UNIVERZITY PALACKÉHO V OLOMOUCI
Filozofická fakulta
Katedra politologie a evropských studií

Renata Štolfová

E-government a rizika plynoucí z využívání současných ICTs ve státní správě

Rozvoj e-governmentu v ČR. Informační a kybernetická bezpečnost aneb Je třeba se obávat kybernetické války?

(Diplomová práce)

Vedoucí diplomové práce: Mgr. Eva Lebedová

OLOMOUC 2009

Prohlašuji, že jsem tuto diplomovou práci vypracovala samostatně na základě uvedených pramenů a literatury.

V Olomouci dne 26. listopadu 2009 Podpis: .....

PODĚKOVÁNÍ

Na tomto místě bych ráda poděkovala vedoucí své diplomové práce Mgr. Evě Lebedové za cenné rady, které mi v průběhu vytváření této studie poskytla. Za vědeckovýzkumné zázemí při jejím dopisování můj vděk náleží také Rakouskému institutu pro evropskou a bezpečnostní politiku (Austria Institut für Europa- und Sicherheitspolitik, AIES) v Maria Enzersdorfu. Dík patří také mým přátelům, jmenovitě Mgr. Jiřímu Štěpánovi za konzultace při finální korektuře a editaci textu, dále Bc. Ondřeji Martínkovi a Bc. Heleně Vavrdové za logistickou asistenci a morální podporu při dokončování práce. Ráda bych také svůj dík dedikovala zaměstnancům Krajského úřadu Moravskoslezského kraje, jmenovitě Bc. Zuzaně Hamzové, Bc. Dagmar Pacutové a Ing. Tomáši Vašicovi za odborné konzultace v oblasti rozvoje a využití nástrojů e-governmentu na regionální úrovni. Své velké poděkování zde věnuji také svým rodičům za podporu, kterou mi poskytovali nejen v období psaní a úprav této diplomové práce, nýbrž v průběhu celého mého dosavadního studia.

OBSAH

Seznam zkratek

3G	Třetí generace (mobilní telefony třetí generace)
ARES	Administrativní registr ekonomických subjektů
B2B	Business to Business, vztah obchodníků mezi sebou
B2C	Business to Customer, vztah obchodníků k zákazníkům
CERT	Computer Emergency Response Team, tým pohotové počítačové reakce
CIA	Central Intelligence Agency, Ústřední zpravodajská služba
CIP	Competitiveness and Innovation Framework Programme, Rámcový program Konkurenceschopnost a inovace
ČR	Česká republika
ČSN	Česká technická norma (původně Česká státní norma)
DG	Directorate-General, generální sekretariát Evropské komise
DoS	Denial-of-Services, odepření služeb
EFTA	European Free Trade Association, Evropské sdružení voleného obchodu
ENISA	European Network and Information Security Agency, Evropskou agenturu pro síťovou a informační bezpečnost
ePUSA	Elektronický portál územních samospráv
EU	Evropská unie
EVA	Elektronicky vlídná administrativa, Elektronická a Vaše administrativa
FBI	Federal Bureau of Investigation, Federální úřad pro vyšetřování
G2B	Government to Business, vztah státní správy k obchodníkům
G2C	Government to Citizen, vztah státní správy k občanům
G2E	Government to Employees, vztah státní správy ke svým zaměstnancům
G2G	Government to Government, vztah orgánů veřejné správy mezi sebou
G2P	Government to Public, vztah státní správy k veřejnosti

ICT	Informační a komunikační technologie
ISSS	Internet ve státní správě a samosprávě
ISVS	Informační systém veřejné správy
IT	Information Technology, informační technologie
ITSEC	Information Technology Security Evaluation Criteria, Kritéria hodnocení bezpečnosti informačních systémů
KIVS	Komunikační infrastruktura veřejné správy
LPIS	Land Parcel Information System, informační systém evidující zemědělskou půdu
MI	Ministerstvo informatiky ČR
MPO	Ministerstvo průmyslu a obchodu ČR
MVČR	Ministerstvo vnitra ČR
NATO	North Atlantic Treaty Organization, Severoatlantická organizace
NPPG	Národní program počítačové gramotnosti
NSIB	Národní strategie informační bezpečnosti
OECD	Organization for Economic Cooperation and Development, Organizace pro ekonomickou spolupráci a rozvoj
OSN	Organizace spojených národů
PKI	Public Key Infrastructure, infrastruktura veřejných klíčů
PSP	Policy Support Programme, program na podporu konkrétní politiky
TCSEC	Trusted Computer System Evaluation Criteria, Kritéria hodnocení zabezpečených počítačových systémů
WB	World Bank, Světová banka
Y2K	Year 2000, Rok 2000

ÚVOD

V závěru 20. století jsme se stali svědky ohromného pokroku a rozvoje v užívání informačních a komunikačních technologií (dále jen ICTs). Ty pronikly do reality každodenního fungování současné moderní či spíše post-moderní společnosti. ICTs, a zdůrazněme zejména Internet či mobilní telefony, které v současnosti již dovedou s tímto médiem také pracovat, se staly našimi věrnými společníky v širokém spektru činností.

Většina naší komunikace se děje jejich prostřednictvím v tzv. kybernetickém prostoru. V něm obchodujeme, nakupujeme, ukládáme v něm ohromné objemy dat a informací. Prostřednictvím kybernetického prostoru komunikujeme se svými blízkými a přáteli, ale také v profesních či obchodních záležitostech. Elektronická komunikace začala být využívána také k jednoduššímu navázání kontaktu mezi občany a veřejnou správou v souvislosti se zaváděním a rozvojem praktik e-governmentu de facto ve všech post-moderních společnostech. Státní správa i politici pak využití těchto ICTs často považují za efektivní a inteligentní způsob jak být v kontaktu se svými občany i voliči.

Rozvoj využívání vyspělých ICTs také přinesl poměrně významné změny do fungování současné post-moderní společnosti. Ustálil se pojem *informační společnost*. Informace jsou považovány za hlavní zdroj, sociálního, ekonomického i kulturního pokroku. Lze také říci, že post-moderní společnost se v tomto ohledu do jisté míry stala závislou na ICTs, které nám tyto informace zprostředkovávají.

Podobně jako jakákoli jiná závislost, tak i tato může být zdrojem zranitelnosti. ICTs mohou být zneužity k nezákonným činům, ale také k narušení bezpečnosti státu. Komunikační a informační systémy a sítě mohou být narušeny neautorizovaným vstupem. Pokud se pak tyto ICTs stávají nedělitelnou součástí našeho obchodního, politického, ale také osobního života a státních bezpečnostních složek, může tato skutečnost znamenat určité riziko pro správný chod státu.

Inspirací k napsání této diplomové práce byly kybernetické útoky na Estonsko na jaře r. 2007. Tato pobaltská země několik týdnů čelila soustředěnému a koordinovanému útoku proti svým klíčovým

infrastrukturám, hlavně bankovnímu sektoru a vládním komunikačním kanálům. Tyto útoky byly vedeny v kybernetickém prostoru, tedy za použití a zneužití ICTs. Estonsko bylo paralyzované a dočasně neschopné zajišťovat běžný chod a služby státu.

Kybernetické útoky v Estonsku vyvolaly zvýšený zájem vědců a pozorovatelů o problematiku kybernetické bezpečnosti i potenciální kybernetické války. Rozsah a úspěšnost těchto útoků vedla k určitému přehodnocení vnímání kybernetické války coby součásti sci-fi a předložila ji k vážnému zájmu a bádání široké veřejnosti i vědecké obce.

Estonsko je charakteristické svou pokročilostí v aplikaci ICTs do různých složek fungování a komunikace společnosti. Pro nás je relevantní zejména rozvoj praxe e-governmentu v rámci veřejné správy. Díky tomu je také někdy tato pobaltská republika přezdívána e-Stonia. Bezprecedentní útok vedený v kybernetickém prostoru ovšem znamenal citelný zásah do integrity tohoto státu, morálky jeho občanů i jejich důvěry v tento model.

Inspirativní pro tento text se stala právě pokročilost rozvoje služeb a možností e-governmentu aplikovaných v Estonsku. V naší práci proto představíme vývoj, hlavní překážky a úspěchy zavádění jeho praxe ČR od počátku 90. let do současnosti, kdy můžeme pozorovat největší a do určité míry až revoluční změny v oblasti zavádění nástrojů tohoto způsobu veřejné správy. Hovoříme o projektu tzv. datových schránek, který zásadně mění způsob komunikace občana se státní správou a úřady, a také o projektu základních registrů veřejné správy, jež by měly sjednotit a zefektivnit nakládání s údaji a daty spravovanými státními orgány a úřady.

Zaměříme se také na vliv EU a jejích iniciativ pro podporu a rozvoj využívání ICTs ve společnostech jejích členských i kandidátských států. Věříme totiž, že toto působení mělo na rychlost zavádění a aplikace e-governmentu v ČR zásadní vliv. Největší rozvoj je možné zaznamenat v první dekádě tohoto století, resp. posledních několika letech. Je zde patrná korelace s čerpáním finančních prostředků evropských fondů v rámci současného rozpočtového období Unie (2007-2013) pro zajištění prostředků zavádění e-governmentu. Nicméně nelze opomenout ani iniciativy *eEurope* a na ně navazující *i2010*, které povzbuzují členské i kandidátské země k rozvoji a využívání post-moderních ICTs, a to hlavně

k zajištění ekonomického pokroku, ale také větší demokracie skrze využívání praktik e-governmentu, který má přivést veřejnou správu blíže k občanovi.

Premisa zrychleného rozvoje zavádění nástrojů e-governmentu v posledních letech je také spojena se stále rychlejším zdokonalováním a zpřístupňováním sofistikovaných ICTs. Tento technologický rozvoj je ale také spojen se zvyšujícím se rizikem zneužití těchto ICTs proti veřejnosti a státu. Další část textu je proto věnovaná informační, resp. kybernetické bezpečnosti, kdy estonská zkušenost nám dala možnost pocítit a uvědomit si riziko, které se v této oblasti v současnosti vyskytuje.

Téma e-governmentu je rozpracováváno zejména v zahraniční literatuře, kde má také jeho praxe delší tradici než v ČR.[1] Nicméně i v této oblasti jsme u nás spolu s jeho úspěšnými praktickými projevy v posledních letech zaznamenali výraznější posun. Čeští autoři se však spíše než na teoretická východiska zaměřují právě na praktický výkon e-governmentu. Odpovídá se tak pravděpodobně potřebám současnosti, kdy je nutné vymezit a zmapovat využívání a možnosti tohoto způsobu veřejné správy v ČR. Výrazná část publikací věnujících se e-governmentu má často charakter příruček či návodů, jak se v problematice elektronické správy pohybovat. V této oblasti nicméně lze očekávat další vývoj související s rozvojem e-governmentu, a který je již patrný také v některých studiích menšího rozsahu či diplomových pracích.

Od r. 2001 čtvrtletně vychází časopis *Egovernment*, který se zabývá tématem elektronizace a informatizace české veřejné správy i společnosti. Je zaměřen zejména na poskytování relevantních informací pracovníkům státní správy, nicméně dostupný je všem. V jeho rámci je také vydávána výroční publikace *The Best* obsahující výběr z nejlepších projektů v oblasti elektronizace veřejné správy daného roku.[2]

[1] Z anglicky psané literatury zmiňme např. editovanou knihu *The World of E-government* autorů Gregory G. Curtina, Michaela H. Sommera a Veroniky Vis-Sommer, *Development in E-government: a Critical Analysis* autorů Davida Griffina, Philippy Trevorrow a Edwarda F. Halpina, *Practising E-Government. A Global Perspective* sestavena Mehdi Khosrowpourem či *Online Citizenship. Emerging Technologies for European Cities* sestavené Eleonorou DiMaria a Stefanem Micellim.

[2] Časopis Egovernment je dostupný online na http://www.egovernment.cz/.

V oblasti kybernetické či informační bezpečnosti je možné největší rozvoj výzkumu a literatury sledovat od přelomu milénia. Je to opět spojeno s technologickým rozvojem a rozšiřováním užití moderních a vyspělých ICTs do stále většího okruhu lidské činnosti, ať už civilní, tak i vojenské či obranné. Otázka zajištění bezpečnosti informačních a komunikačních sítí se také stala naléhavější v prostředí zvýšených rizik plynoucích z teroristických útoků a nekonvenčních způsobů vedení boje. Svoji roli měl ale také tzv. fenomén Y2K neboli obavy spojené s přelomem milénia.

Výzkum problematiky informační bezpečnosti má nicméně o něco delší tradici. Jeho vznik datujeme do období 80. let minulého století, kdy se ve větší míře začalo využívat ICTs pro spravování ohromného objemu dat, které státy, ale i soukromé firmy, banky a podobně začaly shromažďovat o svých občanech, zaměstnancích i zákaznících. Stanovení pravidel a východisek pro bezpečné nakládání s těmito cennými informacemi se stalo zásadní záležitostí.

Oblast kybernetické bezpečnosti a zajištění bezpečnosti státu v rámci kybernetického prostoru upoutala větší vědecký zájem koncem 90. let 20. století. Od té doby je možné sledovat zvyšující se počet kybernetických útoků s více či méně závažnými dopady na stát coby entitu, ale také na společnost. Důraz je pak v rámci hledání adekvátních reakcí na tyto kybernetické útoky často kladen na zajištění tzv. kritických infrastruktur a jejich vymezení. V ČR kupříkladu od července 2007 do konce r. 2010 probíhá výzkum *Problematika kybernetických hrozeb z hlediska bezpečnostních zájmů České republiky*. Jeho cílem je celková analýza současného globálního informačního prostoru a stavu jeho ochrany. Ambicí projektu je také navržení dalších možností a forem zabezpečení počítačů a počítačových systémů ČR před kybernetickými hrozbami. Vzory pro přístupy ke kybernetické bezpečnosti pak je možné nacházet ve vysoce „internetizovaných" zemích, jakými jsou Korejská republika, USA, Japonsko, ale také některé země EU, zejména Německo, severské státy a další.

Kybernetická bezpečnost se stala součástí výzkumu post-moderních nekonvenčních konfliktů, do jejichž charakteristiky řadíme také

kybernetické útoky, resp. kybernetické války. Rozvoj této disciplíny je patrné sledovat také v učebních programech některých vysokých škol v ČR (např. Fakulta sociálních studií Masarykovy univerzity a její obor Bezpečnostní a strategická studia, Policejní akademie, Matematicko-fyzikální fakulta Univerzity Karlovy a její Katedra softwarového inženýrství či České vysoké učení technické se svým Ústavem informatiky a telekomunikací ad.).

Při zpracování této diplomové práce vycházíme z česky i anglicky psaných titulů. Nezbytný zdroj relevantních informací představuje rovněž Internet, konkrétně webové stránky důležitých organizací a institucí zabývajících se (alespoň částečně) problematikou e-governmentu a kybernetické či informační bezpečnosti. Uveďme zde hlavně příklady Organizace spojených národů (OSN), Organizace pro ekonomickou spolupráci a rozvoj (OECD), Severoatlantickou alianci (NATO) či EU. Pro sledování a rozbor konkrétních projevů a přístupů k e-governmentu v ČR byly relevantním zdrojem stránky Ministerstva vnitra ČR, dále stránky spojené s projekty CzechPOINT či datových schránek. Důležité informace čerpáme také ze serveru Informační systémy veřejné správy či ze stránek krajských i místních samospráv.

Pro sledování tématu e-governmentu a vývoje jeho zavádění v ČR slouží jako základní literatura knihy *E-government v českém právu* autorů Pavla Matesa a Vladimíra Smejkala a *eGovernment bezpečně* sepsané Vítem Lidínským a kolektivem. P. Mates a V. Smejkal poměrně podrobně sledují cestu vývoje a využití e-governmentu od počátku 90. let 20. století do poloviny první dekády 21. století. Jejich zájem je obrácen zejména k právním aspektům a normám, které tento vývoj ovlivnily, nevyjímaje vliv mezinárodních organizací a úmluv, na kterých ČR participuje. V. Smejkal patří mezi přední české odborníky v oblasti práva souvisejícího s informačními technologiemi a elektronizací státní správy. Vycházíme také z jeho odborného článku *Datové schránky nastupují*, kde shrnuje dosavadní vývoj e-governmentu v ČR a představuje projekt datových schránek.

Autoři kolem V. Lidínského zpracovali téma e-governmentu do jakési příručky občana pro orientaci v základní problematice jeho nástrojů

a možností. Zohledňovány jsou opět právní normy a základní dokumenty s vysvětlením konkrétních praktických dopadů e-governmentu.

Problematikou e-governmentu v ČR a rozvojem elektronické komunikace se zabývá i Jiří Peterka. Čerpáme zde z jeho třech článků *i2010 místo eEurope 2005, Ohlédnutí za zanikajícím Ministerstvem informatiky* a *Osm priorit státní informační politiky*.

V oblasti informační bezpečnosti je českým expertem Josef Požár působící na Policejní akademii v Praze. V této práci pracujeme se dvěma jeho tituly. Nejprve se jedná o skriptum *Základy teorie informační bezpečnosti* kolektivu autorů kolem J. Požára a dále pak o knihu *Informační bezpečnost*, kterou již J. Požár vydal sám. Tento autor se ve svých pracích podrobně věnuje tématu informační bezpečnosti jak z pohledu teoretického, tak i technického. Jeho publikace se proto staly cenným zdrojem informací o typech a metodách hrozeb informační bezpečnosti, stejně jako o možnostech jejího zajištění a posílení.

K problematice informační bezpečnosti bychom ještě zmínili skriptum Romana Jaška *Informační a datová bezpečnost*. Jeho zájem je obrácen k problematice šifrování a přístupu firem k zabezpečení svých informačních systémů. Na podzim 2008 byl založen také odborný internetový magazín o bezpečnosti ICTs, *ICT Security*, který se věnuje aktuálním trendům i problémům souvisejících s využíváním současných ICTs.[3]

Přejdeme-li k tématu možnosti zneužití kybernetického prostoru k útokům proti státu, vycházíme z mnoha zdrojů české i zahraniční provenience. Základní knihou pro pochopení a uchopení současných konfliktů je kniha Mary Kaldor *New and Old Wars. Organised Violence in a Global Era*. Autorka svůj výzkum vystavěla na pozorování konfliktů, které propukly po konci studené války či krátce před jejím skončením. Z jejího pohledu jsou tyto nové konflikty více zaměřené na civilní obyvatelstvo a jsou charakteristické smazáváním dělící linie mezi kriminálním a válečným aktem. Bezpečnostní nejistota pak není výsledkem jen politického či státního násilí.

[3] Internetová adresa magazínu ICT Security - http://www.ictsecurity.cz/.

Otázkám kybernetických konfliktů se zevrubně věnují autoři Andy Jones, Gerald L. Kowacich a Perry G. Luzwick ve své knize *Global Information Warfare. How Businesses, Governments and Others Achieve Objectives and Attain Competitive Advantages*. Sledují zde vývoj konceptu informační války a dále také přístup k němu v různých státech či regionech.

Jako jeden z nejčerstvějších příspěvků do diskuze o kybernetických výzvách současnosti představíme knihu editovanou Athinou Karatzogianni *Cyber-conflict and Global Politics*. Jednotliví autoři zde analyzují 14 konfliktů, jež využívají, resp. zneužívají možnosti kybernetického prostoru. Sledují také vliv post-moderních ICTs na současná bezpečnostní studia a témata, na politiku, média i společnost obecně.

Z českých řad bychom rádi zmínili Martina Bastla, který působí na Fakultě sociálních studií Masarykovy univerzity a zabývá se strategickými studii, soudobými konflikty a souvisejícími bezpečnostními hrozbami. V této práci využíváme jeho článku *Budoucnost nekonvenčních forem boje*. V jeho pojetí je nekonvenční způsob boje přirozeným vývojem způsobu vedení válečného konfliktu. Ve svém textu Bastl pracuje se dvěma příklady, a to s kybernetickými konflikty coby poměrně novým typem konfliktů a dále s terorismem coby příkladem psychologicky vedené, nekonvenční války. Oblast kybernetického terorismu pak rovněž rozpracovává Michal Janoušek ve svém článku *Kybernetický terorismus: terorismus informační společnosti.* Kybernetický terorismus je zde vnímán jako extenze klasického terorismu do kybernetického prostoru využívající možnosti nabízené informační společností.

Přístupy EU k informační bezpečnosti, ale i k rozvoji e-governmentu analyzujeme zejména na základě oficiálních dokumentů Společenství i textů jednotlivých výzev v této oblasti. Zdůraznili bychom iniciativy e*Europe* a *i2010* či *Strategii pro bezpečnou informační společnost. Dialog, partnerství a posílení*. K relevantním zdrojům informací patří také oficiální webové stránky Unie, především Evropské komise a jejího tematického portálu o evropské informační společnosti.[4]

[4] Webová adresa - http://ec.europa.eu/information_society/

Texty dokumentů, sdělení a dalších je možné vyhledat v rámci Portálu EU[5] a jeho sekce Eur-lex.

Podobně jako v případě sledování problematiky EU, také v oblasti rozvoje e-governmentu v ČR čerpáme z primárních zdrojů, tedy zákonných úprav a vyhlášek, ale také z textů různých strategií a iniciativ (např. *Národní strategie informační bezpečnosti ČR, Státní informační a komunikační politika* ad.). Je nutné zdůraznit zejména dva zákony, které přinesly dosud zřejmě nejpodstatnější změny a posuny v elektronizaci veřejné správy. Jedná se o *Zákon č. 227/2000 Sb., o elektronickém podpisu* a *Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů*. Texty zákonů i vyhlášek lze dohledat na webových stránkách nakladatelství ekonomické a právní literatury Sagit, dále také v relevantních odkazech na webových stránkách Ministerstva vnitra ČR či v rámci Portálu veřejné správy ČR. Významným zdrojem informací byla také programová prohlášení jednotlivých vlád od r. 2002,[6] která jsou dostupná na webových stránkách Vlády ČR.

Pro rozbor současných trendů a podob kybernetických útoků jsme vycházeli také z výročních a shrnujících zpráv některých soukromých firem a korporací. Vyzdvihli bychom publikační činnost společností zabývajících se internetovou bezpečností, a to Symantec a McAfee. Zejména zpráva druhé uvedené, *Virtual Criminology Report – Cybercrime: The Next Wave,* nám byla zdrojem relevantních informací. Také studie institutu Information Warfare Monitor, *Tracking GhostNet: Investigating a Cyber Espionage Network,* jež je zaměřená na zhodnocení vyšetřování kybernetických útoků proti tibetské komunitě v exilu, předkládá současný stav kybernetických hrozeb ve světě, konkrétně možnosti a metody kybernetické špionáže.

Tato práce je členěna tematicky do dvou základních částí. První z nich je věnovaná problematice e-governmentu, kdy se nejdříve zaměříme na vymezení tohoto pojmu. Z tohoto důvodu zde bude použito zejména metody analýzy a syntézy, neboť budeme vycházet z různých konceptů a uchopení tohoto fenoménu.

[5] Webová adresa: http://europa.eu

[6] Vlády předchozí, tedy Klausovy, Tošovského a Zemanova, se elektronizaci veřejné správy ve svých programových prohlášeních příliš nevěnovaly.

Pro další kapitoly první části textu jsme zvolili empiricko-analytický přístup, protože zde vycházíme z primárních zdrojů, zákonů a strategií EU i ministerstev ČR. Sledujeme také aktuální praktický vývoj a způsoby, jak ho tyto iniciativy a zákonné úpravy ovlivňují. Druhá kapitola první části tedy konkrétně prezentuje vývoj zavádění nástrojů e-governmentu do české praxe. Budeme analyzovat hlavní úspěchy a neúspěchy v tomto procesu. Navazovat bude oddíl věnovaný iniciativám EU, které měly na tento vývoj nezanedbatelný vliv. A ve čtvrté kapitole představíme proces právního ukotvení e-governmentu v českém prostředí.

Pátá kapitola části o e-governmentu v ČR předkládá jeho nejzásadnější praktické projevy. Představíme si koncept elektronického podpisu a institut elektronického podání a doručování. Následovat bude prezentace projektů CzechPOINT a datových schránek. Sledovat budeme jejich základní charakteristiky a zhodnotíme jejich přínos pro rozvoj e-governmentu, stejně jako jejich úspěšnost, resp. neúspěšnost v tomto procesu.

E-government coby elektronická veřejná správa využívající možností ICTs je právě na základě spoléhání na tyto prostředky a technologie zranitelná a ohrozitelná. E-government lze také vnímat jako pozitivní využití ICTs. Existuje pak také možnost jejich zneužití proti státu i společnosti. Druhá část této diplomové práce je proto věnovaná rizikům souvisejícím s aplikací nástrojů e-governmentu, konkrétně pak informační a kybernetické bezpečnosti.

Nejprve přiblížíme problematiku, aspekty a metody zabezpečení informačních systémů. Druhá kapitola této části se blíže zaměří na problematiku informační bezpečnosti, jejího zajištění i jejích základních hrozeb. Pro tyto oddíly jsme zvolili metody analýzy a syntézy, kdy vycházíme z právních základů, dalších teoretických rámců, přístupů a návodů i dokumentů předkládajících strategii informační bezpečnosti (např. *Národní strategie informační bezpečnosti ČR*).

Ve třetí kapitole druhé části sledujeme hlavní metody a podoby zneužití ICTs proti státu. Věnovat se budeme motivacím ke kybernetickým útokům. Přiblížíme tři nejčastější příklady kybernetických útoků proti státu - kybernetickou špionáž, kybernetický terorismus a tzv.

hacktivismus. Nejprve budeme vycházet z metody analýzy a syntézy, jelikož nám půjde o představení základních přístupů k těmto rizikům a útokům. Při rozboru konkrétních příkladů kybernetických útoků bude využito empiricko-analytického přístupu.

Poslední kapitola prezentuje přístupy EU k informační a kybernetické bezpečnosti. Zaměříme se na iniciativy *eEurope* a *i2010* a možnosti jejich dalšího rozvoje resp. revize. Za užití analyticko-empirického přístupu zde prezentujeme konkrétní unijní dokumenty, iniciativy a postupy, které byly přijaty a aplikovány v oblasti informační a kybernetické bezpečnosti.

Hypotézou této diplomové práce je vnímání EU coby stěžejní entity stojící za zrychleným vývojem zavádění nástrojů e-governmentu v ČR v první dekádě 21. století, a to z důvodů finanční i morální podpory rozvoje elektronizace státní správy ve Společenství. Druhou výzkumnou tezí této studie je pojetí a pochopení kybernetické bezpečnosti a kybernetických hrozeb coby relevantních strategických a bezpečnostních výzev současnosti, které je třeba zahrnout do bezpečnostních strategií států i mezinárodních organizací jako je EU či NATO.

Oblast e-governmentu představuje velice širokou oblast pro výzkum i praktické rozvíjení přístupů. Proto je cílem této práce předložit základní milníky vývoje e-governmentu v ČR, který ještě není ukončen. Nebylo tedy možné dostatečně zmapovat a zanalyzovat zejména poslední dosud navržené fáze elektronizace státní správy, plné spuštění projektu datových schránek či zřízení centrálních registrů veřejné správy, a to jednoduše z důvodu poměrně krátkého časového odstupu nebo vzhledem k tomu, že se nacházíme v období před začátkem daného projektu. Nicméně i přesto se zde o zhodnocení pokusíme a svá východiska a závěry v textu uvádíme. Je však třeba poukázat na to, že zde stále zůstává prostor pro další analýzy a bádání (např. problematika eHealth, eJustice, otázky ICTs a životního prostředí ad.). Podobně tak v případě EU můžeme očekávat rozvoj přístupů k informační a kybernetické bezpečnosti a případné, avšak z našeho pohledu nezbytné, přijetí jednotné politické a strategické koncepce věnující se kybernetické bezpečnosti, jak ji navrhuje komisařka Viviane Reding.

Téma kybernetické bezpečnosti představuje v zásadě rodící se a postupně se rozšiřující výzkumnou oblast. V této práci si dáváme za cíl předložit a analyzovat základní východiska tohoto konceptu. Níže představený výklad by se mohl jevit v některých ohledech jako poněkud zkratkovitý. Nicméně záměrem je v tomto textu poukázat na existenci problematiky a reálné hrozby kybernetických útoků proti státu a s tím pak sledovat teoretické základy kybernetické bezpečnosti i soudobé praktické jevy a kroky učiněné v této oblasti. Můžeme předpokládat, že téma kybernetické bezpečnosti bude předmětem dalších studií a výzkumů.

1. E-GOVERNMENT

V současnosti můžeme sledovat poměrně významné kroky v rozvoji elektronizace státní správy neboli e-governmentu v ČR. V hojné míře je využíváno kontaktního místa CzechPOINT, kde občané získávají výpisy z různých rejstříků a databází veřejné správy. Letošní r. 2009 uvedl projekt datových schránek, jenž by měl znamenat určitou revoluci ve způsobu komunikace občanů s orgány veřejné moci. V roce následujícím je naplánované zřízení tzv. centrálních registrů veřejné správy, v nichž mají být efektivněji spravována data, která státní správa shromažďuje pro své náležité fungování. Nicméně úsilí o rozvoj nástrojů e-governmentu, s většími či menšími úspěchy i klopýtnutími, je možné v ČR sledovat již od počátku 90. let minulého století.

V první kapitole této práce se nejprve zaměříme na vymezení pojmu e-government. Zodpovíme otázku, co si konkrétně pod tímto pojmem představit. Prezentujeme základní vnímání a přístupy k této problematice v rámci vědecko-výzkumné obce, ale také některých významných mezinárodních organizací a samozřejmě také české vlády, konkrétně Ministerstva vnitra, které je za realizaci e-governmentu u nás zodpovědné.

Následně přiblížíme vývoj zavádění nástrojů e-governmentu i politických přístupů a postojů k němu v ČR. Sledovány budou také posuny v rámci právních norem a právního ukotvení e-governmentu, jež je stěžejní pro proces jeho úspěšné realizace. V této souvislosti navážeme uvedením základních praktických projevů českého e-governmentu, tedy elektronického podpisu, elektronického podání a doručení, projektu CzechPOINT a konečně datových schránek.

