EVROPSKÁ
KOMISE

VYSOKÁ PŘEDSTAVITELKA
EVROPSKÉ UNIE
PRO ZAHRANIČNÍ VĚCI A
BEZPEČNOSTNÍ
POLITIKU

V Bruselu dne 7.2.2013
JOIN(2013) 1 final

SPOLEČNÉ SDĚLENÍ EVROPSKÉMU PARLAMENTU, RADĚ, EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ

Strategie kybernetické bezpečnosti Evropské unie:

Otevřený, bezpečný a chráněný kyberprostor

SPOLEČNÉ SDĚLENÍ EVROPSKÉMU PARLAMENTU, RADĚ, EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ

Strategie kybernetické bezpečnosti Evropské unie:

Otevřený, bezpečný a chráněný kyberprostor

1. ÚVOD

1.1. Souvislosti

Internet a obecněji kyberprostor mají v posledních dvou desetiletích nesmírný vliv na všechny složky společnosti. Náš každodenní život, základní práva, sociální interakce i ekonomika závisí na dokonalém fungování informačních a komunikačních technologií (IKT). Otevřený a svobodný kyberprostor pomohl prosazovat politické a sociální začleňování na celém světě; odstranil překážky mezi zeměmi, komunitami a občany a umožnil celosvětovou interakci a sdílení informací a myšlenek; poskytl fórum pro svobodu projevu a výkon základních práv a byl oporou pro ty, kteří usilovali o demokratickou a spravedlivější společnost, nejvýrazněji během arabského jara.

Aby zůstal kyberprostor otevřený a svobodný, musí EU na internetu uplatňovat stejné normy, zásady a hodnoty jako mimo něj. V kyberprostoru je třeba chránit základní práva, demokracii a právní stát. Naše svoboda a prosperita stále více závisí na spolehlivém a inovativním internetu, který se bude dále rozvíjet, pokud budou inovace soukromého sektoru a občanská společnost přispívat k jeho růstu. Svoboda na internetu si však také žádá bezpečnost a ochranu: kyberprostor je nutné chránit před incidenty, zlovolnými aktivitami a zneužitím. Významnou úlohu z hlediska zajištění svobody a bezpečnosti kyberprostoru hrají vlády, mezi jejichž úkoly patří: zabezpečovat přístup a otevřenost, respektovat a chránit na internetu základní práva a zachovávat spolehlivost a interoperabilitu internetu. Značnou část kyberprostoru ale vlastní a provozuje soukromý sektor, a tak iniciativy, jež mají v této oblasti uspět, musí vycházet z uznání jeho vedoucího postavení.

Informační a komunikační technologie se staly páteří našeho ekonomického růstu a nanejvýš významným zdrojem, na němž závisí všechna hospodářská odvětví. Jsou základem komplexních systémů, jež udržují naši ekonomiku v chodu v klíčových odvětvích, jako jsou finanční služby, zdravotnictví, energetika a doprava, a mnoho podnikatelských modelů se opírá o nepřetržitou dostupnost internetu a bezproblémové fungování informačních systémů.

Dokončením jednotného digitálního trhu by Evropa mohla zvýšit svůj HDP o téměř 500 miliard EUR ročně[1], což v průměru představuje 1 000 EUR na osobu. Aby se ujaly nové propojené technologie, včetně elektronických plateb, „cloud computing“ nebo komunikace mezi stroji[2], bude třeba, aby jim občané věřili a dokázali je s jistotou používat. Z průzkumu Eurobarometr z roku 2012[3] bohužel vyplývá, že téměř jedna třetina Evropanů nemá velkou důvěru ve svou schopnost používat internet pro bankovnictví nebo nákupy. Naprostá většina respondentů přitom uvedla, že na internetu neprozrazuje své osobní údaje z důvodu obav o jejich bezpečnost. Obětí podvodu online se v rámci EU stal již více než každý desátý uživatel internetu.

---

1 http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf

2 Například rostliny vybavené čidly, která by upozornila zavlažovací systém, že je čas tyto rostliny zalít.

3 Zvláštní průzkum Eurobarometr 390 o kybernetické bezpečnosti (2012).

V posledních letech jsme svědky toho, že digitální svět sice přináší obrovské výhody, ale je také zranitelný. Incidenty v oblasti kybernetické bezpečnosti[4] – ať už úmyslné, či náhodné – se množí znepokojivou rychlostí a mohly by narušovat poskytování základních služeb, jež považujeme za samozřejmé (např. zásobování vodou, zdravotní péče, dodávky elektřiny nebo mobilní služby). Hrozby mohou mít různý původ – včetně kriminálních, politicky motivovaných, teroristických či státem podporovaných útoků, jakož i přírodních katastrof a neúmyslných chyb.

Ekonomika EU je již postižena kyberkriminálními[5] aktivitami zaměřenými proti soukromému sektoru a jednotlivcům. Pachatelé kyberkriminality používají stále rafinovanější metody pro neoprávněný přístup do informačních systémů, krádeže kritických údajů nebo požadování výkupného od společností. Nárůst hospodářské špionáže a státem podporovaných činností v kyberprostoru představuje novou kategorii hrozeb pro vlády a obchodní společnosti v EU.

V zemích mimo EU mohou vlády rovněž zneužívat kyberprostor pro dohled a kontrolu nad svými vlastními občany. Evropská unie může této situaci čelit podporou svobody a dodržování základních práv na internetu.

Všechny tyto faktory objasňují, proč vlády na celém světě začaly vypracovávat strategie kybernetické bezpečnosti a kyberprostor považovat za stále významnější mezinárodní otázku. Nastal čas, aby i EU zintenzivnila svou činnost v této oblasti. Tento návrh strategie kybernetické bezpečnosti Evropské unie, předkládaný Komisí a vysokou představitelkou Unie pro zahraniční věci a bezpečnostní politiku (dále jen „vysoká představitelka“), představuje vizi EU v této oblasti, vysvětluje úlohy a povinnosti a uvádí opatření, jež jsou na základě silné a účinné ochrany a podpory práv občanů nutná k tomu, aby se online prostředí EU stalo nejbezpečnějším na světě.

1.2. Zásady kybernetické bezpečnosti

Mnohovrstevný internet, v němž neexistují hranice, se stal jedním z nejúčinnějších nástrojů celosvětového pokroku bez vládního dohledu či regulace. Soukromý sektor by měl sice i nadále zaujímat vedoucí postavení při vytváření a každodenní správě internetu, ale jako stále významnější se jeví nutnost zavést požadavky týkající se transparentnosti, odpovědnosti a bezpečnosti. Tato strategie objasňuje zásady, jimiž by se měla řídit politika kybernetické bezpečnosti v EU a na mezinárodní úrovni.

Základní hodnoty EU platí jak v digitálním, tak v reálném světě

Stejné právní předpisy a normy, které se uplatňují v jiných oblastech našeho každodenního života, platí i v kybernetické oblasti.

---

[4] Kybernetická bezpečnost se obvykle vztahuje na záruky a opatření, jež mohou být použity k ochraně kyberprostoru v civilní i vojenské oblasti před hrozbami, které mají spojitost se vzájemně závislými sítěmi a informační infrastrukturou nebo které je mohou poškodit. Kybernetická bezpečnost má zachovat dostupnost a integritu sítí a infrastruktury, jakož i důvěrnost informací, jež jsou v nich obsaženy.

[5] Kyberkriminalitou se obvykle rozumí široká škála různých druhů trestné činnosti, jejichž primárním nástrojem nebo cílem jsou počítače a informační systémy. Kyberkriminalita zahrnuje tradiční trestné činy (např. podvod, padělání a krádež identity), trestné činy související s obsahem (např. online šíření dětské pornografie nebo podněcování k rasové nenávisti) a trestné činy specifické pro počítače a informační systémy (např. útoky proti informačním systémům, odepření služby a škodlivý software („malware“)).

Ochrana základních práv, svobody projevu, osobních údajů a soukromí

Kybernetická bezpečnost může být řádná a účinná, pouze pokud se opírá o základní práva a svobody zakotvené v Listině základních práv Evropské unie a o základní hodnoty EU. Práva jednotlivců na druhé straně nelze zajistit bez bezpečných sítí a systémů. Jakékoliv sdílení informací pro účely kybernetické bezpečnosti, když jde o osobní údaje, by mělo být v souladu s právními předpisy EU o ochraně údajů a mělo by plně zohledňovat práva jednotlivců v této oblasti.

