KOMISE EVROPSKÝCH SPOLEČENSTVÍ

V Bruselu dne 30.3.2009
KOM(2009) 149 v konečném znění

# SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, RADĚ, EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ

## o ochraně kritické informační infrastruktury

## „Ochrana Evropy před rozsáhlými počítačovými útoky a narušením: zvyšujeme připravenost, bezpečnost a odolnost“

**{SEK(2009) 399}**
**{SEK(2009) 400}**

(předložená Komisí)

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

**o ochraně kritické informační infrastruktury**

**„Ochrana Evropy před rozsáhlými počítačovými útoky a narušením: zvyšujeme připravenost, bezpečnost a odolnost“**

## 1. ÚVOD

Informační a komunikační technologie (IKT) jsou stále úžeji propojeny s naším každodenním životem. Některé z těchto systémů, služeb, sítí a infrastruktur IKT (krátce infrastruktur IKT) tvoří zásadní součást evropského hospodářství a společnosti, neboť jednak poskytují základní zboží a služby, jednak tvoří podpůrnou platformu dalších kritických infrastruktur. Obvykle se považují za kritické informační infrastruktury (KII)[1], protože jejich narušení nebo zničení by mělo závažný dopad na životně důležité společenské funkce. K nedávným příkladům patří rozsáhlé počítačové útoky na Estonsko v roce 2007 a poškození transkontinentálních kabelů v roce 2008.

Podle odhadů Světového hospodářského fóra z roku 2008 existuje v následujících deseti letech 10–20% pravděpodobnost závažné poruchy KII s potenciálními celosvětovými hospodářskými náklady ve výši přibližně 250 miliard USD[2].

Toto sdělení se zaměřuje na prevenci, připravenost a informovanost a stanoví plán okamžitých opatření na posílení bezpečnosti a odolnosti KII. Toto zaměření je v souladu s rozpravou, která byla zahájena na žádost Rady a Evropského parlamentu a zabývá se problémy a prioritami politiky bezpečnosti sítí a informací (NIS) a nejvhodnějšími nástroji na úrovni EU k jejich vyřešení. Navrhovaná opatření současně doplňují opatření určená k předcházení trestných a teroristických akcí namířených proti KII, boji s nimi a jejich trestní stíhání, a jsou v součinnosti se současným a budoucím výzkumným úsilím EU v oblasti bezpečnosti sítí a informací, jakož i s mezinárodními iniciativami v této oblasti.

## 2. POLITICKÉ SOUVISLOSTI

Toto sdělení rozvíjí evropskou politiku k posílení bezpečnosti informační společnosti a důvěry v ni. Už v roce 2005 zdůraznila Komise[3] naléhavou potřebu koordinovat úsilí k vybudování důvěry zúčastněných stran v elektronické komunikace a služby. Za tímto účelem byla v roce 2006 přijata strategie pro bezpečnou informační společnost[4]. Její hlavní prvky včetně bezpečnosti a odolnosti infrastruktur IKT byly schváleny usnesením Rady 2007/068/01. Míra odpovědnosti a provádění těchto úkolů zúčastněnými stranami se však zdají nedostatečné. Touto strategií se rovněž posiluje taktická a provozní úloha Evropské agentury pro bezpečnost sítí a informací (ENISA), která byla založena v roce 2004 a jejímž

---

1 Definice KII byla navržena v KOM(2005) 576 v konečném znění.
2 Celosvětová rizika 2008.
3 KOM(2005) 229.
4 KOM(2006) 251.

úkolem je přispívat k dosahování cílů při zajišťování vysoké a účinné úrovně NIS ve Společenství a rozvoji kultury NIS ku prospěchu občanů, spotřebitelů, podniků a veřejných správ EU.

V roce 2008 byl mandát agentury ENISA v nezměněné podobě prodloužen do března 2012[5]. Rada a Evropský parlament současně vyzvaly k „*dalšímu jednání o budoucnosti agentury ENISA a o obecném směřování evropského úsilí o vyšší bezpečnost sítí a informací*." Na podporu této diskuse zahájila Komise prostřednictvím internetu v listopadu veřejnou konzultaci[6] a analýza jejích výsledků by měla být už brzy k dispozici.