1. 1. Vymezení pojmu

Pro výraz *e-government* se v současnosti často nehledá odpovídající překlad do jiných jazyků. Stal se pojmem, který se v moderních společnostech používá v původním anglickém tvaru a vymezuje se spíše v rovině obsahové. V zásadě je vnímán jako soubor úkolů, *„které se*

zabývají elektronizací výkonu činnosti veřejné správy nebo v širším pojetí spíše orgánů veřejné moci vůbec."[7]

E-government představuje neologismus vzniklý ze zkrácení anglického výrazu „electronic government" čili elektronická správa či vláda,[8] jak lze také tento výraz přeložit do češtiny.[9] E-government můžeme tedy definovat *„jako využití informačních a komunikačních technologií[10] (např. dálkové počítačové sítě, internet, mobilní technologie apod.) veřejnou správou k poskytování informací a veřejných služeb nejširší veřejnosti.*"[11] Z podobného základu vychází také definice Evropské komise, která e-government vnímá jako *„užití informačních a komunikačních technologií ve veřejné správě, kdy jsou spojeny organizační změny a nové možnosti za účelem zlepšit veřejné služby a demokratické procesy.*"[12] Aspekt zlepšení veřejné služby občanům pak vede také k chápání výrazu e-government jako spojení dvou slov, a to „efektivní vládnutí či správa".[13]

Přístupy k vysvětlení pojmu e-government a jeho vnímání obecně se liší. Představíme ovšem pouze některé z nich, jež považujeme za nejvýstižnější k pochopení tohoto výrazu i jeho fungování. Centrum pro technologie ve správě[14] předkládá poměrně jednoduchou definici e-governmentu: *E-government je užití informačních technologií k podpoře vládních kroků, k zapojení občanů a k poskytování vládních služeb.*[15] Důraz je kladen na čtyři základní dimenze, které odpovídají funkcím veřejné správy - *e-services* (elektronicky dostupné informace, programy a služby veřejné správy, často skrze internet), *e-democracy* (užití elektronických médií ke zvýšení účastni občanů na rozhodovacích

[7] MATES, Pavel – SMEJKAL, Vladimír: *E-government v českém právu.* Praha 2006, s. 9.
[8] TUŠEROVÁ, Lenka: *E-government a jeho projevy v českém právu.* Právnická fakulta Masarykovy univerzity, http://www.law.muni.cz/edicni/dp08/files/pdf/sprava/tuserova.pdf (6. července 2009)
[9] V tomto textu však budeme používat výraz e-government. Při citaci budeme uvádět výraz, jak je uveden v originále.
[10] Information and communication technologies (ICTs).
[11] TUŠEROVÁ, L.: c.d.
[12] GRAMLICH, Ludwig: *Recent Developments Relating to Electronic Government.* In: POLČÁK, Radim - ŠKOP, Martin - ŠMAHEL, David (eds.): *Cyberspace 2005.* Brno 2006, s. 81.
[13] Viz např. *Putting Citizens First.* In: European Commission, Europe's Information Society, http://ec.europa.eu/information_society/tl/soccul/egov/index_en.htm (8. září 2009)
[14] Centre for Technology in Government při New York State University.
[15] *A working definition of e-government.* In: State University of New York, Center for Technology in Government, The Future of eGovernment, http://www.ctg.albany.edu/publications/reports/future_of_egov?chapter=2 (8. července 2009)

procesech), *e-commerce* (elektronická výměna peněz za zboží a služby, elektronická platba daní či složenek apod.) a *e-management* (užití informačních technologií ke zlepšení fungování veřejné správy). Právě e-management je stěžejní pro dobré fungování e-governmentu, neboť se zaobírá jeho správným využíváním a spravováním.[16]

Výkonem a implementací e-governmentu se zabývá také intenzivně EU. Ta jej také definuje jako zavádění ICTs k zajištění lepších služeb veřejné správy občanům i firmám. Komunikace s orgány veřejné správy má být snadnější a levnější. S pohledu EU efektivní e-government představuje zdokonalení správy obecně a umožnění většího zapojení občanů do politického procesu.[17]

OECD se pak ve své definici e-governmentu zaměřuje na způsoby veřejné správy a opět její možné další zlepšení. E-government může rovněž zvyšovat důvěru občanů ve veřejnou správu. Občan má totiž možnost přímo a aktivněji se zapojit do politického procesu, a to snadnějším přístupem k informacím i státním službám či kontrolou práce svých zastupitelů. Je tak vytvářena otevřená a zodpovědnější správa, což napomáhá omezit korupci.[18]

OECD také předkládá čtyři základní principy výkonu e-governmentu – vize a politická vůle, společná struktura a kooperace, zaměření na zákazníka (občana) a zodpovědnost. *Vize a politická vůle* souvisí s vůdcovstvím a závazkem, které jsou podmínkou změny k lepší správě, a integrací e-governmentu do širší politické reality a praxe vedoucí k tomuto zlepšení. *Společná struktura a spolupráce* znamená propojení práce různých státních úřadů, aby nedocházelo zejména k duplicitě, a zajištění dostatečného financování jejich fungování souvisejících projektů. *Zaměření na uživatele–občana* představuje princip dostupnosti, možnosti výběru způsobu komunikace s úřady, aktivního zapojení občana a konečně důvěrnosti, tedy zajištění ochrany osobních údajů uživatelů. *Zodpovědnost*

[16] *A working definition of e-government*.
[17] *eGovernment.* In: European Commission, Europe´s Information Society, http://ec.europa.eu/information_society/activities/egovernment/index_en.htm (11. listopadu 2009); viz také *Putting Citizens First.*
[18] MATES, P. – SMEJKAL, V.: c.d., s. 2.

souvisí s transparentností a jasným stanovením kompetencí úřadů i jednotlivců, stejně jako sledování a vyhodnocení služeb.[19]

Na definici e-governmentu předloženou OECD navazuje vysvětlení pojmu ze strany Institutu pro rozvojovou politiku a management Manchesterské univerzity.[20] Podle jeho definice e-government opět znamená zavedení ICTs prostředků ke zlepšení veřejné správy. Zahrnuje tři oblasti: zlepšení vládních procesů (eAdministration), napojení a spojení občanů (eCitizens a eServices) a budování vnějších kontaktů a interakcí (eSociety).[21]

Občan je v rámci těchto pojetí e-governmentu ve vztahu k veřejné správě vnímán jako zákazník. Vlády se snaží zlepšit vztah a kontakt mezi svými občany a orgány státní moci. E-government je také chápán jako forma veřejné správy orientovaná na zákazníka neboli občana. Vláda, která aktivně využívá nástrojů e-governmentu, pak bývá označována jako „costumer-centric". Jejím hlavním cílem je využívání daňových prostředků ke zvyšování spokojenosti zákazníků-občanů.[22]

Světová banka (WB) uvádí definici e-governmentu coby využití prostředků ICTs vládními úřady. Výsledkem je opět změna vztahu mezi občany a podnikatelskou sférou a státem. Ta může vést k *„lepší dostupnosti vládních služeb občanům, ke zlepšení kontaktů a vztahů s podnikatelským sektorem a průmyslem, k posílení pozice občanů prostřednictvím přístupu k informacím a také k efektivnější správě. Výslednými výhodami pak může být nižší míra korupce, větší transparentnost a spokojenost, růst příjmů a snížení nákladů."*[23]

---

[19] *The e-government imperative: main findings.* In: OECD, Policy Brief, březen 2003, http://www.oecd.org/dataoecd/60/60/2502539.pdf (6. července 2009), s. 3.

[20] Institute for Development Policy and Management, University of Manchester.

[21] *eAdministration* je zaměřená na snižování nákladů, vytváření strategických kontaktů v rámci státní správy, správné nakládání s prezentací systému státní správy a na přesun center moci ve veřejné správě. V pojetí *eCitizens* či *eServices* je občan mimo jiné chápán jako zákazník-klient, který přijímá služby státu. Je zde zahrnutá aktivnější komunikace s občany, jejich informovanost a naslouchání jim, a též zlepšení veřejných služeb. *eSociety* se zaměřuje na lepší spolupráci s obchodním sektorem, na rozvoj specifických komunit a na budování partnerství mezi orgány státní správy a ostatními zájmovými skupinami a organizacemi, stejně jako s jednotlivci. (*What is eGovernment?* In: Institute for Development Policy and Management, Manchester University, eGovernment for Development, http://www.egov4dev.org/success/definitions.shtml#eAdmin (8. července 2009)

[22] *At the Dawn of e-Government: The Citizen as Customer*. In: Government Finance Review, říjen 2000, http://www.entrepreneur.com/tradejournals/article/67323089_1.html (6. července 2009)

[23] *Definition of E-Government.* In: The World Bank (WB), http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUN

Dosáhnout na požadované služby státu a jeho úřadů stejně jako komunikace s nimi má být pro občana jednodušší.[24]

WB uvádí v popisu vztahu mezi občanem a veřejnou správou analogii e-governmentu a e-commerce (elektronického obchodu), kdy se obchodník snaží navázat bližší vztah se zákazníkem (B2C, business to customer) či kdy dochází ke zlepšování vztahů mezi jednotlivými firmami a podniky (B2B, business to business). V oblasti e-governmentu se státní správa snaží navázat bližší a lepší kontakty s občany (G2C, government to citizen), s obchodními společnostmi (G2B, government to business) a také mezi svými orgány navzájem (G2G, government to government).[25]

L. Lowery ve své studii ještě přidává vztahy mezi státní správou a veřejností (G2P, government to public) a vládním aparátem a jeho zaměstnanci (G2E, government to employees). Důležitými pojmy jsou u Lowery veřejná dostupnost a poskytnutí (public provision), digitální demokracie (digital democracy) a hospodářský rozvoj (economical development).

Veřejná dostupnost znamená nepřetržitý přístup ke všem službám a informacím veřejné správy. *Digitální demokracie* souvisí s definicí e-governmentu coby procesu užití prostředků elektronické komunikace k dosažení kontaktu s voličem i občany, stejně jako využití elektronických médií k volbám či v rámci volební kampaně. To by mohlo zvýšit politickou účast, zájem i znalost občanů. *Rozvoj ekonomiky*, který je stěžejní pro úspěšnou vládu, vychází z předpokladu, že tento je do značné míry závislý na využití moderních komunikačních technologií a dostupnosti informací.[26]

V. Lidínský a kol. ve své knize vychází z definice OSN, kdy e-government představuje *„(T)rvalou povinnost veřejné správy zlepšovat vztah mezi občany a veřejným sektorem poskytováním levných a*

ICATIONANDTECHNOLOGIES/EXTEGOVERNMENT/0,,contentMDK:20507153~menuPK:702592~pagePK:148956~piPK:216618~theSitePK:702586,00.html (8. července 2009)

[24] Např. Czech POINT (viz níže kapitola 1.5.3. CzechPOINT) či osobní počítač.

[25] *Definition of E-Government.*

[26] LOWERY, Liza M.*: Developing a Successful E-Government Strategy*. In: United Nations (UN), unpan1.un.org/intradoc/groups/public/.../UNPAN000343.pdf (8. července 2009), s. 2.

efektivních služeb, informací a znalostí.“[27] Dále je v jejich publikaci představena definice Ministerstva vnitra resp. bývalého Ministerstva informatiky, kdy *„eGovernment představuje transformaci vnitřních a vnějších vztahů veřejné správy pomocí informačních a komunikačních technologií s cílem optimalizovat interní procesy.“*[28] A konečně autoři kolem Lidínského uvádějí také svoji vlastní definici: *„eGovernment je využívání informačních technologií veřejnými institucemi pro zajištění výměny informací s občany, soukromými organizacemi a jinými veřejnými institucemi za účelem zvyšování efektivity vnitřního fungování a poskytování rychlých, dostupných a kvalitních informačních služeb.“*[29]

Na závěr uvedeme pojetí e-governmentu ze strany české vlády a Ministerstva vnitra ČR. Tento přístup je pak stěžejní pro postupy a projekty zavádění jeho nástrojů u nás. E-government je symbolizován postavou *eGona*, který de facto představuje e-government.[30] Základními součástmi e-governmentu, resp. základními životními funkcemi eGona jsou mozek (základní registry veřejné správy), srdce (eGovernment Act, čili zákon o e-governmentu[31]), oběhový systém (komunikační infrastruktura veřejné správy, KIVS) a prsty (CzechPOINT coby univerzální kontaktní místo). Fungování e-governmentu je pak vysvětleno analogicky jako fungování živého organismu. Skrze prsty je přijat podnět. Skrze oběhový systém je vyslán signál do mozku, který informaci vyhodnotí a správný orgán rozhodne. Prstům je pak vyslána informace o tom, co mají dělat.[32]

Pro potřeby této práce jsme výše uvedená pojetí a vysvětlení propojili a e-government vnímáme jako způsob veřejné správy, kdy státní moc i jiné veřejné instituce využívají prostředků moderní elektronické komunikace (zejména Internetu) za účelem zlepšení a zefektivnění

[27] LIDÍNSKÝ, Vít a kol.: *eGovernment bezpečně.* Praha 2008, s. 7.; viz také *E-governance and Access to Information.* In: Organizace spojených národů (OSN), Democratic Governance, http://ictd.undp.org/e-gov/ (31. října 2009)

[28] Tamtéž, s. 7; srov. HRAJNOCHA, Luděk: *Projekty MI v oblasti e-governmentu.* In: Institut mikroelektronických aplikací (IMA), http://www.ima.cz/download/cz/aktuality/platformai2010/seminare/S5_i2010_Hrajnoha.pdf (12. září 2009).

[29] LIDÍNSKY, V. a kol.: c. d., s. 7.

[30] Projekt eGon tedy projekt elektronizace veřejné správy byl zahájen v r. 2006.

[31] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. (Viz níže kapitoly 1.2. Rozvoj e-governmetu v ČR, 1.4. Právní ukotvení e-governmentu v ČR a 1.5.4. Datové schránky.)

[32] *E-government. Veřejná správa jako živý organismus.* In: CzechPOINT, http://www.czechpoint.cz/web/?q=node/18 (5. července 2009)

fungování státní správy. Stěžejní je zkvalitnění vztahů s občany i firmami a usnadnění jejich přístupu k orgánům veřejné administrativy a získání informací o veřejné správě (zejména téměř nepřetržitým online přístupem k internetovým stránkám či aplikacím). Efektivita státní správy má být dosažena mimo jiné také odstraňováním duplicit skrze žádoucí fungování jejích centrálních registrů, což přispěje k omezení množství informací shromažďovaných o občanech často vícekrát v různých, navzájem nepropojených databázích. Cílem je zlepšení komunikace také mezi orgány a úřady státní správy.

1. 2. Rozvoj e-governmentu v České republice

Rozvoj e-governmentu v ČR datujeme již na počátek 90. let. To souviselo se změnou sociálních i politických okolností, ale také s technologickým rozvojem. Počátky e-governmentu v ČR však byly poznamenány nedostatkem znalostí, informací i koordinace v jeho implementaci.[33] Zajímavý je také vývoj technických podmínek vedení informačních systémů v ČR. Před rokem 1990 bylo charakteristické spravování dat v papírových kartotékách či jinými klasickými formami. Období 90. let pak představuje nástup postupně se zkvalitňující a propracovanější výpočetní techniky. Její prvky však byly zaváděny relativně spontánně.[34]

Česká vláda se problematikou e-governmentu zabývala od r. 1992. V lednu 1993 měl být na základě vládního usnesení č. 78 předložen projekt globální architektury informační soustavy ČR[35] a o dva roky později pak vláda vypracovala návrh vybudování jednotného státního informačního systému.[36] Z tohoto podkladu pak v září 1995 vyšel materiál pod názvem

[33] Blíže k „chaotickým" začátkům e-governmentu v ČR viz MATES, P. – SMEJKAL, V.: c.d., s. 13-14.
[34] Tamtéž, s. 25.
[35] Blíže k projektu viz Tamtéž, s. 13-14.
[36] Informační systém je soubor lidí zdrojů, zpracovatelů, uživatelů, technických prostředků a metod, zabezpečujících sběr, přenos, uchování a zpracování data účelem tvorby a prezentace informací pro potřeby uživatelů. (POŽÁR, Josef: *Informační bezpečnost*. Plzeň 2005, s. 26.) Informačním systémem veřejné správy rozumíme funkční celek zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací. Každý takový systém zahrnuje informační základnu, technické a programové prostředky, technologie a procedury a také pracovníky. Zákon č. 365/2000 Sb. informační systém definoval jako funkční celek i jeho část zajišťující cílevědomou a systematickou informační činnost. (Blíže k zákonu o informačních systémech veřejné správy viz MATES, P. – SMEJKAL, V.: c. d., kap. 1.2.)

Výstavba státního informačního sytému ČR, který navrhoval zahrnutí registrů nemovitostí i obyvatel včetně registrů sociálních dávek, zdravotního pojištění i ekonomických subjektů do jednoho informačního systému. Nicméně zejména kvůli postupným přesunům kompetencí mezi rezorty a jinými orgány státní správy došlo k podstatnému zpomalení této iniciativy. O rok později byl založen Úřad pro státní informační systém, který však zůstal v zásadě bez kompetencí, neboť v praxi si každý resort vytvářel vlastní informační systémy.[37]

Významným posunem byl strategický dokument *Státní informační politika – cesta k informační společnosti* schválený vládou v r. 1999.[38] Dokument měl představovat národní koncepci budování tzv. informační společnosti.[39] Podstatou státní informační politiky se stalo *„vytvoření veřejně přístupné služby přes příslušné komunikační rozhraní za účelem rozvoje oboustranné komunikace mezi veřejnou správou a občany.“*[40] Ve stejném roce byla přijata *Koncepce budování informačních systémů.*[41]

Základní zásadou budování informačních systémů v ČR se stal princip minimalizace. Jeho podstatou *„byla snaha po minimalizaci informací, které jsou požadovány veřejnou správou po adresátech, zejména vyloučit situaci, kdy jsou data vyžadována vícekrát, a to i chybně… informaci, kterou již stát, resp. jeho orgán jednou má, nebude vyžadovat znovu. Princip minimalizace se měl prosadit, i pokud jde o počet registrů, případně jejich obsah.“*[42] Tento princip je v koncepci elektronizace veřejné správy přítomen stále (např. v konceptu centrálních

[37] Okolnosti vývoje státního informačního sytému rozebírají Mates a Smejkal. (MATES, P. – SMEJKAL, V.: c. d., s. 14-15).
[38] Text dokumentu viz *Státní informační politika – cesta k informační společnosti.* In: Britské listy, 5. září 2006, http://blisty.cz/2006/9/5/art30127.html (10. listopadu 2009)
[39] PETERKA, Jiří: *Osm priorit státní informační politiky*. In: Archiv článků a přednášek Jiřího Peterky, http://www.earchiv.cz/anovinky/ai2364.php3 (12. srpna 2008)
[40] MATES, P. – SMEJKAL, V.: c.d., s. 15.
[41] Koncepce budování informačních systémů schválena Vládou ČR v říjnu 1999 je úzce spojena s informatizací veřejné správy, tedy využití moderních ICT prostředků pro zefektivnění veřejné správy. Viz *Koncepce budování informačních systémů veřejné správy*. In: Informační systémy veřejné správy, http://www.isvs.cz/user_data/dokumenty/UVIS-Koncepce-ISVS-1999.pdf (12. srpna 2009)
Blíže k vývoji vládní politiky týkající se státních informačních systémů viz MATES, P. – SMEJKAL, V.: c. d., s. 25-26.
[42] Tamtéž, s. 27.

registrů[43]), kdy se vedená data nemají duplikovat a každý registr je jejich jediným garantovaným zdrojem.

V r. 2000 byl Úřad pro státní informační systém nahrazen Úřadem pro veřejné informační systémy, který se měl věnovat rozvoji a vytváření informačních systémů veřejné správy.[44] Došlo k posunu od ideje vytvoření jednotného státního informačního systému k reálnější soustavě informačních systémů veřejné správy (ISVS).[45] Ty jsou *„souborem informačních systémů, které slouží pro výkon veřejné správy.“*[46]

Úřad pro ISVS byl však také zrušen a v r. 2002 přešly jeho pravomoci i působnost na Ministerstvo informatiky.[47] Jedním z nejvýznamnějších počinů ministerstva v této oblasti se stalo spuštění Portálu veřejné správy[48] v říjnu 2003, který *„představuje informační systém, poskytující systematické informace o jednotlivých subjektech, jejich činností a výsledcích těchto činností.“*[49] Mimo celostátní informační systémy byly budovány také sítě na regionální či místní úrovni.[50]

I přes některé vládní iniciativy v oblasti rozvoje e-governmentu[51] její úsilí nepředstavovalo v této době přílišný úspěch a posun. Za nejzávažnější nedostatek a komplikaci v rozvoji e-governmentu lze v této době považovat nedobudování základních registrů veřejné správy a

---

[43] Viz níže kapitola 1.4. Vývoj právního ukotvení e-governmentu a vládních postojů k němu.

[44] Na základě zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. (MATES, P. – SMEJKAL, V.: c.d., s. 16)

[45] Tamtéž, s. 27-28.

[46] *Informační systémy veřejné správy.* In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/informacni-systemy-verejne-spravy.aspx (1. února 2009)

[47] Blíže k vývoji a přesouvání kompetencí jednotlivých úřadů a resortů v souvislosti s rozvojem e-governmentu viz MATES, P. – SMEJKAL, V.: c.d., s. 14-16. K Ministerstvu informatiky viz níže.

[48] Internetová adresa portálu: http://portal.gov.cz

[49] MATES, P. – SMEJKAL, V.: c.d., s. 16.

[50] Např. Regionální informační servis (RIS) a nadstavbový Integrovaný regionální informační systém (IRIS). Tyto portály slouží zejména coby informační nástroj pro podporu tvorby koncepce a realizaci regionálního rozvoje ČR. Regionální i centrálně zjišťovaná data a informace jsou určena pro potřeby centrálních orgánů, krajských úřadů, samosprávy, podnikatelské sféry a také široké občanské veřejnosti. (*RIS – Regionální informační servis.* In: Agentura regionálního rozvoje, http://www.arr-nisa.cz/iware_cz/?D=21 (19. října 2008)
Blíže oběma systémům také viz MATES, P. – SMEJKAL, V.: c.d., s. 17.

[51] Např. usnesení vlády č. 237/2004 o Postupu a hlavních směrech reformy a modernizace ústřední státní správy pro období 2005-2010 nebo č. 1306/2004 k budování registrů veřejné správy. (Dokumenty viz *Usnesení Vlády České republiky o Postupu a hlavních směrech reformy a modernizace ústřední státní správy*. In: Vláda ČR, http://racek.vlada.cz/usneseni/usneseni_webtest.nsf/0/4D45F2283205A4F2C12571B6006D669A (20. října 2009); *Usnesení Vlády České republiky k budování registrů veřejné správy*. In: Vláda ČR, http://racek.vlada.cz/usneseni/usneseni_webtest.nsf/web/cs?Open&2004&12-22 (20. října 2009).

způsobů jejich spravování, které by také umožňovaly jejich sdílení.[52] Toto se postupně daří naplňovat až spolu s aplikací a užíváním kontaktního místa CzechPOINT a plánovaným projektem vytvoření centrálních registrů, tedy mozku Egona.

V rámci rozvoje informačních systémů nicméně r. 2000 vznikl elektronický portál místních samospráv ePUSA.[53] Informační systém ePusa[54] je společný pro Ministerstvo vnitra ČR, kraje a ostatní samosprávy. Jeho základním cílem je *„být jediným garantovaným zdrojem informací o subjektech samosprávy, a zamezit tak jejich duplicitnímu zjišťování orgány veřejné správy.“*[55] ePusa má poskytovat informace jak zaměstnancům krajských úřadů, tak také veřejnosti. Kraje i ostatní orgány veřejné správy jsou odpovědné za správnost údajů o nich v ePuse vedených.[56]

Na úroveň obcí, které by aktivním přístupem k obohacování obsahu portálu ePusa měly také zvýšit zájem svých občanů o zavádění a využívání Internetu a elektronické komunikace s úřady, je směřován také projekt EVA neboli Elektronicky vlídná administrativa či Elektronická a Vaše Asistentka.[57] Jeho působnost je v kompetenci Ministerstva vnitra ČR. Cílem projektu je *„umožnit zveřejňování kontaktních údajů o jednotlivých obcích pro potřeby podnikatelské, informování veřejnosti, ale také řešení krizových situací.“*[58]

Dalšímu rozvoji využívání elektronických komunikačních prostředků a e-governmentu na místní úrovni však často brání nedostatek finančních prostředků.[59] Důležité je také poskytnutí potřebného školení úředníků kompetentních k výkonu a užití nástrojů a úkolů spojených s e-governmentem.

---

[52] MATES, P. – SMEJKAL, V.: c.d., s. 16-17.
[53] Partnerem tohoto projektu je také portál Města a obce online, který funguje od r. 1996. Internetová adresa projektu – http://www.mool.cz.
[54] Webová adresa portálu: http://www.epusa.cz
[55] *Elektronický portál územních samospráv*. In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/elektronicky-portal-uzemnich-samosprav.aspx (5. července 2009)
[56] Na jejich základě jsou také krajům zasílány přístupové informace pro zřízení datových schránek (viz níže).
[57] Internetová adresa projektu: http://www.naseeva.cz/
[58] MATES, P. – SMEJKAL, V.: c.d., s. 17.
[59] Tamtéž, s. 21.

Vláda Vladimíra Špidly ve svém programovém prohlášení z roku 2002 věnovala problematice budování informačního systému veřejné správy poměrně velkou pozornost.[60] Vláda se zde přihlásila *„k myšlence podpory a rozvoje informační společnosti jako důležitého nástroje pro rozvoj vzdělanosti, ekonomiky a služeb veřejné správy."*[61] Patrný je tady odkaz na iniciativy eEurope[62] a také Státní informační politiku. Elektronizace veřejné správy zde byla chápána jako nástroj úspory financí a také podpora zvýšení komfortu vztahu mezi státem a občanem. Tento úkol měl podle představy vlády *„průřezový, nadresortní charakter."*[63]

V roce 2002 tak bylo pro naplňování tohoto úkolu vytvořeno Ministerstvo informatiky[64] coby *„ústřední orgán správy pro informační a komunikační technologie, pro telekomunikace a poštovní služby."*[65] Budování informační společnosti v ČR mělo vycházet z principů Státní informační politiky a dokumentů EU, zejména tzv. *eEurope*.[66] Následné vlády Stanislava Grosse i Jiřího Paroubka ve svých programových prohlášeních sledovaly trend efektivizace veřejné správy skrze aplikace a rozšiřování využitelnosti jednotného informačního systému veřejné správy.[67]

V dalších letech byly schvalovány další strategické dokumenty pro rozvoj e-governmentu v ČR, například *Státní informační a komunikační politika – e-Česko 2006* s výhledem do r. 2006.[68] Tato iniciativa navazuje

---

[60] *Programového prohlášení vlády (2002).* In: Vláda ČR, http://www.vlada.cz/assets/clenove-vlady/historie-minulych-vlad/prehled-vlad-cr/1993-2007-cr/vladimir-spidla/Programove-prohlaseni-vlady_1.pdf (12. srpna 2009), Oddíl 4. 6. – Informační společnost.

[61] Tamtéž.

[62] Viz níže kapitola 1.3. Působení EU na rozvoj e-governmentu v ČR.

[63] *Programového prohlášení vlády (2002).*

Vytvoření informačního systému veřejné správy bylo uvedeno také v programovém prohlášení předchozí Zemanovy vlády (1998-2002). (*Programové prohlášení vlády (srpen 1998)*. In: Vláda ČR, http://www.vlada.cz/assets/clenove-vlady/historie-minulych-vlad/prehled-vlad-cr/1993-2007-cr/milos-zeman/Programove-prohlaseni-vlady_1.pdf (28. října 2009)

[64] Viz výše.

[65] MATES, P. – SMEJKAL, V.: c.d., s. 28.

[66] *Programové prohlášení vlády (2002).* Iniciativy *eEurope* viz níže kapitola 1.3. Působení EU na rozvoj e-governmentu v ČR.

[67] *Programové prohlášení vlády (2004*). In: Vláda ČR, http://www.vlada.cz/assets/clenove-vlady/historie-minulych-vlad/prehled-vlad-cr/1993-2007-cr/stanislav-gross/Programove-prohlaseni-vlady-Ceske-republiky_1.pdf (28. října 2009); *Programové prohlášení vlády (2005).* In: Vláda ČR, http://www.vlada.cz/assets/clenove-vlady/historie-minulych-vlad/prehled-vlad-cr/1993-2007-cr/jiri-paroubek/Programove-prohlaseni-vlady-Jiriho-Paroubka_1.pdf (28. října 2009)

[68] *Státní informační a komunikační politika. e-Česko 2006.* In: Národní knihovna České republiky, http://knihovnam.nkp.cz/docs/SIKP_def.pdf (12. srpna 2009)

na Státní informační politiku z r. 1999 a je zaměřena na rozvoj tzv. informační společnosti v ČR, stejně jako náležité rozšíření tzv. vysokorychlostního Internetu.[69]

Kroky k rozvoji informačních systémů u nás rovněž vycházely z iniciativ EU (eEurope a i2010) a byly postaveny na čtyřech základních prioritách - *zajištění bezpečné a dostupné komunikační služby, informační vzdělanost, moderní veřejné služby on-line* a *dynamické prostředí pro elektronické podnikání.* Česká vláda se zaměřila na budování elektronických služeb veřejné správy, pokračování liberalizace sektoru elektronických komunikací, dále na rozvoj vysokorychlostního Internetu. Potřeba bylo také vytvořit odpovídající právní strukturu pro informační společnost. Dále byla podporována informační gramotnost a elektronické podnikání.[70]

Kolem r. 2005 však došlo opět ke zpomalení vývoje e-governmentu na celostátní úrovni. Ministerstvo informatiky se zaměřilo na elektronickou komunikaci a digitální vysílání. Budování informačního systému bylo upozaděno. V říjnu 2005 však přesto byla vládním usnesením č. 1340 přijata *Národní strategie informační bezpečnosti ČR*.[71]

Ministerstvo informatiky bylo zrušeno k 1. červnu 2007. Jeho kompetence v rámci informační politiky převzala tři ministerstva, Ministerstvo obchodu a průmyslu (problematika související s hospodářským rozvojem země a elektronického obchodování a podnikání),[72] Ministerstvo pro místní rozvoj (problematika spojená

[69] Státní informační a komunikační politika byla vládou schválena v březnu 2004 a usilovala o reakci na vývoj v oblasti informační společnosti tak také telekomunikace, kdy tyto dva pojmy se vzájemně prolínají. Je zde také reflektován vstup ČR do EU, a tedy také dokumenty Společenství týkající se informační společnosti (zejména *eEurope 2005: Informační společnost pro všechny*) stejně jako konkurenceschopnost ČR v této oblasti. Stěžejními jsou v dokumentu *eČesko 2006* tyto body: 1) budování moderních a bezpečných služeb veřejné správy dostupných on-line; 2) pokračování liberalizace sektoru elektronických komunikací s cílem zajistit efektivní konkurenční prostředí; 3) podpora rozšíření vysokorychlostního přístupu k internetu a zajištění jeho dostupnosti pro všechny skupiny obyvatelstva; 4) pokračování legislativního zakotvení informační společnosti; 5) podpora zvyšování počítačové gramotnosti obyvatel; 6) podpora rozvoje elektronického podnikání vytvářením vhodných technologicky neutrálních podmínek. (*Státní informační a komunikační politika. e-Česko 2006.)*

[70] MATES, P. – SMEJKAL, V.: c.d., s. 29.

[71] Problematika informační bezpečnosti viz níže kapitola 2.2. Informační bezpečnost.

[72] Zvyšování konkurenceschopnosti (zavádění inovací technologií, výrobků a služeb; podpora vědy a výzkumu a jejich vazeb na průmysl a podnikání; snižování surovinové a energetické náročnosti průmyslové výroby; podpora informačních technologií), podpora podnikání a podpora

s informační metodickou pomocí vyšším územním samosprávným celkům, městům, obcím a jejich sdružením)[73] a konečně Ministerstvo vnitra, které převzalo kompetence v oblasti e-governmentu.

Ministerstvo informatiky bylo zrušeno v souladu s programovým prohlášením Topolánkovy vlády. Jeho činnost měla v oblasti rozvoje e-governmentu převzít mimo jiné také Rada pro rozvoj informační společnosti. Jako důvody zrušení ministerstva se uvádí zejména jeho nedostatečná „síla“, kdy jeho kompetence byly tak specifické, že svou velikostí odpovídalo spíše odboru určitého ministerstva. Na druhou stranu projekt rozvoje e-governmentu, který se pro jeho činnost jevil jako stěžejní, potřeboval kooperaci a zapojení napříč ministerstvy.[74]

Rada pro rozvoj informační společnosti je odborným poradním orgánem vlády, která jej zřídila svým usnesením č. 293 z 28. března 2007. Má plnit koordinační roli místo zrušeného Ministerstva informatiky a poskytovat vládě vědomostní základnu zejména pro její rozhodování v koncepčních otázkách rozvoje informační společnosti. Jejím účelem je dosažení co největší meziresortní koordinace v této oblasti. Radu vlády pro rozvoj informační společnosti, která má 28 členů,[75] vede řídící výbor, v jehož čele stojí premiér a jehož dalšími členy jsou ministři vnitra, financí a průmyslu a obchodu. Další členové jsou jmenováni na základě svých expertních a odborných znalostí. V Radě jsou zastoupeni také nejdůležitější instituce, kterých se rozvoj informační společnosti a budování e-governmentu týká, tedy zástupci státní správy a samosprávy,

---

exportu. (*Informační politika MPO*. In: Ministerstvo průmyslu a obchodu ČR, http://www.mpo.cz/dokument495-strana1.html (1. 2. 2009))

[73] *Ministerstvo*. In: Ministerstvo pro místní rozvoj ČR, http://www.mmr.cz/ministerstvo (2. 2. 2009)

[74] Blíže k důvodům a okolnostem zániku Ministerstva informatiky viz např. *Jiří Peterka se zamýšlí nad zánikem Ministerstva informatiky*. In: Informační systémy veřejné správy, http://www.isvs.cz/e-government/jiri-peterka-se-zamysli-nad-zanikem-ministerstva-informatiky.html (12. srpna 2009); PETERKA, Jiří*: Ohlédnutí za zanikajícím Ministerstvem informatiky*. In: www.zive.cz, http://www.zive.cz/clanky/ohlednuti-za-zanikajicim-ministerstvem-informatiky/sc-3-a-135620/default.aspx (12. srpna 2009)

[75] Členy byli nebo jsou např. Jan Fischer (premiér úřednické vlády květen 2009-jaro 2010 a předseda Českého statistického úřadu), Michal Mejstřík (ředitel Institute of Economic Studies, Univerzita Karlova), Jaroslav Míl (předseda Svazu obchodu a průmyslu ČR), Edvard Kožušník (vedoucí projektu e-Stat) či Evžen Tošenovský (bývalý předseda Asociace krajů a hejtman Moravskoslezského kraje).