Přístup pro všechny

Vzhledem k tomu, nakolik digitální svět proniká do činností ve společnosti, představují omezený nebo žádný přístup k internetu a počítačová negramotnost pro občany nevýhodu. Každý by měl mít přístup k internetu a neomezenému toku informací. Aby byl umožněn bezpečný přístup pro všechny, je třeba zaručit integritu a bezpečnost internetu.

Demokratické a účinné mnohostranné řízení

Digitální svět nekontroluje jediný subjekt. V současnosti existuje několik zúčastněných stran (z nichž mnohé jsou komerční a nevládní organizace), které se podílejí na každodenní správě internetových zdrojů, protokolů a standardů a na budoucím rozvoji internetu. Evropská unie potvrzuje význam všech zúčastněných stran v rámci současného modelu správy internetu a podporuje tento mnohostranný přístup ke správě[6].

Společná odpovědnost za zajištění bezpečnosti

Rostoucí závislost na informačních a komunikačních technologiích ve všech oblastech lidského života vedla k odkrytí slabých míst, jež je třeba řádně definovat, důkladně analyzovat a odstranit či omezit. Všechny příslušné zúčastněné strany – veřejné orgány, soukromý sektor i jednotliví občané – musí uznat tuto společnou odpovědnost, přijmout kroky za účelem vlastní ochrany a v případě potřeby zajistit koordinovanou reakci k posílení kybernetické bezpečnosti.

2. STRATEGICKÉ PRIORITY A OPATŘENÍ

Evropská unie by měla chránit online prostředí a poskytovat přitom co nejvíce svobody a bezpečnosti pro všechny. I když uznává, že řešení problémů v oblasti bezpečnosti v kyberprostoru je především úkolem členských států, tato strategie navrhuje konkrétní opatření, která mohou zlepšit celkové výsledky EU. Jedná se o opatření krátkodobého i dlouhodobého charakteru, jež zahrnují celou řadu politických nástrojů[7] a také různé typy subjektů, ať už jsou to orgány EU, členské státy či odvětví.

Vize EU, kterou představuje tato strategie, je rozdělena do pěti strategických priorit, jež řeší výše uvedené problémy:

- Dosažení kybernetické odolnosti
- Výrazné omezení kyberkriminality

[6] Viz rovněž KOM(2009) 277, Sdělení Komise Evropskému parlamentu a Radě „Řízení internetu: další kroky“.

[7] Opatření související se sdílením informací, když jde o osobní údaje, by měla být v souladu s právem EU v oblasti ochrany údajů.

- Rozvoj politiky a kapacit kybernetické obrany v souvislosti se společnou bezpečnostní a obrannou politikou (SBOP)
- Rozvoj průmyslových a technologických zdrojů pro kybernetickou bezpečnost
- Zavedení soudržné mezinárodní politiky Evropské unie týkající se kyberprostoru a podpora základních hodnot EU

2.1. Dosažení kybernetické odolnosti

V zájmu podpory kybernetické odolnosti v EU musejí jak veřejné orgány, tak soukromý sektor rozvíjet příslušné kapacity a účinně spolupracovat. Další opatření EU mohou v návaznosti na pozitivní výsledky dosavadní činnosti[8] pomáhat zejména čelit kybernetickým rizikům a hrozbám s přeshraničním rozměrem a přispívat ke koordinované reakci v krizových situacích. Přispěje to výrazně k podpoře dobrého fungování vnitřního trhu a zvýšení vnitřní bezpečnosti v EU.

Evropa bude i nadále zranitelná, pokud nevyvine značné úsilí k posílení veřejných a soukromých kapacit, zdrojů a procesů s cílem předcházet incidentům v oblasti kybernetické bezpečnosti, odhalovat a řešit je. Z toho důvodu Komise vytvořila politiku bezpečnosti sítí a informací (NIS)[9]. V roce 2004 byla zřízena **Evropská agentura pro bezpečnost sítí a informací (ENISA)**[10] a Rada a Evropský parlament nyní projednávají nové nařízení o posílení této agentury a modernizaci jejího mandátu[11]. Rámcová směrnice o elektronických komunikacích[12] kromě toho požaduje, aby poskytovatelé elektronických komunikací přiměřeně řídili rizika ohrožující jejich sítě a informovali o závažných případech narušení bezpečnosti. V právních předpisech EU o ochraně údajů[13] se vyžaduje také to, aby správci údajů zajistili požadavky a záruky ochrany údajů, včetně opatření týkajících se bezpečnosti, a v oblasti veřejně dostupných služeb elektronických komunikací musí správci údajů oznamovat incidenty, při nichž dojde k narušení osobních údajů, příslušným vnitrostátním orgánům.

I přes dosažený pokrok na základě dobrovolných závazků přetrvávají v celé EU nedostatky, a to zejména pokud jde o kapacity jednotlivých států, koordinaci v případech incidentů překračujících hranice a zapojení soukromého sektoru a jeho připravenost. K této strategii je připojen **legislativní návrh**, jehož cílem je především:

- stanovit společné minimální požadavky na bezpečnost sítí a informací na vnitrostátní úrovni, které by zavazovaly členské státy k tomu, aby: určily příslušné vnitrostátní orgány pro bezpečnost sítí a informací; vytvořily dobře fungující skupinu pro reakci na počítačové hrozby (CERT) a přijaly vnitrostátní strategii bezpečnosti sítí a informací a vnitrostátní plán spolupráce v této oblasti. Budování kapacit a koordinace se týkají také

---

8 Viz odkazy v tomto sdělení, jakož i v pracovním dokumentu útvarů Komise – posouzení dopadů, jenž je připojen k návrhu směrnice o bezpečnosti sítí a informací, který vypracovala Komise (viz zejména oddíly 4.1.4 a 5.2 a přílohy 2, 6 a 8).

9 V roce 2001 Komise přijala sdělení „Bezpečnost sítí a informací: návrh evropského politického přístupu“ (KOM(2001) 298); v roce 2006 přijala Strategii pro bezpečnou informační společnost (KOM(2006) 251). Od roku 2009 Komise rovněž přijala akční plán a sdělení o ochraně kritické informační infrastruktury (CIIP) (KOM(2009) 149, schváleno usnesením Rady 2009/C 321/01; a KOM(2011) 163, schváleno v závěrech Rady 10299/11).

10 Nařízení (ES) č. 460/2004.

11 KOM(2010) 521. Opatření navrhovaná v této strategii nemají za následek změnu stávajícího nebo budoucího mandátu agentury ENISA.

12 Články 13a a 13b směrnice 2002/21/ES.

13 Článek 17 směrnice 95/46/ES; článek 4 směrnice 2002/58/ES.

orgánů EU: v roce 2012 byla trvale zřízena skupina pro reakci na počítačové hrozby odpovědná za bezpečnost IT systémů orgánů, agentur a subjektů EU („CERT-EU“).

- zavést koordinované mechanismy pro prevenci, odhalování, zmírňování a reakci, díky nimž budou příslušné vnitrostátní orgány pro bezpečnost sítí a informací moci sdílet informace a vzájemně si pomáhat. Od vnitrostátních orgánů pro bezpečnost sítí a informací se bude požadovat, aby zajistily vhodnou spolupráci v rámci celé EU, a to zejména na základě plánu Unie pro spolupráci v oblasti bezpečnosti sítí a informací, zaměřeného na reakce na kybernetické incidenty s přeshraničním rozměrem. Tato spolupráce bude stavět rovněž na pokroku, který byl učiněn v souvislosti s „Evropským fórem členských států (EFMS)“[14], v rámci něhož proběhly produktivní diskuse a výměny názorů o veřejné politice v oblasti bezpečnosti sítí a informací a které lze začlenit do mechanismu spolupráce (po jeho zavedení).
- zlepšit připravenost a zapojení soukromého sektoru. Velkou většinu sítí a informačních systémů vlastní a provozují soukromé subjekty, proto je z hlediska podpory kybernetické bezpečnosti naprosto nezbytné se soukromým sektorem posílit spolupráci. Soukromý sektor by měl na technické úrovni rozvíjet své vlastní kapacity kybernetické odolnosti a sdílet osvědčené postupy s jinými sektory. Nástroje vytvořené odvětvím s cílem reagovat na incidenty, určovat příčiny a provádět forenzní šetření by měly být přínosem i pro veřejný sektor.

