EVROPSKÁ KOMISE

V Bruselu dne 30.9.2010
SEK(2010) 1127

PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE

SOUHRN POSOUZENÍ DOPADŮ

Průvodní dokument

k návrhu

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

týkající se Evropské agentury pro bezpečnost sítí a informací (ENISA)

{KOM(2010) 521 v konečném znění}
{SEK(2010) 1126}

SOUHRN POSOUZENÍ DOPADŮ

1. OBLAST PŮSOBNOSTI A SOUVISLOSTI

1.1. Oblast působnosti

Posouzení dopadů se zaměřuje na to, jak by se modernizovaná agentura pro bezpečnost sítí a informací (NIS), která je široce uznávaná jako vhodný a nezbytný politický nástroj k řešení úkolů NIS, měla co nejlépe zformovat, aby orgány členských států a Komise podporovala v dosahování politických cílů NIS, když platnost mandátu Evropské agentury pro bezpečnost sítí a informací (ENISA) skončí v březnu 2012.

1.2. Souvislosti

V současném světě se společnost a ekonomika zásadně spoléhají na řádné fungování informačních a komunikačních technologií (IKT). Je proto velmi důležité zajistit, aby byly systémy stabilní a aby jim uživatelé důvěřovali. Zvyšující se počet hrozeb, útoků a škodlivého softwaru používaných proti systémům by mohl ohrozit řádné fungování základní infrastruktury sítí a informací. Vzhledem k tomu, že tyto systémy a sítě jsou nadnárodní, je nutné v rámci Evropy reagovat na úkoly bezpečnosti sítí a informací (NIS).

Pro řešení těchto otázek byla v roce 2004 na dobu pěti let vytvořena Evropská agentura pro bezpečnost sítí a informací (ENISA)[1] s cílem *„zajistit vysokou a účinnou bezpečnost sítí a informací v rámci Společenství (...) a vytvořit kulturu bezpečnosti sítí a informací v zájmu občanů, spotřebitelů, podniků a organizací veřejného sektoru v Evropské unii a přispět tím k řádnému fungování vnitřního trhu“*.

Od té doby se úkoly NIS neustále měnily v souladu s technologickým vývojem a vývojem trhu. Proto Komise spolu s příslušnými zúčastněnými stranami s dostatečným předstihem před ukončením platnosti nařízení ENISA v březnu 2009 zahájila postup stanovení, jaké politické návrhy by po roce 2009 nejlépe odpovídaly cílům NIS EU. Po hodnocení agentury ENISA v polovině období v roce 2007[2] a po veřejné konzultaci[3] přijaly Rada a Evropský parlament dne 24. září 2008 nařízení, kterým se mandát agentury ENISA beze změny prodlužuje o tři roky do 13. března 2012[4]. V odůvodnění k tomuto nařízení Rada a Evropský parlament vyzvaly k ***„dalšímu jednání o agentuře [a] o obecném směřování evropského úsilí o vyšší bezpečnost sítí a informací“.***

V listopadu 2008 Komise přispěla k diskusi zahájením další veřejné konzultace o možných cílech posílené politiky NIS na úrovni EU a o prostředcích k dosažení těchto cílů[5]. V prosinci 2008 Komise uspořádala rovněž seminář o nástrojích a mechanismech posílené politiky EU

---

1 Nařízení Evropského parlamentu a Rady (ES) č. 460/2004 ze dne 10. března 2004 o zřízení Evropské agentury pro bezpečnost sítí a informací.

2 Sdělení Komise Evropskému parlamentu a Radě ohledně hodnocení Evropské agentury pro bezpečnost sítí a informací (ENISA), KOM(2007)285 v konečném znění, 1.6.2007, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:EN:NOT.

3 Konzultace probíhala od 13. června do 7. září 2007.

4 Nařízení Evropského parlamentu a Rady (ES) č. 1007/2008 ze dne 24. září 2008, kterým se mění nařízení (ES) č. 460/2004 o zřízení Evropské agentury pro bezpečnost sítí a informací, pokud jde o období její činnosti, Úř. věst. L 293, 31.10.2008.