Parlamentu ČR, odborných a podnikatelských asociací i akademické sféry.[76]

V rámci Konference ISSS[77] v dubnu 2008 schválila Rada pro rozvoj informační společnosti *Strategii rozvoje služeb pro informační společnost*. Vizí tohoto dokumentu je zařadit ČR mezi pět nejlepších zemí EU v úrovni rozvoje e-governmentu.[78] Jeho hlavním cílem pak je „*změnit českou veřejnou správu takovým způsobem, aby byla občanovi plnohodnotným partnerem v moderní demokratické společnosti, využívající informační a komunikační technologie pro svůj rozvoj a posílení konkurenceschopnosti.*“[79]

Implementace Strategie má vycházet z realizace několika vzájemně provázaných projektů rozdělených do pěti oblastí: základní registry státní správy, univerzální kontaktní místo, zaručená a bezpečná elektronická komunikace mezi úřady navzájem a úřady a občanem, dále digitalizace datových fondů a konečně služby pro informační společnost (zdravotnictví, sociální služby, veřejná správa jako soudnictví apod., správa státního rozpočtu ad.).[80]

Strategie také stanovuje milníky v rozvoji informační společnosti v časovém horizontu. V roce 2009 mají být spuštěny datové schránky spolu s existencí sítě univerzálních kontaktních míst veřejné správy.[81] V roce 2010 mají být zprovozněny základní registry v rámci existujících kontaktních míst. Ve stejném roce má být také dokončen legislativní proces spojený s realizací cílů Strategie. V roce 2012 mají být funkční aplikace pro oblasti zdravotnictví, sociální péče, správního, soudního a

---

[76] *O Radě vlády pro informační společnost.* In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/egovernment-rada-vlady-pro-informacni-spolecnost-o-rade-vlady-pro-informacni-spolecnost.aspx (11. srpna 2009)

Blíže k Radě vlády pro informační společnost viz *Rada vlády pro informační společnost*. In: Ministerstvo vnitra ČR, http://www.mvcr.cz/egovernment-rada-vlady-pro-informacni-spolecnost.aspx (31. října 2009)

[77] Internet ve státní správě a samosprávě.

[78] *Strategie rozvoje služeb pro informační společnost.* In: www.businessinfo.cz, http://www.businessinfo.cz/cz/clanek/koncepce-a-politiky/informacni-spolecnost-strategiie-rozvoje/1000502/48353/ (11. srpna 2009), s. 4.

[79] *Rada vlády pro informační společnost schválila Strategii rozvoje služeb pro informační společnost.* In: www.businessinfo.cz, http://www.businessinfo.cz/cz/clanek/koncepce-a-politiky/informacni-spolecnost-strategiie-rozvoje/1000502/48353/ (11. srpna 2009)

[80] Tamtéž.; srov. *Strategie rozvoje služeb pro informační společnost.*, s. 5.

[81] V tomto bodě je možné zaznamenat úspěch strategie. Projekt datových schránek byl spuštěn k 1. červenci 2009. Kontaktní místa CzechPOINT fungují a dále se úspěšně rozvíjejí.

daňového řízení a má být funkční infrastruktura pro dlouhodobé ukládání a archivaci elektronických dokumentů. V roce 2015 se plánuje dokončení procesu elektronizace datové základny, včetně elektronizace geografických informací.[82]

Programové prohlášení vlády Mirka Topolánka z ledna 2007 se také vyslovuje pro rozvoj sítě kontaktních míst CzechPOINT. A zavazuje se k předložení zákona o elektronické komunikaci (eGovernment Act). Programové prohlášení vlády také pojednává o zvýšení výkonnosti českého soudnictví skrze elektronizaci, tedy zavádění projektu tzv. eJustice.[83] Konkrétně se zde hovoří o elektronickém platebním rozkazu pro zjednodušení platby jednoduchých a typizovaných peněžitých částek. Navrhované bylo také zavedení plně elektronizovaného insolvenčního rejstříku a tzv. elektronického spisu, který by měl zlepšit a zjednodušit komunikaci mezi jednotlivými justičními orgány. Má být také umožněna plně elektronická komunikace mezi účastníky soudního řízení.[84]

Období vlády 2007-2009 je charakteristické dosud největším pokrokem v elektronizaci veřejné správy.[85] Ivan Langer coby tehdejší ministr vnitra hovoří o jednom z největších posunů ve státní správě od dob rakouského mocnářství.[86] Projekt rozvoje e-governmentu se stal jakousi vlajkovou lodí jeho působení na ministerstvu. Pozitivnímu vývoji v této oblasti napomohl také fakt, že ČR má v současnosti jedinečnou možnost čerpat prostředky strukturálních fondů EU, které může využívat pro financování elektronizace své veřejné správy.[87]

Nicméně úspěchy v oblasti rozvoje e-governmentu Topolánkova vláda nebyla schopna dostatečně prezentovat a jejich vliv byl upozaděn jinými politickými tématy. Následná úřednická Fischerova vláda se ve svém programovém prohlášení z června 2009 zavázala pokračovat v projektech rozvoje e-governmentu, jak je specifikovala vláda předchozí.

---

[82] *Strategie rozvoje služeb pro informační společnost.*, s. 4.
[83] Viz níže kapitola 1.5.2. Elektronické doručování a podání.
[84] *Programové prohlášení vlády (2007).* In: Vláda ČR, http://www.vlada.cz/scripts/detail.php?id=20780 (11. srpna 2009)
[85] Zavedení CzechPOINTu, datové schránky a schválení zákona o centrálních registrech státní správy.
[86] *Vláda schválila zákon o e-governmentu.* In: Portál veřejné správy ČR, http://portal.gov.cz/wps/portal/_s.155/708/_ps.1272/M/_s.155/8414?docid=114412 (9. září 2009)
[87] *Naše cesta k e-governmentu je pro Unii inspirativní.* In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/nase-cesta-k-egovernmentu-je-pro-unii-inspirativni.aspx (9. září 2009)

Důraz je kladen zejména na úspěšné zavádění datových schránek a podporu projektu CzechPOINT. Fischerova vláda usiluje o zajištění financování současného rozvoje e-governmentu přednostně ze zdrojů poskytnutých EU.[88]

Je však třeba také uvést, že zejména samosprávy resp. krajské úřady se při aplikaci principů e-governmentu potýkaly a často potýkají s nejasným centrálním konceptem. Vládní iniciativy jako *Státní informační politika – cesta k informační společnosti* či *Státní informační a komunikační politika* měly spíše deklaratorní charakter. Byly koncipovány jako strategické plány. Chyběly však závazné právní normy, které by sjednocovaly postup zavádění nástrojů e-governmentu v ČR. Krajské úřady si tak vytvářely metodiku užití e-governmentu samy.[89] Postup informatizace krajů schválila vláda až v první polovině roku 2001,[90] kdy termín dokončení první etapy zabezpečení podmínek pro „rozběh" základní informatizace krajských úřadů byl stanoven již na 30. června 2001.[91] Můžeme zde tedy vidět určitý nedostatek času na přípravu.

Od června 2001 má Asociace krajů ČR členství v Radě vlády pro státní informační politiku. Je tak zajištěn podíl krajů na vývoji elektronizace a informatizace veřejné správy. V samotné Asociaci krajů ČR je vytvořena Pracovní skupina informatiků krajských úřadů. Jejím úkolem je řešit *„především integritu prostředí informačních systémů jednotlivých krajů"* a koordinovat *„vznik nových informačních systémů, které se mají provozovat na všech krajích."*[92] Vytvoření zákonných norem, tedy zákona

---

[88] *Programové prohlášení vlády. (2009)* In: Vláda ČR, http://www.vlada.cz/cz/jednani-vlady/programove-prohlaseni/programove-prohlaseni-vlady-cr-58369/ (11. srpna 2009), s. 4.

Financování zavádění prostředků a nástrojů nezbytných pro datové schránky viz např. PROTIVOVÁ, Ivana a kol.: *Analýza dopadu zákona č. 300/2008 Sb. a návrh zajištění implementace tohoto zákona pro Krajský úřad Plzeňského kraje.* In: Egovernment, http://egovernment.cz/schranky/anal%C3%BDza/anal%C3%BDza%20komplet.pdf (6. září 2009), s. 22-25.

[89] Aktivní v tomto ohledu byl např. Plzeňský kraj, který vytvářel metodiku a analýzy, jež přejímaly i další kraje.

[90] Usnesením vlády č. 216/2001 a 398/2001. K vládní koncepci informatizace krajů viz *Informatizace územních orgánů VS*. In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/informatizace-uzemnich-organu-vs.aspx (28. října 2009)

[91] Do konce roku pak měla být dokončena 2. etapa - integrace a systémový rozvoj základní informatizace krajských úřadů a do konce ledna 2003 pak také 3. etapa - postupné zabezpečení komplexní informatizace všech krajských úřadů. (*Koncepce informatizace Plzeňského kraje.* In: Portál Plzeňského kraje, www.kr-plzensky.cz, http://www.kr-plzensky.cz/article.asp?itm=10322 (5. září 2009), s. 4.)

[92] *Koncepce informatizace Plzeňského kraje.*, s. 7.

o e-governmentu (eGovernment Act),[93] se stalo stěžejní pro efektivnější zavádění prostředků e-governmentu na krajské úrovni. Také financování elektronizace veřejné správy je silně ovlivněno stále se vyvíjející legislativou i pravidly pro zavádění e-governmentu. Je totiž obtížné v prostředí významné finanční podpory elektronizace veřejné správy z evropských strukturálních i komunitárních fondů vytvořit patřičné projektové žádosti a reagovat na patřičné projektové výzvy.

Krajské úřady lze však považovat za určité průkopníky v rozvoji využívání nástrojů e-governmentu. Staly se také jakýmsi lídry v tomto procesu. Všechny krajské úřady disponují možností elektronického podání, komunikace i prezentace na Internetu. Souvisí to s obdobím, kdy byla upravena struktura územní samosprávy a kraje byly r. 2000 zřízeny coby vyšší územně správní celky. Od počátku fungování krajských úřadů existovala jakási centrální vize na české i evropské[94] úrovni o elektronizaci veřejné správy, byť konkrétní kroky k jejímu provedení v ČR nebyly ještě známé. Existovaly také potřebné technologické podmínky pro rozvoj elektronického spravování dat. Údaje krajských úřadů pak mohly být elektronicky vedeny od počátku, čímž se vyhnuly poměrně náročné konverzi dokumentů z fyzické do elektronické podoby.

Se zaváděním elektronických systémů souvisí také patřičný rozvoj elektronické komunikační technologie a schopnosti úředníků státní správy i občanů je využívat a používat.[95] Existuje zde též riziko vytváření informačních propastí mezi občany způsobené rozdílnými možnostmi přístupu k těmto komunikačním prostředkům. Proto je věnován poměrně velký prostor iniciativám orientujícím se na zpřístupnění tzv. veřejného Internetu, často zdarma.[96] S rozvojem elektronické komunikační technologie a podpory schopnosti úředníků i občanů užívat nástroje e-governmentu souvisí již výše zmíněna *Státní informační a komunikační politika e-Česko 2006*. S jejím cílem rozšíření vysokorychlostního

[93] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů viz níže kapitola 1.4. Vývoj právního ukotvení e-governmentu a vládních postojů k němu.
[94] EU již měla podíl na vytváření této vize skrze své projekty *eEurope*, v případě ČR v této době *eEurope+*. (Viz níže kapitola 1.3. Působení EU na rozvoj e-governmentu v ČR.)
[95] K rozvoji využívání a podpory hlubší implementace elektronických komunikačních prostředků (zejména internetu) viz MATES, P. – SMEJKAL, V.: c.d., s. 18-19.
[96] Viz výše např. Národní plán počítačové gramotnosti.

Internetu souvisí také program rozvoje online služeb i jejich dostupnosti pro co nejširší okruh osob *Národní politika pro vysokorychlostní internet – broadband strategie*.[97] Nelze také opominout vliv EU a jejích strategických dokumentů souvisejících s podporou informační společnosti.

1. 3. Působení EU na rozvoj e-governmentu v ČR

Významným aspektem podpory a rozvoje informační společnosti v rámci EU a jejích členských států je reakce Společenství na tzv. Lisabonskou strategii.[98] V době jejího vzniku byly ICT prostředky vnímány jako zásadní hnací síla ekonomického úspěchu a pokroku EU, a tudíž stěžejní pro úspěch celé Lisabonské strategie. Proto se EU zaměřila na rozvoj informační společnosti. Postupně byly přijaty dokumenty, *eEurope 2002* pro období let 2000-2002 a *eEurope 2005* pro období 2003-2005.[99] Pro

[97] Národní politika pro vysokorychlostní internet byla vládou schválena v lednu 2005. „Národní politika pro vysokorychlostní přístup klade důraz na podporu rozvoje online služeb pro vysokorychlostní přístup ze strany státu, a to v oblasti vzdělávání, kultury, zdravotnictví a veřejné správy a identifikuje hlavní příčiny pomalého rozvoje broadbandu v České republice: nedostatečná dostupnost vysokorychlostního připojení zejména mimo velká města, nepříznivý poměr mezi cenou a kupní silou obyvatel, nízká kvalita nabízených služeb, které nemají garantovaný charakter, a nedostatečná nabídka služeb a obsahu a z ní plynoucí nedostatečná motivace uživatelů pořídit si vysokorychlostní připojení k internetu.“ (*Národní politika pro vysokorychlostní internet - broadband strategie.* In: Archiv stránek bývalého Ministerstva informatiky, http://web.mvcr.cz/archiv2008/micr/scripts/detail.php_id_3157.html (12. srpna 2009))

[98] Tzv. Lisabonská strategie pro růst a zaměstnanost byla Evropskou radou přijata v březnu 2000 v hlavním městě Portugalska. EU si v jejím rámci položila za cíl stát se do roku 2010 nejdynamičtější a nejkonkurenceschopnější znalostní ekonomikou, která bude zároveň schopná trvale udržitelného růstu. Byla reakcí na postupující globalizaci. Spoluprací členských států má být dosaženo žádoucího růstu a zaměstnanosti, a to skrze investování do lidských zdrojů a modernizaci evropského sociálního modelu, podpory vědy, výzkumu a inovací (včetně podpory rozšiřování informační společnosti) a rozvoje dynamického obchodního prostředí v rámci posíleného a správně fungujícího jednotného trhu. (Viz *Presidency Conclusions. Lisbon European Council 23 and 24 March 2000.* In: Rada EU, http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/00100-r1.en0.htm (11. listopadu 2009), oddíl I.) V r. 2001 na evropském summitu v Göteborgu byl ke strategii připojen ještě aspekt tzv. zeleného hospodářství, tedy důraz na ekologicky šetrné technologie. (Viz *The „Lisbon Strategy“ in Short.* In: Výbor regionů, http://portal.cor.europa.eu/lisbon/Profiles/Pages/welcome.aspx (11. listopadu 2009)

[99] Akční plán *eEurope 2002* se týkal zejména umožnění alespoň nějakého přístupu k internetu. Akční plán *eEurope 2005* se pak zaměřil na všeobecné zpřístupnění vysokorychlostního internetu. (PETERKA, Jiří: *i2010 místo eEurope 2005.* In: Archiv článků a přednášek Jiřího Peterky, http://www.earchiv.cz/b05/b0607001.php3 (12. srpna 2009).

Více k iniciativám eEurope viz *Before i2010: Eeurope Initiative*. In: European Commission, Europe´s Information Society, http://ec.europa.eu/information_society/eeurope/2002/index_en.htm (12. srpna 2009); srov. GRAMLICH, L.: c. d., s. 81-86.

Iniciativám *eEurope* se budeme věnovat také v závěru této práce v kapitole 2.4. EU a její pojetí informační a kybernetické bezpečnosti.

nové kandidátské státy[100] byla vypracována ještě třetí strategie, *eEurope+*, zaměřená na co největší rozšíření alespoň nízkorychlostního Internetu.[101]

Na strategie *eEurope* navázala tzv. *i2010 (A European Information Society for growth and employment)*[102] zaměřená na oblast nejen ICT prostředků a informační společnosti, ale také problematiku médií. Je založena na třech hlavních prioritách, které jsou někdy označovány jako tři „i" – inovace, investice a integrace.[103] Jejím účelem je naplňovat cíle Lisabonské strategie skrze ICT prostředky. Společenství se prostřednictvím *i2010* snaží prosadit *jednotný evropský informační prostor* (rozvoj vnitřních trhů elektronických komunikací, médií a obsahu), *inovace a investice do vývoje* (kromě podpory výzkumu v oblasti ICT zde jde také o rozvoj elektronického podnikání a reorganizaci podnikatelských procesů skrze využití ICT) a *inkluzívní společnost, lepší veřejné služby* a *vyšší kvalita života pro každého*.[104] Iniciativa *i2010* usiluje o to, aby možnosti informační společnosti byly dostupné pro všechny.[105]

V rámci EU je problematika informační společnosti (information society) a e-governmentu spravována v působnosti komisaře pro informační společnost a média.[106] Tato společná oblast souvisí s vytvořením jednotného trhu i harmonizací pravidel v rámci Společenství. V prostředí, kdy je výrazný počet finančních transakcí i nákupů učiněn přes Internet, bylo třeba také vytvořit jednotné principy v rámci celé EU. Ta se tedy tradičně zaměřuje na tržní otázky spojené s elektronizací.[107]

---

[100] Tzv. východního rozšíření v letech 2004 a 2007.

[101] Po vstupu těchto zemí do EU se jich však už týkal Akční plán *eEurope 2005*. Na ten ČR zareagovala svými strategiemi, zejména *Státní informační a komunikační politikou* a *Národní politika pro vysokorychlostní internet* (viz výše).

[102] *i2010 - A European Information Society for growth and employment.* In: European Commission, Europe´s Information Society, http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm (12. srpna 2009)

[103] Blíže k evropské iniciativě *i2010* a jejich cílech viz MATES, P. – SMEJKAL, V.: c.d., s. 20; srov. PETERKA, J.: *i2010 místo eEurope 2005*.

[104] PETERKA, J.: *i2010 místo eEurope 2005.*

[105] Viz *Social inclusion, better public services and quality of life.* In: European Commission, Europe´s Information Society, http://ec.europa.eu/information_society/eeurope/i2010/inclusion/index_en.htm (12. září 2009)

[106] V současnosti (Evropská komise s mandátem 2004-2009) je to komisařka Viviane Reding. Internetové stránky s informacemi o ní: http://ec.europa.eu/commission_barroso/reding/index_en.htm (12. září 2009)

[107] E-commerce, e-banking, ale také působení na srovnání roamingových cen volání s těmi místními.

Nicméně problematika rozvoje elektronické veřejné správy je sledované rovněž, a to zejména z hlediska jejího zefektivnění a zlevnění.[108] Důraz je kladen také na větší demokratizaci a personalizaci veřejné správy. Občané totiž budou moci pohodlněji z prostředí svých domovů i adresněji skrze obrácení se na konkrétní úřad komunikovat se státní správou.[109]

V případě, že je přístup k vyspělým ICTs i informacím některým skupinám či obyvatelům nedostatečný, může také docházet k jakési manipulaci ze strany osob disponujícími těmito prostředky. EU se tedy zaměřuje na zvyšování počítačové gramotnosti.[110] Orgány EU dále sledují rizika spojená s případným zneužitím informací o občanech, které jsou zprostředkovávány elektronicky.[111] Komisařka V. Reding se zaměřila ve svém nedávném návrhu projektu *Digital Europe (Digitální Evropa)*, který by měl navázat na končící *i2010*, mimo jiné na rozšíření vysokorychlostního Internetu pro všechny občany EU. V její vizi představuje Digitální Evropa též prostředí zvýšených možností investic a obchodování.[112]

V listopadu 2009 se ve švédském Malmö konala již pátá konference ministrů zodpovědných za problematiku e-governmentu v členských i kandidátských státech EU a v zemích EFTA.[113] Výsledkem

---

[108] *eGovernment: Commission calls for Ambitious Objectives in EU for 2010*. In: European Commission, Europe´s Information Society, http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2601 (12. září 2009)

[109] *Putting Citizens First*.

[110] Např. v rámci projektu eLearning (Blíže viz http://ec.europa.eu/education/archive/elearning/index_en.html; http://www.elearningeuropa.info/main/index.php?lng=cs&page=search_results&qry=Digital+literacy&service=1) či v rámci Evropského sociálního fondu (*European Social Fund.* In: European Commission, http://ec.europa.eu/employment_social/esf/index_en.htm (12. září 2009)).

K problematice počítačové gramotnosti viz např. HINKELBEIN, Oliver: *'Digital literacy': the central cultural technique of the 21st century.* In: http://ec.europe.eu, http://ec.europa.eu/education/archive/elearning/doc/workshops/digital_literacy/position_papers/hinkelbein_oliver.pdf (12. září 2009)

[111] Viz níže kapitola 2.4. EU a její pojetí informační a kybernetické bezpečnosti.

[112] *Digital Europe – Europe's Fast Track to Economic Recovery.* In: Europa Press Releases, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/09/336&format=HTML&aged=0&language=EN&guiLanguage=en (12. září 2009)

V srpnu 2009 Komise spustila veřejnou debatu o přístupech EU k Digitální Evropě. Debata byla ukončena 12. října 2009. Její výsledky a vyhodnocení však v době dokončení této práce (konec listopadu 2009) nebyly známy.

[113] První z konferencí věnovaných problematice e-governmentu se konala v listopadu 2001 v průběhu belgického předsednictví, kdy se jednalo mimo jiné o příležitost výměny zkušeností mezi členskými státy EU. Další ministerská konference zaměřené na rozvoj a posílení e-governmentu se konala v červenci 2003 v italském Como, kdy byl e-government označen jako

tohoto setkání je *Ministerská deklarace o e-governmentu*. Ten je v ní popsán jako nadnárodní fenomén, který usnadní rozvoj *„celoevropských politických cílů napříč různými oblastmi, od justice k sociální politice, k obchodování ad.“*[114] Deklarace představuje vizi vývoje e-governmentu v letech 2011-2015. Jedná se tedy také o reakci Společenství v oblasti elektronizace veřejné správy na vypršení iniciativy *i2010*.

Dokument zdůrazňuje inkluzivitu a aktivnější zapojení co největšího počtu aktérů do úspěšného rozvoje e-governmentu. Ten má být zaměřený na občana a na usnadnění využívání jeho služeb (citizen-centric, resp. user-centric). Předpokládá se také zapojení tzv. třetí strany, tedy zintenzivnění vzájemné spolupráce mezi státní správou, soukromými firmami, občanskou společností i samotnými občany. Opět je akcentován význam jednotného evropského trhu, kdy využití a nástroje e-governmentu mají odpovídat jeho principům (zejména přeshraniční služby, mobilita občanů[115] ad.).[116]

EU z podstaty svého existence a základních idejí podporuje spolupráci svých členů a vzájemné sdílení jejich zkušeností nejen v oblasti zavádění a rozvoje e-governmentu. Patrný je tento trend v závěrech deklarace z Malmö, ale jak si ukážeme později, také v dokumentech a praxi vztahujících se k zajištění kybernetické bezpečnosti ve Společenství. Informační společnost a s ní spojené využití ICTs jako základ

---

jeden z aspektů posílení evropské konkurenceschopnosti (cíl inovace dle Lisabonské strategie) a demokracie (princip inkluze). Následně britské předsednictví uspořádalo třetí konferenci o e-governmentu v listopadu 2005 v Manchesteru, kde byl diskutován vývoj e-governmentu v členských státech v období do r. 2010 v souvislosti s aplikací a principů iniciativy i2010. A konečně čtvrtá konference se konala v září 2007 v Lisabonu. Zdůrazňována byla zejména posílená mezinárodní spolupráce, inkluzivita a transparentnost služeb veřejné správy a e-governmentu (Viz *5 telecom priorities for Belgian Presidency*. In: Euractive.com, http://www.euractiv.com/en/general/5-telecom-priorities-belgian-eu-presidency/article-116150# (21. Listopadu 2009); *EU: Como Conference: Interoperability is key, says European Commissioner*. In: ePractice.eu, http://www.epractice.eu/en/news/283954 (22. listopadu 2009); Ministerial eGovernment Conference 2005, 24-25 November in Manchester, UK. In: European Commission, Europe´s Information Society, http://ec.europa.eu/information_society/activities/egovernment/conferences/past/2005/index_en.htm (22. listopadu 2009); *Ministerial Declaration*. In: 4th Ministerial eGovernment Conference, http://www.egov2007.gov.pt/images/stories/ministerial_declaration_final_version_180907.pdf (22. listopadu 2009).

[114] *Ministerial Declaration on eGovernment*. In: Swedish Presidency of the EU, http://www.se2009.eu/polopoly_fs/1.24306!menu/standard/file/Ministerial%20Declaration%20on%20eGovernment.pdf (21. listopadu 2009), s. 1

[115] Např. zapojení občanů států a usnadnění jejich komunikace s úřady, pokud studují či pracují v jiných členských státech Unie.

[116] *Ministerial Declaration on eGovernment.*, s. 2-3.

ekonomického i společenského rozvoje EU je z tohoto důvodu rovněž zaštiťováno ze stran centrálních orgánů Společenství, zejména Komise. V tomto spatřujeme jakousi morální podporu EU pro rozvoj elektronizace a efektivizace veřejné správy, která je také spojená s demokratizací a možností většího zapojení občanů do veřejného života (viz princip inkluzivní společnosti z iniciativy i2010 či myšlenka customer-centric zaměřené veřejné správy apod.).

Nezanedbatelná či spíše zásadní je také finanční podpora Společenství pro rozvoj elektronizace veřejné správy ve svých členských zemích. Současné unijní rozpočtové období 2007-2013 dosud nápadně koreluje s největšími pokroky v zavádění nástrojů e-governmentu v ČR.

V rozpočtovém období EU 2007-2013 spadá financování projektů elektronizace veřejné správy do rámce Integrovaného operačního programu, konkrétně podpora zavádění ICT prostředků do veřejné správy a modernizace veřejné správy.[117] Téma modernizace veřejné správy a veřejných služeb pak spadá do působnosti Operačního programu lidské zdroje a zaměstnanost. Konkrétně jeho 4. prioritní osa Veřejná správa a veřejné služby je mimo jiné zaměřená na zefektivnění veřejné správy jak na centrální, tak také regionální úrovni a její přiblížení občanovi, k čemuž e-government svým charakterem významně přispívá.[118] Některé aspekty rozvoje e-governmentu jsou sponzorovány také z tzv. komunitárních fondů

[117] Prioritní osy 1 a, 1b (modernizace veřejné správy) a 2 (zavádění ICT v územní veřejné správě). Pro tyto dvě osy bylo vyčleněno 505,3 milionů euro, což představuje 31,9 % částky Integrovaného operačního programu. (*Prioritní osy IOP*. In: Centrum pro regionální rozvoj ČR, http://www.crr.cz/index.php?did=828 (16. října 2009). Blíže viz také *Integrovaný operační program pro období 2007-2013*. In: Ministerstvo vnitra ČR, Strukturální fondy, Integrovaný operační program, http://www.mvcr.cz/clanek/strukturalni-fondy-integrovany-operacni-program.aspx (16. října 2009), s. 99-117.

Seznam předpokládaných projektů v rámci rozvoje e-governmentu viz *Seznam záměrů strategických projektů pro čerpání prostředků ze Strukturálních fondů EU v rámci Smart Administration.* In: Ministerstvo vnitra ČR, Smart Administration, http://www.mvcr.cz/clanek/odbor-reformy-a-regulace-kvality-verejne-spravy-smart-administration.aspx (16. října 2009)

[118] Blíže viz *Operační program lidské zdroje a zaměstnanost*. In: Ministerstvo vnitra ČR, Strukturální fondy, http://www.mvcr.cz/clanek/operacni-program-lidske-zdroje-a-zamestnanost-500016.aspx (16. října 2009); *Operační program lidské zdroje a zaměstnanost 2007-2013*. In: Ministerstvo vnitra ČR, Strukturální fondy, http://www.mvcr.cz/clanek/operacni-program-lidske-zdroje-a-zamestnanost-500016.aspx (16. října 2009), s. 130-138.

Operační program lidské zdroje vyčlenil pro oblast Veřejné správy a veřejných služeb částku 195,1 milionů euro, což představuje asi 10,6 % finančních prostředků EU v rámci tohoto programu. (*Operační program lidské zdroje a zaměstnanost 2007-2013.*, s. 159.)

Společenství, v rámci 3. projektové výzvy označené CIP ICT PSP.[119] Komunitární program na rozvoj ICTs je zaměřen na plnění cílů Lisabonské strategie resp. iniciativy *i2010*.[120]

Zhodnocení čerpání evropských finančních zdrojů bude možné až po ukončení výzev i konkrétních projektů. Například v srpnu 2009 však byla většina schválených projektů alokovaných v 2. prioritní ose Integrovaného operačního programu orientovaná na zavádění a rozvoj sítě kontaktních míst Czech POINT.[121] Nicméně již teď můžeme říci, že finance využité v projektech spojených s elektronizací veřejné správy posunuly celkový vývoj e-governmentu výrazně dopředu.

1. 4. Vývoj právního ukotvení e-governmentu a vládních postojů k němu

Problematiku zavádění informačních systémů a s tím spojené zpracovávání osobních údajů určitým způsobem právně ukotvit. Totalitní režim před rokem 1990 právní úpravy nakládání s osobními daty nepovažoval za důležité, zejména z důvodů udržování občanů v nevědomosti o svých praktikách.[122] Nastolení demokratického režimu znamenalo změnu vnímání v nakládání s informačními systémy. Jejich vedení je třeba považovat za výkon státní či veřejné moci, kterou je nutno provádět jen v mezích a způsoby stanovenými zákonem.[123] Každý informační systém státní správy tak musí být podložen nějakou zákonnou úpravou, která vymezuje jeho vznik, způsob zpracovávání dat v něm obsažených a dále

[119] CIP ICT je rámcový program Konkurenceschopnost a inovace v oblasti informačních a komunikačních technologií. V jeho rámci je vyčleněno dalších 780 milionů euro. Výzva byla otevřena v lednu 2009 a do konce roku se očekává její vyhodnocení a přidělení dotací konkrétním projektům. (Viz KUSÁK, Martin*: CIP - Program pro podporu ICT*. In: euroskop.cz, http://euroskop.cz/gallery/39/11821-cip_ict_psp.pdf (16. října 2009)

Blíže viz *Komunitární programy v oblasti informační společnosti*. In: Ministerstvo vnitra ČR, Komunitární programy, http://www.mvcr.cz/clanek/komunitarni-programy-v-oblasti-informacni-spolecnosti.aspx (16. října 2009)

[120] Blíže ke komunitárním fondům viz *Komunitární programy*. In: euractive.cz, http://www.euractiv.cz/komunitarni-programy (16. října 2009)

[121] *Měsíční monitorovací zpráva o průběhu čerpání strukturálních fondů, fondu soudržnosti a národních zdrojů v programovém období 2007-2013. Srpen 2009.* In: Fondy Evropské unie, http://www.strukturalni-fondy.cz/Narodni-organ-pro-koordinaci/Dokumenty/Zpravy-2/MMZ/FileList/2009/MMZ---srpen-2009 (16. října 2009), s. 55.

[122] MATES, P. – SMEJKAL, V.: c. d., s. 24.

[123] Viz čl. 2 odst. 3 Ústavy (*Ústava České republiky*. In: www.hrad.cz, http://www.hrad.cz/cz/ustava_cr/index.shtml (12. září 2009)

také stanovuje kompetence orgánu, kterému je fungování daného systému svěřeno.[124]

E-government je v ČR založen na několika zákonných a podzákonných úpravách. Nicméně jejich počet i proměnlivost často znesnadňuje orientaci v nich a schopnost veřejnosti správně přijmout technické i politické možnosti e-governmentu.[125]

V r. 2000 byl vytvořen Úřad pro veřejné informační systémy[126], který měl zajišťovat realizaci Státní informační politiky. ISVS jsou spravovány na základě zákona č. 365/2000 Sb., o informačních systémech veřejné správy.[127] Zákon stanovuje práva a povinnosti správců ISVS a dalších subjektů, jež souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy. V návaznosti na to upravuje působnost Ministerstva vnitra jako ústředního správního úřadu pro tvorbu a rozvoj informačních systémů veřejné správy.[128] Ministerstvo vnitra na základě projektového přístupu omezuje vznik duplicit při provozování ISVS a zabezpečuje reálné požadavky na čerpání financí z veřejných rozpočtů v oblasti ICTs. Připravuje také technologické podmínky pro efektivnější výkon veřejné moci.[129] Zákon o ISVS rovněž zřizuje již výše uvedený Úřad pro ISVS.