Činnosti plánované v tomto sdělení probíhají v rámci Evropského programu na ochranu kritické infrastruktury (EPCIP)[7] i souběžně s ním. Klíčovým prvkem EPCIP je směrnice[8] o určování a označování evropských kritických infrastruktur[9], která označuje odvětví IKT jako budoucí prioritní odvětví. Dalším významným prvkem EPCIP je Výstražná informační síť kritické infrastruktury (CIWIN)[10].

Pokud se jedná o regulativní aspekty, obsahuje návrh Komise na reformu regulačního rámce pro sítě a služby elektronických komunikací[11] nová ustanovení o bezpečnosti a integritě, zejména s cílem zpřísnit povinnosti operátorů, aby se zajistilo, že budou přijata vhodná opatření k řešení určených rizik, zaručení kontinuity dodávek služeb a hlášení narušení bezpečnosti[12]. Tento přístup přispěje k dosažení všeobecného cíle, jímž je zlepšení bezpečnosti a odolnosti KII. Evropský parlament a Rada tato ustanovení důrazně podporují.

Opatření navrhovaná v tomto sdělení doplňují stávající a budoucí opatření v oblasti policejní a soudní spolupráce určená k předcházení trestných a teroristických akcí namířených proti infrastrukturám IKT, plánovaných mimo jiné v rámcovém rozhodnutí Rady o útocích na informační systémy[13] a jeho připravované aktualizaci[14], boji s nimi a jejich trestní stíhání.

Tato iniciativa bere v úvahu činnosti NATO v oblasti společné politiky počítačové obrany, tj. Řídicí orgán kybernetické obrany a středisko excelence pro společnou počítačovou obranu.

Rovněž přihlíží k mezinárodnímu politickému vývoji, zejména zásadám G8 týkajícím se CIIP[15], rezoluci Valného shromáždění OSN 58/199 *Vytvoření celosvětové kultury kybernetické bezpečnosti a ochrana kritických informačních infrastruktur* a nedávné doporučení OECD o ochraně kritických informačních infrastruktur.

---

5 Nařízení (ES) č. 1007/2008.
6 http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4464
7 KOM(2006) 786 v konečném znění.
8 2008/114/ES.
9 http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/gena/104617.pdf.
10 KOM(2008) 676 v konečném znění.
11 KOM(2007) 697, KOM(2007) 698, KOM(2007) 699.
12 Článek 13 rámcové směrnice.
13 2005/222/SVV.
14 KOM(2008) 712.
15 http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf.

## 3. CO JE V SÁZCE

### 3.1. Kritické informační infrastruktury jsou životně důležité pro hospodářství a společenský růst EU

Hospodářskou a společenskou úlohu odvětví IKT a infrastruktur IKT zdůrazňují nedávné zprávy o inovacích a hospodářském růstu. Patří k nim sdělení o přezkumu i2010 v polovině období[16], zpráva Ahovy skupiny[17] a roční hospodářské zprávy Evropské unie[18]. OECD zdůrazňuje význam IKT a internetu pro „*zlepšování hospodářské výkonnosti a sociálního blahobytu a zvyšování schopnosti společnosti zlepšovat kvalitu života občanů na celém světě*“[19]. Dále doporučuje politiky, které upevní důvěru k internetové infrastruktuře.

Odvětví IKT má zásadní význam pro všechny vrstvy společnosti. Podniky závisejí na odvětví IKT jak z hlediska přímých prodejů, tak účinnosti vnitřních procesů. IKT představují kritickou složku inovací a jsou zodpovědné za téměř 40 % růstu produktivity[20]. IKT rovněž stále více pronikají do fungování vlád a orgánů veřejné správy: přebírání služeb elektronické správy na všech úrovních, jakož i nových aplikací, jako jsou inovativní řešení spojená se zdravotnictvím, energetikou a politickou spoluprací přináší značnou závislost veřejného sektoru na IKT. V neposlední řadě jsou na využívání IKT při každodenních činnostech v rostoucí míře závislí občané: zvýšení bezpečnosti KII by zvýšilo i důvěru občanů k IKT, a to i díky lepší ochraně osobních údajů a soukromí.

### 3.2. Rizika spojená s kritickými informačními infrastrukturami

Rizika spojená s útoky člověka, přírodními pohromami či technickými selháními nejsou mnohdy zcela pochopena a/nebo dostatečně analyzována. V důsledku této skutečnosti nemají zúčastněné strany dostatečné povědomí, aby mohly vytvářet účinná ochranná opatření a protiopatření.