5 Od 7. listopadu 2008 do 9. ledna 2009, zpráva je k dispozici na http://ec.europa.eu/information_society/policy/nis/nis_public_consultation/index_en.htm.

týkající se NIS za účasti odborníků na otázky NIS z příslušných subjektů členských států. Kromě toho v březnu 2009 Komise přijala sdělení o ochraně kritické informační infrastruktury (CIIP)[6], které stanoví klíčovou úlohu agentury ENISA v podpoře EU za účelem zvýšení bezpečnosti, odolnosti a připravenosti. Tento přístup byl schválen na ministerské konference o ochraně kritické informační infrastruktury, která se konala ve dnech 27. – 28. dubna 2009 v Talinu; v jednom z jejich závěrů se uvádí, že ***„nové a dlouhotrvající úkoly, které stojí před námi, si vyžadují důkladné přehodnocení a přeformulování mandátu agentury s cílem lepšího zaměření na priority a potřeby Unie;*** *dosažení schopnosti pružnější reakce; rozvoje evropských dovedností a odborných schopností; a podpory provozní efektivnosti a celkového vlivu agentury. Takto by se agentuře ENISA mohly poskytnout stálé prostředky ve prospěch každého členského státu a Evropské unie jako celku“*.

Dne 18. prosince 2009 bylo přijato usnesení Rady o *„společném evropském přístupu k bezpečnosti sítí a informací“*[7], které kromě jiného zdůraznilo, že ***„ENISA by v rámci revidovaného mandátu měla sloužit jako odborné středisko EU v záležitostech spojených s bezpečností sítí a informací v EU“***.

Ve strategii Komise Evropa 2020 pro inteligentní a udržitelný růst podporující začlenění[8] je jednou ze stěžejních iniciativ Digitální agenda pro Evropu, v níž hraje NIS ústřední roli. **Cílem této politické iniciativy za důvěru a bezpečnost v Digitální agendě pro Evropu je umožnit EU, členských státům a zúčastněným stranám rozvíjet vysoký stupeň schopnosti a připravenosti prevence problémů NIS, jejich odhalování a lepší reakci na ně.** Přispěje to ke zvýšení důvěry v jednotný digitální trh Evropy, k jeho bezpečnosti a k lepší konkurenceschopnosti evropských podniků.

2. VYMEZENÍ PROBLÉMŮ

2.1. V čem spočívá problém?

Byly určeny tyto příčiny problému, které způsobují, že zúčastněné strany jsou citlivé na hrozby pro NIS a bezpečnostní události v NIS. Ty všechny ukazují, že je potřebná spolehlivá struktura na úrovni EU s cílem řešit problém a udržet krok s neustále se měnící technologií a podmínkami trhu ve vztahu k NIS v celé Evropě.

- **Rozdílnost a roztříštěnost vnitrostátních přístupů.** Problémy NIS nejsou omezeny státními hranicemi, a proto je nelze účinně řešit pouze na vnitrostátní úrovni. Současně existují velké rozdíly v tom, jak tento problém řeší veřejné orgány v různých členských státech. Mnohočetné požadavky na bezpečnost v různých členských státech mají za následek nákladovou zátěž pro podniky, které působí na úrovni celé Evropské unie, a vedou k roztříštěnosti a nedostatečné konkurenční schopnosti na evropském vnitřním trhu.

- **Omezená schopnost evropského včasného varování a reakce.** Současné vnitrostátní systémy včasného varování a řešení bezpečnostních událostí se v členských státech značně liší a neexistuje žádný systém EU. EU potřebuje politický nástroj, který by určoval rizika

---

6 Sdělení Komise Evropskému parlamentu a Radě o ochraně kritické informační infrastruktury, KOM (2009) 149 v konečném znění, 30.3.2009.