Až tento zákon č. 365/2000 Sb. přinesl jasné právní uchopení elektronické správy dat veřejné moci a dal jasnější základ dalšímu rozvoji e-governmentu. Před r. 2000 mělo úsilí státních orgánů o pokrok v elektronizaci spíše deklaratorní a iniciativní charakter. Nebylo ale podloženo zákonem, tedy nebylo závazné

ISVS jsou tvořeny registry veřejné správy. V současnosti je třeba zaměřit se zejména na odstranění duplicit a neaktuálních informací v nich, které plynou z měnícího se a vyvíjejícího se životního stylu občanů.

[124] MATES, P. – SMEJKAL, V.: c. d., s. 24.
[125] Právě usnadnění chápání konceptu e-governmentu se Lidínský a kol. snaží ve své knize. (LIDÍNSKÝ, V. a kol: c. d., s. 8.
[126] Nahradil Úřad pro státní informační systém. (Viz kapitola 1.2. Rozvoj e-governmentu v ČR)
[127] Zákon o ISVS byl několikrát novelizován, nejpozději zákony č. 190/2009 Sb., 223/2009 Sb. a 227/2009 Sb. (Viz *Zákon č. 365/2000 Sb., o informačních systémech veřejné správy.* In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/legislativa-zakon-c-365-2000-sb-o-informacnich-systemech-verejne-spravy.aspx (9. září 2009)
[128] Zákon byl naposledy novelizován zákonem č. 130/2008 Sb. z dubna 2008. (*Legislativa.* In: MV, http://www.mvcr.cz/clanek/legislativa-zakon-c-365-2000-sb-o-informacnich-systemech-verejne-spravy.aspx (1. 2. 2009))
[129] *Informační systémy veřejné správy.*

Duplicity jsou také často způsobeny nedostatečnou komunikací mezi orgány státní správy. V tomto smyslu byla dne 13. února 2009 Sněmovnou Parlamentu ČR schválena novela zákona č. 365/2000 Sb., o ISVS a také byl přijat návrh zákona o základních registrech.[130] Dle bývalého ministra vnitra I. Langera se jedná o třetí stěžejní krok k rozvoji e-governmentu v ČR.[131] Jedná se o završující krok zavádění projektu e-governmentu v ČR.[132] Základní registry by měly fungovat od 1. července 2010.

V registrech budou uchovávány pouze aktuální údaje a ty budou považovány za správné. Občané tak nebudou muset stále dokola zapisovat své základní informace na různých úřadech. *„Zákon stanoví i propojení základních registrů, které bude realizováno prostřednictvím informačního systému základních registrů, jehož správcem bude nově vytvořený úřad Správa základních registrů.“*[133] Tento úřad bude fungovat v rámci Ministerstva vnitra. Bude také zodpovědný za údaje vedené v základních registrech. Ty představují mozek tzv. Egona.[134] Lze je chápat jako výrazný posun k efektivnější správě odstraňující zejména problém duplikování úřední činnosti. Z hlediska praktického využití občany se jedná o čtvrtý nejhmatatelnější posun v rámci využití prostředků e-governmentu.[135]

Navrhovány jsou čtyři základní registry veškerých potřebných údajů o občanech. Nejprve to bude *Registr obyvatel*, který povede referenční údaje o občanech ČR a cizincích s dlouhodobým pobytem na území ČR a jeho správcem bude Ministerstvo vnitra. Druhým je *Registr osob*, jenž povede referenční údaje o právnických osobách, podnikajících fyzických osobách a orgánech veřejné moci a jehož správcem bude Český statistický úřad. Třetím bude *Registr územní identifikace, adres a nemovitostí*, kde budou vedeny referenční údaje o územních prvcích

[130] Dne 26. března 2009 pak byl tento návrh schválen také Senátem ČR. Text zákona je dostupný na webových stránkách Senátu PČR: http://www.senat.cz/xqw/xervlet/pssenat/historie?action=detail&value=2423.
[131] Prvními dvěma jsou CzechPOINT a datové schránky.
[132] *Zákon o základních registrech prošel třetím čtením.* In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/zakon-o-zakladnich-registrech-prosel-tretim-ctenim.aspx (4. srpna 2009)
[133] *Zákon o základních registrech prošel třetím čtením.*
[134] Viz výše kapitola 1.1. Vymezení pojmu.
[135] Jako první praktické využití e-governmentu chápeme elektronický podpis, dále zavedení CzechPOINTu, třetí pak datové schránky a konečně registry veřejné správy.

(například území státu, území samosprávného nebo správního kraje, území okresu, území obce, katastrální území, stavební objekt, adresní místo, pozemek v podobě parcely) a referenční údaje o územně evidenčních jednotkách (například části obce, ulice nebo jiná veřejná prostranství), a jehož správcem bude Český úřad zeměměřický a katastrální. A konečně čtvrtým bude *Registr práv a povinností*, který upravuje vedení referenčních údajů o agendách orgánů veřejné moci a dále reguluje vedení referenčních údajů o některých právech a povinnostech fyzických a právnických osob a vedení oprávnění přístupu k datům vedeným v základních registrech nebo v agendových informačních systémech. Správcem Registru práv a povinností bude Ministerstvo vnitra.[136] Zákon o základních registrech také klasifikuje jimi vedené údaje na referenční, referované a ostatní.[137]

Dne 19. srpna 2008 byl ve sbírce zákonů zveřejněn *Zákon o elektronických úkonech a autorizované konverzi dokumentů č. 300/2008 Sb.,*[138] neboli tzv. eGovernment Act (srdce eGona). Zákon upravuje *„autorizovanou konverzi písemností, legalizaci elektronického podpisu, jednoznačné určení osoby při elektronické komunikaci a poskytnutí služeb pro komunikaci s orgány veřejné moci.“*[139] Hlavním cílem zákona č. 300/2008 Sb. je tedy nastavení jasných podmínek zavádění principů e-governmentu v ČR. Konkrétně se jedná o zrovnoprávnění listinné a elektronické verze dokumentu.[140] Zlepšení komunikace mezi občany a úřady státní správy je v zákoně podpořeno zavedením institutu datových schránek.

---

[136] *Zákon o základních registrech schválil Senát Parlamentu ČR*. In: Portál veřejné správy ČR, http://portal.gov.cz/wps/portal/_s.155/7226/_s.155/10202?docid=120601 (4. srpna 2009)
Srov. také LIDÍNSKÝ, V. a kol.: c. d., s. 77-78; *Zákon o základních registrech prošel třetím čtením.*

[137] Blíže k problematice typů údajů vedených v centrálních registrech viz LIDÍNSKÝ, V. a kol.: c. d., s. 77.

[138] *Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.* In: Sbírka zákonů, Sagit, http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb08300&cd=76&typ=r (6. září 2009)

[139] *Egovernment Act – zákon o egovernmentu.* In: Egovernment, http://egovernment.cz/best/PDF%2007/EgovAct.pdf (10.sprpna 2009)

[140] Zrovnoprávnění listinné a elektronické má však určité limity. Tento aspekt upravuje § 18, ods. 2 zákona č. 300/2008. (*Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů,* § 18, ods. 2.)

Zákon o e-governmentu je také vnímán jako nepostradatelný pro rozvoj tzv. smart administration,[141] která umožňuje zefektivnění, zprůhlednění, zrychlení, zkvalitnění a také zlevnění výkonu veřejné správy v ČR.[142] Svým stanovením zákonných podmínek se stal klíčovým pro jednodušší a jasnější aplikace e-governmentu v ČR.

1. 5. Praktické projevy e-governmentu v ČR

Jak jsme si ukázali úsilí o zavedení a rozvinutí e-governmentu je možné v ČR sledovat v zásadě po celá 90. léta minulého století až do současnosti. Bylo třeba však překonat některé překážky a komplikace. Nejprve se jednalo zejména o problémy technického rázu (neexistence vyhovujícího připojení k Internetu a nedostatečná šířka pásma), ale také právního (absence pozitivní právní úpravy, nezbytná pro oblast orgánů veřejné moci). Významnou roli v tomto ohledu sehrála také určitá neschopnost jednotlivých resortů domluvit se na jednotné koncepci a postupu v rámci zavádění nástrojů e-governmentu, což nevyřešilo ani mocensky slabé Ministerstvo informatiky ČR.[143] V této kapitole si přiblížíme konečně úspěšné a praktické projevy e-governmentu v ČR.

1. 5. 1. Elektronický podpis

Elektronický podpis byl prvním z významných a pro veřejnost nejviditelnějších kroků k praktickému využití e-governmentu v ČR. Právním základem pro elektronický podpis je zákon č. 227/2000 Sb., o elektronickém podpisu.[144] Byl poměrně rychlou reakcí na směrnici EU č.

[141] Současná strategie aplikace smart administration v ČR byla schválena v červenci 2007 (*Efektivní veřejná správa a přátelské veřejné služby. Strategie realizace Smart Administration v období 2007-2015.* In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/odbor-reformy-a-regulace-kvality-verejne-spravy-smart-administration.aspx (12. září 2009)

[142] *Egovernment Act – zákon o egovernmentu.*

[143] SMEJKAL, Vladimír: *Datové schránky nastupují*. In: ihned.cz, 22. července 2009, http://pravniradce.ihned.cz/c4-10078260-37865170-F00000_d-datove-schranky-nastupuji (12. října 2009)

[144] *Zákon č. 227/2000 Sb., o elektronickém podpisu. In*: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx (8. září 2009).

1999/93/EC[145] o zásadách Společenství pro elektronické podpisy. [146] Důraz autoři zákona kladli na jeho obecnost a co nejmenší technologickou závislost, aby nemusel být měněn s každým posunem v oblasti ICTs.[147]

V souvislosti s tím, že všechny dokumenty lze v současnosti převést do jejich elektronické podoby, lze podobně konvertovat také podpis jedince. Elektronický podpis pak umožňuje takto signovat dokumenty, u kterých by to v jejich fyzické podobě těžko šlo (např. fotografii, obsahy různých datových médií apod.).[148] Zákon o elektronickém podpisu rozlišuje elektronický podpis obyčejný a elektronický podpis zaručený. Obyčejný elektronický podpis má podobu *„údajů v elektronické podobě…, které umožňují ověření totožnosti podepsané osoby…*“[149] Může se tedy jednat o naskenovaný podpis sloužící např. jako podpisový vzor v bankách. Srovnání a posouzení pravosti podpisu je tedy založené na vizuálním zkoumání a je subjektivní.

Zaručený elektronický podpis[150] je založen na principu tzv. *podpisu digitálního*.[151] Ten je tvořen kombinací řady číslic.[152] Ověření digitálního podpisu probíhá na základě tzv. *veřejného klíče*, neboli veřejným ověřovacím číslem. Ten musí být veřejně k dispozici podobně jako podpisový vzor tradičního podpisu.[153]

---

[145] ČR byla třetím státem, kde vstoupil zákon o elektronickém podpisu v platnost.
Text Směrnice 1999/93/EC je dostupný na http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:NOT.

[146] Státy EU spěly k přijímání jednotných postupů v zavádění pravidel použití elektronického podpisu, a to zejména v návaznosti na elektronický obchod na společném trhu. V říjnu 1997 Evropský parlament obdržel studii *O zajištění bezpečnosti a důvěryhodnosti elektronické komunikace – směřování k evropským zásadám pro digitální podpisy a šifrování*. Z ní pak vzešla Směrnice 1999/93/EC. (LIDÍNSKÝ, V. a kol.: c. d., s. 39.)

[147] MATES, P. – SMEJKAL, V.: c. d., s. 145.

[148] Tamtéž, s. 123.

[149] Tamtéž, s. 126.

[150] Zaručený elektronický podpis je elektronický podpis, který splňuje čtyři základní požadavky. Zaprvé je jednoznačně spojen s podepisující osobou. Zadruhé umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě. Zatřetí byl vytvořen a k datové zprávě připojen za pomocí prostředků, které má podepisující osoba pod svou výhradní kontrolou. A konečně je tento elektronický podpis k datové zprávě připojen tak, že je možno zjistit jakoukoli následnou změnu dat. Zaručený elektronický podpis splňuje při správné implementaci nejvyšší bezpečnostní pravidla, což souvisí s jeho praktickým využitím, zejména při úřední komunikaci občana a orgánů veřejné správy či v elektronickém bankovnictví. (LIDÍNSKÝ, V. a kol.: c. d., s. 40.)

[151] Ten je tvořen kombinací řady číslic. Jedná se tedy o číslo, jehož výpočet je třeba provést pomocí počítače. Ověřit a vytvořit toto číslo dokáže počítač nebo čip.

[152] Blíže k vytváření a šifrování algoritmů digitálního podpisu viz MATES, P. – SMEJKAL, V.: c. d., s. 128-129.

[153] Tamtéž, s. 134.

Podepisující pak vytváří svůj digitální podpis na základě vlastního a jedinečného šifrovacího *privátního klíče*. Výhodou elektronického, resp. digitálního podpisu je jeho jednoznačná příslušnost k digitálnímu dokumentu, který nelze změnit beze změny tohoto podpisu.[154]

Elektronický podpis představuje jeden z nástrojů bezpečné elektronické komunikace. Základními bezpečnostními principy systému elektronického podpisu jsou *důvěrnost informací* (přístup k důvěrným informacím mají pouze určené subjekty), *integrita* (informace musejí být zabezpečeny proti modifikaci) a *neodmítnutelnost odpovědi* (je třeba dokázat přesvědčit třetí stranu o přímé odpovědnosti subjektu za autorství, vlastnictví, odeslání i přijetí zprávy).[155]

Elektronický podpis má dvě úrovně, které zajišťují a zvyšují bezpečnost podepisovacího procesu. Je to zaručený elektronický podpis a tzv. kvalifikovaný certifikát.[156] Záruku o propojení konkrétní osoby, jejích osobních dat a jejího osobního digitálního podpisu poskytují tzv. certifikáty.[157] Certifikát lze chápat jako obdobu identifikační karty či průkazu totožnosti v elektronickém světě.[158]

Tyto certifikáty vydává a stvrzuje tzv. certifikační autorita.[159] Jedná se o nezávislou třetí stranu, která zaručuje, že veřejný klíč skutečně náleží uvedené osobě.[160] Certifikační autorita zajišťuje kvalitu a důvěryhodnost vydaných certifikátů, což je podpořeno i legislativními a technickými pravidly provozu instituce této certifikační autority.

Ta musí splňovat podmínky stanovené zákonem o elektronickém podpisu i upřesnění dle vyhlášky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb. Certifikační autorita

---

[154] Blíže k problematice jedinečnosti digitálního podpisu a principu této jedinečnosti viz MATES, P. – SMEJKAL, V.: c. d., s. 132.
[155] LIDÍNSKÝ, V. a kol.: c. d., s. 38.
[156] Certifikát je definován jako datová zpráva, kterou vydal poskytovatel certifikačních služeb a která spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost. Kvalifikovaný certifikát je pak certifikát, který má náležitosti stanové zákonem o elektronickém podpisu a byl vydán certifikační autoritou splňující předpisy tohoto zákona. (*Zákon č. 227/2000 Sb., o elektronickém podpisu,* §12; MATES, P. – SMEJKAL, V.: c. d., s. 145-146.)
[157] Ty obsahují mimo svoji platnost, svého čísla ad., zejména také údaje identifikující danou osobu a její ověřovací veřejný klíč
[158] LIDÍNSKÝ, V. a kol.: c. d., s. 39.
Postup vytvoření certifikátu viz např. Tamtéž, s. 41-42.
[159] Nebo také poskytovatel elektronického klíče.
[160] To dělá zpravidla fyzickou kontrolou, tedy očním překontrolováním. Jedná se o tzv. certifikační roli. Certifikační autorita poskytuje také validační službu, tedy potvrzuje platnost certifikátu.

pak získává od Ministerstva vnitra akreditaci k poskytování certifikačních služeb.[161] Kvalifikované certifikáty, které tato akreditovaná certifikační autorita vydává, jsou pak považovány za nejkvalitnější a nejkvalifikovanější ve vztahu k elektronickému podpisu a standardem v komunikaci se státní správou.[162] Certifikační autorita je tedy pověřená jakousi správou klíčů potřebných k bezpečnému elektronickému přenosu dat.[163]

Důvěryhodnost poskytovatele certifikačních služeb je klíčová pro využití elektronické výměny dokumentů. Tato důvěra je v digitálním prostředí budována skrze infrastruktury veřejných klíčů (Public Key Infractructure, PKI). Tuto infrastrukturu lze definovat několika způsoby. V zásadě se jedná o *„souhrn hardwaru, softwaru, lidí, metod a procesů potřebných pro použití kryptografie veřejných klíčů pro určitou množinu osob.“*[164] Je to soubor serverů, certifikačních autorit, registračních autorit, adresářů a aplikací, které umožňují elektronicky modelovat důvěru. PKI sama o sobě fyzicky neexistuje. Vždy se jedná o soubor provázaných řešení. Zpravidla se skládá z poskytovatele certifikačních služeb, centrální databáze PKI, kde jsou k dispozici seznamy vydaných certifikátů a certifikátů s ukončenou platností.[165]

PKI tedy uživatelům umožňuje v prostředí v zásadě nebezpečného Internetu i jiných veřejných sítí si bezpečně vyměňovat data i finance prostřednictvím veřejného i tajného klíče.[166] PKI je základním komponentem celkové bezpečnostní strategie a musí pracovat společně s ostatními bezpečnostními mechanismy. Představuje stále se vyvíjející

---

[161] *Vyhlášky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb.* In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/vyhlaska-c-378-2006-sb-o-postupech-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb.aspx (4. srpna 2009)

V současnosti existují v ČR tři akreditované certifikační agentury: První certifikační autorita, a.s. (http://www.ica.cz/), Česká pošta, s. p. (https://qca.postsignum.cz/) a eIdentity, a. s. (http://www.eidentity.cz/) (*Přehled udělených akreditací.* In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx (4. srpna 2009)

Blíže k otázce certifikačních autorit viz ŠTĚDROŇ, Bohumír: *Úvod do eGovernmentu*. Praha 2007, s. 50-59.

[162] LIDÍNSKÝ, V. a kol: c. d., s. 41.

[163] ŠTĚDROŇ, B.: c.d, s. 50.

[164] MATES, P. – SMEJKAL, V.: c. d., s. 143.

[165] Tamtéž, s. 143.

[166] *What is PKI?* In: Searchecurity.com, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214299,00.html (8. září 2009); srov. BINDER, Jean Carlo: *Public Key Infractructures (PKIs): What are they?*. In: VACCA, John R. (ed.): *Public Key Infrastructure: building trusted applications and Web services*. Auerbach 2004, s. 8.(http://books.google.com); dále viz také: MERKOW, Mark: *Growing a Tree of Trust*. In: VACCA, J. R. (ed.): c. d., s. 34-35).

koncept reagující na vývoj v elektronickém, ICT, ale také obchodním světě.[167]

Nejvýraznějšími bezpečnostními riziky elektronického podpisu jsou zpravidla odcizení privátního klíče, situace, kdy vydavatel si neoprávněně uchová soukromý klíč, resp. ho poskytne další osobě. Dále to může být padělání veřejného klíče odesílatele, tedy narušení autentičnosti veřejného klíče. Nicméně tento postup odporuje zákonu o elektronickém podpise a je postižitelný dle tohoto zákona.

Bezpečnost elektronického podpisu je tedy založena na třech podmínkách. Nejprve se jedná o zajištění tajnosti privátního klíče uživatele. Dále se jedná o neprolomení kryptografického algoritmu. A konečně nesmí dojít k porušení autentičnosti veřejného klíče, tedy že tento náleží dané podepisující osobě.[168] Zneužití veřejného i privátního klíče brání především matematické zákonitosti, tedy jeho složitý matematický výpočet.

1. *5. 1. 1. Novelizace zákona o elektronickém podpise – kvalifikované časové razítko a elektronická značka*

Dne 26. července 2004 vstoupila v platnost novela zákona o elektronickém podpisu.[169] Ta zavádí dva nové pojmy – *kvalifikované časové razítko* a *elektronická značka*. Kvalifikované časové razítko prokazuje existenci elektronického dokumentu v čase.[170] Je to datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb[171] a důvěryhodně spojuje data v elektronické podobě s časovým okamžikem.[172]

---

[167] WEISE, Joel: *Public Key Infrastructure Overview.* In: Sun Blueprints Online, srpen 2001, http://www.sun.com/blueprints/0801/publickey.pdf (8. září2009), s. 1.
[168] MATES, P. – SMEJKAL, V.: c. d., s. 141.
[169] *Zákon č. 440/2004 Sb., kterým se mění zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů.* In: Sbírka zákonů, roč. 2004, 26. července 2004, http://web.mvcr.cz/archiv2008/sbirka/2004/sb144-04.pdf (9. září 2009)
[170] *Zákon č. 227/2000 Sb., o elektronickém podpisu.* In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx (5. července 2007)
[171] Osoba vydávající kvalifikované certifikáty, kvalifikované systémové certifikáty, kvalifikovaná časová razítka nebo prostředky pro bezpečné vytvoření elektronických podpisů.
[172] Toto razítko musí obsahovat své číslo unikátní u daného poskytovatele certifikačních služeb, označení pravidel, podle kterých bylo razítko vydáno, a označení vydavatele razítka. Dále musí

Elektronická značka[173] je de facto totéž jako elektronický podpis. Je však vytvořena technickým zařízením, nikoli osobou. Její tvoření je automatizované. Termín podepisující osoba je nahrazen termínem označující osoba,[174] což může být fyzická osoba, právnická osoba nebo organizační složka státu. Vydání elektronické značky je jednodušší, časově i personálně méně náročné. Označující osoba nemusí nutně znát obsah označovaného dokumentu, resp. datové zprávy, která může být velmi rozsáhlá (např. při vydávání elektronických výpisů z úředních databází či při potvrzování přijetí elektronických zpráv apod.).[175]

Elektronické značky mají také díky novele zákona o elektronickém podpisu stejnou vlastnost a funkci jako úřední razítko a podpis úřední osoby na listině. Pokud jsou tyto dokumenty vydány orgány veřejné správy, jsou nazývány veřejnými listinami. Jejich obsah nemusí být dokazován na příklad při soudním jednání.[176]

Zákon o elektronickém podpisu je dále doplněn nařízením vlády č. 495/2004 Sb., které stanovuje povinnost orgánů veřejné správy zřídit elektronické podatelny.[177] Toto nařízení vlády o e-podatelnách souvisí s

---

kvalifikované časové razítko obsahovat hodnotu času odpovídající koordinovanému světovému času při vytváření kvalifikovaného časového razítka, data v elektronické podobě, pro která je toto razítko určeno, a konečně je třeba elektronická značka kvalifikovaného poskytovatele certifikačních služeb. (MATES, P. – SMEJKAL, V.: c. d., s. 153.; další vymezení časového razítka viz také *Zákon č. 440/2004 Sb., §2, ods. r*)

[173] Náležitosti elektronické značky vymezuje *Zákon č. 440/2004 Sb., čl. 1, § 2, ods. c.*

[174] *Zákon č. 440/2004 Sb., čl. 1, §2, ods. f a § 5a.*

[175] MATES, P. – SMEJKAL, V.: c. d., s. 151.

[176] Tamtéž, s. 152.

[177] V případě malého objemu elektronické komunikace musí orgán veřejné správy zajistit možnost elektronické komunikace skrze elektronickou podatelnu jiného úřadu. Nařízení vlády č. 495/2004 Sb. bylo schváleno dne 25. srpna 2004. (*Nařízení vlády č. 495/2004 Sb, kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů*. In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/narizeni-vlady-c-495-2004-sb-kterym-se-provadi-zakon-c-227-2000-sb-o-elektronickem-podpisu-a-o-zmene-nekterych-dalsich-zakonu.aspx (5. července 2009)

Dle informací Ministerstva informatiky ke dni 1. ledna 2007 mělo e-podatelnu k dispozici 14 z 15 ministerstev, 10 z 11 dalších z ústředních orgánů státní moci (Český statistický úřad, Český úřad zeměměřický a katastrální, Český báňský úřad, Úřad průmyslového vlastnictví, Úřad pro ochranu hospodářské soutěže, Státní úřad pro jadernou bezpečnost, Národní bezpečnostní úřad, Energetický regulační úřad, Úřad vlády České republiky a Český telekomunikační úřad. Pouze Správa státních hmotných rezerv v té době svou e-podatelnu zřízenu neměla. V současnosti jí však disponují také všechny krajské úřady a 97 % obcí s rozšířenou působností Ze závěru zprávy Ministerstva informatiky pak vyplývá, že *„(P)očet úřadů, které splňují požadavky nařízení vlády č. 495/2004 Sb. a provozují elektronickou podatelnu v souladu s vyhláškou 496/2004 Sb., o elektronických podatelnách, již dosahuje dostatečnou základnu pro elektronickou komunikaci občana s orgány veřejné moci."* Komunikovat lze nejen s nejvyššími orgány státní správy, ale také s většinou obcí i krajských úřadů. V současnosti (4. srpna 2009) má zřízeno elektronickou podatelnu všech 16 ministerstev i Vláda ČR samotná. (*Informace o zřízení elektronických podatelen u orgánů veřejné moci.* In: Ministerstvo vnitra ČR,

vyhláškou č. 496/2004 Sb. k elektronickým podatelnám. Ta *„upravuje postup, jak mají orgány veřejné moci přijímat a odesílat datové zprávy prostřednictvím elektronické podatelny.“*[178] Jsou zde také uvedeny postupy ověřování platnosti zaručeného elektronického podpisu a elektronické značky, stejně jako platnosti kvalifikovaného certifikátu a kvalifikovaného systémového certifikátu.[179] Vyhláška upravuje rovněž způsoby a okolnosti podání a doručení datové zprávy.[180]

Zavedení elektronického podpisu bylo dobře technicky připravené, nicméně hlavními překážkami pro jeho plošnější užití je zejména jeho omezená platnost a také zpoplatnění. Pro jedince či malé firmy se tak elektronická komunikace s úřady prostřednictvím elektronické podatelny a elektronického podpisu jeví jako nevýhodná a neefektivní. Institutu elektronického podpisu však nelze upřít pozitivní vliv na vývoj e-governmentu v ČR, a to zejména v souvislosti se zrovnoprávněním elektronických a písemných forem dokumentů. Významný je také jeho rys nepopiratelnosti zprávy, kterou doprovází, a také možnosti jednoznačně ověřit identitu podepisujícího.[181] Omezené využívání elektronického podpisu lze také připsat nedostatečné propagaci mezi veřejností.[182]

1. 5. 2. Elektronické doručování a podání

V souvislosti s elektronickým podpisem je třeba také uvést problematiku elektronického doručování a podání na úřady. To umožňuje Správní řád ČR. Povinné pro úřady je také provozování elektronické úřední desky.

---

http://www.mvcr.cz/clanek/informace-o-zrizeni-elektronickych-podatelen-u-organu-verejne-moci.aspx (4. srpna 2009)

[178] *Vyhláška č. 496/2004 Sb. k elektronickým podatelnám*. In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/vyhlaska-c-496-2004-sb-k-elektronickym-podatelnam.aspx (5. července 2009)

[179] Tamtéž.

[180] Za doručenou se považuje datová zpráva, která je k dispozici v elektronické podatelně. Zde se ukládá do úložiště spolu s uznávaným elektronickým podpisem či uznávanou elektronickou značkou. Elektronická podatelna ověřuje jejich pravost a správnost dle zákona. (Blíže viz MATES, P. – SMEJKAL, V.: c. d., s. 190-192)

[181] *Elektronický podpis a jeho využití.* In: businessinfo.cz, http://www.businessinfo.cz/cz/clanek/podnikatelske-prostredi/elektronicky-podpis-a-jeho-vyuziti/1001234/2984/ (5. září 2009)

[182] SMEJKAL, Vladimír: *Datové schránky nastupují*. In: ihned.cz, 22. července 2009, http://pravniradce.ihned.cz/c4-10078260-37865170-F00000_d-datove-schranky-nastupuji (12. října 2009)

Zákon o elektronickém podpisu dává občanu možnost činit podání k orgánům státní moci elektronicky za použití zaručeného elektronického podpisu. Nicméně již dva roky po jeho vydání, tedy v roce 2002 např. občanský soudní řád tuto možnost nahradil podáním s běžným elektronickým podpisem. To je pak třeba do tří dnů doplnit fyzickým písemným dokumentem. Podle Matesa a Smejkala se jednalo o krok zpět a poukazuje to na nedostatečnou podporu elektronické komunikace v rámci státní správy.[183]

K menší podpoře e-governmentu se vyjadřuje také A. Ptašnik v závěru své stati, kdy zdůrazňuje efektivitu a snižování nákladů při zavádění prvků e-governmentu do veřejné správy. Poukazuje na správně „namířené" kroky z centrální úrovně, které však podrývá nejednotnost, nepochopení, ignoranci či pouze konzervatismus objevující se na různých úrovních veřejné správy.[184]

Státní orgány zatím elektronickou komunikaci v praxi příliš nepreferují, a to zejména kvůli nízkému zájmu občanů využívat tuto možnost, informační gramotnosti úředníků a technických možností na příklad u malých obcí a také kvůli obtížnému zpracovávání dokladů pro správní řízení do elektronické podoby (např. smluv s podpisem, notářsky ověřených zápisů apod.).[185]

Přesto se však situace pro elektronická podání a doručování za užití zaručeného elektronického podpisu postupně stává příznivější a většina orgánů státní správy jsou jí podstatně nakloněnější než dříve. Elektronická komunikace[186] umožňuje omezit fyzickou přítomnost občana

[183] MATES, P. – SMEJKAL, V.: c. d., s. 162.
O některých problémech zavádění elektronického podání a doručování viz Tamtéž, s. 162-163.
[184] PTAŠNIK, Adam: *Cyberspace in Public Administration*. In: POLČÁK, R. – ŠKOP, M. – ŠMAHEL, D.: c. d., s. 116.
[185] LIDÍNSKÝ,V. a kol.: c. d., s. 48.
[186] V souvislosti s rozšiřováním možnosti užití elektronické komunikace a doručování je třeba se zabývat také problematikou konverze fyzických dokumentů v elektronické se zachováním jejich důkazní hodnoty. V tomto ohledu sehrává základní roli legislativní úprava, která definuje pravidla elektronické komunikace i podmínky zrovnoprávnění listinných a elektronických dokumentů. Stěžejní se v tomto ohledu jeví definice *originálu* resp. *autentického dokumentu*. Ten musí splňovat tato kritéria: je zachována integrita informací obsažených v dokumentu od okamžiku jeho dokončení v libovolné podobě, datová zpráva je v písemné podobě a konečně informace zůstanou nezměněné a kompletní ve srovnání s právě dokončeným dokumentem (s výjimkou připojení příslušných potvrzení nebo certifikátů zajišťujících integritu, eventuálně s výjimkou nezbytných změn vzniklých při komunikaci, úschově či převedení informací). (LIDÍNSKÝ, V. a kol.: c. d., s. 73.)

na úřadě, což vede k určitému usnadnění práce úředníka. Je také možno „odbavit“ více žádostí a dokumentů při stejném počtu zaměstnanců.[187] Elektronická komunikace v rámci státní správy v ČR dostává nový impuls v podobě zavádění datových schránek či projektu eJustice.[188] Je tak zde zřetelný posun ve prospěch četnějšího využití elektronické komunikace ve státní správě.

Zákon o ISVS[189] zavedl možnost doručit datové zprávy orgánům státní moci prostřednictvím Portálu veřejné správy.[190] Pro větší komfort a ochranu podavatele, tedy občana, je důležitý moment podání, tedy převzetí správcem portálu, od kdy běží předepsané lhůty. Správce musí zprávu dodat do tří dnů od okamžiku podání. Prodleva tedy je „k tíži“ veřejné správy.[191] S datovou zprávou má do jejího dodání oprávnění nakládat pouze odesílatel a správce.[192]

Dle Matesa a Smejkala je způsob elektronického doručování a dodání nejasný, nesrozumitelný, a tedy nedostačující.[193] Je to zapříčiněno hlavně nejednotností zákonných úprav o elektronickém podání a doručování pro různé orgány státní moci. Zavedení jednoho a efektivnějšího způsobu elektronického podání a doručení v rámci celé státní správy je *„základním předpokladem pro plnohodnotné zavedení služeb e-governmentu a je plně v souladu s vládní politikou e-governmentu.“*[194] Řešením se jeví zavedení tzv. datových schránek 1. července 2009, resp. 1. listopadu 2009, kdy byl zahájen jejich ostrý provoz.