Počítačové útoky jsou nebývale důmyslné. Jednoduché experimenty se mění v složité činnosti vykonávané pro zisk nebo z politických důvodů. Nejčastěji uváděným příkladem tohoto obecného vývoje jsou nedávné rozsáhlé počítačové útoky v Estonsku, Litvě a Gruzii. Závažnost problému potvrzuje obrovský počet virů, programů typu worm a jiného škodlivého softwaru, šíření botnetů a neustálý nárůst spamů[21].

Vzhledem k velké míře závislosti na KII, k jejich přeshraničnímu propojení s ostatními infrastrukturami a jejich vzájemné závislosti, jakož i ke zranitelnosti a hrozbám, kterým čelí, vyvstává potřeba systémově řešit jejich bezpečnost a odolnost jako přední linie obrany proti selháním a útokům.

---

16 KOM(2008) 199 v konečném znění.

17 http://ec.europa.eu/invest-in-research/action/2006_ahogroup_en.htm.

18 Přezkum hospodářství EU za rok 2007 http://ec.europa.eu/economy_finance/publications/publication10130_en.pdf.

19 http://www.oecd.org/dataoecd/1/29/40821707.pdf.

20 http://epp.eurostat.ec.europa.eu/ - Věda a technologie/Informační společnost.

21 KOM(2006) 688 v konečném znění.

### 3.3. Bezpečnost a odolnost kritických informačních infrastruktur pro upevnění důvěry v informační společnost

S cílem zajistit, aby se infrastruktury IKT využívaly v nejvyšší možné míře, a plně se tak uplatnily hospodářské a společenské příležitosti informační společnosti, musí jim všechny zúčastněné strany více důvěřovat. Závisí to na různých aspektech, z nichž nejdůležitějším je zajištění vysoké úrovně jejich bezpečnosti a odolnosti. Rozmanitost, otevřenost, interoperabilita, použitelnost, průhlednost, zodpovědnost, ověřitelnost různých složek a hospodářská soutěž jsou klíčovými faktory rozvoje bezpečnosti a podněcují zavádění výrobků, postupů a služeb, které zvyšují bezpečnost. Jak už Komise zdůraznila[22], jedná se o společnou odpovědnost: žádná z jednotlivých zúčastněných stran nemá prostředky k zajištění bezpečnosti a odolnosti všech infrastruktur IKT a k provedení všech souvisejících úkolů.

Zhostit se těchto úkolů vyžaduje přístup a kulturu založenou na řízení rizik, schopnou reagovat na známé hrozby a předvídat neznámé budoucí hrozby bez nepřiměřené reakce, která by zadusila vznikání inovativních služeb a aplikací.

### 3.4. Úkoly pro Evropu

Navíc a jako doplnění veškerých činností spojených s prováděním směrnice o určování a označování evropských kritických infrastruktur, zejména určování kritérií specifických pro odvětví IKT, je třeba v zájmu posílení bezpečnosti a odolnosti KII řešit celou řadu rozsáhlých úkolů.

#### *3.4.1. Nejednotné a nekoordinované vnitrostátní postupy*

Přestože problémy a úkoly, kterým čelíme, mají mnoho společných rysů, opatření a režimy k zajištění bezpečnosti a odolnosti KII a úroveň odborných znalostí a připravenosti se v jednotlivých členských státech liší.

Čistě vnitrostátní přístup znamená pro Evropu riziko roztříštěnosti a neúčinnosti. Rozdíly ve vnitrostátních přístupech a nedostatečná systematická přeshraniční spolupráce značně omezuje účinnost vnitrostátních protiopatření, mimo jiné protože díky vzájemné propojenosti KII znamená nízká úroveň bezpečnosti a odolnosti KII v jedné zemi případné zvýšení zranitelnosti a rizika v jiných zemích.

K překonání této situace je potřeba celoevropské úsilí, které dodá přidanou hodnotu vnitrostátním politikám a programům podporou rozvoje informovanosti a společného chápání těchto problémů, stimulací přijímání sdílených politických cílů a priorit, upevňováním spolupráce mezi členskými státy a začleňováním vnitrostátních politik do evropského a celosvětového rámce.