7 Usnesení Rady ze dne 18. prosince 2009 o společném evropském přístupu k bezpečnosti sítí a informací, (2009/C 321/01).

8 KOM(2010) 2020.

a zranitelnost NIS, vytvořil vhodné mechanismy reakce a zajistil, aby tyto mechanismy reakce byly známy a aby je zúčastněné strany uplatňovaly.

- **Nedostatek spolehlivých údajů a omezené znalostí o nově vznikajících problémech.** Existuje velmi málo spolehlivých kvantitativních informací o dopadu nebo dokonce i o výskytu bezpečnostních událostí NIS, což tvůrcům politik stěžuje přijímání odpovídajících politických opatření a podnikům komplikuje rozhodování o investicích do bezpečnosti.

- **Nízká úrovně informovanosti o rizicích a úkolech NIS.** Odpovědnost za zajištění NIS spočívá na jednotlivých zúčastněných stranách; jejich odpovědnost však není vždy jasně vymezena a uložena. Na jedné straně spotřebitelé často podceňují rizika NIS a zanedbávají osobní odpovědnost za zajištění svých systémů IKT. Na druhé straně podniky mnohdy vidí hlavně náklady na NIS a ne potenciální úspory, které přináší.

- **Mezinárodní rozměr problémů bezpečnosti sítí a informací.** Hrozby pro NIS a jakékoli další bezpečnostní události mají mezinárodní povahu, takže opatření EU mohou být méně účinná, pokud se problémy NIS nebudou odpovídajícím způsobem řešit také v mezinárodním rámci. Musíme rozvíjet strategii EU a referenční bod pro NIS, aby EU zaujala lepší postavení na mezinárodním poli.

- **Potřeba modelů spolupráce pro zajištění odpovídajícího provádění politik.** Odpovídající provádění politik NIS si vyžaduje modely spolupráce na úrovni EU. Zúčastněné strany potřebují návod v určování hrozeb NIS a rozvíjení osvědčených postupů v provádění existujících politik NIS.

- **Potřeba účinnějších opatření proti počítačové trestné činnosti.** Úsilí v NIS bylo vyvíjeno převážně na základě dřívějšího prvního pilíře, tj. otázky projednávané mezi institucemi. Se vstupem Lisabonské smlouvy v platnost je však nutné zohlednit širší balíček úkolů pro agenturu NIS, které by se vztahovaly rovněž na oblasti „druhého a třetího pilíře“, tj. otázky, o nichž dříve rozhodovala sama Rada.

2.2. Koho se problém nejvíce dotýká?

Bezpečnostní události NIS by mohly mít velký dopad na různé zúčastněné strany zahrnující velké a malé podniky, veřejné orgány a správy a jednotlivé občany. Jinými slovy, NIS se dotýká každého a každý je za ni odpovědný.

K dispozici je pouze málo objektivních kvantitativních informací o přesném počtu bezpečnostních událostí v NIS a/nebo o jejich příslušných ekonomických dopadech, nebo nejsou žádné takové informace. Jedna zmínka je ve studii trhu IDC EMEA[9], kde se uvádí, že za posledních 12 měsíců mělo 28 % domácností EU-27 problémy se spamem nebo viry. Průměrně se bezpečnostní události v uplynulém roce vyskytly u přibližně 7 % uživatelů z řad podniků.

[9] IDC EMEA, Evropský trh bezpečnosti sítí a informací, scénář, trendy a úkoly, duben 2009, s odkazem na průzkum elektronických komunikací Eurobarometru, duben 2007.

3. ZDŮVODNĚNÍ OPATŘENÍ EU, PŘIDANÁ HODNOTA EU A SUBSIDIARITA

Vzájemná závislost sítí a informačních systémů mimořádně stěžuje, jestli dokonce vůbec neznemožňuje, jednotlivým subjektům správně posoudit globální ekonomický a sociální dopad opatření na ochranu proti bezpečnostním událostem v NIS. Rozdílné vnitrostátní politiky a postupy narušují vnitřní trh z důvodů negativních vnějších faktorů bezpečnostních událostí v NIS (neadekvátní politiky se dotýkají trhů v jiných členských státech), jakož i z důvodů pozitivních vnějších faktorů osvědčených postupů NIS (osvědčený postup v jednom členském státě zvýší NIS jako celek a přinese tím zřejmý prospěch pro společnost). Proto je politický zásah EU odůvodněný, neboť poskytne skutečnou přidanou hodnotu k fungování vnitřního trhu. Tato přidaná hodnota byla uznána také v nařízení (ES) č. 460/2004 o zřízení agentury ENISA, které uvádí, že pravomoci agentury ENISA jsou zaměřeny na to, aby přispívaly k řádnému fungování vnitřního trhu.