---

[187] Proto se také průkopníky ve využívání elektronické komunikace staly banky, které poskytováním svých elektronických bankovnictví umožnily vykonávání běžných úkonů spojených s ovládáním vlastního účtu prostřednictvím Internetu. Omezil se tak počet návštěv klienta v bance.

[188] Projekt eJustice byl spuštěn 1. října 2007 a jeho cílem je zefektivnění českého soudnictví. Prostřednictvím elektronických médií mají být vykonávány zejména jednoduché a opakující se postupy. V současnosti jsou součástí projektu eJustice ePlatební příkaz, ePodatelna, eTrestní řízení, infoDeska, infoJednání, infoSoud, Insolvenční rejstřík, Judikatura, Obchodní rejstřík a Rejstřík trestů. (*eJustice*. In: Justice.cz, http://obcanskyzakonik.justice.cz/ejustice/index.html (4. srpna 2009)

[189] Viz výše.

[190] Správcem Portálu veřejné správy, který nese zodpovědnost za podání i doručení této zprávy, je Ministerstvo vnitra ČR.

[191] MATES, P. – SMEJKAL, V.: c.d., s. 185.

[192] V případě správce portálu se jedná pouze o úkony nezbytné k dodání zprávy. Odesílatel má více možností. Může zprávu vzít zpět i změnit její obsah a podobně. Správce má však právo datovou zprávu zlikvidovat, pokud ji nelze dodat ani vrátit nebo pokud zpráva obsahuje nebezpečné složky, které by mohly přinést škodu (např. viry).

Tamtéž, s. 187.

[193] Viz také SMEJKAL, V.: c.d.

[194] MATES, P. – SMEJKAL, V.: c. d., s. 192.

1. 5. 3. Czech POINT

Významným posunem v rozvoji e-governmentu ve vztahu občan-veřejná správa bylo zavedení Českého **P**odacího **O**věřovacího **I**nformačního **N**árodního **T**erminálu neboli Czech POINTu v roce 2007.[195] Czech POINT je zakotven již v zákoně č. 365/2000 Sb., o ISVS[196] a je s ISVS úzce propojen. Projekt CzechPOINT rovněž spolupracuje s projektem ePUSA. Jedná se o druhý nejviditelnější a nejúspěšnější krok v elektronizaci veřejné správy.[197] Projekt je společnou iniciativou sdružení eStat.cz[198] a Ministerstva vnitra ČR.

Záměrem koncepce CzechPOINT je koncentrace výkonu státní správy do jednoho kontaktního místa, ze kterého občan může komunikovat s různými orgány a úřady státní moci. Obíhat mají data, nikoli občan. Na jednom univerzálním místě lze *„získat a ověřit data z veřejných i neveřejných informačních systémů, úředně ověřit dokumenty a listiny, převést písemné dokumenty do elektronické podoby a naopak, získat informace o průběhu správních řízení ve vztahu k občanovi a podat podání pro zahájení řízení správních orgánů.“*[199] V konečné fázi projektu se předpokládá, že občan bude všechny tyto úkony vykonávat z domova přes internet a nebude muset navštěvovat už ani kontaktní místo.[200] Zde je používán pojem CzechPOINT@home, kdy se jedná o informační portál, jehož účelem je vytvořit jednoduchou a intuitivní platformu pro komunikaci občana s veřejnou správou a pomoci tak přesunout eGovernment z prostředí podatelen úřadů do domácího pohodlí občanů.[201]

Dalším rozšířením možností a působení CzechPOINTu je uvedení tzv. CzechPOINT@office. Jedná se o vnitřní CzechPOINT v rámci úřadů a

---

[195] Název lze vnímat také jako slovní hříčkou odkazující na „check point“, tedy místo kontroly.
[196] Viz výše.
[197] Spolu se zavedením elektronického podpisu a datových schránek (Viz níže kapitola 1.5.4. Datové schránky.).
[198] eStat.cz neboli „efektivní stát“ je občanským sdružením zaměřeným na podporu efektivizace státní správy. Organizaci lze charakterizovat za pravicově orientovaný think tank. Webové stránky organizace: http://estat.cz
[199] *Co je Czech POINT.* In: CzechPOINT, http://www.czechpoint.cz/web/?q=node/22 (5. července 2009)
[200] Tamtéž.
[201] Viz např. *CzechPOINT@home.* In: Asseco Czech Republic, http://www.eobec.eu/egovernment/czechpoint-home/ (6. září 2009); LEDVINKA, Robert a kol.: *Technologická centra krajů a obcí s rozšířenou působností, včetně spisových služeb. Koncept a východiska.* In: Ministerstvo vnitra ČR, http://www.mvcr.cz/soubor/koncept-a-vychodiska-projekt-tc.aspx (6. září 2009), s. 9.

orgánů veřejné moci. Jeho prostřednictvím lze provézt autorizovanou konverzi elektronických dokumentů dle zákona č. 300/2008 Sb. a také výpis z rejstříku trestů z moci úřední. Služby CzechPOINT@office budou dále rozšiřovány.[202]

Původními výstupy CzechPOINTu byly výpisy z Katastru nemovitostí, Obchodního rejstříku a Živnostenského rejstříku. Postupně se možnosti přístupu k výpisům z veřejných i neveřejných registrů[203] stejně jako možnosti podání ke správnímu řízení i autorizované konverze dokumentů[204] rozšiřovaly. V roce 2008 přibyl přístup do Trestního rejstříku. Rok 2009 přinesl zatím nejrozsáhlejší posun ve službách poskytovaných CzechPOINTem. Bylo umožněno podávat podání k Živnostenskému úřadu, získávat výpisy z registru řidičů, Seznamu kvalifikovaných dodavatelů, Registru účastníků provozu modulu autovraky ISOH a Insolvenčního rejstříku.[205] Zároveň je možné na CzechPOINTu vykonávat některé úkony spojené s používáním datové schránky (např. její zřízení, změna či zneplatnění přístupových údajů apod.).[206]

Využívání kontaktního místa CzechPOINT z hlediska přístupu občanů lze hodnotit pozitivně. V jeho rámci již bylo vydáno více než dva miliony výpisů z různých rejstříků a rozšiřuje se také síť jeho provozoven.[207]

1. 5. 4. Datové schránky

Datové schránky[208] uvedl zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů platný od 1. července

---

[202] *CzechPOINT@office - Agendy pro vnitřní použití na úřadech.* In: CzechPOINT, http://www.czechpoint.cz/web/?q=node/382 (6. září 2009).

[203] Veřejné registry: Obchodní rejstřík, Katastr nemovitostí, Živnostenský rejstřík, Seznam kvalifikovaných dodavatelů a Insolvenční rejstřík.

Neveřejné registry: Trestní rejstřík, Registr účastníků provozu modulu autovraky ISOH a Bodové hodnocení osoby - registr řidičů.

[204] Z listinné do elektronické a naopak. CzechPOINT umožňuje také ověření provedení autorizované konverze.

[205] *CzechPOINT*. In: www.ostrava.cz, http://www.ostrava.cz/jahia/Jahia/site/ostrava/cache/offonce/ostrava/obcan/czech-point;jsessionid=127A1344E2E4A6C7EC167E5945311CDB (11. srpna 2009)

[206] Viz níže kapitola 1.5.4. Datové schránky.

[207] *Statistiky vydaných výstupů v rámci projektu CzechPOINT k 18. 10. 2009.* In: CzechPOINT, http://www.czechpoint.cz/web/?q=statistiky_aktualni (20. října 2009)

[208] Informačním i komunikačním portálem datových schránek je http://www.datoveschranky.info.

2009.[209] Jedná se o *„elektronické úložiště, které je určeno k doručování dokumentů orgánů veřejné moci a k provádění podání vůči nim.“*[210] Dochází také k částečnému, ale významnému nahrazení klasického doručování v listinné podobě.[211] Dokumenty doručené prostřednictvím datové schránky budou mít stejnou váhu a platnost jako doručená zásilka s dodejkou i do vlastních rukou.[212] Tyto úpravy *„přinášejí zásadní změny v komunikaci mezi orgány veřejné moci a adresáty veřejné správy a v oblasti nakládání s dokumenty v rámci orgánů veřejné moci.“*[213]

Podobně jako elektronický podpis datová schránka zajišťuje nepopiratelnost odesílatele i příjemce. Rozdíly mezi datovou schránkou a v současnosti poměrně běžně používaným e-mailem spočívají především v právní podstatě věci. Datová schránka také zatím neumožňuje komunikaci mezi právnickými a fyzickými osobami navzájem. Komunikovat lze tedy pouze s orgány veřejné správy.[214]

---

[209] *Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů*

Dále vstupují v platnost zákon č. 301/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronických úkonech a autorizované konverzi dokumentů, jakož i zákon č. 7/2009 Sb., kterým se mění zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů, a další související zákony. Od 1. července 2009 nabyla účinnosti také novela zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů. Publikovány byly také související vyhlášky: Vyhláška č. 192/2009 Sb., kterou se mění vyhláška č. 645/2004 Sb., kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů*;* Vyhláška č. 191/2009 Sb., o podrobnostech výkonu spisové služby*;* Vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů*;* Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek. (*Právní předpisy k datovým schránkám.* In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/navrhy-provadecich-pravnich-predpisu-k-datovym-schrankam.aspx (9. září 2009)

[210] *Datové schránky. Typový postup implementace. Občan.* In: datoveschranky.info, http://www.datoveschranky.info/obcan/?PHPSESSID=187b6fefcb77aa068914df2363f6eba3 (5. září 2009), s. 3.

[211] Viz *Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů*, § 18, ods. 2.

[212] *Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů*, § 17, ods. 6.

Dodejka je ke zprávě připojena v okamžiku jejího dodání do datové schránky adresáta. Doručenka je vytvořena v okamžiku přihlášení adresáta do jeho datové schránky či po uplynutí lhůty 10 dnů, kdy dochází k tzv. fikci doručení. (*Datové schránky. Typový postup implementace. Občan.*, s. 12.)

[213] *Prováděcí právní předpisy k datovým schránkám*. In: datoveschranky.info, http://www.datoveschranky.info/vyhlasky/?PHPSESSID=780cc31f7eb987e497fbfdc5478bdcb3 (14. července 2009)

[214] Blíže viz *Datové schránky. Typový postup implementace. Občan*., s. 3. Novela zákona č. 300/2008 z května 2009 však umožňuje komunikaci mezi právnickými osobami od 1. ledna 2010. Orgány veřejné moci rozumíme organizační jednotky státu, orgány územních samosprávných celků (obce a kraje), Pozemkový fond ČR a jiné státní fondy, zdravotní pojišťovny, Český rozhlas, Česká televize, samosprávné komory zřízené zákonem, notáři a soudní exekutoři. (*Datové*

Datová schránka je elektronickým úložištěm čili datovým prostorem, kam budou datové zprávy doručovány a uchovávány po určitou dobu.[215] Datová zpráva, jejíž velikost může být maximálně 10 MB, je tvořena obálkou a obsahem zprávy. Může také obsahovat přílohy v libovolném formátu (s výjimkou přípon .exe a komprimovaných souborů).[216] Jde hlavně o bezpečnostní riziko přenosu virové infekce v informačním systému. Provozovatel datové schránky má také možnost nepřijmout k odeslání zprávu obsahující škodlivý kód.[217] Datovou zprávu definujeme dle zákona o elektronickém podpisu jako *„elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou"*[218]

Datové schránky fungují v prostředí informačního systému datových schránek, což je ISVS dle zákona č. 365/2000 Sb. Jsou v něm obsaženy informace o datových schránkách a jejich uživatelích. Správcem a zřizovatelem systému je Ministerstvo vnitra, jež zajišťuje bezpečnost tohoto ISVS. Jeho provozovatelem je pak Česká pošta.[219] Ani jeden z těchto subjektů však nemá přístup do datových schránek jiných uživatelů.[220] Ministerstvo vnitra je také zodpovědné za zasílání přístupových údajů k datové schránce, která je pak zpřístupněna prvním přihlášením

---

schránky. Typový postup implementace. Občan., s. 4-5*)* Kontrolu, zda je daný úřad orgánem státní moci lze na stránkách www.datoveschranky.info (http://www.datoveschranky.info/ovm.php).

[215] Maximálně 90 dní od doručení do datové schránky adresáta. Doručením se rozumí okamžik, kdy se uživatel datové schránky přihlásil k jejímu užití. Pokud tak však neučiní do 10 dnů od okamžiku, kdy byl dokument dodán do jeho datové schránky, je pak datová zpráva považována za doručenou. Jedná se o tzv. fikci doručení. Zákon umožňuje i jiné podmínky doručení či posunutí termínu doručení apod. (Viz PROTIVOVÁ, I. a kol.: c.d., s. 14; srov. *Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů*, § 17, ods. 4 a 5.) Vymezení datové schránky viz *Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů*, §2.

[216] Seznam podporovaných formátů pro přílohy datových zpráv upravuje vyhláška č. 194/2009 o stanovení podrobností užívání a provozování informačního systému datových schránek (*Vyhláška č. 194/2009, o stanovení podrobností užívání a provozování informačního systému datových schránek*. In: Sagit, http://www.sagit.cz/pages/sbirkatxt.asp?cd=76&typ=r&zdroj=sb09194 (6. září 2009). Nicméně jejich seznam je i dále rozšiřován. Viz např. *Nové přípustné formáty datové zprávy.* In: datoveschranky.info, http://www.datoveschranky.info/clanek/243/ (13. září 2009)

[217] PROTIVOVÁ, I. a kol.: c. d., s. 11.

[218] *Zákon č. 227/2000 Sb., o elektronickém podpisu*, §2, ods. d.

[219] *Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů*, § 14; srov. PROTIVOVÁ, I. a kol.: c. d., s. 14.

[220] *Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů*, § 14, ods. 6.

oprávněné či pověřené osoby, resp. do 15 dnů od doručení přístupových údajů.[221]

Nakládat s datovou schránkou smí pouze tzv. oprávněná osoba.[222] Jedná se v zásadě o osobu (fyzickou i právnickou), pro kterou byla datová schránka zřízena. U velkých organizací (právnické osoby, orgány veřejné moci apod.) pak jsou používáním datové schránky pověřeni tzv. administrátoři.[223] Pro vstup do datové schránky je potřeba disponovat přihlašovacími údaji (jménem a heslem) a je možné použít také digitální neboli kvalifikovaný certifikát pro zvýšení bezpečnosti.[224]

Orgány veřejné moci mají povinnost komunikovat prostřednictvím datové schránky, pokud ji má protistrana zřízenu.[225] Povinné je zřízení datové schránky pro orgány veřejné správy a právnické osoby.[226] Fyzické osoby, občané a živnostníci mají pouze možnost si datovou schránku zřídit.[227]

Spolu s fungováním registrů veřejné správy budou datové schránky znamenat také umožnění kontroly občany, kdy a jak bylo nakládáno s jejich osobními údaji obsaženými v těchto registrech. Do datové schránky totiž přijde zpráva o průběhu použití příslušných osobních údajů.[228]

Na rozdíl od elektronického podpisu je zřízení a využití datové schránky pro většinu subjektů zdarma.[229] Zpoplatněna je jen autorizovaná

---

[221] *Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů*, § 10.

[222] Ministr, hejtman, starosta, ředitel úřadu, jednatelé a vedoucí organizačních složek.

[223] Dále může být využito také institutu pověřené osoby, kterou deleguje administrátor nebo oprávněná osoba. Blíže viz *Zákon 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů,* §8; srov. PROTIVOVÁ, I. a kol.: c. d., s. 31-32.

[224] *Datové schránky. Typový postup implementace. Občan*., s. 5; *Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů*, § 8.

[225] Viz *Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů*, § 17, ods. 1.

[226] Ty je musejí mít zřízeny k 1. listopadu 2009, kdy byla ukončena tzv. přechodná fáze existence datových schránek (od 1. července 2009).

[227] Výjimkou jsou advokáti, daňoví poradci, insolvenční správci, notáři a exekutoři, kterým bude datová schránka zřízena automaticky. Výjimku mají advokáti vedení v seznamu České advokátní komory a daňoví poradci, kteří si datovou schránku musí zřídit nejpozději do 1. července 2012.

[228] *Datové schránky v poločase – dva měsíce po startu a dva měsíce před plným provozem.* In: datoveschranky.info, http://www.datoveschranky.info/clanek/233 (6. září 2009)

[229] Za odeslání datové zprávy platí jen některé orgány veřejné moci. Blíže k problematice zpoplatnění provozu datových schránek viz PROTIVOVÁ, I. a kol.: c. d., s. 22. Poplatek za autorizovanou konverzi je upraven dle zákona č. 634/2004 Sb., o správních poplatcích ve znění zákona č. 301/2008 Sb. V případě autorizované konverze na krajských či obecních úřadech je stanovena výše poplatku 30 korun. (*Datové schránky. Typový postup implementace. Občan*., s. 12.)

konverze[230] dokumentů z a do elektronické podoby[231] a zaslání přístupových údajů, pokud je o ně žádáno do tří let od předchozího předání. Zaslání datové zprávy orgánu veřejné moci budou hrazeny ze státního rozpočtu. V budoucnu se počítá se zpoplatněním komunikace mezi právnickými osobami.[232] Platnost schránky je v podstatě neomezena.[233] Z tohoto důvodu i skutečnosti, že datovou schránkou lze disponovat zdarma, lze očekávat větší zájem veřejnosti o tuto možnost elektronické komunikace se státní správou, než jak tomu bylo u elektronického podpisu či institutu elektronického doručování a podání.

Datová zpráva poslaná skrze datovou schránku nemusí mít sama o sobě elektronický podpis. Informační systém datové schránky automaticky připojuje k datové zprávě kvalifikované časové razítko, které připojuje Ministerstvo vnitra coby správce informačního systému datových schránek.[234] Nicméně elektronický podpis je třeba v situaci, kdy je potřeba ověřený podpis, či pokud je nutné, aby dokument podepsalo více osob.[235]

Problémem fungování datových schránek se v období po 1. červenci 2009 stal zejména nedostatek času pro testování provozu. Proces novelizace zákona o datových schránkách není ukončený.[236] Kupříkladu větší organizace (např. krajské úřady) se potýkaly s touto komplikací kvůli velkému objemu jimi spravovaných dat. Krajský úřad je složitou organizační strukturou, která vykonává velký rozsah agend a má povinnost vést spisovou službu v plném rozsahu.[237] Elektronizace spisové služby v období moderních ICT prostředků tak může podstatně zefektivnit práci

---

[230] Autorizovaná konverze se provádí v okamžiku, kdy je potřeba ověřené kopie v současnosti. Je třeba také poznamenat, že do elektronické podoby nelze konvertovat všechny dokumenty. (Přehled viz *O datových schránkách.* In: datoveschranky.info, http://www.datoveschranky.info/o-datovych-schrankach-text/ (12. září 2009) Konverzi dokumentů vymezují § 22-26 zákona č. 300/2008 Sb. Poslední dva se pak vztahují na tzv. ověřovací doložku konverze, jež doplňuje konvertovaný dokument, a evidenci provedených konverzí, kdy údaje o nich jsou ukládány po dobu 10 let. (*Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů*, § 22-26)

[231] Blíže viz PROTIVOVÁ, I. a kol.: c. d., s. 15-18.
Autorizovanou konverzi provádí kontaktní místo CzechPOINT.

[232] *Informační systém datových schránek. Základní informace.* In: www.datoveschranky.info, http://www.datoveschranky.info/clanek/84/ (12. září 2009), s. 43.

[233] Podmínky zrušení či zneplatnění datové schránky viz *Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů,* § 11-13.

[234] Více k působnosti Ministerstva vnitra v této oblasti viz *Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů,* § 20; srov. PROTIVOVÁ, I. a kol.: c. d., s. 20.

[235] *Datové schránky. Typový postup implementace. Občan.*, s. 5.

[236] V červnu 2009 byla přijata novela, která měnila zejména financování provozu systému datových schránek.

[237] *Datové schránky. Typový postup implementace. Občan.*, s. 3.

úřadu. Elektronickou spisovou službu využívá také např. projekt CzechPOINT při svých výstupech.[238] Při vedení spisové služby elektronicky je pak pro orgán veřejné moci nezbytné umožnit její propojení se systémem datové schránky.

Provozovatel datových schránek, Česká pošta, k jejich užívání připravila také některé doplňkové služby. Jedná se na příklad o SMS upozornění o příchozí datové zprávě, datový trezor či bezpečný klíč k datové schránce.[239] Lze očekávat další rozvoj i vývoj jak v těchto doplňkových službách, tak v celkovém konceptu datových schránek.

Ostrý provoz datových schránek zahájený 1. listopadu 2009 sice dosud neprovázely zásadnější technické problémy,[240] ale systém se potýká spíše s nedůvěrou či nezájmem subjektů, které mají mít datovou schránku ze zákona zřízenu.[241] Ministerstvo vnitra coby správce informačního systému datových schránek tak muselo zřídit 72 % z povinně aktivovaných datových schránek, a to jak právnickým osobám, tak některým orgánům veřejné moci. K 1. listopadu však tento způsob komunikace s veřejnou správou zvolilo přes 10 000 občanů, kteří povinnost zřídit si datovou schránku neměli.[242]

První hodnocení fungování datových schránek představilo Ministerstvo vnitra spolu s Českou poštou na tiskové konferenci dne 18. listopadu 2009. Z jejich pohledu je systém stabilní a funkční. Aktivních je 98,5 % z 371 460 zřízených datových schránek. Úspěšnost doručení

---

[238] Projekt datových schránek je s CzechPOINTem provázaný i v jiných oblastech. Je zde možné si datovou schránku zřídit. Na kontaktních místech Czech POINT lze také zažádat o nové přihlašovací údaje, zneplatnění přístupových údajů nebo znepřístupnění datové schránky. (*O datových schránkách)*

[239] Více k doplňkovým službám České pošty viz *Datový trezor a jiné služby*. In: datoveschranky.info, http://www.datoveschranky.info/aditivni-sluzby/ (12. září 2009)

[240] Technický problém nastal pouze na konci října 2009 v resortu justice, kdy systém datových schránek přestal fungovat. Závada však byla dočasná a provoz datových schránek se dál jeví jako poměrně stabilní a bezpečný. Obavy se v této souvislosti objevily s možností tzv. phishingu, tedy zneužití osobních údajů uživatelů datových schránek (viz níže kapitola 2.3.3.1. Kybernetická špionáž). Ti by tedy měli být obezřetní při přístupu do systému své datové schránky. (Viz *Majitelům datových schránek hrozí, že by mohli přijít o hesla*. In: Ihned.cz, 18. listopadu 2009, http://ihned.cz/?s1=0&m=frommail&article[id]=39115690 (21. listopadu 2009). Dalšími zaznamenanými problémy byla nesprávná činnost některých spisových služeb či aplikací, což provozovatel a správce datových schránek řeší bezplatnou asistencí.

[241] Před stanoveným datem bylo aktivováno 110 284 datových schránek spadajících do této kategorie.

[242] Konkrétně to bylo 10 186 aktivovaných datových schránek v této kategorii.

Statistiky ke dni 1. listopadu 2009 viz *Informační systém datových schránek se rozběhl naplno.* In: datoveschranky.info, http://www.datoveschranky.info/clanek/284 (21. listopadu 2009)

datových zpráv prostřednictvím přihlášení uživatele (nikoli fikcí) je 88,7 %. Vyzvednutí datové zprávy přihlášením ve lhůtě do deseti dnů je téměř 95 %, což je ze strany České pošty hodnoceno jako poměrně úspěšnější způsob doručování než u listovních zásilek. Je také možné sledovat rostoucí počet aktivovaných datových schránek ze strany fyzických osob, ale také právnických osob. Skutečně aktivních datových schránek, tedy takových, ke kterým se jejich uživatelé skutečně přihlásili, je ale 53,6 %.[243]

Tato čísla nás tedy vedou k optimistickému pohledu na využívání systému datových schránek. Pozitivní je z našeho pohledu rostoucí zájem o tento způsob komunikace se státní správou ze strany občanů, kteří nemají zákonnou povinnost mít datovou schránku zřízenu. Další hodnocení tohoto projektu je zejména z důvodu malého časového odstupu obtížné. Nicméně očekáváme zde další pokrok. Státní správa by se v této oblasti měla zaměřit právě na tzv. fyzické osoby a možnost komunikace skrze datové schránky jim co nejvíce zpřístupnit, a to prostřednictvím dostatečného internetového připojení, ale také náležitou propagací a osvětou. Je třeba zapracovat na uživatelském komfortu občanů-zákazníků.[244]

Datové schránky představují pozitivní přínos pro rozvoj e-governmentu v ČR rozšiřováním jeho nástrojů a působnosti. Praktické využití prostředků e-governmentu ze strany občanů nicméně není ještě plně aplikované. V r. 2008 využívalo možnost komunikovat s veřejnou správou elektronicky 14 % Čechů. V tomto čísle zaostáváme za průměrem EU, který činí 28 %.[245]

---

[243] Neaktivních je tedy 46,4 % datových schránek. Nicméně je odhadováno, že 30 % tvoří datové schránky tzv. mrtvých právnických osob, evidovaných v obchodním rejstříku, ale již nepraktikujících.

Viz prezentace Ministerstva vnitra a České pošty CHÝLEK, Jaroslav – STIEGLER, Petr: *Dva týdny ostrého provozu.* In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/dva-tydny-ostreho-provozu-informacniho-systemu-datovych-schranek.aspx (21. listopadu 2009)

[244] *Rozvoj e-governmentu z pohledu Asociace krajů ČR*. In: Veřejná správa online, 2009, č. 3, http://vsol.obce.cz/clanek.asp?id=2009316 (4. října 2009)

[245] Nejvyšší podíl je v severských zemích a v Nizozemí. Nejméně naopak v nově přistoupivších zemích, tedy Bulharsku a Rumunsku. (Viz *Veřejná správa*. In: Český statistický úřad, Informační společnost v číslech 2009, http://www.czso.cz/csu/redakce.nsf/i/e_verejna_sprava_is2009/$File/is09_e.pdf (12. října 2009)

2. RIZIKA E-GOVERNMENTU A ZNEUŽITÍ ICTs PROTI STÁTU

Současná post-moderní společnost se stala do určité, i když významné míry závislá na vyspělých komunikačních prostředcích. Zejména se jedná o Internet, ale také mobilní telefony apod. Internet přestal být pouze místem pro akademickou činnost, ale stal se *„globálním mainstreamovým obchodním a komunikačním médiem."*[246] V první části této práce jsme se zabývali rozvojem a zaváděním prvků e-governmentu, tedy prostředků moderních ICTs, do státní správy s hlavním cílem tuto zefektivnit, lépe zpřístupnit občanům a také zlevnit. Druhou část textu pak věnujeme skutečnosti, že informační systémy, na jejichž bázi e-government funguje, jsou ohrozitelné.

Z pohledu bezpečnosti státu se pak může jednat hlavně o narušení tzv. klíčových infrastruktur, resp. klíčových informačních infrastruktur. V současnosti podstatná část finančních transakcí probíhá prostřednictvím různých sítí (opět hlavně Internetu). K řízení dopravy, transportu či energetické sítě jsou využívány vyspělé ICTs. Správa informací o obranných složkách či komunikace mezi nimi probíhá pomocí těchto prostředků, stejně jako komunikace mezi složkami státní správy i občany. V tomto prostředí existuje reálné riziko zneužití tohoto využívání ICTs ze strany jak počítačových hackerů, tak také státních a nestátních aktérů cílících na omezení schopnosti jiného státu správně fungovat a zajišťovat základní funkce a služby svým občanům.

V této kapitole se však nejdříve budeme věnovat bezpečnosti informačních systémů, zejména ISVS, a také informační bezpečnosti coby teoretickému i praktickému přístupu k řešení problematiky ohrožení bezpečnosti informačních systémů, které jsou základem fungování e-governmentu. Prostor bude věnován také některým konkrétním příkladům zajištění této bezpečnosti. Následovat bude pojetí tzv. kybernetické bezpečnosti a rozpracování možností zneužití ICTs proti státu. V závěru této kapitoly představíme přístupy EU k zajišťování informační či kybernetické bezpečnosti.

[246] BONI, William – KOWACICH, Gerald L.: *Netespionage: The Global Threat to Information*. Woburn 2000, s. 3. (http://books.google.com)

2. 1. Bezpečnost a zabezpečení ISVS

Bezpečnost informačních systémů patří k nejčastěji užívaným pojmům v teorii i praxi e-governmentu. Propojování počítačů veřejné správy do velkých sítí, kdy se orgány veřejné správy v důsledku obrovského objemu spravovaných a zpracovávaných dat musejí de facto spoléhat na moderní prostředky komunikace (zejména Internet a také Intranet), je otázka zajištění bezpečnosti těchto sítí jednou z nejpalčivějších.

I přes poměrně frekventované užívání pojmu bezpečnost informačního systému se jeví, že ne všichni tvůrci, provozovatelé i uživatelé informačních systémů ho chápou stejně. Bezpečnost ISVS lze vnímat jako cíl neboli ideální stav nebo jako prostředek k dosažení tohoto cíle. H. Křepelková ve svém článku popisuje bezpečnost informačního systému jako *„stav informačního systému, kdy rizika, jímž je vystaven, jsou snížena na přijatelnou úroveň na základě vhodných bezpečnostních opatření.“*[247] R. Jašek bezpečným informačním systémem rozumí *„systém, který chrání informace během jejich vstupu, zpracování, uložení, přenosu a výstupu proti ztrátě dostupnosti, integrity a důvěrnosti a při jejich likvidaci proti ztrátě důvěrnosti.“*[248] Server Informační systémy veřejné správy nicméně dále nepředkládá jednoznačné vymezení pojmu bezpečnost informačních systémů, nýbrž prezentuje způsoby, jak tohoto stavu dosáhnout.[249]

Pro stanovení bezpečnosti informačního systému se také uvádí spíše pojem zabezpečený, který také lépe odpovídá realitě. Je totiž třeba určit za jakých podmínek je daný ISVS bezpečný, resp. zabezpečený a míru zabezpečení daného ISVS.[250] Někteří autoři také hovoří spíše o důvěryhodném informačním systému.[251] Není možné zajistit absolutní

[247] KŘEPELKOVÁ, Helena: *Úvodní slovo k novému seriálu o informační bezpečnosti ze všech úhlů.* In: ICT Security, 3. června 2009, http://www.ictsecurity.cz/serial-o-informacni-bezpecnosti/uvodni-slovo-k-novemu-serialu-o-informacni-bezpecnosti-ze-vsech-uhlu.html (19. září 2009)
[248] JAŠEK, Roman: *Informační a datová bezpečnost*. Zlín 2006, s. 10.
[249] *Bezpečnost IS – co to znamená?* In: Informační systémy veřejné správy, http://www.isvs.cz/bezpecnost/bezpecnost-is-co-to-znamena-1-dil-.html (19. září 2009)
[250] MATES, P. – SMEJKAL, V.: c. d., s. 64-65.
[251] POŽÁR, J.: c.d., s. 50.

bezpečnost a je tedy třeba si uvědomit a přijmout určitou míru akceptovatelného rizika.[252]

Bezpečností informačního systému však v zásadě rozumíme zachování *důvěrnosti* (zajištění, že daná informace je dostupná pouze oprávněným osobám; k tomu je zapotřebí identifikace uživatele prostřednictvím ověřeného mechanismu pro zjišťování totožnosti), *integrity* (zajištění kompletnosti a správnosti informací a metod zpracování) a *dostupnosti* (přístupnost informace autorizovaným uživatelům dle jejich potřeby).[253]

OECD v červenci 1992 přijala seznam devíti doporučených principů bezpečnosti informačních systémů s názvem *Guidelines for the Security of Information Systems*.[254] Jejich obecnost umožňuje jejich aplikaci na různé organizace, firmy i úřady a jejich platnost je aktuální i v současnosti. Principy dle OECD tvoří vzájemně provázanou skupinu, kdy odpovědnost účastníků bezpečnostních přístupů se liší dle jejich rolí. Je však zdůrazněn aspekt demokratické společnosti a sdílení informací.[255]

Prvním z principů je *uvědomění* si potřeby bezpečných informačních systémů, dále je to *zodpovědnost* všech účastníků v rámci informačních systémů. Účastníci v rámci informačních systémů mají adekvátně a včas ve vzájemné spolupráci předcházet, odhalovat a *reagovat* na případné bezpečnostní hrozby. Dalšími důležitými aspekty jsou *etika*, kdy jsou respektovány zájmy ostatních účastníků systému, *demokracie* dle principů otevřené, demokratické společnosti charakterizované svobodným tokem informací, a reálné *zhodnocení rizik*. Organizace mají aplikovat bezpečnost jako základní prvek svých informačních systémů a sítí v rámci své *bezpečnostní struktury*. Mají také přijmout jednoznačný přístup k bezpečnostní *správě informačních systémů*. A konečně je zdůrazňované

[252] JAŠEK, R.: c.d., 10.
[253] MATES, P. – SMEJKAL, V.: c. d., s. 65.
Např. v případě elektronické spisové služby je užito autorizovaného přístupu k datovým souborům a dokumentům pouze určité skupině osob s přístupovým právem. (ŠTĚDROŇ, B.: c. d., s. 90.)
[254] *OECD Guidelines for the Security of Information Systems. Towards a Culture of Security*. In: OECD, http://www.oecd.org/dataoecd/16/22/15582260.pdf (3. října 2009)
OECD Guidelines for the Security of Information Systems byly revidovány v r. 1997 a 2001.
[255] Tamtéž, s. 9.

přehodnocování bezpečnostních rizik a politik dle aktuálního vývoje.[256] Tyto principy definované OECD lze považovat za inspiraci pro přístup také českých veřejných orgánů k bezpečnosti ISVS.

