 8: Komise vydá evropským normalizačním organizacím mandát, aby vytvořily normu vycházející ze stávajících systémů řízení jakosti, avšak aplikovanou na řízení problematiky ochrany soukromí během konstrukční fáze.

Období provádění: od poloviny roku 2012 do poloviny roku 2015

5. MONITOROVÁNÍ

Dohled nad monitorováním oznámených politických opatření bude provádět odpovídající skupina odborníků zřízená Komisí. Skupinu budou tvořit všichni relevantní aktéři z oblasti bezpečnosti.

K monitorování pokroku se tato skupina bude scházet nejméně jednou ročně.

6. ZÁVĚR

Toto je první akční plán Komise, který se zaměřuje čistě na odvětví bezpečnosti. Nejde však jen o prvenství oznámených opatření, ale naprostou novinkou je rovněž ucelenost přístupu od vědecko-výzkumné fáze až po normalizaci a osvědčování. V závislosti na budoucím

¹⁹ S výjimkou „nevhodných“ oblastí, např. základního technologického výzkumu a prognostických projektů a scénářů.

²⁰ Více podrobností o ochraně soukromí již od návrhu lze nalézt v pracovním dokumentu útvarů Komise.

²¹ KOM(2012) 11.

posuzování by mezi další případné oblasti harmonizace mohla patřit odvětví pozemní a námořní dopravy a rovněž řešení problematiky omezení odpovědnosti vůči třetím stranám.

Je třeba si uvědomit, že všechna opatření uvedená v tomto dokumentu jsou úzce navázána na ochotu členských států spolupracovat s orgány EU, normalizačními orgány a zúčastněnými subjekty z veřejného i soukromého sektoru, aby se podařilo odstranit roztržitost bezpečnostních trhů v EU. Komise proto členské státy vybízí, aby ji podpořily při její snaze o zvýšení konkurenceschopnosti podniků z EU působících v oblasti bezpečnosti a při zmenšování stávajících překážek bránících vstupu na trh.

Komise je přesvědčena, že politická opatření tohoto akčního plánu výrazně přispějí ke zlepšení konkurenceschopnosti evropského bezpečnostního průmyslu. Cílem Komise je poskytnout bezpečnostnímu průmyslu EU pevnou domácí základnu, z níž bude moci expandovat na nové a rozvíjející se trhy, kde lze do budoucna očekávat velký růst v oblasti bezpečnosti.

Tento růst uvnitř a za hranicemi EU musí jít ruku v ruce s důraznějšími opatřeními zaměřenými na lepší začlenění společenského rozměru do činností bezpečnostního průmyslu. Ochranu soukromí již od návrhu a respektování základních práv je třeba pojmut jako zásadní a nedílný prvek veškerých bezpečnostních technologií pocházejících z EU.