Problémem je, že soukromé subjekty nejsou stále účinně motivovány k tomu, aby poskytovaly spolehlivé údaje o výskytu nebo dopadu incidentů v oblasti bezpečnosti sítí a informací, přijaly kulturu řízení rizik či investovaly do bezpečnostních řešení. Navrhovaný právní předpis má proto zajistit, aby aktéři v řadě významných oblastí (konkrétně v oblasti energetiky, dopravy, bankovnictví, burz cenných papírů a zprostředkování klíčových internetových služeb, jakož i ve veřejné správě) posuzovali rizika, kterým z hlediska kybernetické bezpečnosti čelí, zajišťovali spolehlivost a odolnost sítí a informačních systémů prostřednictvím vhodného řízení rizik a sdíleli zjištěné informace s příslušnými vnitrostátními orgány pro bezpečnost sítí a informací. Zavedení kultury kybernetické bezpečnosti by mohlo zlepšit příležitosti v podnikání a konkurenceschopnost v soukromém sektoru, což by mohlo zvýšit atraktivitu kybernetické bezpečnosti.

Tyto subjekty by příslušným vnitrostátním orgánům pro bezpečnost sítí a informací musely oznamovat incidenty, které by měly významný dopad na kontinuitu základních služeb a dodávek zboží závislých na sítích a informačních systémech.

Příslušné vnitrostátní orgány pro bezpečnost sítí a informací by měly spolupracovat a vyměňovat si informace s ostatními regulačními orgány, především s orgány odpovědnými za ochranu osobních údajů. Orgány pro bezpečnost sítí a informací by následně měly o incidentech, u nichž existuje podezření na vážný trestní charakter, informovat donucovací orgány. Příslušné vnitrostátní orgány by také měly pravidelně uveřejňovat na zvláštních internetových stránkách neutajované informace o aktuálních včasných varováních o incidentech a rizicích a o koordinovaných reakcích. Právní závazky by neměly být náhradou ani překážkou rozvoje neformální a dobrovolné spolupráce – včetně spolupráce mezi veřejným a soukromým sektorem – s cílem zvýšit úroveň bezpečnosti a vyměňovat si informace a osvědčené postupy. V tomto ohledu je vhodnou a platnou platformou na úrovni

[14] Evropské fórum členských států bylo vytvořeno na základě dokumentu KOM(2009) 149 jako platforma na podporu diskuse mezi veřejnými orgány členských států o osvědčených postupech v oblasti bezpečnosti a odolnosti kritické informační infrastruktury.

EU zejména Evropské partnerství mezi veřejným a soukromým sektorem pro odolnost (EP3R)[15], které je třeba dále rozvíjet.

Z nástroje pro propojení Evropy (CEF)[16] by byla poskytnuta finanční podpora na klíčovou infrastrukturu spojující kapacity členských států v oblasti bezpečnosti sítí a informací, čímž by se usnadnila spolupráce v rámci celé EU.

V neposlední řadě je třeba zmínit nezbytná cvičení na úrovni EU zaměřená na kybernetické incidenty s cílem simulovat spolupráci mezi členskými státy a soukromým sektorem. První cvičení se zapojením členských států proběhlo v roce 2010 („Cyber Europe 2010“) a druhé, jehož se účastnil i soukromý sektor, se konalo v říjnu 2012 („Cyber Europe 2012“). V listopadu 2011 se uskutečnilo simulační cvičení EU-USA („Cyber Atlantic 2011“). Další cvičení, včetně cvičení s mezinárodními partnery, jsou naplánována na příští roky.

Komise přijme tato opatření:

- Bude pokračovat ve své činnosti, kterou provádí Společné výzkumné středisko v úzké spolupráci s orgány členských států a vlastníky a provozovateli kritické infrastruktury a jejímž cílem je určit slabá místa evropské kritické infrastruktury z hlediska bezpečnosti sítí a informací a podporovat rozvoj odolných systémů.
- Na začátku roku 2013 zahájí pilotní projekt[17] týkající se **boje proti botnetům a malwaru**, financovaný z prostředků EU. Cílem bude poskytnout rámec pro koordinaci a spolupráci mezi členskými státy EU, organizacemi soukromého sektoru, např. poskytovateli internetových služeb, a mezinárodními partnery.

Komise žádá agenturu ENISA, aby:

- Pomohla členským státům vytvořit silné **vnitrostátní kapacity zajišťující kybernetickou odolnost**, zejména budováním odborných znalostí v oblasti bezpečnosti a odolnosti průmyslových řídicích systémů, dopravy a energetické infrastruktury.
- V roce 2013 přezkoumala možnost vytvoření týmu(ů) reakce na incidenty v oblasti počítačové bezpečnosti se zaměřením na průmyslové řídicí systémy (ICS-CSIRT) pro EU.
- Nadále podporovala členské státy a orgány EU v provádění pravidelných **celoevropských cvičení pro případy kybernetických incidentů**, jež budou zároveň představovat provozní základ pro účast EU v mezinárodních cvičeních tohoto typu.

Komise vyzývá Evropský parlament a Radu, aby:

---

15 Evropské partnerství mezi veřejným a soukromým sektorem pro odolnost bylo vytvořeno na základě dokumentu KOM(2009) 149. Tato platforma zahájila činnost a podpořila spolupráci mezi veřejným a soukromým sektorem, pokud jde o stanovení klíčových aktiv, zdrojů, funkcí a základních požadavků na odolnost, jakož i potřeby a mechanismy spolupráce pro reakci na rozsáhlá narušení elektronických komunikací.

16 https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. CEF, rozpočtová položka 09.03.02 – telekomunikační sítě (na podporu propojení a interoperability vnitrostátních veřejných služeb online, jakož i přístupu k nim).

17 CIP-ICT PSP-2012-6, 325188. Disponuje celkovým rozpočtem ve výši 15 milionů EUR, k nimž EU přispívá 7,7 miliony EUR.

- Co nejdříve **přijaly** návrh směrnice o **vysoké společné úrovni bezpečnosti sítí a informací** v celé Unii, který se zabývá vnitrostátními kapacitami a připraveností, spoluprací na úrovni EU, zavedením postupů řízení rizik a sdílením informací o bezpečnosti sítí a informací.

Komise žádá odvětví, aby:

- Převzalo vedoucí úlohu, pokud jde o **investice** do zajištění vysoké úrovně kybernetické bezpečnosti, a rozvíjelo osvědčené postupy a sdílení informací na odvětvové úrovni a s veřejnými orgány s cílem zajistit silnou a účinnou ochranu majetku a osob, zejména prostřednictvím partnerství veřejného a soukromého sektoru, např. EP3R a Trust in Digital Life (TDL; důvěra v digitální život)[18].

Zvyšování informovanosti

Zajištění kybernetické bezpečnosti je odpovědností všech. Klíčovou úlohu při zajišťování bezpečnosti sítí a informačních systémů hrají koncoví uživatelé, kteří musejí znát rizika, jimž na internetu čelí, a mít možnost přijímat na ochranu proti nim jednoduchá opatření.

V posledních letech bylo vyvinuto několik iniciativ, v nichž je třeba pokračovat. Agentura ENISA se na zvyšování informovanosti podílela zejména zveřejňováním zpráv, pořádáním odborných seminářů a rozvojem partnerství veřejného a soukromého sektoru. Aktivní v této oblasti jsou rovněž Europol, Eurojust a vnitrostátní orgány pro ochranu údajů. V říjnu 2012 ENISA spolu s některými členskými státy realizovala pilotní akci „Evropský měsíc kybernetické bezpečnosti“. Zvyšování informovanosti je jednou z oblastí, jimiž se zabývá pracovní skupina EU-USA pro kybernetickou bezpečnost a kyberkriminalitu[19], a je také nedílnou součástí programu Bezpečnější internet[20] (zaměřeného na bezpečnost dětí na internetu).

Komise žádá agenturu ENISA, aby:

- V roce 2013 navrhla plán vytvoření „řidičského průkazu pro bezpečnost sítí a informací“ jako dobrovolného certifikačního programu s cílem podpořit zlepšení dovedností a schopností odborníků v oblasti IT (např. správců internetových stránek).

Komise přijme tato opatření:

- S pomocí agentury ENISA v roce 2014 zorganizuje **šampionát** v kybernetické bezpečnosti, na němž budou studenti vysokých škol soutěžit v navrhování řešení v

[18] http://www.trustindigitallife.eu/

[19] Tato pracovní skupina, zřízená na summitu EU-USA v listopadu 2010 (MEMO/10/597), je pověřena vypracováváním společných přístupů k celé řadě problémů souvisejících s kybernetickou bezpečností a kyberkriminalitou.