Zásah EU do politiky NIS je dále odůvodněn *zásadou subsidiarity*. Jak bylo uvedeno ve sdělení o CIIP, strategie EU spočívající v úplném nezasahování do vnitrostátních politik NIS se spíše blíží požadavku, aby si každý členský stát kryl vlastní záda bez ohledu na vzájemnou závislost informačních systémů. Příslušný stupeň koordinace mezi členskými státy s cílem zajistit, aby přeshraniční důsledky rizik NIS bylo možné dobře zvládnout, je proto v souladu se zásadou subsidiarity. Opatření EU dále zvýší účinnost existujících vnitrostátních politik.

Občané EU svěřují své údaje čím dál tím víc komplexním informačním systémům (např. „cloud computing"). Vytvoření harmonizované a společné politiky NIS může mít proto velmi příznivý vliv na účinnou *ochranu základních práv*, a zejména práv na *ochranu osobních údajů a soukromí*. Také z tohoto důvodu se další politické opatření zdá být dostatečně odůvodněné.

4. CÍLE POLITIKY

Toto posouzení dopadů zkoumá rozsah, v jakém by modernizovaná agentura NIS, která je široce uznávaná jako nejvhodnější organizační struktura, mohla být co nejlépe zformována, aby spolu s jinými nástroji Unie přispívala k dosahování cílů politiky.

Obecným cílem je umožnit EU, členských státům a zúčastněným stranám rozvíjet vysoký stupeň schopnosti a připravenosti pro zamezení problémům NIS, pro jejich zjišťování a pro lepší reakci na ně. Přispěje to ke zvýšení důvěry v jednotný digitální trh Evropy a jeho bezpečnost a k lepší konkurenceschopnosti evropských podniků.

Tento cíl je rozdělen do sedmi **specifických cílů:**

1) **soulad regulačních přístupů** – poskytování návodů a poradenství pro Komisi a členské státy o aktualizaci a rozvoji holistického právního rámce v oblasti NIS;

2) **prevence, odhalování a reakce** – zlepšení připravenosti přispíváním k evropskému včasnému varování a schopnosti reagovat na bezpečnostní události, celoevropské pohotovostní plány a cvičení;

3) **podpora vytváření politik** – poskytování pomoci a poradenství Komisi a členským státům;

4) **oprávnění zúčastněných stran** – vytváření kultury bezpečnosti a řízení rizik stimulováním sdílení informací a široké spolupráce mezi subjekty veřejného a soukromého sektoru, také za účelem přímého přínosu pro občany a malé a střední podniky a vytváření kultury informovanosti o NIS.

5) **Evropa jako životaschopný hráč na mezinárodní úrovni** – dosažení vysoké úrovně spolupráce se třetími zeměmi a mezinárodními organizacemi za účelem podpory společného globálního přístupu k NIS a vyvíjení vlivu na mezinárodní iniciativy v Evropě na vysoké úrovni;

6) **společné provádění** – usnadňování spolupráce v provádění politik NIS;

7) **boj s počítačovou trestnou činností** – rozvoj účinné reakce na aspekty počítačové trestné činnosti ve vztahu k NIS za pomoci spolupráce s orgány (dřívějšího) druhého a třetího pilíře, např. s Europolem.