Zákon č. 365/2000 Sb., o ISVS uvádí, že o bezpečnost provozu ISVS je zodpovědný jeho provozovatel, tedy orgány veřejně správy.[257] Vyhláška č. 529/2006 Sb., o dlouhodobém řízení ISVS stanovuje,[258] že orgán veřejné správy ve své informační koncepci určí dlouhodobé cíle pro řízení bezpečnosti ISVS. Těmito cíli jsou bezpečnost dat zpracovávaných v daném systému (nelze je neoprávněně číst, mazat či jinak měnit), bezpečnost programových a technických prostředků (tedy není možné měnit zdrojový kód programu bez oprávnění, ve vytvářených programech je nutné ověřovat všechna vstupní data) a také bezpečnost služeb, které ISVS poskytuje (poskytované služby musí být přístupné jen oprávněným uživatelům, o přístupu ke službám musí být pořizovány záznamy).

Orgán veřejné správy také stanovuje požadavky na bezpečnost ISVS a *„stanoví plán řízení bezpečnosti, který obsahuje popis činností, které orgán veřejné správy vykonává pro dosažení stanovených požadavků na bezpečnost ISVS, včetně časového harmonogramu jejich plnění.“*[259] Bezpečnostní dokumentace ISVS je také součástí provozní dokumentace ISVS. Bezpečnostní dokumentace obsahuje bezpečnostní směrnice pro činnost bezpečnostního správce systému. Pokud daný orgán veřejné moci není provozovatelem tohoto ISVS či pokud má vazby s ISVS jiného správce, musí bezpečnostní dokumentace obsahovat také bezpečnostní politiku.[260]

Bezpečnostní politika obsahuje popis opatření, která orgán veřejné správy uplatňuje při zajištění bezpečnosti ISVS. Je to klíčový dokument pro řešení bezpečnosti informačních systémů jakékoli instituce a je schválený nejvyšším vedením této organizace. Vychází ze studie

---

[256] *OECD Guidelines for the Security of Information Systems. Towards a Culture of Security*, s. 10-12.; srov. POŽÁR, J.: c.d., 95-96.

[257] *Zákon č. 365/2000 Sb., o ISVS.*
Správcem je OVM, který může pověřit provozovatele.

[258] *Vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy.* In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/vyhlaska-c-529-2006-sb-o-dlouhodobem-rizeni-informacnich-systemu-verejne-spravy.aspx (19. září 2009)

[259] Tamtéž,, § 4.

[260] Tamtéž, § 10.

bezpečnosti či ze zadání instituce ve formě definovaných cílů, požadavků a analýzy rizik. Definuje tedy, co má být chráněno a také stanovuje rámec, jak této ochrany dosáhnout. Ukládá příslušné zodpovědnosti a pravomoci.[261] Musí také existovat bezpečnostní směrnice pro činnost bezpečnostního správce systému.[262] Ten je pak osoba pověřená orgánem veřejné správy pro výkon kontroly bezpečnosti ISVS.[263]

Další aspekty bezpečnosti ISVS v ČR vycházejí také ze souvisejících zvláštních předpisů, zejména pak ochrany osobních údajů. Zabezpečením osobních údajů se zabývají paragrafy 13 až 15 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.[264] Zákon také uvádí bezpečnost v souvislosti s elektronickým podpisem, kdy systém certifikační služby je bezpečný, pokud jím zpracovávaná data jsou důvěryhodná, je u nich zajištěna integrita, dostupnost a je prokazatelný jejich původ.[265]

Bezpečnost ISVS je spojená rovněž s dodržováním určitých technických předpisů. Ty jsou uvedeny v zákoně č. 22/1997 Sb., o technických požadavcích na výrobky.[266] Ten v § 4 zavádí „českou technickou normu“ v podobě dokumentu schváleného právnickou osobou pro opakované nebo stálé použití. Označována je jako ČSN. Není však obecně závazná.[267]

Zaveden byl také pojem *harmonizované* ČSN. Jeho definice vychází z evropských právních úprav a dokumentů, zejména z rezoluce Evropské rady ze 7. května 1985 *Nový přístupu k technické harmonizaci a normám (New Approach to technical harmonization and*

---

[261] POŽÁR, J.: c.d., s. 88-89.

[262] *Vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy*, § 11, ods. 3 a 4.

[263] Tamtéž, § 12, ods. 1 b.

Blíže k funkci správce bezpečnosti informačního systému viz také POŽÁR, J.: c.d., s. 78-79.

Organizace či úřad může také disponovat tzv. manažerem bezpečnosti informačního systému, který svou funkcí spadá do oblasti správy organizace, zabývá se poradenstvím pro oblast informační bezpečnosti, reprezentuje organizaci z hlediska bezpečnoti apod. (POŽÁR, J.: c. d., s. 80-81)

[264] *Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.* In: Sagit, http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00101&cd=76&typ=r (19. září 2009)

[265] Více k problematice bezpečnosti a jejích kritérií viz MATES, P. – SMEJKAL, V.: c. d., s. 66-67. K otázce ověřování bezpečnosti viz Tamtéž, s. 68.

Přehled právních předpisů týkající se bezpečnosti ISVS předkládají rovněž Mates a Smejkal v kap. 2. 4. (Tamtéž, s. 79-80). Bezpečnost související s užitím elektronického podpisu již byla přiblížena v kapitole 1. 5. 1. Elektronický podpis.

[266] *Zákon č. 22/1997 Sb., o technických požadavcích na výrobky.* In: Portál veřejné správy ČR, http://portal.gov.cz/wps/portal/_s.155/701?kam=zakon&c=22/1997 (19. září 2009)

[267] MATES, P. – SMEJKAL, V.: c. d., s. 81-82.

standardization),[268] která úzce souvisela s přijetím principů a vytvořením jednotného evropského trhu.[269] Společenství také vydalo harmonizovaná *Kritéria hodnocení bezpečnosti informačních* systémů, tzv. *ITSEC (Information Technology Security Evaluation Criteria)*.[270] Tato kritéria byla Evropskou komisí poprvé přijata v r. 1990.[271]

Normy a standardy pro hodnocení bezpečnosti informačních systémů se v civilní sféře vyvíjejí a postupně aktualizují. Je to dáno vývojem v nástrojích, které by mohly tuto bezpečnost ohrozit. Jedná se zejména o zdokonalování dovedností a prostředků tzv. malwaru, který může informační bezpečnost narušit.[272] Normy lze rozdělit podle různých kritérií. Např. Mates se Smejkalem uvádějí kategorizaci dle jejich poslání a náplní.[273] Za úspěšné dovršení vývoje bezpečnosti informačních technologií považují normu ČSN ISO/IEC 15408 Informační technologie – Kritéria pro hodnocení IT, která prošla dvěma úpravami a zdokonalením svého působení. Na ni také navazují další normy stanovující postupy a principy hodnocení konkrétních informačních systémů.[274]

---

[268] *Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards.* In: Portál EU, http://eur-lex.europa.eu/Notice.do?val=117475:cs&lang=en&list=120608:cs,120607:cs,120606:cs,117958:cs,117475:cs,&pos=5&page=2&nbl=15&pgs=10&hwords=&checktexte=checkbox&visu=#texte (11. listopadu 2009)

[269] Blíže viz *New Approach to technical harmonization and standardization*. In: Portál EU, Summaries of EU Legislation, http://europa.eu/legislation_summaries/internal_market/single_market_for_goods/technical_harmonisation/l21001a_en.htm (11. listopadu 2009)

[270] Kritéria ITSEC specifikují sedm tříd zaručitelnosti bezpečnosti IT pod označením E0-E6. ITSEC jsou formulovaná obecněji než původně pro vojenské účely vytvoření TCSEC (Trusted Computer System Evaluation Criteria), která jsou zaměřená na ochranu důvěrnosti informací. (Viz POŽÁR, J.: c. d., s. 50-52.)

[271] RANNENBERG, Kai: *Recent Development in Information Technology Security Evaluation – The Need for Evaluation Criteria for multilateral Security.* In: Institut für Wirtschaftsinformatik, http://www.is-frankfurt.de/publikationenNeu/RecentDevelopmentinInformation.pdf (11. listopadu 2009), s. 3

[272] Malwarem rozumíme tzv. škodlivý software (malicious software). Viz níže kapitola 2.2.1. Hrozby informační bezpečnosti.

[273] Rozdělení norem na: 1. základní bezpečnostní normy pro obecné použití (bezpečnostní architektury); 2. funkční normy (popisují realizaci požadavků vyplývajících z obecných norem); 3. hodnotící normy (pro hodnocení bezpečnosti např. IS, produktů, postupů aj. Jsou to např. ITSEC, TCSEC.); 4. speciální normy (pro určitou činnost, např. telekomunikace, či určité odvětví, obor nebo uživatele, např. armádu, finanční instituce, zpracování osobních údajů.) (MATES, P. – SMEJKAL, V.: c. d., s. 83.)

[274] Blíže viz Tamtéž, s. 84.

Přehled nejvýznamnějších norem souvisejících s bezpečností informačních systémů uvádí také H. Křepelková. (Viz KŘEPELKOVÁ, H.: c.d.)

Za bezpečnost informačního systému v oblasti veřejné správy je zodpovědné Ministerstvo vnitra, konkrétně oddělení jeho Odboru služeb a projektu e-governmentu. Ten v této oblasti hlavně koordinuje bezpečnost informačních systémů orgánů veřejné správy skrze přípravu strategických a metodických dokumentů pro tuto oblast, zajištění spolupráce v oblasti informační a síťové bezpečnosti na evropské a mezinárodní úrovni.[275]

2.2. Informační bezpečnost

V souvislosti s riziky e-governmentu a s ním spojeným vytvářením různých registrů státní správy a ISVS je třeba uvést také pojem informační bezpečnosti (information security). Požár jej definuje jako *„obor zabývající se zabezpečením informací v informačních a komunikačních technologiích.“* Informační bezpečnost lze popsat také jako *„vzájemně provázaná opatření organizační, administrativní, personální a fyzické bezpečnosti a opatření bezpečnosti informačních a komunikačních technologií pro zajištění dostupnosti,[276] důvěryhodnosti[277] a integrity[278] informací.“*[279]

Ministerstvo vnitra ČR informační bezpečnost definuje jako *„multidisciplinární obor, usilující o komplexní pohled na problematiku ochrany informací během jejich vzniku, zpracování, ukládání, přenosu a likvidace.“* Informační bezpečnost může být vnímána také jako *„odvětví zabývající se snižováním rizik vztahujících se k fenoménu informací.“*[280] Může také navrhovat řešení řídících, metodických, technických, právních i

[275] Na evropské úrovni se jedná zejména o spolupráci s Evropskou agenturou pro síťovou a informační bezpečnost (ENISA), o které bude více uvedeno níže v kapitole 2.4. EU a její pojetí kybernetické a informační bezpečnosti. Dále se jedná o Pracovní skupinu pro informační bezpečnost a soukromí při OECD (viz *Information Security and Privacy.* In: OECD, http://www.oecd.org/department/0,3355,en_2649_34255_1_1_1_1_1,00.html (19. září 2009).
Odbor rozvoje služeb a projektů eGovernmentu. In: Ministerstvo vnitra ČR, www.mvcr.cz, http://www.mvcr.cz/clanek/odbor-rozvoje-sluzeb-a-projektu-egovernment.aspx (19. září 2009)
[276] Informace a s nimi spojené aktivity jsou dostupné autorizovaným uživatelům dle jejich potřeby.
[277] Informace je dostupná pouze osobám s autorizovaným přístupem, tedy že se k nim nedostane nepovolaná osoba.
[278] Zabezpečení přesnosti a kompletnosti informací a metod zpracování.
[279] POŽÁR, Josef a kol.: *Základy teorie informační bezpečnosti*. Praha 2007, s. 16.
[280] *Základní definice vztahující se k tématu kybernetické bezpečnosti.* In: Ministerstvo vnitra ČR, www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx (20. září 2009), s. 1

jiných otázek v rámci příslušných organizací. Užší chápání pojmu se může týkat výhradně bezpečnosti informačních a komunikačních technologií.

Pokud informační bezpečnost chápeme jako bezpečnost informací, pak ji lze definovat jako *„ochranu dat organizace před neautorizovaným přístupem nebo změnou a zajištění dostupnosti, důvěrnosti a integrity."*[281]Jašek uvádí definici informační bezpečnosti coby *„zodpovědnost za ochranu informací během jejich vzniku, zpracování, ukládání, přenosů a likvidace prostřednictvím logických, technických, fyzických a organizačních opatření, která musí působit proti ztrátě důvěrnosti, integrity a dostupnosti těchto hodnot."*[282]

Informační bezpečnost je poměrně mladým oborem. Jeho počátky jsou kladeny do první poloviny 80. let, kdy se poměrně masově začaly přesouvat agendy a data všeho druhu do privátních výpočetních systémů. Ty se stávají centrem soustředění vysokých hodnot, neboť např. banky v nich vedou evidence účtů svých klientů, podniky či organizace je používají pro řízení výroby, bezpečnostní složky státu do nich ukládají data různých stupňů utajení.[283] Je tedy nezbytné jak ze strany státních orgánů, tak firem formulovat strategické přístupy k informační bezpečnosti.

Vláda ČR přijala na základě svého usnesení č. 1340 v říjnu 2005 *Národní strategii informační bezpečnosti ČR (NSIB)*. Jejím cílem bylo především *„zvýšit důvěru občanů a subjektů komerční i nekomerční sféry v informační společnost, zlepšit celkové řízení informační bezpečnosti, rozvíjet znalosti o informační bezpečnosti, zlepšit mezinárodní spolupráci, shromáždit a doporučit nejlepší praxi pro oblast řízení informační bezpečnosti, zajistit základní lidská práva při používání informačních a komunikačních technologií a podporovat konkurenceschopnost české ekonomiky."*[284] Patrné je navázání na koncepty informační společnosti a bezpečnosti EU.[285] Strategie formuluje snahy vlády ČR zavést cíle a směr informační bezpečnosti do praxe.

---

[281] *Information Security*. In: BusinessDictionary.com, http://www.businessdictionary.com/definition/information-security.html (20. září 2009)
[282] JAŠEK, Roman: c.d., s. 10.
[283] Tamtéž, 9.
[284] *Národní strategie informační bezpečnosti ČR.* In: Archiv stránek bývalého Ministerstva informatiky, http://web.mvcr.cz/archiv2008/micr/scripts/detail.php_id_2705.html (9. září 2009), s. 3.
[285] Viz níže kapitola 2.4. EU a její pojetí informační a kybernetické bezpečnosti.

Strategie vytváří společnou platformu pro zabezpečení informací veřejné správy, subjektů komerční i nekomerční sféry a jednotlivých občanů.

NSIB byla vypracována na základě úkolu stanoveném v dokumentu *e-Česko 2006*[286] a rozpracovává *Bezpečnostní strategii ČR*[287] z roku 2003 pro oblast informačních sítí a systémů. Je také národním naplněním směrnice OECD pro bezpečnost informačních systémů a sítí[288] přijaté 25. července 2002. Stanovuje šest základních priorit, strategických cílů a účelů.[289]

NSIB doplňují dvě přílohy.[290] První se věnuje řízení informační bezpečnosti v rámci orgánů státu a veřejné správy a přiřazuje jim patřičné kompetence. K hlavním cílům rozvíjení informační bezpečnosti má být osvojení dobré praxe při zpracování informací a nastavení přiměřené základní úrovně bezpečnosti, dále pak zabezpečení vysoké úrovně informační bezpečnosti u kritických činností zaručující zpracování informací za mimořádných podmínek. Důležité je také angažování pracovníků orgánů veřejné moci k uvědomělé podpoře budování důvěryhodných informačních systémů, prosazování etického chování při užití, provozování a správě informačních a komunikačních systémů a konečně je třeba podpora aplikací nových zabezpečovacích prostředků.[291]

Druhá příloha pak předkládá přehled právních předpisů a norem týkajících se informační bezpečnosti. Dává také doporučení pro její řízení a

[286] Viz výše Kapitola 1. 2. Rozvoj e-governmentu v ČR.
[287] *Bezpečnostní strategie České republiky*. Praha 2003. In: Ministerstvo zahraničních věcí ČR, http://www.mzv.cz/jnp/cz/zahranicni_vztahy/bezpecnostni_politika/bezpecnostni_strategie_ceske_republiky.html (10. listopadu 2009); srov. *Bezpečnostní strategie České republiky*. Praha 2003. In: idnes.cz, http://data.idnes.cz/soubory/prk-fakta/A080313_R00_BEZPECNOSTNI_STRATEGIE_CR.PDF (10. listopadu 2009).
[288] *Směrnice OECD pro bezpečnost informačních systémů a sítí. Směrem ke kultuře bezpečnosti.* In: Archiv stránek bývalého Ministerstva informatiky, http://web.mvcr.cz/archiv2008/micr/images/dokumenty/cz_security_guidelines_4_3__03.pdf (19. září 2009)
[289] Jsou to 1. zlepšení řízení informační bezpečnosti a řízení rizik, 2. rozvoj znalostí o informační bezpečnosti, 3. podpora národní a mezinárodní spolupráce v oblasti informační bezpečnosti, 4. podpora používání nejlepší praxe v oblasti informační bezpečnosti, 5. podpora ochrany lidských práv a svobod a 6. podpora konkurenceschopnosti české ekonomiky.
[290] Blíže viz MATES, P. – SMEJKAL, V.: c. d., s. 92-93.
[291] *Národní strategie informační bezpečnosti ČR. Příloha 1*. In: Archiv stránek bývalého Ministerstva informatika, http://web.mvcr.cz/archiv2008/micr/scripts/detail.php_id_2705.html (19 . září 2009), s. 2.

stanovuje její obecné zásady, postupy spravování a typy bezpečnostní dokumentace.[292]

NSIB předpokládala také založení Výboru pro informační bezpečnost ČR, jehož účelem má být koordinace, vývoj, realizace vyhodnocování cílů NSIB. Vymezen byl také jako poradní orgán ministra informatiky. Zastoupení v něm měly mít všechno orgány státní správy nějakým způsobem zodpovědné za naplňování NSIB.[293]

2.2. 1. Hrozby informační bezpečnosti

Bezpečnost informací uložených a spravovaných v daném informačním systému může být ohrožená nejen neadekvátním nakládáním s informacemi, ale také zvenčí, resp. proniknutím do informačního systému skrze škodlivý software (tzv. malware) nebo nabouráním se tedy hackingem. V této kapitole se budeme věnovat pojetí nástrojů a aspektů těchto hrozeb.

Hrozbu lze vnímat jako jakoukoli okolnost či událost působící na zranitelnou část informačního systému, která na něm může způsobit potenciální škodu. Hrozba může mít za následek poškození informačního systému nebo i organizace spravující tento systém. Hrozby mohou být náhodné nebo úmyslné, vycházet z vnějšku i vnitřku organizace a mohou mít dočasný i trvalý charakter. Hrozby lze rozdělit na objektivní[294] a subjektivní.[295] Dále můžeme hrozby kategorizovat dle jejich působení.

---

[292] *NSIB. Příloha 2: Standardy a doporučení.* In: Archiv bývalého Ministerstva informatiky, http://web.mvcr.cz/archiv2008/micr/files/2705/06_nsib_cr_priloha_2_v0_8__2_.pdf (1. února 2009), s. 3-9.

[293] Ministerstva informatiky, vnitra, obrany, průmyslu a obchodu, školství a zdravotnictví, Národní bezpečnostní úřad, Bezpečnostní informační služba, Úřad pro zahraniční styky a informace, Policie ČR, Úřad vlády ČR, Úřad na ochranu osobních údajů, Asociace krajů ČR a Svaz měst a obcí.

První pracovní setkání výboru proběhlo 2. února 2006. (*První pracovní setkání Výboru pro informační bezpečnost ČR.* In: Ministerstvo vnitra ČR, http://web.mvcr.cz/archiv2008/micr/scripts/detail.php_id_3090.html (27. října 2009)

[294] Nezávislé na lidském faktoru. Jsou to např. přírodní katastrofy, výpadek elektrické energie, kdy je obtížné je předvídat a je tedy třeba se zaměřit na minimalizaci dopadů vhodným plánem obnovy. Dále jsou to např. elektromagnetické záření či poruchy technické a logické (porucha paměti, softwarová porucha apod.).

[295] Hrozby plynoucí z lidského faktoru. Jsou to hrozby neúmyslné, způsobené prostřednictvím např. působení neškoleného uživatele systému, nebo úmyslné, subjektivní hrozby, které jsou představovány potenciální existencí vnějších útočníků (cizí zpravodajské služby, kybernetičtí

Jedná se o přerušení, kdy je některá část systému ztracena nebo nedosažitelná, či zachycení, kdy neautorizovaný subjekt získá přístup k některým datům obsaženým v informačním systému (příkladem může být odposlech telefonické konverzace či špionážní akce skrze tzv. spyware[296]). Dalším příkladem je modifikace, tedy úmyslné změnění některých dat neautorizovanou osobou. A konečně se jedná o fabrikaci, kdy je neautorizovaně vytvořen nový, klamný objekt, o kterém uživatel nemusí vědět (např. trojský kůň). Útočník pak může provádět nekontrolované akce, které narušují informační bezpečnost počítačového systému.[297]

Jašek uvádí kategorizaci hrozeb pro informační bezpečnost na kompromitaci, nedovolenou modifikaci hodnot, destrukci části nebo celého informačního systému zneužitím citlivých informací, použití klamných dat, špatná interpretace hodnot, neoprávněný přístup k hmotným (hardware) i nehmotným (data, informace) hodnotám a únik informací (kopie, krádež, odvození apod.).[298] V oblasti bezpečnosti státu se může jednat o narušení či ohrožení základních infrastruktur a komunikačních kanálů.

Útočníky na informační systém lze klasifikovat podobně jako typy hrozeb, tedy na vnitřní (osoba připojená do vnitřní komunikační sítě organizace, tedy současný nebo bývalý zaměstnanec), vnější (osoba, která nemá přístup k vnitřní komunikační síti a musí překonávat její bezpečností aspekty). Výhodou vnějšího útočníka je jeho obtížná vystopovatelnost, neboť se díky technologii world wide web může vyskytovat kdekoli na svět. Nejnebezpečnějším útočníkem pak je „celý svět“ neboli Internet, kdy útok je veden z několika počítačů najednou (příkladem je tzv. denial-of-services, DoS). Útočníci mohou být také dle účinku svého útoku rozděleni na amatéry či náhodné útočníky, hackery, kteří usilují o prolomení

---

teroristé, hackeři, konkurenti apod.). Nicméně existují, a jsou také častější, vnitřní útoky z řad zaměstnanců organizace. Nejefektivnější je pak útok propojující vnější a vnitřní typy útočníků.
POŽÁŘ, J. a kol.: c. d., s. 23-24.

[296] Software implementovaný do systému, aby získával a shromažďoval data za účelem průmyslové, komerční, ale také vojenské špionáže, resp. kybernetické špionáže (viz níže kapitola 2.3.3.1. Kybernetická špionáž.).

[297] Hrozba plynoucí z fabrikace se vztahuje také k využití tzv. zombie počítačů. Modifikace pak je charakteristická pro tzv. defacement. (Viz níže kapitola 2.3.2. Metody kybernetických útoků)

[298] JAŠEK, R.: c.d., s. 18.

bezpečnostních opatření a dostání se k neautorizovaným datům a informacím. A konečně se jedná o profesionální kybernetické zločince, kteří mají neomezený dostatek prostředků i času k provedení útoku. Často se jedná o počítačové profesionály, což odpovídá jejich znalostní kapacitě.[299]

2.2.2. Metody zajištění informační bezpečnosti

Cílem ochrany dat a informací je, jak jsme už uvedli dříve, zajistit jejich utajení, integritu a dostupnost. Některé metody počítačové bezpečnosti se zaměřují na předcházení útoků, jiné na jejich detekování.

Bezpečnosti lze obecně dosáhnout implementací určitých pravidel, postupů, procedur, organizační struktury i programových funkcí.[300] Bezpečnostní opatření mohou být organizační i personální (např. povinnost pověřeného zaměstnance pravidelně zálohovat data, odkládat do trezoru prostředky umožňující přístup do systému apod.). Aplikovat lze také ochranu logickou, a to aplikací kryptografie neboli šifrování, či fyzickou, kdy je počítač oddělený od dostupných komunikačních prostředků a sítí.[301] Je tak tedy zabráněno napadení celého systému virem či jiným malwarem, evententuálně hackerskému útoku, tedy nabourání se do daného systému.

Pro zajištění bezpečnosti informačních systémů je pak důležité zajistit komplexnost a provázanost jednotlivých opatření. Je nutná spolupráce informační bezpečnosti s personální, majetkovou, fyzickou i administrativní bezpečností. Zajištění bezpečnosti pak probíhá zejména prostřednictvím autorizovaného přístupu do systému, vytvářením záloh, instalací antivirových programů apod. Informační bezpečnost je tedy odpovědnost za ochranu informací při jejich vzniku, zpracování, ukládání,

[299] POŽÁR, J. a kol.: c. d., s. 39-41.
Motivaci útoků skrze Internet a proti informačním systémům se budeme věnovat v kapitole 2.3.1. Motivace k útokům v kybernetickém prostoru.
[300] Např. v případě elektronické spisové služby je užito autorizovaného přístupu k datovým souborům a dokumentům pouze určité skupině osob s přístupovým právem. (ŠTĚDROŇ, B.: c.d., s. 90.)
[301] ŠTĚDROŇ, B.: c.d., s. 43.

přenosu i likvidaci.[302] Při přenosu dat se jako jediná možná a efektivní možnost ochrany dat jeví logická ochrana, tedy šifrování.[303] Za použití této metody nejsou data pomocí běžných prostředků čitelná. Pro zajištění integrity je zde třeba vytvořit speciální protokol pro výměnu informací.[304]

Ochrana informací je možná také skrze softwarové a hardwarové kontroly.[305] Hardwarová bezpečnost informačních systémů je založená na omezení, resp. umožnění přístupu do systému konkrétním osobám na základě užití identifikačních karet či biometrických systémů.[306] Stěžejním aspektem ochrany informačních systémů je také již výše zmiňovaná, efektivní a pochopitelná bezpečnostní politika.[307]

Dále lze bezpečnost informačního systému chránit také za pomocí počítačových programů, které jsou zaměřeny proti jiným aplikačním programům schopným poškodit či zcela zničit obsažená data, omezit, až vyloučit funkčnost systému či kompromitovat utajované informace.[308] Jako jednoduchý příklad zde poslouží tzv. počítačové viry a antivirové programy.[309]

V oblasti softwarové ochrany bychom ještě rádi uvedli příklad tzv. *spolehlivého softwaru*. Je to takový software, kterému jeho uživatel věří a o němž je přesvědčen, že je funkčně korektní, což „vynucuje“ také u aplikací, které sám spouští. Příkladem spolehlivého softwaru je operační systém. Takový software disponuje také omezenými právy. Kontroluje a minimalizuje tak přístup k datovým fondům jiných, nespolehlivých programů. Omezuje také přístupy jednotlivých uživatelů k systému. Děje se tak hlavně skrze užití hesla.[310]

V souvislosti s riziky e-governmentu je třeba také uvést otázku ochrany osobních údajů. Díky modernějším a sofistikovanějším

---

[302] POŽÁR, J. a kol.: c.d., s. 20-21.
[303] Blíže k metodám šifrování viz Tamtéž, s. 43-46.; srov. POŽÁR, J.: c.d., kap. 14.
[304] Příkladem může být elektronický podpis. (Viz výše kapitola 1.5.1. Elektronický podpis) POŽÁR, J.: c.d., s. 119.
K problematice kryptografie a kryptologie viz také JAŠEK, R.: c.d., kap. 2; POŽÁR, J.: c.d., kap.14.
[305] POŽÁR, J.: c.d., s. 119-120.
[306] Blíže k problematice hardwarové ochrany viz Tamtéž, s. 121-129.
[307] Tamtéž,s. 120.
[308] Tamtéž, s. 130.
[309] Problematika počítačových virů a jiných škodlivých kódů je analyzována např. Tamtéž, kap. 15.
[310] Blíže viz Tamtéž, s. 136-138.

technologiím lze schraňovat obrovské množství údajů. Tato skutečnost je zejména typická pro moderní státy charakteristické shromažďováním velkých objemů dat o svých občanech. S těmito daty je pak různě nakládáno v souladu s potřebami státní správy zajistit fungování svého mocenského aparátu, ale také dostatečně zabezpečit sociální systém apod. Je tedy nezbytné způsoby a rozsah sbírání a spravování různých dat (zejména osobních údajů občanů[311]) státem ošetřit vhodnou právní normou. V ČR platí zákon č. 101/2000 Sb., o ochraně osobních údajů.[312]

Správce osobního údajů (v tomto případě orgán státní správy) musí s těmito údaji nakládat v souladu s tímto zákonem. Ke správě mu musejí být poskytnuty pouze se souhlasem osoby, které se týkají. Bez tohoto souhlasu lze s osobními údaji pracovat jen v případě povinnosti plynoucí ze zákona, ze smlouvy či jedná-li se o údaje zveřejněné dle zvláštních právních předpisů (např. obchodní nebo živnostenský rejstřík). Zamezit možnému zneužití osobních údajů má jejich zpracovatel. [313]

V problematice zajištění žádoucí míry informační bezpečnosti je také využíváno praxe tzv. auditů. Auditem informačního systému rozumíme analýzu informačního systému, *„jejímž cílem je posoudit, zda je systém ve shodě se stanovenými požadavky (uživatelskými, legislativními, kvalitativními, bezpečnostními, normalizačními apod.). Audit provádí nezávislá autorizovaná osoba nebo instituce, která nemá přímou odpovědnost za funkce prověřovaného systému…* (Dále se může jednat o…) *záznam událostí a činností vykonaných uživatelem nebo jeho jménem, důležitých z hlediska bezpečnosti informačního systému (tzv. bezpečnostní audit). Spolu s identifikací a autentizací slouží k určení*

[311] Osobní údaje jsou informace o osobě, na jejichž základě tuto osobu můžeme jednoznačně identifikovat. Může se jednat o rodné číslo či adresa, nepředpokládáme-li, že v daném domě nebydlí dva lidé stejného jména. (LIDÍNSKÝ, V. a kol.: c. d., s. 32)

[312] Vychází z mezinárodních úmluv a právních dokumentů – Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. In : OECD, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (20. října 2009) a Směrnice EP s Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volným pohybem těchto údajů (*Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data*. In: Portál EU, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (20. října 2009)

[313] LIDÍNSKÝ, V. a kol.: c. d., s. 33-34.

zodpovědnosti při vyšetřování bezpečnostních incidentů."[314] Audit informačních systémů často provádí nezávislá instituce. Je tak využíváno služeb soukromých auditorských firem.