[20] Z programu Bezpečnější internet je financována síť nevládních organizací, jež působí v oblasti ochrany zájmů dítěte na internetu, síť donucovacích orgánů, které si vyměňují informace a osvědčené postupy týkající se využívání internetu k trestné činnosti spočívající v šíření materiálů souvisejících s pohlavním zneužíváním dětí, a síť výzkumných pracovníků, kteří shromažďují informace o způsobech užívání online technologií, jejich rizicích a důsledcích pro životy dětí.

oblasti bezpečnosti sítí a informací.

Komise vyzývá členské státy[21], aby:

- Počínaje rokem 2013 za podpory agentury ENISA a účasti soukromého sektoru každoročně organizovaly **měsíc kybernetické bezpečnosti** s cílem zvýšit informovanost koncových uživatelů. Měsíc kybernetické bezpečnosti, který bude probíhat současně v EU a USA, se začne organizovat od roku 2014.
- **Zintenzivnily své úsilí v oblasti vzdělávání a odborné přípravy týkající se bezpečnosti sítí a informací**, a to zavedením: odborné přípravy o bezpečnosti sítí a informací ve školách do roku 2014; odborné přípravy o bezpečnosti sítí a informací, vývoji bezpečného softwaru a ochraně osobních údajů pro studenty informatiky a základní odborné přípravy v oblasti bezpečnosti sítí a informací pro zaměstnance veřejné správy.

Komise vyzývá odvětví, aby:

- Podporovalo **na všech úrovních informovanost** o kybernetické bezpečnosti, a to v rámci podniků i ve vztahu k zákazníkům. Odvětví by se mělo zabývat zejména tím, jak dosáhnout větší odpovědnosti vrcholného vedení a managementu za zajištění kybernetické bezpečnosti.

2.2. Výrazné omezení kyberkriminality

Čím více žijeme v digitálním světě, tím více příležitostí mohou využívat pachatelé kybernetických trestných činů. Kyberkriminalita je jednou z nejrychleji rostoucích forem trestné činnosti, jejímiž oběťmi se denně stává více než jeden milion lidí na celém světě. Rafinovanost pachatelů kybernetických trestných činů a sítí této trestné činnosti roste a k boji s nimi potřebujeme správné operační nástroje a kapacity. Kybernetické trestné činy jsou velmi výnosné a jen málo rizikové a pachatelé často využívají anonymity internetových domén. Kyberkriminalita nezná hranic – globální dosah internetu znamená, že při prosazování práva je nutno k reakci na tuto rostoucí hrozbu přijmout koordinovaný a společný přeshraniční přístup.

Silné a účinné právní předpisy

Evropská unie a jednotlivé členské státy potřebují silné a účinné právní předpisy k potírání kyberkriminality. Úmluva Rady Evropy o kyberkriminalitě, rovněž známá jako Budapešťská úmluva, je závazná mezinárodní smlouva, jež poskytuje účinný rámec pro přijímání vnitrostátních právních předpisů.

Evropská unie již přijala právní předpisy o kyberkriminalitě, včetně směrnice o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii[22]. Brzy se EU také dohodne na směrnici o útocích proti informačním systémům, zejména pomocí botnetů.

---

[21] Rovněž za účasti příslušných vnitrostátních orgánů, včetně příslušných orgánů pro bezpečnost sítí a informací a orgánů pro ochranu údajů.

[22] Směrnice 2011/93/EU, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV.

Komise přijme tato opatření:

- Zajistí rychlé provedení a uplatňování směrnic týkajících se kyberkriminality.
- Bude naléhat na ty členské státy, které dosud neratifikovaly **Budapešťskou úmluvu Rady Evropy o kyberkriminalitě**, aby tak co nejdříve učinily a uplatňovaly její ustanovení.

Posílení operační kapacity pro boj proti kyberkriminalitě

Vývoj metod kyberkriminality se rapidně zrychlil: donucovací orgány nemohou proti kyberkriminalitě bojovat se zastaralými operačními nástroji. V současné době nemají některé členské státy EU operační kapacitu, kterou potřebují k účinné reakci na kyberkriminalitu. Všechny členské státy musí mít efektivní vnitrostátní útvary pro boj proti kyberkriminalitě.

Komise přijme tato opatření:

- Prostřednictvím svých programů financování[23] bude podporovat členské státy při **zjišťování nedostatků a posilování kapacity** pro vyšetřování kyberkriminality a boj proti ní. Komise bude navíc podporovat subjekty, které přispívají k propojení výzkumného a akademického prostředí, donucovacích orgánů a soukromého sektoru a vykonávají tedy podobnou činnost jako již fungující střediska excelence pro problematiku kyberkriminality, zřízená v některých členských státech a financovaná Komisí.
- Spolu s členskými státy bude koordinovat úsilí o stanovení osvědčených postupů a nejlepších dostupných technik pro boj proti kyberkriminalitě, a to rovněž za podpory Společného výzkumného střediska (např. s ohledem na vývoj a použití forenzních nástrojů nebo na analýzu hrozeb).
- Bude úzce spolupracovat s nedávno otevřeným **Evropským centrem pro boj proti kyberkriminalitě (EC3), v rámci Europolu a s Eurojustem**, aby sladil tyto politické přístupy s osvědčenými postupy z operačního hlediska.

Lepší koordinace na úrovni EU

Evropská unie může doplňovat činnost členských států tím, že bude usnadňovat koordinovaný a společný přístup, v rámci něhož budou spolupracovat donucovací a soudní orgány, jakož i veřejné a soukromé zúčastněné strany z EU i mimo ni.

Komise přijme tato opatření:

- Bude podporovat nedávno otevřené **Evropské centrum pro boj proti kyberkriminalitě** (EC3) jako evropské ústředí boje proti kyberkriminalitě. Toto centrum bude poskytovat analýzy a zpravodajské informace, podporovat vyšetřování, zabezpečovat vysokou úroveň forenzních postupů, usnadňovat

[23] V roce 2013 v rámci programu Předcházení trestné činnosti a boj proti ní (ISEC). Po roce 2013 z Fondu pro vnitřní bezpečnost (nový nástroj víceletého finančního rámce).

spolupráci, vytvářet kanály pro sdílení informací mezi příslušnými orgány v členských státech, soukromým sektorem a dalšími zúčastněnými stranami a postupně sloužit jako mluvčí komunity zabývající se prosazováním práva[24].

- Bude podporovat úsilí o zvýšení odpovědnosti registrátorů názvů domén a zajištění přesnosti informací o vlastnictví internetových stránek, zejména na základě doporučení týkajících se prosazování práva pro Internetové sdružení pro přidělování jmen a čísel (ICANN), a to v souladu s právními předpisy Unie včetně pravidel o ochraně údajů.
- Bude se opírat o nejnovější právní předpisy a nadále posilovat úsilí EU v boji proti pohlavnímu zneužívání dětí na internetu. Komise přijala Evropskou strategii pro internet lépe uzpůsobený dětem[25] a spolu se státy EU i zeměmi mimo ni vytvořila **Globální alianci proti pohlavnímu zneužívání dětí prostřednictvím internetu**[26]. Tato aliance je prostředkem pro další opatření členských států za podpory Komise a EC3.

Komise žádá Europol (EC3), aby:

- Nejprve zaměřil svou analytickou a operační podporu vyšetřování případů kyberkriminality v členských státech na pomoc při odstraňování a narušování sítí pachatelů kyberkriminality, především v oblasti pohlavního zneužívání dětí, platebních podvodů, botnetů a neoprávněných vniknutí.
- Pravidelně vypracovával strategické a operační zprávy o trendech a nových hrozbách s cílem určit priority a zaměření vyšetřovacích činností útvarů pro boj proti kyberkriminalitě v členských státech.

Komise žádá Evropskou policejní akademii (CEPOL), aby ve spolupráci s Europolem:

- Koordinovala podobu a plánování kurzů, jež by měly pracovníky donucovacích orgánů vybavit znalostmi a odbornými poznatky pro účinný boj proti kyberkriminalitě.

Komise žádá Eurojust, aby:

- Určil hlavní překážky justiční spolupráce při vyšetřování kyberkriminality a překážky koordinace mezi členskými státy a se třetími zeměmi a podporoval vyšetřování a stíhání kyberkriminality na operační i strategické úrovni, jakož i vzdělávací činnost v této oblasti.