5. PŘÍPADNÉ ORGANIZAČNÍ FORMY A MOŽNOSTI POLITIKY

V posuzování dopadů (kapitola 4 a příloha 4) se zkoumá řada případných organizačních forem za účelem provádění výše uvedených možností politiky, včetně: i) agentury, ii) více nebo méně formalizovaného partnerství mezi veřejným a soukromým sektorem (PPP), iii) neformální kontaktní sítě, iv) stálé sítě příslušných orgánů a v) přímého začlenění do útvaru Komise.

Když se srovnají tyto různé organizační formy, forma agentury se podle všeho nejlépe hodí jako politický nástroj výběru, neboť má výhody týkající se: 1) právní jistoty organizační struktury a také podstaty věci, 2) její vhodnosti pro konkrétní otázky v tak citlivé oblasti jako NIS (subjekt vnější odbornosti, koordinace vztahu se zúčastněnými stranami, zapojení/závazek členských států) a 3) přijetí agentury ENISA do společenství NIS a její dobrá pověst v něm.

Byly tedy zpracovány tyto možnosti politiky, které byly podrobně posouzeny z hlediska organizační formy agentury.

Možnost politiky 1: žádná politika

Možnost „žádná politika“ předpokládá, že ENISA přestane po březnu 2012 existovat a žádná jiná instituce EU nepřevezme všechny současné činnosti agentury ENISA ani jejich část.

Ukončení činnosti agentury ENISA by znamenalo, že veškeré investice vynaložené dosud např. na zřízení organizace, která je schopna získat vysoce specializované odborníky, na sbírání zkušeností a na vytváření sítí se zúčastněnými stranami a mezi nimi a s mezinárodními institucemi, by byly pozastaveny ve chvíli, kdy se existující agentura začala dobře fungovat.

Složitá povaha problému NIS v Evropě si vyžaduje modernizovanou a posílenou agenturu a ne ukončení činnosti existující agentury. Je to potvrzeno výslovnou úlohou přidělenou agentuře například v upraveném regulačním rámci pro elektronické komunikace[10]

[10] Viz http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2009:337:SOM:EN:HTML.

a ve všeobecné podpoře významnější úlohy evropské agentury NIS vyjádřené zúčastněnými stranami.

Možnost politiky 2: Pokračování stejně jako dřív

Možnost 2 představuje scénář „obvyklého stavu“, tj. pokračování téhož politického nástroje ve stejné formě a se stejnými zdroji. Mezi zúčastněnými stranami existuje všeobecná shoda, že ENISA dozrála do důvěryhodného referenčního bodu pro otázky NIS a vyvinula se jako středisko excelence ve své oblasti.

S ohledem na současný stav zaměstnanců a rozpočtová omezení bude agentura schopna ovlivňovat pouze velmi omezený počet otázek NIS. To je však v rozporu s celkovými očekáváními zúčastněných stran. Pokud se agentuře nedá možnost dalšího rozvoje a nevyhoví se těmto zvyšujícím se očekáváním, mohlo by to nakonec vést ke krizi důvěryhodnosti.

Možnost politiky 3: Rozšíření úkolů vymezených v současné době pro agenturu ENISA a doplnění donucovacích orgánů a orgánů pro ochranu soukromí jako plnohodnotných zúčastněných stran.

Na základě této možnosti by se úloha agentury NIS rozšířila se zaměřením na:

- vytváření a udržování spojovací sítě mezi zúčastněnými stranami a sítě informací;
- působení jako středisko podpory NIS pro rozvoj politik a jejich provádění (zejména s ohledem na soukromí a elektronické komunikace, elektronický podpis, elektronickou identifikaci a norem zadávání veřejných zakázek pro NIS);
- podpora CIIP EU a politiky odolnosti (např. cvičení, EP3R[11], Evropský systém pro varování a sdílení informací atd.);
- vytvoření rámce EU pro sběr údajů o NIS, včetně rozvoje metod a postupů pro podávání a sdílení zpráv, které vyplývají z právních předpisů;
- zkoumání ekonomiky NIS a podávání zpráv o ní;
- stimulování spolupráce se třetími zeměmi a mezinárodními organizacemi za účelem podpory společného globálního přístupu k NIS a vyvíjení vlivu na mezinárodní iniciativy na vysoké úrovni v Evropě;
- plnění neoperativních úkolů týkajících se aspektů NIS v oblasti vymáhání práva a justiční spolupráce.