Podobná situace je také v oblasti zajišťování bezpečnosti ISVS. Orgány veřejné správy jsou v důsledku expertní náročnosti a kapacity nuceny najímat soukromé subjekty k zajištění informační bezpečnosti svých systémů.[315] Důvodem tzv. outsourcingu, tedy najímání externí organizace pro zajištění určité části činnosti firmy či instituce za účelem snížení nákladů,[316] jsou zejména mzdové otázky.[317] Je však třeba dbát na náležitou důvěryhodnost poskytovatele služeb informační bezpečnosti. V ČR vznikl také Český institut manažerů informační bezpečnosti, jehož cílem je zejména propagace a rozvoj odborné praxe manažerů informační bezpečnosti skrze výměnu zkušeností, pravidelná školení a publikační činnost.[318]

2.3. Zneužití ICT prostředků k útokům proti státu

Útoky proti státu skrze zneužití vyspělých prostředků ICT, které post-moderní společnost současnosti téměř neustále využívá, jsou vedeny v rámci tzv. kybernetického prostoru (cyberspace). Tento výraz poprvé uvedl spisovatel W. Gibson ve své knize *Neuromancer* v roce 1984.[319] Jeho popis kybernetického prostoru pojmenovává novou úroveň vývoje lidské

[314] *Audit informačního systému*. In: Vydavatelství VŠCHT Praha, http://vydavatelstvi.vscht.cz/knihy/uid_es-005/hesla/audit_informaCnIho_systEmu.html (4. října 2009)

[315] Přehled dodavatelů aplikací informační bezpečnosti viz *Přehled dodavatelů řešení informační bezpečnosti.* In: SystemOnLine, http://www.systemonline.cz/dodavatele-it-sluzeb-a-reseni/informacni-bezpecnost/ (4. října 2009)

[316] Definice viz např. *Outsourcing.* In: Adaptic, http://www.adaptic.cz/znalosti/slovnicek/outsourcing.htm (4. října 2009); *Co je to outsourcing a kdy jej využít*. In: ASI informační technologie, http://www.asi.cz/Podpora/OdborněčlánkyzesvětaIT/tabid/54/articleType/ArticleView/articleId/91/Co-je-to-outsourcing-a-kdy-jej-vyuzit.aspx (4. října 2009).

[317] Zaměstnání IT experta na plný úvazek se jeví jako neefektivní. (*Outsourcing bezpečnostních služeb v IT*. In: Moderní řízení, modernirizeni.ihned.cz, 12. září 2003, http://modernirizeni.ihned.cz/c4-10007700-13346250-600000_detail-outsourcing-bezpecnostnich-sluzeb-v-it (4. října 2009)

[318] Viz Český institut Manažerů informační bezpečnosti, http://www.cimib.cz.

[319] GIBSON, William: *Neuromancer.* Plzeň1998.

kultury, obchodování i technologie. Všechny tyto tři aspekty jsou zároveň spojeny v jeden.[320]

Dále se nabízejí také další vysvětlení pojmu kybernetický prostor. J. Whittaker uvádí, že se jedná spíše o sérii symbolických definicí.[321] Kybernetický prostor může být vnímán jako *„nefyzické prostředí tvořené propojenými počítači pracujícími v síti. V kybernetickém prostoru počítačoví uživatelé vzájemně komunikují podobnými způsoby jako v reálném světě, s jedinou výjimkou, kybernetické interakce nevyžadují fyzický pohyb, až na psaní.“*[322] Kybernetický prostor popisuje svět počítačů.[323] Základním předpokladem je telekomunikace čili komunikace na vzdálenost.[324] Gattiker pak kybernetickým prostorem rozumí *„paralelní vesmír vytvořený a udržovaný počítači celého světa a komunikačními technologiemi, a který je jednoduše dosažitelný skrze počítač, kabel nebo telefonní modem připojený k systému.“*[325]

Kybernetický prostor také představuje místo, kde se odehrává podstatná část lidské aktivity.[326] Lze také očekávat vzrůstající rozsah a objem lidských vztahů, ale také práce i toku peněz v rámci kybernetického prostoru. A to činí tento fenomén důležitým. Jak už jsme uvedli, v rámci kybernetického prostoru jsou aplikované prostředky ICT. Ty do určité míry přinesly společnosti zcela novou zkušenost, virtuální svět, který je celosvětový a nezná hranic. Propojují se soukromé počítače a sítě s těmi veřejnými, vojenskými i civilními.[327]

ICTs jsou v současnosti využívány v ekonomickém sektoru (např. elektronický obchod či elektronické bankovnictví), ale také ve stále větší míře ve státní správě (e-government) či vojenství. Zde elektronizace správy a komunikace nemusí znamenat jen zefektivnění a zlevnění veřejného sektoru, resp. obrany, ale také získání technologické výhody při podpoře

---

[320] GATTIKER, Urs E.: *The Internet as a Diverse Community: cultural, organizational, and political issues.* Mahwah (NJ) 2001, s. 12. (http://books.google.com) (Přeloženo autorkou)
[321] WHITTAKER, Jason: *The cyberspace handbook.* London 2004, p. 3. (http://books.google.com)
[322] *What is Cyberspace?* In: Wisegeek, http://www.wisegeek.com/what-is-cyberspace.htm. (10. září 2009) (Přeloženo autorkou)
[323] *What is cyberspace?* In: Iwebtool, http://www.iwebtool.com/what_is_cyberspace.html (10. září 2009)
[324] WHITTAKER, J.: c. d., s. 5.
[325] GATTIKER, U. E.: c. d., s. 12.
[326] Lidé se zde potkávají, pracují nebo si i hrají, učí se a objevují věci.
[327] BASTL, Martin: *Budoucnost nekonvečních forem boje.* In: Rexter, 2008, č. 2, http://www.rexter.cz/budoucnost-nekonvencnich-forem-boje/2008/11/01/ (11. září 2009)

vojenských operací, sofistikovanou výzvědnou službou či skrze rychlé a spolehlivé komunikační kanály.[328] Z vojenského hlediska znamená využití či zneužití kybernetického prostoru pro vojenský záměr či operaci možnost získání asymetrické převahy slabšího útočníka nad podstatně silnějším protihráčem.[329] Využití kybernetického prostoru v tak širokém spektru fungování společnosti rozšiřuje také možnosti, jak na i stát zaútočit a omezit je.

Důležitým aspektem použití metody kybernetického útoku je anonymita, a to díky anonymnímu charakteru moderních technologií. Je velmi komplikované až nemožné přesně určit původce konkrétního útoku v kybernetickém prostoru. [330] Hackeři zneužívají počítače po celém světě skrze aplikaci škodlivých kódů (virů apod.). Vyšetřování kybernetického útoku pak vede většinou k těmto zneužitým počítačům (tzv. zombie počítačům). Hackeři také často využívají počítačů v zemích, které nemají příliš dobré diplomatické vztahy či možnost právního vynucení a mezinárodní spolupráce s atakovaným státem. [331]

Využívání ICTs pro vojenské či útočné akce tak nabývá na reálnosti. P. D. Allen a Ch. C. Demchak ve svém článku o izraelsko-palestinském konfliktu rozebírají čtyři fáze možné kybernetické války. Za prvé bude využito *momentu překvapení a přizpůsobení*. Stát bude atakovaný kvůli zranitelnosti svých webových stránek či informačních systémů, vlastněných soukromými subjekty i veřejným sektorem. Za druhé dojde k rychlé *horizontální eskalaci*, kdy se konflikt rozšíří do další země,

---

[328] Ukazuje se také, že rozvoj informačních a komunikačních technologií vede k jejich stále většímu zapojování do moderních vojenských operací. Lze také říci, že alespoň část vojenských akcí je vedena v kybernetickém prostoru (např. kybernetická výzvědná služba, propaganda skrze kybernetický prostor či omezení až deaktivování důležitých infrastrukturních serverů). (GEERS, Kenneth: *Cyberspace and the changing nature of warfare*. In: SC Magazine, 27. srpna 2008, http://www.scmagazineus.com/Cyberspace-and-the-changing-nature-of-warfare/article/115929/ (9. září 2009)

[329] Cílem kybernetických útoků se tak často stávají vojensky nejsilnější státy světa, např. USA. Porazit jinými než asymetrickými prostředky by je bylo možné jen stěží. (Viz *Symantec Global Internet Security Threat Report. Trends for 2008.* In: Symantec, duben 2009, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf (11. září 2009)

[330] PARKER, Tom: *Cyber Adversary Characterization: auditing the hacker mind.* Rockland (MA) 2004, s. 234. (http://books.google.com)

[331] Z tohoto důvodu jsou často zneužívány počítače ze zemí tzv. Třetího světa či rozvojových zemí.

GEERS, K.: c. d.

či dokonce zemí.[332] Za třetí autoři uvádějí rychlou *nestátní internacionalizaci*, kdy útoky jsou často vedeny ze zahraničí individuálními kybernetickými útočníky. A za čtvrté bude docházet ke *globálnímu poučení a zintenzivnění rozvoje kybernetických zbraní*, což souvisí s velice rychlým pokrokem a rozvojem v oblasti ICTs.[333]

Společnost zabývající se bezpečností sítí, Cyberoam, představuje tři kroky případné úspěšné kybernetické války. Nejprve dojde k získání *kontroly nad protivníkovou sítí* s cílem zastavit, přesměrovat či znemožnit systému správně pracovat. Atakovaný pak nebude moci správně identifikovat útočníka. Za druhé bude *útok* veden *na finanční systém* za účelem jeho zhroucení. A konečně kybernetický útočník převezme *kontrolu nad národními službami* jako je energetická distribuce či telekomunikační systém. *„V okamžiku, kdy je nepřítel schopen kontrolovat národní veřejné služby, finanční a komunikační systém, stát je přemožen."*[334]

Společnost Cyberoam prezentuje také podmínky úspěšného vedení kybernetického útoku. Dochází k zacílovaní těchto útoků na specifické „oběti", ale také na jejich konkrétní slabá místa. Informace o zaměstnancích atakovaných entit jsou veřejně dostupné. Kybernetický útočník tak ví, komu má adresovat případný e-mail se škodlivým obsahem. Kybernetické útoky jsou také charakteristické svou krátkou životností a bleskovým vývojem v čase, což způsobuje obtíže v jejich vystopování i odhadu dalších útočníkových kroků. Zvýhodňují také spíše tyto útočníky, a to díky rychlému vývoji v technologiích. Kybernetická obrana stále ještě není dostatečně připravená k adekvátním reakcím na konkrétní kybernetické útoky.[335]

V souvislosti s ohrožením státu skrze zneužití kybernetického prostoru uvádíme pojem kybernetická bezpečnost. Výše uvedená

---

[332] V případě izraelsko-palestinského konfliktu jsou do určité míry zapojené také USA, jejichž stránky jsou napadány palestinskými hacktivisty. Izraelská strana se pak obrací na webové stránky v Libanonu či Íránu.

[333] ALLEN, Patrick D. – DEMCHAK, Chris C.: *The Palestinian – Israeli Cyberwar*. Military Review, březen-duben 2003, s. 54-57. (http://web.ebscohost.com)

[334] *Full Blown Cyber War: An Information Age War in the Making. Cyber War: The Third World War*. In: Cyberoam, http://newsletters.cyberoam.com/072008/images/FullBlownCyberWar.pdf (17. září 2009) (Přeloženou autorkou)

[335] Tamtéž.

informační bezpečnost je spojená s ochranou dat, informací v informačních systémech. Nicméně kybernetický útok nemusí být veden jen proti těmto systémům. Tento útok je veden za využití, resp. zneužití prostředků ICTs, tedy v kybernetickém prostoru. Může být veden proti informačním systémům, ale také proti komunikačním systémům a jiným kritickým infrastrukturám státu (např. energetická soustava, dopravní služby apod.). Kybernetickou bezpečností tedy rozumíme zajištění dostatečné bezpečnosti kybernetického prostoru a proti hrozbám v jeho rámci. Kybernetická bezpečnost může být vnímána jako rezistence vůči kybernetickým útokům.

V. Jirovský, V. Hník a O. Krulík uvádějí definici kybernetické bezpečnosti coby bezpečnostní disciplínu vztahující se na jakákoli technická zařízení pracující s daty (počítače, mobilní telefony, síťová zařízení a další hardware).[336] EU v dokumentu *eEurope 2005* kybernetickou bezpečnost vymezuje jako komunikační sítě očištěné od hackerů, virů a bezpečné tak, že bude možné vybudovat důvěru zákazníků k elektronickým platbám.[337]

2.3.1. Motivace k útokům v kybernetickém prostoru

Motivace kybernetických útoků může různá. Většina z nich je vedena za účelem dosažení ekonomického zisku.[338] Hlavním cílem tak je zneužití ICT prostředků i dat ke škodě firmy, ale také jednotlivců. My se však zaměříme na politicky motivované kybernetické útoky.

V motivaci hackerů vykonávat svou činnost můžeme v průběhu času sledovat určitý vývoj. Nejprve tzv. nabourání se do systému či komunikační sítě představovalo jakýsi internetový exhibicionismus na

[336] JIROVSKÝ, Václav – HNÍK, Václav – KRULÍK, Oldřich: *Základní definice, vztahující se k tématu kybernetických hrozeb*. In: Ministerstvo vnitra ČR, http://web.mvcr.cz/archiv2008/bezpecnost/informacni/zakladni_info.pdf (20. října 2009)

[337] *eEurope – An Information Society for All*. In: Euractive.com, http://www.euractiv.com/en/infosociety/eeurope-information-society/article-117472# (6. října 2009)

[338] MARSAN, Carolyn Duffy: *How close is World War 3.0?* Network World, 24, 27. srpna 2007, č. 33, s. 24 (http://web.ebscohost.com); *Symantec Global Internet Security Threat Report. Trends for 2008.,* s.8.

veřejnosti či alespoň v rámci hackerské komunity.[339] Tato původní hackerská motivace je stále přítomná i u současných kybernetických útoků. Jde o jakousi výzvu a dokázání, že je možné to udělat. Proto je hacking spojen zejména se skupinou mladých, talentovaných uživatelů počítačů. E. Maiwald hovoří o tzv. nezacílených hackerech (untargeted hackers).[340] Ti mohou být vedeni také záměrem vyjádřit svůj názor či ospravedlnit své počínání.[341]

Další motivací kybernetického útoku může být závist či úmysl získat něčí bohatství. To se děje zejména skrze narušení důvěrnosti a neoprávněné získání přístupu do obchodních, finančních či komunikačních sítí.[342] Rozvoj této motivace je možné sledovat s rozvojem využívání moderních ICTs pro komerční účely, zejména elektronické bankovnictví.

A konečně může mít hackerský útok původ v poškozujícím záměru (malicious intent) či vandalismu. Cílem je způsobit škody a ztráty. Jedná se často o tzv. zacílené hackery (targeted hackers). Jejich nebezpečí spočívá hlavně ve vyspělé technice, kterou užívají a disponují, a také v jednoznačně stanoveném cíli útoku.[343] V této skupině kybernetických útočníků můžeme vidět největší riziko pro bezpečnost státu.

Kybernetické útoky proti státu mohou být také zaměřeny proti jeho ekonomickým entitám a strukturám. Jejich cílem je ale omezit či zlikvidovat infrastrukturu oběti kybernetického útoku. Motivace těchto kybernetických útoků může vycházet ze všech úrovní vývoje hackerských zájmů. Jejich míra nebezpečnosti se pohybuje od nízké úrovně tzv. defacementu přes středně ohrožující bezpečnost státu charakterizované užitím metody DoS[344] dočasně paralyzující některou společnost či společnosti, část infrastruktury nebo úřad veřejné správy až

---

[339] JANOUŠEK, Michal: *Kybernetický terorismus: terorismus informační společnosti.* In: Obrana a strategie, 2006, č. 2, http://www.defenceandstrategy.eu/cs/archiv/rocnik-2006/2-2006/kyberterorismus-terorismus-informacni-spolecnosti.html (22. září 2009), s. 63.

[340] MAIWALD, Eric: *Network Security. A Beginner's Guide*. 2nd Edition. Emeryville 2003, s. 36-37. (http.//books.google.com)

[341] Blíže k vyjadřování názorů skrze hacking viz kapitola 2.3.3.3. Kybernetická propaganda a hacktivismus.

[342] MAIWALD, E.: c.d., s. 37-38.

[343] Tamtéž, s. 38.

[344] Denial-of-services, v českém překladu pak odepření služeb. Blíže viz kapitola 2.3.2. Metody kybernetických útoků.

k nejzávažnějším kybernetickým útokům proti státní ekonomice, kritické infrastruktuře či vojenským zařízením. Zde je nejčastěji užito metody distributivního DoS či škodlivého softwaru aplikovaného do napadeného informačního systému, který je schopen zničit data či systém jako celek. Útočníky mohou být nadaní individuálové, vysoce profesionalizovaní nestátní aktéři, ale také státem podporované skupiny.[345]

2.3.2. Metody kybernetických útoků

Metody pro vedení kybernetických útoků se také vyvíjí a zlepšují. Je to spojené zejména s technologickým vývojem v kybernetickém prostoru i komunikačních aplikacích.[346]

Programové nástroje kybernetických útoků vycházejí v zásadě z využití tzv. škodlivého softwaru (malwaru). Jeho hlavní podoby jsou adware,[347] spyware,[348] trojské koně[349] a viry.[350] Zmínit je třeba také využití tzv. vnitřního nepřítele (insider threat). Kybernetické útoky vedené z vnitřku napadené entity, tedy například současnými nebo bývalými zaměstnanci, tvoří přibližně 55 % současných útoků proti kybernetickým sítím.[351]

---

[345] FBI předpokládá, že více než 100 států je schopno disponovat kybernetickými ofenzivními nástroji, zejména pro kybernetickou špionáž. (HUBER, Jordana: *Cyber Attacks „Grossly Underestimated". Industries lack technology and skill to counter dangerous hackers, security expert says.* In: Financial Post, 26. června 2009, http://www.financialpost.com/m/story.html?id=1731010 (29. října 2009)

[346] Viz např. ROTSCHILD, Michael: *The Threat from within: the evolution of cyber attacks*. In: Computer Technology Review, březen-duben 2006. (http://findarticles.com)

[347] Adware je speciální programový prostředek sloužící k získávání informací a odposlouchávání na koncových bodech počítačových sítí. V ČR představuje adware nejčastěji šířený škodlivý kód. Na počítače uživatelů se většinou dostává jako součást instalace nejrůznějších zkušebních verzí programů stažených z internetu. (*Světové počítače v září nejvíce trápil červ Conficker, ty naše reklamní software.* In: ihned.cz, 9. října 2009, http://digiweb.ihned.cz/c1-38595350-svetove-pocitace-v-zari-nejvice-trapil-cerv-conficker-ty-nase-reklamni-software (9. října 2009)

[348] Spyware je speciální softwarový doplněk sloužící k tajnému zasílání uživatelových osobních dat. Původně se jednalo o nástroj využívaný v cíleném marketingu.

[349] Trojští koně jsou speciální druhy počítačových virů, které jsou schopné skrýt svou pravou identitu. Obvykle jsou to tzv. programy zadních vrátek, které jsou schopné spustit určitou činnost v konkrétním čase a bez vědomí regulárního uživatele.

[350] Počítačové viry jsou speciální programové prostředky schopné znefunkčnit některé služby či procesy počítačové sítě.

[351] *Full Blown Cyber War: An Information Age War in the Making. Cyber War: The Third World War.*

Nejčastější technikou hacktivistů, hackerů se zájmem vyjádřit svůj postoj,[352] se stal *defacement*, tedy změnění, odstranění nebo doplnění obsahu nebo přesměrování původní webové stránky. Význam pro určité ohrožení kybernetické bezpečnosti je u této metody v možné úpravě oficiálních informací (např. úřední deska orgánu veřejné správy), které pak mohou vést k nesprávnému postupu. V případě změnění obsahu vládních či armádních komunikačních kanálů může být následkem také nesprávně vedená obranná akce.[353] Nicméně tzv. Intranet vládních i vojenských struktur je poměrně dobře chráněnou entitou a nesrovnalosti v něm je možné relativně rychle odhalit.[354]

Další častou metodou současných kybernetických útoků je tzv. *odepření služeb* (DoS) nebo také distribuovaný DoS. Server je zahlcen příliš velkým počtem žádostí o připojení, což vede k jeho kolapsu a nemožnosti správně fungovat. Útoky metodou DoS jsou vedeny pomocí tzv. botnetů neboli tisíců počítačů propojených pomocí škodlivého programu (trojský kůň apod.), které jsou na dálku kontrolovány a ovládány kybernetickým útočníkem. Jejich úkolem je opakovaně zasílat e-maily či žádat o přístup na konkrétní webovou stránku. Infikovaným počítačům se někdy také říká „zombie" počítače, jelikož jejich běžní uživatelé nemusí o jejich účasti v kybernetickém útoku ani vědět.[355]

2.3.3. Příklady kybernetických útoků proti státu

Kybernetický prostor představuje širokou škálu možností a prostředků, jak ohrozit bezpečnost státu jako celku či alespoň jeho části. Metody a motivaci útoků jsme si představili v předchozích kapitolách. V této se bude věnovat třem konkrétním příkladům, jak lze skrze kybernetický prostor ohrozit integritu státu.

---

[352] Blíže viz níže kapitola 2.3.3.3. Kybernetická propaganda a hacktivismus.
[353] GEERS, K.: c. d.
[354] *Profile of a Real Cyberware.* In: The Washington Times, 5. srpna 2009, http://www.washingtontimes.com/news/2009/aug/05/profile-of-a-real-cyberwar/ (14. září 2009)
[355] BARBER, Richard: *Hacking Techniques. The tools that hackers use, and how they are evolving to become more sophisticated.* Computer. Fraud and Security. 1. března 2003, č. 3, p. 9-10. (http://web.ebscohost.com)

2.3.3.1. Kybernetická špionáž

Kybernetická špionáž představuje rozšíření tradičního pojetí špionáže, tedy nekooperativní aktivity mezi stát, do oblasti kybernetického prostoru za využití post-moderních nástrojů ICTs.[356] Použití Internetu *„může snížit náklady a zkrátit čas sběru informací a může také zlepšit kvalitu získávaných informací."*[357] Dochází tak k zefektivnění práce rozvědky i kontrarozvědky.

Tak jak je výzvědná služba integrální částí bezpečnostních politik všech států,[358] stala se i kybernetická špionáž součástí bezpečnostních přístupů post-moderních států. Zpráva o virtuální kriminologii společnosti McAfee vydaná r. 2008[359] odhaduje, že v kybernetické špionáži je aktivních přibližně 120 států a Čína je na vedoucí pozici.[360] Americká CIA pak odhaduje, že státem sponzorovanou kybernetickou špionáží se zabývá 23 zemí s vedoucí pozicí Íránu, Sýrie a Indie.[361] Information Warfare Monitor[362] pak za lídry v oblasti kybernetické špionáže považuje USA, Velkou Británii a Izrael. Tyto země vnímají kybernetický prostor jako strategickou oblast podobně jako zemi, vzduch, moře a vesmír.[363]

Čína coby jeden z předních představitelů v této oblasti[364] využívá tzv. strategické kybernetické špionáže pro získávání informací o

---

[356] Špionáž samu o sobě lze popsat jako akt tajného sbírání informací za účelem získání určité míry výhody v soutěživém prostředí. (HASTEDT, Glenn: *Espionage: e reference handbook.* Santa Barbara 2003, s. 1. (http://books.google.com). Krejčí ji vnímá jako nekooperativní aktivitu mezi dvěma suverénními státy. (KREJČÍ, Oskar: *Mezinárodní politika.* Praha 1997, s. 272.)

[357] BONI, W. – KOWACICH, G. L.: c.d., s. X.

[358] Přehled výzvědných služeb států světa viz např. stránky Federace amerických vědců (Federation of American Scientists, FAS), http://www.fas.org/irp/world/index.html.

[359] *Virtual Criminology Report – Cybercrime: The Next Wave.* In: McAfee, http://www.mcafee.com/us/research/criminology_report/default.html (14. září 2009)

[360] WALTERS, Conrad: *Cyber cold war a threat to all.* The Sydney Morning Herald, 24. prosince 2007, http://www.smh.com.au/articles/2007/12/23/1198344874193.html (5. března 2007)

[361] JONES, Andy – KOVACICH, Gerald L. – LUZWICK, Perry G.: *Global Information Warfare. How Businesses, Governments and Others Achieve Objectives and Attain Competitive Advantages*. Boca Raton 2002, s. 169. (http://books.google.com)

[362] Kanadský veřejně-soukromý výzkumný ústav tvořený Centrem pro mezinárodní studia Torontské univerzity a think tankem SecDev Group a zabývající se výzkumem kybernetického prostoru coby nové strategické domény. V nedávné době vešel Information Warfare Monitor ve známost odhalením kybernetické špionáže vedené proti tibetské komunitě v exilu. Webové stránky ústavu viz http://www.infowar-monitor.net/.

[363] *Tracking GhostNet: Investigating a Cyber Espionage Network.* In: F-Secure, http://www.f-secure.com/weblog/archives/ghostnet.pdf (21. září 2009), s. 7.

[364] Posledním velkým projevem čínské schopnosti využívat možnosti kybernetického prostoru byl špionážní atak na tibetskou komunitu odhalený na jaře 2009. (Blíže viz např. ŠTOLFOVÁ, Renata: *Contemporary Security Threats within Cyberspace. NATO and EU Approaches to Cybersecurity*. Maria Enzersdorf, AIES 2009. (Dosud nepublikovaný manuskript)

nejnovějších technologiích.[365] Cílem je dosáhnout asymetrické výhody proti vojensky silnějším protivníkům (např. USA). Čína se stala také jedním z prvních států, která začala používat tuto metodu oficiálně pro vojenské i politické cíle.[366] Čínští představitelé ohlásili vytvoření „jednotek informačního válečnictví" na 10. národně lidovém kongresu v r. 2003. Kybernetické útoky mají předcházet klasické bojové akci s cílem omezit protivníka.[367] Kybernetický prostor se stal jedním z pilířů čínské koncepce národní bezpečnosti.[368]

Kybernetická špionáž se tak stala jedním z významných aspektů státní bezpečnosti. Jednotlivé státy tedy budují jak kybernetické rozvědky, tak kontrarozvědky. Pro ukázku, USA se svými spojenci, Velkou Británií, Austrálií, Novým Zélandem a Kanadou spolupracují na projektu globálního monitorovacího a sledovacího systému s názvem Echelon.[369] Ten je schopen sledovat telefonické konverzace, e-mailové zprávy i faxovou komunikaci. V Evropě jsou za nejaktivnější v oblasti kybernetické špionáže pokládány země jako Francie, Švédsko či Německo.[370]

Kybernetická špionáž může být v zásadě dvojího typu. Prvním je tzv. obranná kybernetická špionáž zaměřená na sběr a analýzu dat o možných kybernetických útocích. Jejím cílem je také práce na vytváření účinného systému včasného varování před těmito útoky. Druhou podobou kybernetické špionáže pak je ofenzivní kybernetická výzvědná služba. Jejím cílem je zisk informací s ekonomickou, politickou, bezpečnostní či technologickou hodnotou.[371]

Malware, který se pro účely kybernetické špionáže nejčastěji používá, je spyware nebo trojský kůň (zejména tzv. zadní vrátka, jež jsou

---

[365] NAGESH, Gautham: *Latest Security Threat Lies in Trusted Software and Hardware*. In: Nextgov, http://www.nextgov.com/nextgov/ng_20080825_7185.php (18. září 2009)
[366] *Virtual Criminology Report 2007*., s. 12.
[367] MOORE, Malcolm: *China's global cyber-espionage network GhostNet penetrates 103 countries*. In: http://telegraph.co.uk, 29. března 2009, http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html (21. září 2009)
[368] *Tracking GhostNet: Investigating a Cyber Espionage Network.*, s. 7
[369] Viz *Echelon.* In: Federation of American Scientists (FAS), http://www.fas.org/irp/program/process/echelon.htm (23. září 2009)
[370] JONES, A. – KOVACICH, G. L. – LUZWICK, P. G.: c.d., s. 4.
[371] DANCHEV, Dancho: *Cyber Intelligence – CYBERINT*. In: Dancho Danchev' s Blog, http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html (18. září 2009)

vytvářena spolu s oficiálním programem, aby byla později zneužita k jeho napadení).

Kybernetickou špionáž můžeme zaznamenat také v soukromém sektoru, kde se jedná zejména o tzv. průmyslovou špionáž.[372] V oblasti kybernetické špionáže na osobní úrovni se jedná o tzv. phishing, kdy jsou sofistikovanou a psychologickou metodou získávána citlivá data uživatele.

2.3.3.2. Kybernetický terorismus

Kybernetické útoky lze vnímat jako příklad nekonvenční a asymetricky vedené války či konfliktu. Toto uchopení kybernetických hrozeb může vést k paralele s terorismem. Ucelená a obecně přijímaná definice tohoto jevu v současnosti neexistuje.[373] EU nicméně usiluje o sjednocení pojetí terorismu napříč svými členskými státy. Jednotná definice by pak měla obsahovat objektivní (seznam vážných ohrožení) a subjektivní (akty považované za teroristické, úmyslně páchané s teroristickým záměrem) složky.[374] OSN dosud nevyvinula žádnou definici terorismu,[375] podobně jako NATO.

Někteří autoři či jiné instituce však vymezení pojmu terorismus nabízejí.[376] Americké ministerstvo obrany například terorismus definuje jako *„záměrné užití bezprávného násilí či hrozby s cílem vyvolat strach.“*[377] Jeho cílem je přesvědčit vládu či společnost následovat určité myšlenky či zájmy, které mohou být politické, náboženské i ideologické.

Pro účely této práce bychom zdůraznili vyvolání strachu a vliv na morálku obyvatelstva, který teroristický čin způsobuje. Kybernetický prostor totiž poskytuje ideální možnosti pro zneužití vysoké závislosti

---

[372] HINES, Matt: *Cyber-espionage moves into B2B.* In: InfoWorld, http://www.infoworld.com/t/business/cyber-espionage-moves-b2b-546 (15. září 2009)

[373] BASTL, Martin: c.d.

[374] *European Union plugging the gaps in the fight against terrorism.* In: European Commission, Justice and Home Affairs, http://ec.europa.eu/justice_home/fsj/criminal/terrorism/fsj_criminal_terrorism_en.htm (22. září 2009)

[375] Viz *There Is No UN Definition on Terrorism*. In: Eye on the UN, http://www.eyeontheun.org/facts.asp?1=1&p=61 (22. září 2009)

[376] Viz např. BASTL, M.: c.d. Autor v tomto článku nabízí poměrně širokou škálu uchopení pojmu terorismu.