Komise žádá Eurojust a Europol (EC3), aby:

- Úzce spolupracovaly, mj. prostřednictvím výměny informací, na zajištění vyšší účinnosti boje proti kyberkriminalitě v souladu se svými mandáty a pravomocemi.
-

[24] Dne 28. března 2012 Evropská komise přijala sdělení „Řešení trestné činnosti v digitálním věku: zřízení Evropského centra pro boj proti kyberkriminalitě“.

[25] COM(2012) 196 final.

[26] Závěry Rady o Globální alianci proti pohlavnímu zneužívání dětí prostřednictvím internetu (společné prohlášení EU-USA) ze 7. a 8. června 2012 a Prohlášení o vytvoření Globální aliance proti pohlavnímu zneužívání dětí prostřednictvím internetu (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm).

2.3. Rozvoj politiky a kapacit kybernetické obrany v souvislosti s rámcem společné bezpečnostní a obranné politiky (SBOP)

Úsilí v oblasti kybernetické bezpečnosti v EU zahrnuje také rozměr kybernetické obrany. Aby se zvýšila odolnost komunikačních a informačních systémů, jež podporují obranné zájmy a zájmy národní bezpečnosti členských států, měl by se rozvoj kapacit kybernetické obrany soustředit na odhalování sofistikovaných kybernetických hrozeb, reakci na ně a na nápravu jejich následků.

Vzhledem k tomu, že hrozby mají mnoho podob, měla by se posilovat součinnost mezi civilními a vojenskými přístupy k ochraně kritických kybernetických aktiv. Tyto snahy je třeba podpořit výzkumem a vývojem a užší spoluprací mezi vládami, soukromým sektorem a akademickou obcí v EU. Aby nedocházelo ke zdvojování činností, EU prozkoumá možnosti, jak se mohou EU a NATO ve svém úsilí o zvýšení odolnosti kritických vládních, obranných a jiných informačních infrastruktur, na nichž závisí členové obou organizací, vzájemně doplňovat.

Vysoká představitelka se zaměří na následující hlavní činnosti, přičemž ke spolupráci vyzve členské státy a Evropskou obrannou agenturu:

- Posouzení operačních požadavků kybernetické obrany EU a podpora rozvoje kapacit a technologií EU v oblasti kybernetické obrany s cílem řešit všechny aspekty rozvoje kapacit, včetně doktríny, otázek vedení, organizace, pracovníků, odborné přípravy, technologií, infrastruktury, logistiky a interoperability.

- Vypracování politického rámce EU pro kybernetickou obranu za účelem ochrany sítí v rámci misí a operací SBOP, včetně dynamického řízení rizik, lepší analýzy hrozeb a sdílení informací. Zlepšení možností odborné přípravy a cvičení v oblasti kybernetické obrany pro ozbrojené síly v evropském a mezinárodním kontextu, včetně začlenění prvků kybernetické obrany do stávajících katalogů cvičení.

- Podpora dialogu a koordinace mezi civilními a vojenskými subjekty v EU – se zvláštním důrazem na výměnu osvědčených postupů, výměnu informací a na včasná varování, reakce na incidenty, posuzování rizik, zvyšování informovanosti a zavedení kybernetické bezpečnosti jako priority.

- Zajištění dialogu s mezinárodními partnery, včetně NATO, dalších mezinárodních organizací a mezinárodních středisek excelence, s cílem zabezpečit kapacity účinné obrany, vymezit oblasti spolupráce a zabránit zdvojování úsilí.

2.4. Rozvoj průmyslových a technologických zdrojů pro kybernetickou bezpečnost

Evropa má vynikající výzkumné a vývojové kapacity, ale mnoho nejvýznamnějších světových poskytovatelů inovativních produktů a služeb v oblasti IKT se nachází mimo EU. Existuje riziko, že Evropa se stane příliš závislou nejenom na informačních a komunikačních technologiích pocházejících odjinud, ale i na bezpečnostních řešeních, jež byla vyvinuta za jejími hranicemi. Je klíčové, aby hardwarové a softwarové komponenty, jež se vyrábějí v EU a ve třetích zemích k použití v kritických službách a infrastruktuře a stále více také v mobilních zařízeních, byly spolehlivé, bezpečné a zaručovaly ochranu osobních údajů.

Podpora jednotného trhu s produkty souvisejícími s kybernetickou bezpečností

Vysokou úroveň bezpečnosti lze zajistit pouze tehdy, jestliže všechny složky hodnotového řetězce (např. výrobci zařízení, vývojáři softwaru, poskytovatelé služeb informační společnosti) budou k bezpečnosti přistupovat jako ke své prioritě. Zdá se však[27], že mnoho subjektů na bezpečnost stále pohlíží spíše jako na další zátěž, a po bezpečnostních řešeních je jen malá poptávka. V rámci celého hodnotového řetězce produktů IKT, jež se v Evropě používají, je třeba uplatňovat vhodné výkonnostní požadavky z hlediska kybernetické bezpečnosti. Soukromý sektor potřebuje k zajištění vysoké úrovně kybernetické bezpečnosti pobídky, např. prostřednictvím označování upozorňujícího na přiměřenou úroveň kybernetické bezpečnosti, jež umožní společnostem s dobrými výsledky v oblasti kybernetické bezpečnosti využít této skutečnosti jako argumentu na podporu prodeje a získat konkurenční výhodu. Povinnosti stanovené v navrhované směrnici o bezpečnosti sítí a informací by rovněž výrazným způsobem přispěly k posílení konkurenceschopnosti podniků v příslušných odvětvích.

Je také třeba stimulovat poptávku po vysoce bezpečných produktech na trzích v celé Evropě. Za prvé, tato strategie má posílit spolupráci a transparentnost, pokud jde o bezpečnost u produktů IKT. Vyžaduje to zřízení platformy sdružující příslušné evropské veřejné a soukromé zúčastněné strany, jejímž úkolem by bylo určit osvědčené postupy v oblasti kybernetické bezpečnosti v celém hodnotovém řetězci a vytvořit příznivé tržní podmínky pro přípravu a přijetí bezpečných IKT řešení. Hlavní důraz by měl být kladen na vytvoření pobídek k provádění vhodného řízení rizik a na přijetí bezpečnostních norem a řešení, jakož i případné zavedení dobrovolných celoevropských systémů certifikace na základě stávajících systémů v EU a na mezinárodní úrovni. Komise bude podporovat členské státy v přijímání jednotných postupů, aby nedocházelo k rozdílnostem, jež by mohly podniky znevýhodňovat kvůli jejich umístění.

Za druhé, Komise bude podporovat rozvoj bezpečnostních norem a pomáhat s dobrovolnými celoevropskými systémy certifikace v oblasti „cloud computing“, přičemž náležitou pozornost bude věnovat potřebě zajištění ochrany údajů. Je třeba se zaměřit na bezpečnost dodavatelského řetězce, zejména v kritických hospodářských odvětvích (průmyslové řídicí systémy, energetické a dopravní infrastruktury). Tato činnost by měla vycházet z probíhající normalizační práce evropských normalizačních organizací (CEN, CENELEC a ETSI)[28], koordinační skupiny pro kybernetickou bezpečnost (CSCG) a z odborných znalostí agentury ENISA, Komise a dalších příslušných subjektů.

Komise přijme tato opatření:

- V roce 2013 spustí **platformu** veřejného a soukromého sektoru **pro řešení v oblasti bezpečnosti sítí a informací** s cílem vytvářet pobídky pro přijímání bezpečných IKT řešení a pro uplatňování požadavku dobré úrovně kybernetické bezpečnosti u produktů IKT používaných v Evropě.
- V roce 2014 navrhne doporučení k zajištění kybernetické bezpečnosti v celém hodnotovém řetězci IKT, přičemž bude vycházet z práce této platformy.
- Bude zkoumat, jak by hlavní poskytovatelé hardwaru a softwaru IKT mohli

[27] Viz pracovní dokument útvarů Komise – posouzení dopadů, který je připojen k návrhu směrnice o bezpečnosti sítí a informací vypracovanému Komisí, oddíl 4.1.5.2.

[28] Zejména v rámci normy pro inteligentní sítě M/490 pro první soubor norem pro inteligentní sítě a referenční architekturu.

informovat příslušné vnitrostátní orgány o zjištěných slabých místech, která by mohla mít výrazný vliv na bezpečnost.

Komise žádá agenturu ENISA, aby:

- Vypracovala – ve spolupráci s příslušnými vnitrostátními orgány, příslušnými zúčastněnými stranami, mezinárodními a evropskými normalizačními orgány a Společným výzkumným střediskem Evropské komise – **technické pokyny a doporučení pro přijetí norem a osvědčených postupů v oblasti bezpečnosti sítí a informací** ve veřejném a soukromém sektoru.