Agentura by měla k dispozici veškeré zdroje potřebné k tomu, aby své činnosti vykonávala s uspokojivou důkladností, tj. tak, aby mohla vyvíjet skutečný vliv. Pokud by ENISA disponovala více zdroji, mohla by převzít aktivnější roli a ujmout se více iniciativ s cílem stimulovat aktivní účast zúčastněných stran. Tato nová situace by kromě toho umožnila pružněji a rychle reagovat na změny v neustále se vyvíjejícím prostředí NIS.

Možnost politiky 4: doplnění boje proti počítačovým útokům a reakce na počítačové bezpečnostní události do operativních úkolů.

Kromě činností uvedených v možnosti 3 by agentura plnila operativní úkoly, jako je převzetí aktivnější úlohy v CIIP EU, např. v předcházení bezpečnostním událostem a v reakci na ně,

[11] Evropské partnerství mezi veřejným a soukromým sektorem pro odolnost (E3PR), viz KOM(2009) 149.

zejména působením jako skupina pro reakci na počítačové hrozby (CERT) v NIS EU a koordinováním vnitrostátních skupin CERT jako středisko EU proti útokům na NIS, včetně běžných činností řízení a poskytování pohotovostních a záchranných služeb.

Tato možnost by si vyžádala značné zvýšení rozpočtu a lidských zdrojů agentury, což vyvolává obavy o její kapacitu čerpání a efektivního využívání rozpočtu ve vztahu k přínosům, jichž má být dosaženo.

Možnost politiky 5: doplnění podpory donucovacích a justičních orgánů v boji s počítačovou trestnou činností do operativních úkolů.

Kromě činností uvedených v možnosti 4 by tato možnost zahrnovala úkoly agentury týkající se:

- poskytování podpory v procesním právu (viz Úmluva o počítačové trestné činnosti): např. sběr provozních údajů, zachycování údajů o obsahu, monitorování toků v případě útoků, jejichž důsledkem je odepření služby;
- působení jako středisko odbornosti pro trestní vyšetřování, včetně aspektů NIS.

Stejně jako v případě možnosti 4 by si to vyžádalo podstatné zvýšení zdrojů agentury a vznikají podobné obavy o kapacitu čerpání a efektivního využívání rozpočtu.

6. SROVNÁNÍ MOŽNOSTÍ POLITIKY A POSOUZENÍ DOPADŮ

Analýza možných ekonomických a sociálních dopadů a dopadů na životní prostředí ukazuje, že ***možnost 1*** by měla v každém ohledu negativní účinky a situace by se zhoršila.

Možnost 2 se nezdá být optimální, neboť agentura by neměla potřebné zdroje pro náležité plnění úkolů neustále se měnícího prostředí NIS, což by mohlo vést k riziku poškození dobrého jména a – nakonec – ke krizi důvěryhodnosti.

Na základě ***možnosti 3*** by modernizovaná agentura NIS přispěla ke:

Snížení roztříštěnosti vnitrostátních přístupů (příčina problému 1), zvýšení politiky založené na údajích a znalostech/informacích a rozhodování (příčina problému 3) a zvýšení celkové informovanosti o rizicích a úkolech NIS a jejich řešení (příčina problému 4) tím, že by napomáhala

- účinnějšímu shromažďování příslušných informací o rizicích, hrozbách a zranitelnosti každým jednotlivým členským státem;
- lepší dostupnosti informací o současných a budoucích úkolech a rizicích NIS;
- zajišťování kvalitnější politiky NIS v členských státech.

zlepšení schopnosti evropského včasného varování a reakce (příčina problému 2):

- napomáháním Komisi a členským státům v uspořádání celoevropských cvičení, čímž by bylo dosaženo úspor z rozsahu v reakci na bezpečnostní události v rámci celé EU;

- usnadňováním fungování EP3R, což by nakonec vedlo k vyšším investicím vyvolaným společnými politickými cíli a normám pro bezpečnost a odolnost na úrovni EU.

podpoře společného globálního přístupu k NIS (příčina problému 5):

- zvýšenou výměnou informací a znalostí s nečlenskými zeměmi EU.