#### *3.4.2. Potřeba nového evropského modelu řízení KII*

Posilování bezpečnosti a odolnosti KII představuje z hlediska správy neobvyklé úkoly. Členské státy jsou i nadále plně odpovědné za stanovení politik souvisejících s KII, jejich provádění však závisí na zapojení soukromého sektoru, který vlastní nebo ovládá velký počet KII. Trhy na druhou stranu nedávají vždy soukromému sektoru dostatečné podněty, aby

[22] KOM(2006) 251 v konečném znění.

investoval do ochrany KII takovou měrou, kterou by vládní orgány za normálních okolností vyžadovaly.

K řešení tohoto problému vzniklo jako příklad na vnitrostátní úrovni partnerství veřejného a soukromého sektoru. Nicméně navzdory obecné shodě, že partnerství veřejného a soukromého sektoru by byla žádoucí i na evropské úrovni, takováto partnerství dosud nevznikla. Celoevropský mnohostranný rámec řízení, který může zahrnovat i rozšířenou úlohu ENISA, by podpořil zapojení soukromého sektoru do určování strategických cílů veřejné politiky a provozních priorit a opatření. Takový rámec by překlenul rozdíl mezi vnitrostátní tvorbou politiky a provozní realitou.

### *3.4.3. Omezená evropská schopnost včasného varování a reakce na incidenty*

Řídicí mechanismy budou skutečně účinné, pouze pokud všichni zúčastnění budou mít spolehlivé informace, na jejichž základě budou moci jednat. Týká se to zejména vlád, které nesou konečnou odpovědnost za zajišťování bezpečnosti a blaha občanů.

Procesy a postupy pro sledování bezpečnostních incidentů sítí a jejich hlášení se však v jednotlivých členských státech značně liší. Některé ani nemají určenou sledovací organizaci. Důležitější však je, že spolupráce a sdílení spolehlivých a využitelných informací o bezpečnostních incidentech mezi členskými státy není dostatečně vyvinutá, má spíše neformální charakter nebo se omezuje na dvoustranné, v menší míře i mnohostranné výměny. Strategický význam pro zvyšování bezpečnosti a odolnosti KII má kromě toho stimulace incidentů a provádění cvičení k otestování reakčních schopností, zejména prostřednictvím zaměření na flexibilní strategie a postupy pro zvládání případných nepředvídatelných krizí. V EU jsou cvičení v oblasti počítačové bezpečnosti stále ještě v plenkách. Cvičení s přeshraničním dosahem se konají jen v omezené míře. Jak ukázaly nedávné události[23], vzájemná pomoc je zásadním prvkem řádné reakce na rozsáhlé hrozby a útoky na KII.

Silná schopnost včasného varování a reakce na události v Evropě se musí opírat o dobře fungující vnitrostátní/vládní skupiny pro reakci na počítačové hrozby (CERT), tj. musí mít společný základ, pokud jde o schopnosti. Tyto orgány musí působit jako vnitrostátní katalyzátory zájmů a schopností zúčastněných stran v oblasti činnosti veřejné politiky (včetně činností týkajících se systémů sdílení informací a varování s dosahem k občanům a malým a středním podnikům) a musí se zapojovat do účinné přeshraniční spolupráce a výměny informací, a využívat k tomu případně stávající organizace, jako je Evropská vládní skupina CERT (EGC)[24].

### *3.4.4. Mezinárodní spolupráce*

Nárůst internetu jako klíčové KII vyžaduje, aby se jeho odolnosti a stabilitě věnovala zvláštní pozornost. Ukazuje se, že internet je díky své rozložené, redundantní koncepci velmi robustní infrastrukturou. Jeho neobyčejný nárůst však způsobil i růst fyzické a logické složitosti a vznik nových služeb a způsobů využití: je jen správné zpochybňovat schopnost internetu odolávat rostoucímu počtu narušení a počítačových útoků.

Rozdílnost názorů na kritičnost prvků tvořících internet lze částečně vysvětlit rozmanitostí vládních postojů vyjadřovaných na mezinárodních fórech a často i protichůdným vnímáním

---

23 http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/.

24 http://www.egc-group.org/.

významu této záležitosti. Mohlo by to bránit řádné prevenci hrozeb týkajících se internetu, připravenosti na ně a schopnosti se z nich zotavit. Například následky přechodu z IPv4 na IPv6 by se rovněž měly posuzovat k hlediska bezpečnosti KII.