Komise vyzývá zúčastněné strany z veřejného a soukromého sektoru, aby:

- Podporovaly rozvoj a přijetí **bezpečnostních norem** iniciovaných odvětvím, technických norem a zásad použití prvků bezpečnosti a ochrany soukromí již ve fázi návrhu výrobci a poskytovateli služeb IKT, včetně poskytovatelů cloudových služeb; nové generace softwaru a hardwaru by měly být vybaveny **silnějšími, vestavěnými a uživatelsky přívětivými bezpečnostními** prvky.
- Vypracovaly normy iniciované odvětvím a týkající se úrovně jednotlivých společností z hlediska kybernetické bezpečnosti a zlepšily dostupnost informací pro veřejnost rozvojem **bezpečnostních štítků** nebo značek, které by spotřebiteli pomáhaly orientovat se na trhu.

Podpora investic do výzkumu a vývoje a inovace

Výzkum a vývoj může podpořit silnou průmyslovou politiku, posílit důvěryhodnost evropského odvětví IKT, přispět k rozvoji vnitřního trhu a snížit evropskou závislost na zahraničních technologiích. Měl by zaplnit technologické mezery v oblasti bezpečnosti IKT, připravit odvětví na příští generaci bezpečnostních výzev, zohlednit neustálý vývoj potřeb uživatelů a využít výhod duálních technologií. Měl by rovněž dále podporovat rozvoj šifrování. To vše je třeba doplnit úsilím o převedení výsledků výzkumu a vývoje do komerčních řešení poskytnutím nezbytných pobídek a zavedením příslušných politických podmínek.

Evropská unie by měla co nejlépe využít rámcového programu pro výzkum a inovace Horizont 2020[29], jenž bude zahájen v roce 2014. Návrh Komise obsahuje specifické cíle pro důvěryhodnost IKT a boj proti kyberkriminalitě, které jsou v souladu s touto strategií. Horizont 2020 bude podporovat výzkum v oblasti bezpečnosti týkající se nových informačních a komunikačních technologií; poskytovat řešení pro koncové bezpečné systémy, služby a aplikace IKT; vytvářet pobídky pro provádění a přijímání stávajících řešení a řešit interoperabilitu mezi sítěmi a informačními systémy. Zvláštní pozornost se bude na úrovni EU věnovat optimalizaci a lepší koordinaci různých programů financování (Horizont 2020, Fond pro vnitřní bezpečnost, výzkum Evropské obranné agentury (EDA), včetně evropské rámcové spolupráce).

[29] Horizont 2020 je finanční nástroj, jímž se provádí Unie inovací, jedna ze stěžejních iniciativ strategie Evropa 2020, jejímž cílem je zajistit konkurenceschopnost Evropy v celosvětovém měřítku. Tento nový rámcový program EU pro výzkum a inovace bude probíhat od roku 2014 do roku 2020 a bude součástí úsilí o nastartování nového růstu a tvorbu nových pracovních míst v Evropě.

Komise přijme tato opatření:

- Využije program Horizont 2020 pro řešení různých otázek týkajících se soukromí a bezpečnosti IKT, od výzkumu a vývoje až po inovace a zavádění. V rámci programu Horizont 2020 budou rovněž vyvíjeny nástroje a prostředky pro boj proti trestné činnosti a teroristickým akcím namířeným proti kybernetickému prostředí.
- Vytvoří mechanismy pro lepší koordinaci výzkumných plánů orgánů Evropské unie a členských států a bude podněcovat členské státy, aby více investovaly do výzkumu a vývoje.

Komise vyzývá členské státy, aby:

- Do konce roku 2013 vyvinuly správné postupy k využití **kupní síly orgánů veřejné správy** (například prostřednictvím veřejných zakázek) s cílem stimulovat rozvoj a zavádění bezpečnostních prvků u produktů a služeb IKT.
- Podporovaly včasné zapojení odvětví a akademické obce do přípravy a koordinace řešení. To by se mělo realizovat za maximálního využití evropské průmyslové základny a souvisejícího výzkumu a vývoje inovativních technologií a mělo by zahrnovat koordinaci výzkumných plánů civilních a vojenských organizací.

Komise žádá Europol a agenturu ENISA, aby:

- Určily nové trendy a potřeby z hlediska vývoje druhů kyberkriminality a kybernetické bezpečnosti s cílem vytvořit přiměřené digitální forenzní nástroje a technologie.

Komise vyzývá zúčastněné strany z veřejného a soukromého sektoru, aby:

- Ve spolupráci s odvětvím pojišťovnictví vyvinuly **harmonizované metody výpočtu rizikových přirážek**, díky nimž by společnosti, jež investovaly do bezpečnosti, mohly získat nižší pojistné.

2.5. Zavedení soudržné mezinárodní politiky Evropské unie týkající se kyberprostoru a podpora základních hodnot EU

Zachování otevřeného, svobodného a bezpečného kyberprostoru je celosvětovou výzvou, kterou musí EU řešit společně s příslušnými mezinárodními partnery a organizacemi, soukromým sektorem a občanskou společností.

V rámci své mezinárodní politiky týkající se kyberprostoru bude EU usilovat o podporu otevřenosti a svobody internetu, povzbuzovat snahy o vypracování norem chování a uplatňovat stávající mezinárodní právní předpisy v kyberprostoru. Zároveň bude pracovat na odstranění digitální propasti a aktivně se podílet na mezinárodním úsilí o vybudování kapacity kybernetické bezpečnosti. Mezinárodní působení EU v otázkách kyberprostoru se bude řídit základními hodnotami EU, pokud jde o lidskou důstojnost, svobodu, demokracii, rovnost, právní stát a dodržování základních práv.

Začlenění otázek kyberprostoru do vnějších vztahů a společné zahraniční a bezpečnostní politiky EU

Komise, vysoká představitelka a členské státy by měly vypracovat soudržnou mezinárodní politiku EU týkající se kyberprostoru, jež bude zaměřena na posílení spolupráce a vztahů s hlavními mezinárodními partnery a organizacemi, jakož i s občanskou společností a soukromým sektorem. Konzultace EU s mezinárodními partnery o otázkách kyberprostoru je třeba navrhovat, koordinovat a provádět tak, aby byly přínosem s ohledem na stávající dvoustranné dialogy mezi členskými státy EU a třetími zeměmi. Evropská unie bude opět klást důraz na dialog se třetími zeměmi, přičemž se bude zaměřovat především na podobně smýšlející partnery, kteří s EU sdílejí stejné hodnoty. Bude podporovat dosažení vysoké úrovně ochrany údajů, včetně případů převodu osobních údajů do třetí země. V zájmu řešení globálních výzev v kyberprostoru bude EU usilovat o užší spolupráci s organizacemi, jež působí v této oblasti, jako je Rada Evropy, OECD, OSN, OBSE, NATO, AU, ASEAN a OAS. Na dvoustranné úrovni je obzvláště důležitá a dále se bude rozvíjet spolupráce s USA, zejména v rámci pracovní skupiny EU-USA pro kybernetickou bezpečnost a kyberkriminalitu.

Jedním z hlavních prvků mezinárodní politiky EU v oblasti kybernetiky bude podpora kyberprostoru jako prostoru svobody a základních práv. Rozšíření přístupu na internet by mělo uspíšit demokratické reformy a posílit jejich celosvětovou podporu. Lepší globální propojení by neměla provázet cenzura ani masový dohled. Evropská unie by měla podporovat sociální odpovědnost podniků[30] a přicházet s mezinárodními iniciativami ke zlepšení celosvětové koordinace v této oblasti.

Odpovědnost za bezpečnější kyberprostor mají všechny subjekty globální informační společnosti, od občanů po vlády. Evropská unie podporuje úsilí o vymezení norem chování v kyberprostoru, jež by měly zachovávat všechny zúčastněné strany. Stejně tak jako občané, od nichž EU očekává, že budou na internetu respektovat občanské povinnosti, sociální odpovědnost a zákony, měly by i státy dodržovat normy a stávající právní předpisy. V otázkách mezinárodní bezpečnosti EU podporuje rozvoj opatření k budování důvěry v oblasti kybernetické bezpečnosti s cílem zvýšit transparentnost a snížit riziko nepochopení chování státu.

Evropská unie nevyžaduje vytvoření nových mezinárodních právních nástrojů pro otázky týkající se kybernetiky.