účinnějšímu a efektivnějšímu boji s počítačovou trestnou činností (příčina problému 7):

- zapojením do neoperativních úkolů týkajících se vymáhání práva a justiční spolupráce v aspektech NIS, jako je obousměrná výměna informací a školení (např. ve spolupráci s Evropskou policejní akademií CEPOL).

Možnost 4 by kromě dopadů na základě možnosti 3 měla větší vliv na operativní úrovni. Kdyby agentura působila jako CERT NIS EU a koordinovala vnitrostátní skupiny CERT, přispěla by k vyšším úsporám z rozsahu v reakci na bezpečnostní události v rámci celé EU a nižším provozním rizikům pro podnikání, například zásluhou vyšší úrovně bezpečnosti a odolnosti.

Možnost 5 by dosáhla vyšší efektivnosti v boji s počítačovou trestnou činností než možnost 3 a 4 tím, že by podpora donucovacích a justičních orgánů byla doplněna do jejich operativních úkolů.

I kdyby však možnost 4 a 5 měla větší pozitivní dopady než možnost 3, obě tyto možnosti by byly pro členské státy politicky citlivé, pokud jde o jejich úkoly CIIP (tj. řada členských států by nebyla pro centralizované operativní úkoly). Kromě toho rozšíření mandátu posuzované na základě možnosti 4 a 5 může vést k nejednoznačnému postavení agentury. Doplnění těchto nových a úplně rozdílných operativních úkolů do mandátu agentury by se v krátkodobém časovém horizontu mohlo navíc ukázat jako velmi náročné a je značné riziko, že by agentura v přiměřené lhůtě nebyla schopna řádně splnit tento druh úkolu. V neposlední řadě jsou náklady na provádění možnosti 4 a 5 příliš vysoké – potřebný rozpočet by byl čtyřikrát nebo pětkrát vyšší než současný rozpočet agentury ENISA.

Když se srovnají dopady všech pěti možností politiky na organizační formu modernizované agentury NIS, možnost l a 2 se musí vyloučit, neboť žádná z nich by neumožnila odpovídající řešení složitého problému NIS na úrovni EU. Na druhé straně možnosti 3, 4 a 5 by EU umožnily náležitě řešit budoucí možnosti politiky NIS. Možnosti 4 a 5 se v současné době zdají být příliš ambiciózní, pokud jde o politickou citlivost většiny členských států i rozpočtové důsledky. ***Možnost 3 se tedy jeví jako nejlepší pro řešení sedmi problémů NIS určených jako nejúčinnější.***

7. MONITOROVÁNÍ A HODNOCENÍ: JAK BY SE MĚLY MĚŘIT SKUTEČNÉ NÁKLADY A PŘÍNOSY A DOSAŽENÍ ŽÁDOUCÍCH ÚČINKŮ?

Politická iniciativa by zajistila pravidelné hodnocení, které by Komise předávala Evropskému parlamentu a Radě a zveřejňovala by je. Tato hodnocení by přihlížela k názorům příslušných zúčastněných stran na základě mandátu agentury schváleného správní radou a posuzovala by efektivnost agentury v dosahování jejích cílů a zda je agentura nadále účinným nástrojem, zda by měly být přijaty nějaké změny v jejím mandátu a/nebo jiných aspektech nařízení o jejím zřízení. Po hodnocení by správní rada agentury dala Komisi doporučení týkající se všech

příslušných změn nařízení, které by měly být přijaty. Správní rada a výkonný ředitel agentury přihlédnou k výsledkům hodnocení ve víceletém plánování agentury.

Činnost agentury je pod dohledem veřejného ochránce práv v souladu s článkem 228 Smlouvy.