Internet je celosvětová a velmi distribuovaná síť sítí, jejíž kontrolní střediska se nutně neřídí hranicemi mezi státy. Zajištění odolnosti a stability tedy vyžaduje to specifický, cílený přístup založený na dvou vzájemně se doplňujících opatřeních. Zaprvé je to dosažení společného konsenzu o evropských prioritách v oblasti odolnosti a stability internetu, a to z hlediska veřejné politiky a nasazování a provozu. Zadruhé zapojení celosvětové společnosti do procesu vytvoření souboru zásad odrážejících základní evropské hodnoty v zájmu odolnosti a stability internetu, a to v rámci našeho strategického dialogu a spolupráce se třetími zeměmi a mezinárodními organizacemi. Tyto činnosti by vycházely z toho, že Světový summit o informační společnosti[25] uznal klíčový význam stability internetu.

## 4. CESTA VPŘED: K LEPŠÍ KOORDINACI A SPOLUPRÁCI V EU

Vzhledem k tomu, že tento problém zasahuje Společenství a má i mezinárodní rozměr, znamenal by integrovaný přístup EU ke zlepšení bezpečnosti a odolnosti KII doplnění a přidanou hodnotu k vnitrostátním programům a stávajícím dvoustranným a mnohostranným režimům spolupráce mezi členskými státy.

Veřejné politické diskuse po událostech v Estonsku naznačují, že účinky podobných útoků by bylo možné pomocí preventivních opatření a koordinovaného postupu při skutečné krizi omezit. Strukturovanější výměna informací a osvědčené postupy v celé EU by mohly značně usnadnit potírání přeshraničních hrozeb.

Je nezbytné posílit stávající nástroje spolupráce včetně agentury ENISA a vytvořit nové nástroje, bude-li třeba. Zásadní význam má přístup zahrnující všechny zúčastněné strany na různých úrovních, který se bude uskutečňovat na evropské úrovni a plně respektovat a doplňovat vnitrostátní odpovědnosti.

Nezbytné je rovněž důkladné pochopení prostředí a různých omezení. Jedním z problémů je například distribuovaná povaha internetu, v jejímž rámci lze okrajové uzly použít jako východiska k útokům, např. botnetům. Tato distribuovaná povaha je však klíčovým prvkem stability a odolnosti a může pomoci internetu k rychlejší obnově, než by tomu bylo v případě vysoce formalizovaných hierarchických postupů. Vyžaduje to pečlivou a jednotlivou analýzu veřejných politik a provozních postupů.

Důležitý je i časový horizont. Existuje jasná potřeba jednat ihned a rychle zavést nezbytné prvky k vytvoření rámce, který nám umožní reagovat na současné problémy a který bude možné využít při tvorbě budoucí strategie bezpečnosti sítí a informací.

K řešení těchto úkolů se navrhuje pět pilířů:

1. Připravenost a prevence: zajištění připravenosti na všech úrovních;

2. Detekce a reakce: vytvoření přiměřeného mechanismu včasného varování;

---

[25] Tuniská agenda pro informační společnost, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.

3. Zmírňování a obnova: posílení obranných mechanismů EU pro KII;

4. Mezinárodní spolupráce: mezinárodní podpora priorit EU;

5. Kritéria pro odvětví IKT: podpora provádění směrnice o určování a označování evropských kritických infrastruktur[26].

## 5. AKČNÍ PLÁN

### 5.1. Připravenost a prevence

Základ schopností a služeb pro celoevropskou spolupráci. Komise vyzývá členské státy a zúčastněné strany, aby

- s pomocí agentury ENISA v zájmu podpory celoevropské spolupráce určily minimální úroveň schopností a služeb vnitrostátních/vládních skupin CERT a operace odezvy na incidenty,
- zajistily, že vnitrostátní/vládní skupiny CERT budou jednat jakožto klíčové složky vnitrostátní schopnosti týkající se připravenosti, sdílení informací, koordinace a reakce.

*Cíl: dohodnout se na minimálních standardech do konce roku 2010; vytvořit dobře fungující vnitrostátní/vládní skupiny CERT ve všech členských státech do konce roku 2011.*

Evropské partnerství mezi veřejným a soukromým sektorem pro odolnost (E3PR). Komise

- bude podporovat spolupráci mezi veřejným a soukromým sektorem v oblasti cílů bezpečnosti a odolnosti, základních požadavků, osvědčených politických postupů a opatření. EP3R by se v první řadě zaměřilo na evropský rozměr zahrnující strategická (např. osvědčené politické postupy) i taktická a provozní (např. nasazené v průmyslu) hlediska. EP3R by vycházelo ze stávajících vnitrostátních iniciativ a provozních činností agentury ENISA a doplňovalo by je.