Právní závazky zakotvené v Mezinárodním paktu o občanských a politických právech, Evropské úmluvě o lidských právech a Listině základních práv Evropské unie je také třeba dodržovat na internetu. Evropská unie se zaměří na hledání možností, jak zajistit, aby se tato opatření prosazovala rovněž v kyberprostoru.

Budapešťská úmluva je nástroj, který mohou za účelem řešení kyberkriminality přijmout i třetí země. Představuje vzor pro vypracovávání vnitrostátních právních předpisů o kyberkriminalitě a základ pro mezinárodní spolupráci v této oblasti.

Pokud se do kyberprostoru rozšíří ozbrojené konflikty, uplatní se v daném případě mezinárodní humanitární právo, případně právní předpisy v oblasti lidských práv. **Rozvoj budování kapacit v oblasti kybernetické bezpečnosti a odolných informačních infrastruktur ve třetích zemích**

[30] *Obnovená strategie EU pro sociální odpovědnost podniků na období 2011–2014*; KOM(2011) 681 v konečném znění.

Pro bezproblémové fungování příslušných infrastruktur, které poskytují a usnadňují komunikační služby, bude prospěšná zvýšená mezinárodní spolupráce, jež spočívá mimo jiné ve výměně osvědčených postupů, sdílení informací, včasných varováních, společných cvičeních zaměřených na zvládání incidentů atd. Evropská unie k tomuto cíli přispěje zintenzivněním stávajícího mezinárodního úsilí o posílení sítí spolupráce v oblasti ochrany kritické informační infrastruktury, jejichž součástí jsou vlády a soukromý sektor.

Ne všechny části světa mohou využívat kladného vlivu internetu, protože jim k němu chybí otevřený, bezpečný, interoperabilní a spolehlivý přístup. Evropská unie bude proto nadále podporovat úsilí zemí, jež se snaží zlepšit přístup svých občanů na internet a rozvíjet užívání internetu, zajistit jeho integritu a bezpečnost a účinně bojovat s kyberkriminalitou.

Komise a vysoká představitelka přijmou ve spolupráci s členskými státy tato opatření:

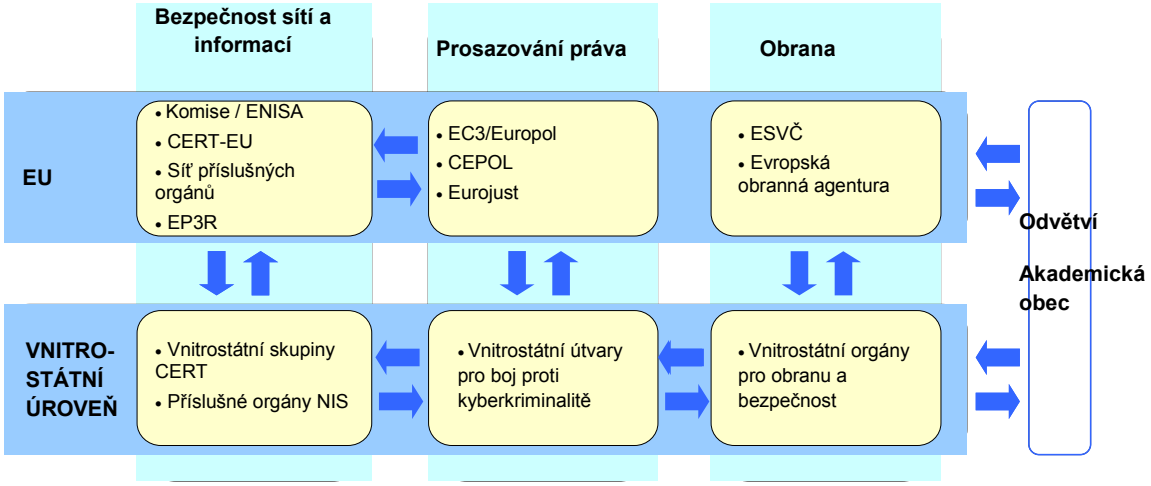
- Budou pracovat na vytvoření soudržné mezinárodní politiky EU týkající se kyberprostoru s cílem prohloubit spolupráci s hlavními mezinárodními partnery a organizacemi, začlenit otázky kyberprostoru do SZBP a zlepšit koordinaci problémů kyberprostoru s celosvětovým dosahem.
- Budou podporovat rozvoj norem chování a opatření k budování důvěry v oblasti kybernetické bezpečnosti. Budou usnadňovat dialog o možnostech použití stávajícího mezinárodního práva v kyberprostoru a podporovat Budapešťskou úmluvu jako nástroj k řešení kyberkriminality.
- Budou podporovat propagaci a ochranu základních práv, včetně přístupu k informacím a svobody projevu, přičemž se zaměří na: a) přípravu nových veřejných pokynů týkajících se svobody projevu online a offline; b) kontrolu vývozu produktů či služeb, které by mohly být použity jako prostředek cenzury nebo masového dohledu na internetu; c) rozvoj opatření a nástrojů k rozšíření přístupu na internet a zvýšení otevřenosti a odolnosti internetu v rámci boje proti cenzuře a masovému dohledu pomocí komunikačních technologií; d) zúčastněné strany, jimž chtějí umožnit používat komunikační technologie na podporu základních práv.
- Ve spolupráci s mezinárodními partnery a organizacemi, soukromým sektorem a občanskou společností budou podporovat globální budování kapacit ve třetích zemích s cílem zlepšit přístup k informacím a k otevřenému internetu, předcházet a čelit kybernetickým hrozbám, včetně náhodných událostí, kyberkriminality a kyberterorismu, jakož i rozvíjet koordinaci dárců za účelem řízení úsilí o budování kapacit.
- Budou používat různé nástroje pomoci EU k budování kapacit v oblasti kybernetické bezpečnosti, v rámci čehož bude mimo jiné poskytnuta pomoc se vzděláváním zaměstnanců donucovacích a soudních orgánů a technických pracovníků na téma kybernetických hrozeb a jejich řešení, jakož i podpora při vytváření příslušných vnitrostátních politik, strategií a institucí ve třetích zemích.
- Zlepší koordinaci politik a sdílení informací prostřednictvím mezinárodních sítí na ochranu kritické informační infrastruktury, např. sítě Meridian, prostřednictvím spolupráce mezi příslušnými orgány pro bezpečnost sítí a

informací a jinými způsoby.

3. ÚLOHY A POVINNOSTI

V propojené digitální ekonomice a společnosti se kybernetické incidenty nezastavují na hranicích. Všechny zúčastněné strany – od příslušných orgánů pro bezpečnost sítí a informací přes skupiny pro reakci na počítačové hrozby (CERT) a donucovací orgány až po průmysl – musí převzít odpovědnost na vnitrostátní úrovni i na úrovni EU a spolupracovat na posílení kybernetické bezpečnosti. Jelikož to může znamenat použití různých právních rámců a jurisdikcí, nejdůležitějším úkolem pro EU je vyjasnit úlohy a povinnosti tolika subjektů.

Vzhledem ke složitosti dané problematiky a různorodosti jednotlivých zúčastněných stran není centralizovaný evropský dohled řešením. Národní vlády mohou nejlépe organizovat prevenci kybernetických incidentů a útoků a reakci na ně, jakož i navazovat kontakty a vytvářet sítě se soukromým sektorem a širokou veřejností napříč různými zavedenými politickými proudy a právními rámci. Zároveň však povaha rizik, jež jsou potenciálně či skutečně bez hranic, vede k tomu, že účinná reakce na vnitrostátní úrovni by často vyžadovala zapojení na úrovni EU. K řešení kybernetické bezpečnosti komplexním způsobem by měly činnosti probíhat v rámci tří základních pilířů – bezpečnost sítí a informací, prosazování práva a obrana, jež mají rovněž různé právní rámce:



3.1. Koordinace mezi příslušnými orgány pro bezpečnost sítí a informací / skupinami CERT, donucovacími orgány a orgány obrany

Vnitrostátní úroveň

Členské státy by měly mít, a to již v současnosti nebo v důsledku této strategie, struktury pro řešení kybernetické odolnosti, kyberkriminality a obrany a měly by dosáhnout požadované úrovně kapacity k řešení kybernetických incidentů. Vzhledem k tomu, že řada subjektů může mít operační odpovědnost za různé aspekty kybernetické bezpečnosti, a vzhledem k důležitosti zapojení soukromého sektoru je však nezbytné, aby byla koordinace na vnitrostátní úrovni optimalizována napříč různými ministerstvy. Členské státy by ve svých vnitrostátních strategiích kybernetické bezpečnosti měly stanovit úlohy a povinnosti jednotlivých vnitrostátních subjektů.

Je třeba podporovat sdílení informací mezi vnitrostátními subjekty a se soukromým sektorem, aby měly členské státy a soukromý sektor neustále celkový přehled o různých hrozbách a lépe porozuměly novým trendům a metodám používaným k páchání kybernetických útoků i k rychlejší reakci na ně. Zavedením vnitrostátních plánů spolupráce v oblasti bezpečnosti sítí a informací, jež by měly být aktivovány v případě kybernetických incidentů, by měly být členské státy schopny rozdělit jasně úlohy a povinnosti a optimalizovat opatření v reakci na incidenty.

Úroveň EU

Stejně jako na vnitrostátní úrovni existuje také na úrovni EU řada subjektů zabývajících se kybernetickou bezpečností. ENISA, Europol/EC3 a EDA jsou tři agentury, jež působí v oblasti bezpečnosti sítí a informací, prosazování práva a obrany. Tyto agentury mají správní rady, v nichž jsou zastoupeny členské státy, a nabízí platformy pro koordinaci na úrovni EU.

Koordinace a spolupráce mezi agenturou ENISA, Europolem/EC3 a agenturou EDA bude podporována v řadě oblastí, na nichž se společně podílejí, zejména pokud jde o analýzy trendů, posuzování rizik, odbornou přípravu a sdílení osvědčených postupů. Tyto subjekty by měly spolupracovat a přitom zachovávat svá specifika. Společně se skupinou CERT-EU, Komisí a členskými státy by měly podporovat rozvoj důvěryhodné komunity technických odborníků a odborníků na politiky v této oblasti.

Neformální způsoby koordinace a spolupráce budou doplňovat strukturálnější vazby. Vojenský štáb EU a projektový tým EDA zabývající se kybernetickou obranou mohou být využívány k řízení koordinace v oblasti obrany. Programová rada Europolu/EC3 bude sdružovat mimo jiné zástupce Eurojustu, akademie CEPOL, členských států[31], agentury ENISA a Komise a bude zárukou toho, že tyto subjekty budou moci sdílet své specifické know-how a že opatření EC3 budou uskutečňována v partnerství, v rámci něhož budou oceňovány přínosné odborné poznatky a respektovány mandáty všech zúčastněných stran. Nový mandát agentury ENISA by měl umožnit zintenzivnit vazby s Europolem a posílit napojení na zúčastněné strany zastupující odvětví. Co je však nejdůležitější, legislativní návrh Komise týkající se bezpečnosti sítí a informací by stanovil rámec spolupráce prostřednictvím sítě příslušných vnitrostátních orgánů pro bezpečnost sítí a informací a řešil by sdílení informací mezi těmito orgány a donucovacími orgány.

Mezinárodní úroveň

Komise a vysoká představitelka společně s členskými státy zajistí koordinovaná mezinárodní opatření v oblasti kybernetické bezpečnosti. Budou přitom prosazovat základní hodnoty EU a podporovat mírové, otevřené a transparentní využívání kybernetických technologií. Komise, vysoká představitelka a členské státy se podílejí na politickém dialogu s mezinárodními partnery a mezinárodními organizacemi, jako je Rada Evropy, OECD, OBSE, NATO a OSN.

3.2. Podpora EU v případě závažných kybernetických incidentů nebo útoků

Je pravděpodobné, že významné kybernetické incidenty či útoky budou mít dopad na vlády, podniky i jednotlivce v EU. Díky této strategii a zejména navrhované směrnici o bezpečnosti sítí a informací by se měla zlepšit prevence kybernetických incidentů, jejich odhalování a reakce na ně a členské státy a Komise by se měly navzájem lépe informovat o závažných

[31] Prostřednictvím zastoupení v pracovní skupině EU pro boj proti kyberkriminalitě, která se skládá z vedoucích pracovníků útvarů pro boj proti kyberkriminalitě jednotlivých členských států.

kybernetických incidentech a útocích. Mechanismy reakce se nicméně budou lišit v závislosti na povaze, rozsahu a přeshraničních důsledcích každého konkrétního incidentu.

Pokud bude mít incident vážný dopad na kontinuitu činnosti, směrnice o bezpečnosti sítí a informací navrhuje aktivovat v závislosti na přeshraniční povaze incidentu vnitrostátní nebo unijní plány spolupráce v této oblasti. Síť příslušných orgánů pro bezpečnost sítí a informací by se v této souvislosti využívala pro sdílení informací a podporu. Díky tomu by bylo možné zachovat a/nebo obnovit postižené sítě a služby.

Pokud se bude zdát, že incident má souvislost s trestnou činností, je třeba informovat Europol/EC3, aby mohly – spolu s donucovacími orgány z postižených zemí – zahájit vyšetřování, zajistit důkazy, vypátrat pachatele a nakonec se postarat o jejich stíhání.

Pokud se bude zdát, že incident má souvislost s kybernetickou špionáží či státem podporovaným útokem, nebo pokud má dopady na národní bezpečnost, vnitrostátní orgány pro bezpečnost a obranu varují své příslušné protějšky, aby věděly, že jsou cílem útoku, a aby se mohly samy bránit. Následně budou aktivovány mechanismy včasného varování a v případě potřeby také postupy krizového řízení či jiné postupy. Zvláště závažné případy kybernetických incidentů nebo útoků by mohly poskytnout dostatečný důvod pro to, aby členský stát žádal uplatnění doložky solidarity EU (článek 222 Smlouvy o fungování Evropské unie).

Pokud se zdá, že kvůli incidentu byly ohroženy osobní údaje, měly by se zapojit vnitrostátní orgány pro ochranu údajů nebo vnitrostátní regulační orgán v souladu se směrnicí 2002/58/ES.

K řešení kybernetických incidentů a útoků budou rovněž přispívat kontaktní sítě a podpora ze strany mezinárodních partnerů. To může zahrnovat technická opatření ke zmírnění následků, trestní vyšetřování či aktivaci mechanismů krizového řízení v reakci na incidenty.

4. ZÁVĚRY A NÁSLEDNÁ OPATŘENÍ

Tento návrh strategie kybernetické bezpečnosti Evropské unie, předkládaný Komisí a vysokou představitelkou Unie pro zahraniční věci a bezpečnostní politiku, představuje vizi EU v této oblasti a opatření, jež jsou na základě silné ochrany a podpory práv občanů nutná k tomu, aby se online prostředí EU stalo nejbezpečnějším na světě[32].

Tato vize se může naplnit pouze na základě skutečného partnerství mezi mnoha subjekty, jež převezmou odpovědnost a budou řešit výzvy, které je v budoucnu očekávají.

Komise a vysoká představitelka proto vyzývají Radu a Evropský parlament, aby tuto strategii schválily a pomohly realizovat popsaná opatření. Nutná je rovněž pevná podpora a odhodlání

[32] Financování strategie bude probíhat v rámci plánovaných částek pro každou z příslušných oblastí politiky (nástroj pro propojení Evropy, Horizont 2020, Fond pro vnitřní bezpečnost, SZBP a vnější spolupráce, zejména nástroj stability), jak je uvedeno v návrhu víceletého finančního rámce na období 2014–2020, předloženém Komisí (s výhradou schválení rozpočtovým orgánem a konečných částek přijatého víceletého finančního rámce na období 2014–2020). Aby nebyl překročen počet pracovních míst, jež jsou k dispozici pro decentralizované agentury, a dílčí strop pro decentralizované agentury v jednotlivých výdajových okruzích v příštím víceletém finančním rámci, budou agentury (CEPOL, EDA, ENISA, Eurojust a Europol/EC3), které mají podle tohoto sdělení převzít nové úkoly, podporovány v tom, aby se těchto úkolů ujímaly za podmínky, že byla skutečně vytvořena kapacita pro absorpci rostoucích zdrojů a využity všechny možnosti interních přesunů.

soukromého sektoru a občanské společnosti, které hrají klíčovou úlohu v rámci posilování naší úrovně bezpečnosti a ochrany práv občanů.

Nastal čas jednat. Komise a vysoká představitelka jsou odhodlány spolupracovat se všemi subjekty na zaručení bezpečnosti, kterou Evropa potřebuje. Aby zajistily, že je strategie okamžitě prováděna a hodnocena s ohledem na možný vývoj, setkají se za dvanáct měsíců se všemi příslušnými zúčastněnými stranami na konferenci na vysoké úrovni a posoudí dosažený pokrok.