*Cíl: vytvořit plán pro EP3R do konce roku 2009; založit EP3R do poloviny roku 2010; první výsledky činnosti EP3R do konce roku 2010.*

Evropské fórum pro sdílení informací mezi členskými státy. Komise

- zřídí evropské fórum, v jehož rámci budou členské státy sdílet informace a osvědčené politické postupy v oblasti bezpečnosti a odolnosti KII. K tomu by mohla využít výsledků činností dalších organizací, zejména agentury ENISA.

*Cíl: vytvořit fórum do konce roku 2009; získat první výsledky do konce roku 2010.*

### 5.2. Detekce a reakce

Evropský systém pro varování a sdílení informací (EISAS). Komise podpoří

[26] Směrnice Rady 2008/114/ES.

vytvoření a zavedení EISAS, který bude dostupný i občanům a malým a středním podnikům a bude založen na vnitrostátních a soukromých systémech sdílení informací a varování. Komise finančně podpoří dva doplňkové prototypové projekty[27]. Agentura ENISA se vyzývá, aby evidovala výsledky těchto projektů a dalších vnitrostátních iniciativ a sestavila plán dalšího vývoje a nasazování EISAS.

*Cíl: dokončit prototypové projekty do konce roku 2010; plán evropského systému do konce roku 2010.*

### 5.3. Zmírňování a obnova

Vnitrostátní krizové plánování a cvičení. Komise vyzývá členské státy, aby

- jako krok směrem k užší celoevropské koordinaci vytvořily vnitrostátní krizové plány a pořádaly pravidelná cvičení reakce pro případ rozsáhlých síťových bezpečnostních incidentů a obnovy činnosti po katastrofě. Vnitrostátní/vládní skupiny CERT/CSIRT lze pověřit vedením cvičení a testování vnitrostátních krizových plánů za účasti zúčastněných stran z řad soukromého i veřejného sektoru. V zájmu podpory výměny osvědčených postupů mezi členskými státy se vyžaduje zapojení agentury ENISA.

*Cíl: uspořádat alespoň jedno vnitrostátní cvičení v každém členském státě do konce roku 2010.*

Celoevropská cvičení rozsáhlých událostí týkajících se bezpečnosti sítě. Komise

- finančně podpoří přípravu celoevropských cvičení internetových bezpečnostních incidentů[28], které mohou rovněž představovat provozní platformu pro celoevropskou účast na mezinárodních cvičeních síťových bezpečnostních incidentů, jako je americké cvičení US Cyber Storm.

*Cíl: sestavit a uspořádat první celoevropské cvičení do konce roku 2010; celoevropská účast na mezinárodních cvičeních do konce roku 2010.*

Posílená spolupráce mezi vnitrostátními/vládními skupinami CERT. Komise vyzývá členské státy, aby

- upevnily spolupráci mezi vnitrostátními/vládními skupinami CERT a aby rovněž využívaly a rozšiřovaly stávající mechanismy spolupráce, jako je EGC[29]. Agentura ENISA se vyzývá, aby hrála aktivní úlohu při povzbuzování a podpoře celoevropské spolupráce mezi vnitrostátními/vládními skupinami CERT, která by vedla ke zlepšení připravenosti, posílení schopnosti Evropy reagovat na incidenty a řešit je, a celoevropským (a/nebo regionálním) cvičením.

---

27 V rámci programu ES „Prevence, připravenost a řízená následků terorismu a dalších bezpečnostních rizik“ („*Prevention, Preparedness and Consequence Management of terrorism and other Security Related Risks*“), http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm.

28 Poznámka 27 výše.

29 Poznámka 24 výše.

*Cíl: zdvojnásobit počet vnitrostátních orgánů. které se účastní EGC, do konce roku 2010; agentura ENISA vypracuje referenční materiály na podporu celoevropské spolupráce do konce roku 2010.*

### 5.4. Mezinárodní spolupráce

Odolnost a stabilita internetu. Plánují se tři doplňkové činnosti

- Evropské priority pro dlouhodobou odolnost a stabilitu internetu. Komise zahájí celoevropskou diskusi k určení priorit EU pro dlouhodobou odolnost a stabilitu internetu, do které zapojí všechny příslušné veřejné i soukromé zúčastněné strany.

*Cíl: priority EU pro kritické prvky a problémy internetu do konce roku 2010.*

- Zásady a pokyny pro odolnost a stabilitu internetu (na evropské úrovni). Komise bude se členskými státy pracovat na stanovení pokynů pro odolnost a stabilitu internetu a zaměří se mimo jiné na regionální nápravná opatření, dohody o vzájemné pomoci, strategie pro koordinovanou obnovu a kontinuitu, geografické rozložení kritických zdrojů internetu, technologické zabezpečení v internetové architektuře a protokolech a replikaci a rozmanitost služeb a dat. Komise již sestavuje pracovní skupinu pro odolnost DNS, která bude společně s dalšími projekty pomáhat při dosažení konsenzu[30].

*Cíl: evropský plán přípravy zásad a pokynů pro odolnost a stabilitu internetu do konce roku 2009; dohoda prvního návrhu těchto zásad a pokynů do konce roku 2010.*

- Zásady a pokyny pro odolnost a stabilitu (na celosvětové úrovni). Komise bude se členskými státy pracovat na plánu podpory zásad a pokynů na celosvětové úrovni. Rozvine se strategická spolupráce se třetími zeměmi, zejména v rámci dialogu informační společnosti, která bude hnací silou dosažení celosvětového konsenzu[31].

*Cíl: plán mezinárodní spolupráce na zásadách a pokynech pro bezpečnost a odolnost počátkem roku 2010; první návrh mezinárodně uznávaných zásad a pokynů pro diskusi se třetími zeměmi a příslušnými fóry včetně fóra pro správu internetu do konce roku 2010.*

Celosvětové cvičení obnovy a zmírňování rozsáhlých internetových incidentů. Komise vyzývá evropské zúčastněné strany, aby

- zvážily praktický způsob rozšíření celosvětových cvičení pořádaných v rámci pilíře pro zmírnění a obnovu, a to na základě regionálních krizových plánů a schopností.

*Cíl: Komise navrhne rámec a plán na podporu evropské účasti na celosvětových cvičeních obnovy a zmírnění rozsáhlých internetových incidentů do konce roku 2010.*

### 5.5. Kritéria pro evropské kritické infrastruktury v odvětví IKT

Specifická kritéria pro odvětví IKT. Na základě počáteční činnosti vyvíjené v roce 2008 bude Komise

[30] Poznámka 27 výše.
[31] KOM(2008) 588 v konečném znění.

- nadále ve spolupráci se členskými státy a všemi příslušnými zúčastněnými stranami sestavovat kritéria určování kritických evropských infrastruktur v odvětví IKT. K tomu využije příslušné informace z konkrétních studií, které se právě zahajují[32].

*Cíl: Komise určí kritéria pro kritické evropské infrastruktury v odvětví IKT v první polovině roku 2010.*

## 6. ZÁVĚRY

Bezpečnost a odolnost KII představují přední linii obrany proti selháním a útokům. Jejich zlepšení v celé EU je nezbytné, máme-li plně využívat přínosů informační společnosti. K dosažení tohoto ambiciózního cíle se navrhuje akční plán na posílení taktické a provozní spolupráce na evropské úrovni. Úspěch těchto opatření závisí na míře účinnosti, s jakou se jim podaří vycházet z činností veřejného a soukromého sektoru a využívat jich, na angažovanosti a plné účasti členských států, evropských institucí a zúčastněných stran.

To je účelem ministerské konference konané ve dnech 27.–28. dubna 2009, kde se bude se členskými státy diskutovat o navrhovaných iniciativách a kde se zhodnotí jejich ochota diskutovat o modernizované a posílené politice NIS v Evropě.

Zlepšení bezpečnosti a odolnosti KII je dlouhodobým cílem, jehož strategie a opatření vyžadují pravidelné hodnocení. Vzhledem k tomu, že tento cíl je v souladu se všeobecnou diskusí o budoucnosti politiky v oblasti bezpečnosti sítí a informací v EU po roce 2012, zahájí Komise koncem roku 2010 inventarizační cvičení s cílem vyhodnotit první fázi opatření a případně identifikovat a navrhnout další opatření.

[32] Poznámka 27 výše.