[377] *Department of Defence Dictionary of Military Terms.* Washington D.C. 2001, s. 452-453.

společnosti na ICTs a Internetu s cílem psychologicky působit na občany. Kybernetické útoky na strategické infrastruktury mohou způsobit dalekosáhlé škody srovnatelné s tradičním teroristickým útokem. Užití virtuálního světa kybernetického prostoru eliminuje riziko teroristů odhalení, ale také jejich fyzických ztrát.[378]

Vymezení pojmu kybernetický terorismus již tolik komplikací nezpůsobuje a jeho uchopení je předkládáno více zdroji. NATO definuje kybernetický terorismus jako *„kybernetický útok užívající či zneužívající počítač nebo komunikační sítě za účelem způsobení dostatečné škody s cílem zastrašit společnost a mající ideologický podtext.“*[379] Americké ministerstvo vnitra uvádí vysvětlení kybernetického terorismu coby kriminálního aktu vedeného za pomocí počítače nebo telekomunikačních prostředků. Cílem je pak způsobit zmatek a nejistotu za účelem ovlivnit vládu či populaci k přijetí určitých politických, ideologických či sociálních témat.[380] Americká FBI pak tento jev vnímá jako *„politicky motivovaný útok na informační a počítačové systémy, počítačové programy a data.“*[381] Centrum pro strategická a bezpečnostní studia[382] podává vysvětlení kybernetického terorismu coby *„užití nástrojů počítačové sítě s cílem vyřadit národní infrastrukturu či zastrašit vládu i civilní obyvatelstvo.“*[383] V případě napadení kritických infrastruktur, jako např. bank, energetické sítě apod. může způsobit ohromné ekonomické škody. Útok na obranné struktury a sítě spojený s následným fyzickým útokem pak může způsobit škody srovnatelné s válečným stavem. Kybernetický terorismus je považován za tzv. neletální typ teroristické akce.[384]

M. Janoušek ve svém textu rozlišuje dvě základní formy kybernetického terorismu. První je čistě propagační či informační související s vyjádřením negativního postoje či odmítavou reakcí na konkrétní mezinárodní či národní dění skrze využití možností, jež skýtá

[378] EVERARD, Paul: *NATO and Cyber Terrorism*. In: *Response to Cyber Terrorism*. Amsterdam 2008 (http://books.google.com) , s. 118-119.
[379] EVERARD, P.: c.d., s. 119. (Přeloženo autorkou.)
[380] Tamtéž, s. 119.
[381] Tamtéž, s. 119. (Přeloženo autorkou.)
[382] Webová stránka: http://www.cbss.cz/
[383] EVERARD, P.: c.d., s. 119. (Přeloženo autorkou.)
[384] JANOUŠEK, M.: c.d., s. 60.

kybernetický prostor.[385] Daleko závažnější a nebezpečnější je pak vedení kybernetického teroristického útoku proti informačním sítím s cílem jejich likvidace. Zde se však kybernetický terorista vystavuje dalšímu riziku, kdy si de facto zničí vlastní operační prostor. Na druhou stranu však získá informační převahu a maximální informační vítězství, kdy je atakovaný dezorientovaný a nemůže reagovat na případné další útoky na jiných místech. Teroristické skupiny také mohou využívat kybernetického prostoru pro kontakt se svými členy, často lokalizovanými po celém světě.[386]

2.3.3.3. Kybernetická propaganda a hacktivismus

Většina politicky motivovaných kybernetických útoků je vedena za účelem vyjádření deziluze či nesouhlasu se současným národním nebo mezinárodním děním. V tomto případě hovoříme spíše o politicky motivovaném hackování neboli hacktivismu.[387] V jeho pojetí je Internet nejen prostor pro komunikaci, ale také nástroj pro akci (např. politickou).

Jeho rozmach přišel v druhé polovině 90. let minulého století, kdy za první rok skutečného hacktivismu je označován r. 1998. Od té doby začal počet kybernetických útoků významně růst. [388] Je to dané mimo jiné také technologickým rozvojem i rozšiřováním dostupnosti Internetu.

---

[385] Nicméně tento jev spíše odpovídá charakteristice tzv. hacktivismu.

[386] JANOUŠEK, M.: c.d., s. 61-62.

[387] Studii o hacktivismu coby snoubení klasického hackingu a politického aktivismu předkládá A. W. Samuel ve své disertační práci. (Viz SAMUEL, Alexandra Whitney: *Hacktivism and the Future of Political Participation*. Harvard University Cambridge, Massachusetts 2004. (Dostupné na: http://www.alexandrasamuel.com/dissertation/pdfs/index.html))

[388] Viz např. BARBER, Richard: *Hackers Profiled – Who Are They and What Are Their Motivations?* In: Computer Fraud and Security, 2001, únor 2001, č. 2. (http:// web.ebscohost.com), s. 15.

Příkladem první aplikace kybernetických útoků v konfliktu dvou států může být situace mezi Indií a Pákistánem v r. 1998 *(Cyber Wars between Pakistan and India.* In: Articlebase, http://www.articlesbase.com/internet-articles/cyber-wars-between-pakistan-and-india-373872.html (14. září 2009). USA byly překvapeny útokem náctiletého hackera na národní počítačové monitorovací centrum vzdušných sil v únoru 1998. (*U.S. Studies a New Threat: Cyber Attack.* In: Washington Post, 24. května 1998, http://www.washingtonpost.com/wp-srv/washtech/daily/may98/cyberattack052498.htm (14. září 2009), p. A01.). Hacktivisté před švédskými parlamentními volbami v září 1998 napadli webové stránky švédské umírněné strany a přesměrovali je na pornografické stránky, nebo na stránky levicové strany. CURRAN, Kevin – CONCANNON, Kevin – McKEEVER, Sean: *Cyber Terrorism Attacks.* In: Igi Global, http://www.igi-global.com/downloads/excerpts/reference/IGR4726_WbOBBAVgQ2.pdf (14. září 2009), s. 3.

Od r. 1998 se hacktivismus rozšířil jak geograficky, tak i tematicky. Příklad vedení části konfliktu v kybernetickém prostoru je možné vidět v rámci izraelsko-palestinského konfliktu. Také během války na Balkáně v druhé polovině 90. let bylo možné sledovat aktivitu srbských hacktivistů, kteří provedli tzv. defacement a na asi 50 různých webových stránkách se objevil vzkaz „Kosovo je Srbsko." V nedávné době jsme byli svědky dosud asi nejvážnějšího kybernetického útoku s prvky hacktivismu, a to v srdci evropské integrace i NATO, v Estonsku na jaře 2007.[389]

Během bleskové války mezi Ruskem a Gruzií v srpnu 2008 bylo z ruské strany také použito nástrojů vedení kybernetického boje. Hacktivisté morálně podporovaní ruskými oficiálními kruhy pronikli na gruzínské vládní stránky i servery některých částí důležité infrastruktury. Bylo použito zejména nástrojů defacementu, kybernetické propagandy a DoS.[390] Je zde také možné sledovat nový trend ve vedení války, kdy jsou využívány možnosti kybernetického prostoru k podpoře klasických vojenských operací. Další novou charakteristikou vedení boje také může být zapojení civilistů, patrioticky laděných občanů vykonávajících tyto kybernetické útoky.[391]

Nejčastěji užívanou metodou je pro hacktivisty defacement. Dopad na státní bezpečnost není zásadní. Nicméně je třeba zdůraznit jeho vliv na psychiku a morálku společnosti. Hackeři také nepozorovaně vstupují do domácností lidí a mohou tak ovlivňovat jejich názory. Může zde být použita paralela s politickou či ideologickou reklamou či kampaní. Hacktivisté se snaží prezentovat sebe a své postoje.

---

[389] Na přelomu dubna a května 2007 byla estonská elektronická komunikační síť narušena koordinovaným kybernetickým útokem. Cílem se staly vládní servery, ale také webové stránky politických stran, finančních institucí a médií. Pro útoky byl použit zejména tzv. distributivní DoS, ale také defacement. Kybernetické útoky byly reakcí na přesun pomníku Rudé armády z centra Tallinnu. Útoky byly vedeny Kremlem podporovanou skupinou Naši. (Blíže k tématu viz ŠTOLFOVÁ, R.: c.d.

[390] KREBS, Brian: *Report: Russian Hacker Forums Fueled Georgia Cyber Attacks.* In: The Washington Post, 16. října 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html (15th September 2009); MESERVE, Jeanne: Study Warns of Cyberwarfare during Military Conflicts. In: www.cnn.com/US, 17. srpna 2009, http://www.cnn.com/2009/US/08/17/cyber.warfare/index.html (15th September 2009).

[391] Podobnou situaci je možné sledovat v rámci palestinsko-izraelského konfliktu. Hacktivisté na obou stranách jsou podporováni k vedení kybernetických útoků (hlavně defacementu či DoS) proti druhé straně. (Viz ŠTOLFOVÁ, R.: c.d.)

Hacktivismus můžeme vztáhnout k fenoménu tzv. kybernetické propagandy, tedy rozšíření tradičního jevu propagandy do kybernetického prostoru. Kybernetická propaganda se stala součástí současných konfliktů podobně, jako se její klasická předchůdkyně zapojila do konfliktů a válek v průběhu historie. Jako nástroj ovlivňování protivníkovy morálky je užíváno post-moderních nástrojů komunikace široce rozšířených v populaci. Internet nabízí poměrně rychlou a levnou možnost jak šířit názory a působit na širokou skupinu lidí. Dopad propagandy může být různý, od jednoduchého vyjádření postoje bez zásadnější reakce veřejnosti k významným socio-politickým posunům.[392]

2.4. EU a její pojetí kybernetické a informační bezpečnosti

Zájem EU v rámci informační, resp. kybernetické bezpečnosti byl vždy spojený s obchodními a finančními aspekty. Společenství se zaměřilo na fenomén tzv. informační společnosti[393] a její podporu a ochranu. Informační společnost je v EU vnímána jako důsledek jednotného trhu, harmonizace standardů a liberalizace telekomunikací.[394] EU se tak zaměřuje na zabezpečení komunikačních sítí spojených s nejčastějšími elektronickými styky současnosti v běžné populaci, tedy elektronické bankovnictví, elektronické obchodování, ale také e-government apod. Cílem je pak zejména předcházet velkým finančním ztrátám spojených s případnými kybernetickými útoky na tyto komunikační kanály.[395]

EU je na mezinárodním poli považována za klíčovou entitu v oblasti kybernetické bezpečnosti. Souvisí to s její přední pozicí světového ekonomického hráče a v současnosti se rozvíjejících elektronických transakcí, jež se stávají významnou charakteristikou ekonomického rozvoje post-moderní společnosti. Ve své pravomoci podporuje výzkum hodnotící

[392] Např. situace na americké politické scéně po zveřejnění obrázků z věznice Abu Ghrajb).
[393] Informační společnost je charakterizovaná vytvářením, využitím, distribucí a manipulací s informacemi coby nejvýznamnější ekonomickou, politickou a kulturní aktivitou. Základními nástroji informační společnosti jsou počítače a telekomunikační prostředky, tedy ICTs.
[394] *Regulation in the Information Society*. In: European Commission, Europe's Information Society, http://ec.europa.eu/information_society/tl/policy/regulate/index_en.htm (5. října 2009)
[395] Komisařka Reding uvádí, že měsíc dlouhé přerušení služeb Internetu v EU či USA by představovalo finanční ztrátu 150 miliard euro. (*EU Commissioner Reding Calls for Preventive Action to Make the EU Resilient against Cyber Attacks*. In: Press Releases Rapid, http://europa.eu, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/199 (10. října 2009)

různé aspekty jakési informační revoluce posledních let a její dopad na současnou společnost, vzdělanost, obchodování i komunikaci.[396]

Výzkum v oblasti ICTs je také vnímán jako jeden z hlavních faktorů pro zajištění dostatečné míry kybernetické bezpečnosti. Výzkumem pro Komisi EU se zabývá jedno z jejích DG s názvem Joint Research Centre. To se v současnosti zaměřuje na poskytování vědecké i technické podpory pro vytváření koncepcí, zavádění a sledování konkrétních politik EU.[397] Spolu s přijetím konceptu informační či znalostní společnosti se tento fenomén stal také jednou z pracovních oblastí tohoto výzkumného centra, konkrétně jeho Institutu pro ochranu a bezpečnost občanů.[398]

Po teroristických útocích z 11. září 2001 si nejen EU intenzivněji uvědomila potřebu dostatečného zabezpečení tzv. kritických infrastruktur (energetické sítě, telekomunikace, finanční sektor apod.). *Direktiva Evropské rady o určení a tvorbě evropské kritické infrastruktury* z r. 2006 identifikuje oblast ICT jako jednu z částí těchto infrastruktur.[399] V březnu 2009 Komise navrhla přijetí politiky týkající se ochrany kritických informačních infrastruktur. Návrh zdůrazňuje principy prevence, připravenosti a uvědomění si rizik. Stanovuje také plán okamžitých akcí k posílení bezpečnosti a odolnosti kritických informačních infrastruktur.[400]

---

[396] *European Union*. In: BRUNNER, Elgin M. – SUTER, Manuel: *International CIIP Book 2008/2009*. Zurich, http://e-collection.ethbib.ethz.ch/eserv/eth:31095/eth-31095-01.pdf (8. října 2009), p. 465

[397] Joint Research Centre bylo původně založeno jako výzkumný ústav Evropského společenství pro atomovou energii (EURATOM) v r. 1957 zabývající se jádrem postupně byl záběr jeho výzkumu rozšiřován do dalších vědeckých a na politiky Společenství zaměřené oblasti . (*JRC History*. In: European Commission, Joint Research Centre, http://ec.europa.eu/dgs/jrc/index.cfm?id=2260 (7. října 2009)

[398] Institute for the Protection and Security for Citizen. V současnosti se zabývá např. projektem Ochrana a bezpečnost propojených kritických infrastruktur. (Viz *Protection and Security of Networked Critical Infrastructures (SCNI*). In: Euroepan Commission, JRC, Institute for the Protection and Security of the Citizen, http://ipsc.jrc.ec.europa.eu/showaction.php?id=22 (7. října 2009)

[399] *The European Programme for Critical Infrastructure Protection*. In: ProAdrias, http://www.proadrias.isig.it/Documenti/EPCIP%20memo.pdf (7. října 2009)

[400] Ve sdělení Komise se uvádí, že pravděpodobnost rozsáhlého kybernetického útoku na kritickou informační strukturu v následujících deseti letech je přibližně 10-20%. Ztráty v případě takového útoku by mohly činit 250 miliard USD. (*Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výbrou a Výboru regionů o ochraně kritické informační infrastruktury. Ochrana Evropy před rozsáhlými počítačovými útoky a narušení: zvyšujeme připravenost, bezpečnost a odolnost.* In: Portál EU, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:CS:PDF (10. října 2009)

Dokument Komise předkládá pět pilířů řešení bezpečnosti kritických informačních infrastruktur. Nejprve se jedná o *připravenost a prevenci*, tedy určení míry schopností národních týmů reakce na počítačovou pohotovost (Computer Emergency Response Teams, CERTs) a vytvoření jakéhosi evropského partnerství mezi veřejným a soukromým sektorem a fóra pro členské státy ke sdílení informací a tzv. dobrých praktik. Druhým pilířem je náležitá *detekce a reakce*, tedy vytvoření přiměřeného mechanismu včasného varování. Třetím základem kybernetické bezpečnosti má být *zmírňování a obnova* skrze posilování obranných mechanismů EU v oblasti kritických informačních infrastruktur. Předposledním krokem je podpora *mezinárodní spolupráce* mezi členy EU i vně. A konečně mají být stanovena *kritéria pro odvětví kritických informačních infrastruktur*.[401]

Na přelomu milénia jsme mohli být svědky několika iniciativ EU zaměřených na využití ICTs pro rozvoj evropské společnosti i ekonomické síly. Jednalo se o iniciativy nesoucí název *eEurope*.[402] Otázkám kybernetické bezpečnosti se věnovala *eEurope 2005* z června 2002. Tato iniciativa mimo jiné také navrhovala zřízení jednotek pro kybernetickou bezpečnost (Cyber Security Task Force), které by byly podporovány jak veřejným, tak také soukromým sektorem, tedy firmami.

Je zde také uvedena myšlenka *„kultury kybernetické bezpečnosti"*.[403] Všichni, kteří využívají možností kybernetického prostoru, si mají uvědomit rizika plynoucí z užívání tohoto média. Je třeba přijmout jakýsi závazek zodpovědnosti. Iniciativa se obrací na soukromé firmy a společnosti s významným ekonomickým vlivem ve státech, aby se podílely na vytvoření pravidel dobré praxe v užívání ICTs. Nicméně pozornost je věnována také jednotlivcům, občanům, kdy jejich uvědomění si hrozeb bude vycházet z různých dalších projektů EU.

---

[401] *Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výbrou a Výboru regionů o ochraně kritické informační infrastruktury. Ochrana Evropy před rozsáhlými počítačovými útoky a narušení: zvyšujeme připravenost, bezpečnost a odolnost.*, s. 7-11.

[402] Viz výše kapitola 1.3. Působení EU na rozvoj e-governmentu v ČR. *eEurope, eEurope 2002, eEurope 2005, i2010*, pro kandidátské země pak *eEurope+*.

[403] *eEurope 2005: An Information Society for All.* In: European Commission, Europe's Information Society, http://ec.europa.eu/information_society/eeurope/2002/news_library/documents/eeurope2005/eeurope2005_en.pdf (7. října 2009), s. 16.

Současným podkladem přístupu Společenství k informační společnosti i kybernetické bezpečnosti je iniciativa *i2010*. Ta se coby součást Lisabonské strategie zaměřuje zejména na ekonomický růst plynoucí z rozmanitějšího využívání ICTs. Otázky kybernetické bezpečnosti jsou v dokumentu zmíněny spíše okrajově. Samozřejmě povědomí o rizicích plynoucích z možného zneužití post-moderních ICTs bylo přítomno. Nicméně pozitivní aspekty jejich zapojování převážily. EU v dokumentu spíše přistupuje k doporučení členským státům přijímat ochranné prostředky a podmínky zabezpečení svých komunikačních sítí. Je zde opět zdůrazněna spolupráce a sdílení zkušeností v oblasti kybernetické bezpečnosti.

i2010 zmiňuje bezpečnost konkrétněji v pasáži o jednotném evropském informačním prostoru. Cílem je posílit a podpořit bezpečnou a spolehlivou internetovou komunikaci, a zvýšit tak důvěru mezi investory, společnostmi a zákazníky. *i2010* také navrhla, aby Komise vypracovala *Strategii pro bezpečnou informační společnost* s důrazem na růst obeznámenosti veřejnosti o možných kybernetických hrozbách a přístupu k nim.[404]

Strategie pro bezpečnou informační společnost byla Komisí přijata v květnu 2006. Nese podtitul *Dialog, partnerství a posílení*. Základním cílem je zde zajistit pro EU dostupné, bezpečné a spolehlivé komunikační sítě k podpoře evropské ekonomiky i kultury. Dokument jmenuje základní výzvy, kterým informační společnost v současnosti čelí a nabízí také řešení.

Je to *vzrůstající finanční motivace kybernetických útočníků*, tedy zcizení citlivý dat pro neoprávněné finanční obohacení (např. phishing, spyware apod.). Rozšířenější *používání mobilních komunikačních prostředků* (zejména mobilních telefonů využívajících technologii 3G) bude znamenat rozšíření možnosti kybernetických útoků i proti nim. *Nástroje ICT se staly nedělitelnou součástí evropského ekonomického rozvoje*, stejně jako podmínkou správného fungování klíčových

[404] *i2010. An European Information Society for Growth and Employment*. In: Europe's Information Society, i2010 Strategy – key documents, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:EN:PDF (5. října 2009), s. 5-6.

infrastruktur v rámci EU. Nicméně Komise v textu dokumentu poukazuje na určité *podceňování rizik spojených s využíváním ICTs* ve společnosti.[405]

Do posilování bezpečnosti informační společnosti se pak musí zapojit tyto skupiny – veřejná správa, společnosti i soukromé osoby. Veřejné orgány se mají zaměřit zejména na své informační systémy a jejich zabezpečení. Nejen pro zajištění celkové bezpečnosti, ale sloužit tak také jako příklad dobré praxe. Soukromé firmy mají přijmout bezpečnost svých sítí a komunikačních sítí jako pozitivní jev a kompetitivní výhodu. A konečně individuální uživatelé mají pochopit, že jejich soukromá komunikační síť je součástí jakéhosi globálního řetězce, nebo spíše sítě, kde jsou rizika sdílena. Opět je zdůrazněna myšlenka vytvoření obecné kultury kybernetické bezpečnosti. Úspěch strategie pak má být zaručen dialogem, partnerstvím a posílením patřičných nástrojů mezi všemi zúčastněnými stranami.[406]

Strategie Komise z r. 2006 navazuje na komisní sdělení s názvem *Síťová a informační bezpečnost: Návrh evropského politického přístupu*.[407] Informační bezpečnost a bezpečnost sítí je zde popsaná *jako „schopnost sítě či informačního systému odolávat, na určité úrovni důvěry, nahodilým událostem či úmyslně škodlivým akcím.“*[408] Tyto úmyslné akce jsou popsány jako kroky omezující *„dostupnost, autenticitu, integritu a důvěryhodnost uložených či přenášených dat i připojených služeb nabízených přes tyto sítě a systémy*.“[409]

V r. 2004 EU zřídila Evropskou agenturu pro síťovou a informační bezpečnost (European Network and Information Security Agency, ENISA). Skrze toto těleso chce EU prosazovat celoevropskou spolupráci v oblasti informační bezpečnosti mezi státy i soukromým sektorem. Slouží jako

---

[405] *Strategy for a Secure Information Society. Dialogue, Partnership and Empowerment.* In: Portál EU, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:EN:PDF (10. října 2009), s. 5.
[406] Tamtéž, s. 4-6.
[407] Dokument *Síťová a informační bezpečnost: Návrh evropského politického přístupu* (Network and Information Security: Proposal for a European Policy Approach) byl vydán v r. 2001. Evropská rada ho pak přijala rezolucí v únoru 2003.
[408] *Network and Information Society: Proposal for a European Policy Approach.* In: Portál EU, http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf (6. října2009), s. 3.
[409] *Network and Information Society: Proposal for a European Policy Approach*, s. 4

nezávislé expertní středisko pro ostatní orgány EU.[410] Asistenci však poskytuje také členským státům, občanům, zákazníkům, soukromým firmám i veřejné správě.

ENISA je pověřena čtyřmi hlavními úkoly. Zaprvé je to *poradní a asistenční služba* Komisi a členským státům v oblasti zabezpečení sítí a informačních systémů a také v jejich dialogu se soukromým sektorem. Zadruhé ENISA *sbírá a analyzuje data* o bezpečnostních incidentech v Evropě. Dále *poskytuje zhodnocení bezpečnostního rizika* a možnosti jeho zvládnutí za účelem zajistit schopnost EU čelit kybernetickým hrozbám. A konečně *přispívá k rozšiřování povědomí a prohlubování spolupráce* mezi všemi hráči zainteresovanými v informační a kybernetické bezpečnosti. ENISA plní roli jakéhosi poradního vyjednávače (Advice Broker).[411] Dalšími úkoly ENISA je např. koordinace a zlepšení spolupráce mezi jednotlivými národními CERTs, stejně jako podpora jejich fungování.[412]

V prosinci 2008 vydala EU *Zprávu o implementaci Evropské bezpečnostní strategie* z roku 2003. Zpráva hodnotí a analyzuje relevanci původního dokumentu v rámci současných bezpečnostních hrozeb. Po zkušenosti s kybernetickými útoky na Estonsko na jaře 2007, ale i v Gruzii v létě 2008[413] byly tyto typy útoků zahrnuty do bezpečnostních hrozeb současné EU a moderní společnosti. Moderní ICTs se mohou stát *„potenciální novou ekonomickou, politickou i vojenskou zbraní."*[414] Současné ekonomiky jsou významně závislé na kritických infrastrukturách, jejichž jednou podobou je také Internet. Je tedy třeba přijmout patřičná bezpečnostní opatření k jejich ochraně. Zpráva nicméně nepředkládá možnosti či kroky jak kybernetickým hrozbám předcházet a jak je dále řešit. Je v ní jen uvedeno, že je potřeba další práce vedoucí vytvoření

[410] Např. Komisi poskytuje technický základ pro vyvíjení či revizi komunitní legislativy v oblasti informační bezpečnosti.
[411] *Activities*. In: ENISA, http://www.enisa.europa.eu/about-enisa/activities (8. října 2009)
[412] *CERT*. In: ENISA, http://www.enisa.europa.eu/act/cert (8. října 2009)
[413] Během gruzínsko-ruské války v srpnu 2008 byla využita také metoda tzv. hacktivismu, kdy pro-ruští hacktivisté využili defacemenet a DoS při kybernetických útocích na některé gruzínské webové stránky a servery (zejména oficiální vládní stránky, mediální servery apod.). (Viz kapitola 2.3.3.3 Kybernetická propaganda a hacktivismus)
[414] *Report on the Implementation of the European Security Strategy – Providing Security in a Changing World*. In: The European Council, http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf (8. října 2009), s. 5.

komplexního přístupu EU k těmto výzvám. Opět je zdůrazněno rozšiřování povědomí o kybernetických rizicích a mezinárodní spolupráce.[415]

EU jako celek si uvědomuje potřebu dále prohlubovat koordinaci národních přístupů ke kybernetické bezpečnosti. Členské státy jsou zodpovědné za vytváření vlastních politik pro zabezpečení kritických informačních infrastruktur.[416]

V souvislosti s postupným vypršením platnosti iniciativy *i2010* současné švédské předsednictví EU[417] vydalo v září 2009 dokument s názvem *Zelená vzdělanostní společnost (A Green Knowledge Society)*. Stěžejní myšlenkou je zde podpora vytvoření tzv. vědomostní společnosti[418] skrze využívání soudobých ICTs. Dokument reviduje předešlou iniciativu a poukazuje na nové výzvy a rizika bezpečného digitálního světa současnosti. Důraz je pak kladen opět na ochranu kritických infrastruktur, růst povědomí veřejnosti o rizicích a spolupráce v rámci EU.[419]

V dubnu 2009 komisařka V. Reding navrhla vytvoření orgánu EU pro kybernetickou bezpečnost a obranu. V jejím pojetí je ENISA spíše „agenturou pro výměnu informací", ale ve světle nedávných i možných budoucích kybernetických útoků je potřeba nové evropské entity, která by koordinovala postupy různých skupin a vyvinula konkrétní strategii pro boj s kybernetickými hrozbami současnosti.[420] Reding také zdůrazňuje význam preventivních úkonů v rámci zajištění dostatečné bezpečnosti kybernetických sítí činěných v jednotlivých členských státech na určité jednotné rovině.

---

[415] *Report on the Implementation of the European Security Strategy – Providing Security in a Changing World.*, s. 5.

[416] Přehled přístupů jednotlivých států nejen EU k informační a kybernetické bezpečnosti viz BRUNNER, Elgin M. – SUTER, Manuel: *International CIIP Book 2008/2009. An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies.* In: Crisis and Risk Network, http://www.crn.ethz.ch/index.cfm (12. října 2009)

[417] 1. července – 31. prosince 2009.

[418] Vědomostní společnost můžeme popsat jako společnost, kde vzdělanost je základním zdrojem rozvoje.

[419] *Critical Information Infrastructure Protection – a new initiative in 2009*. In: European Commission, Europe's Information Society, http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm (7. října 2009), s. 7.

[420] *EU cyber security and defence body proposed.* In: Secpoint, http://www.secpoint.com/eu-cybersecurity-superbody-proposed.html (8. října 2009)

ZÁVĚR

V uplynulých letech jsme zaznamenali ohromné změny a pokrok ve vývoji informačních a komunikačních prostředků. Tyto ICTs se staly našimi každodenními společníky a také nepostradatelnými doplňky pro mnoho našich aktivit. Rozšířily způsoby, jak můžeme obchodovat, podnikat, být v kontaktu se svými blízkými či ovládat své finance. Moderní ICTs také otevírají nové možnosti kontaktu státní správy s občany. V demokratických společnostech můžeme pozorovat úsilí o vstřícnost a otevřenost vůči občanovi. Veřejná správa se tak snaží do určité míry usnadnit nezbytný kontakt občanů s úřady. E-government coby elektronizovaná státní správa pak může znamenat významný příspěvek k tomuto úsilí.

E-government lze vnímat nejen jako elektronickou správu, kdy dochází k zavádění post-moderních ICTs do fungování veřejné správy, ale také jako správu efektivní. Sofistikované ICTs totiž mohou ulehčit přístup občana k úřadu, ale také zpřehlednit a zjednodušit komunikaci mezi jednotlivými složkami státní moci. Vytváření centrálních registrů má vést k odstranění duplicit i omezení schraňování příliš velkého objemu dat o jednotlivých občanech, často vícekrát v databázích různých úřadů.

Internet coby v rámci praktického e-governmentu nejvyužívanější podoba současných ICTs umožňuje téměř nepřetržitý přístup občanů k informacím. Ti pak nejsou nuceni docházet na úřady příliš často, mohou svůj volný čas rozvrhnout jinak, což nemalou měrou může přispět k zlepšení jejich postoje vůči státní moci. E-government může z podobného důvodu přispět také ke zkvalitnění vztahů s firmami nezbytnými pro ekonomický rozvoj země.

V ČR je možné sledovat snahu o zavedení nástrojů e-governmentu od počátku 90. let minulého století, kdy konec totalitního režimu znamenalo také určité volání po otevřenosti státní správy a větší vstřícnosti vůči občanovi. Nicméně poslední dekáda 20. století větší pokrok v oblasti elektronizace veřejné správy nepřinesla, a to zejména z důvodu nejednotnosti postoje jednotlivých orgánů státní moci k aplikaci e-governmentu. Bylo také třeba přijmout příslušnou právní úpravu, která by umožňovala jeho rozvoj skrze vytváření a správy patřičných registrů.

Pomalý rozvoj e-governmentu je třeba také přičíst nedostatečné počítačové gramotnosti i určité nedůvěře úředníků i občanů k využívání post-moderních ICTs. Tyto problémy jsou provázané a orgány centrální správy se snaží je překonávat různými projekty a programy (např. Národní projekt počítačové gramotnosti apod.). Změna a výraznější posuny nastaly až na přelomu století, resp. v prvních letech 21. století.

Přesto byly od poloviny 90. let spouštěny projekty zlepšující přístup občanů k informacím skrze využití ICTs, zejména tedy Internetu. Jednalo se o portály ePusa, Elektronická a vlídná administrativa (EVA) či Portál veřejné správy ČR. V r. 1999 byl přijat strategický dokument s názvem *Státní informační politika – cesta k informační společnosti*, jehož hlavním cílem bylo zkvalitnění a lepší zpřístupnění vzájemné komunikace mezi státní správou a občany. O rok později pak byl zřízen Úřad pro informační systémy veřejné správy, jež měl zajišťovat naplňování Státní informační politiky a měl koordinovat vytváření a působení soustavy informačních systémů státní správy. Jeho fungování pak bylo nahrazeno v rámci působnosti Ministerstva informatiky, které však bylo později také zrušeno a jeho kompetence v oblasti e-governmentu přešly r. 2007 do rukou Ministerstva vnitra. Otázky rozvíjení a podpory informační společnosti byly převedeny na Radu pro rozvoj informační společnosti se statutem poradního orgánu vlády.

Nejvýraznější posun v rámci rozvoje e-governmentu můžeme sledovat od poloviny první dekády 21. století do současnosti. Významným dokumentem se již v r. 2004 stala *Státní informační a komunikační politika – e-Česko 2006*, kde je elektronizace státní správy vnímána jako nedělitelná součást rozšíření internetové gramotnosti mezi obyvatelstvem stejně jako zajištění dostatečného přístupu k Internetu. Od r. 2007 pak můžeme pozorovat asi nejviditelnější posuny v rozvoji nástrojů e-governmentu.

Byl spuštěn projekt CzechPOINT, kdy občan získal možnost přístupu k různým registrům jako je obchodní rejstřík, trestní rejstřík a podobně, možnost ověřit dokumenty a listiny či sledovat průběh správního řízení, stejně jako dát podnět k jeho zahájení z jednoho kontaktního místa. V nedávné době byl do plného provozu uveden systém tzv. datových

schránek, jež lze s určitou mírou nadsázky označit za revoluci v komunikaci mezi občany a veřejnou správou. Usnadňuje se tím elektronické podávání a doručování, které sice bylo umožněno již dříve prostřednictvím tzv. elektronických podatelen. Nicméně využití této možnosti doručování a podání nebylo plně využíváno v souladu s jeho záměrem, a to zejména kvůli určité nejasnosti, často až nesrozumitelnosti a také nejednotnosti v přístupu napříč veřejnou správou.

První týdny po spuštění ostrého provozu datových schránek nás vedou k v zásadě optimistickému pohledu na tento projekt. Roste počet aktivovaných datových schránek i odeslaných datových zpráv. Úspěšnost jejich doručování se pohybuje kolem 90 %. Jako jednoznačně pozitivní jev vnímáme narůstající zájem o zřízení datové schránky ze strany občanů, jež k tomuto nemají zákonnou povinnost. Právě na ně by se v souvislosti s úspěšným rozvíjením e-governmentu v ČR orgány státní správy měly zaměřit a tuto možnost komunikace s veřejnou mocí jim co nejvíce zpřístupnit, např. dostatečným internetovým připojením či náležitou propagační a informační kampaní.

V souvislosti s elektronickým podáním a komunikací je třeba také zmínit institut elektronického podpisu. Ten představoval jeden z prvních praktických nástrojů, jak elektronicky komunikovat nejen se státní správou. Nicméně jeho využití v ČR neodpovídá jeho potenciálu, což pramení z jeho charakteristiky omezené platnosti i ze skutečnosti, že vytvoření podkladů jeho náležitého užívání (zejména vytvoření potřebných certifikátů) je zpoplatněno. Z hlediska občana jako jedince se tak disponování elektronickým podpisem jeví jako neefektivní. Omezené využívání elektronického podpisu pak také souvisí s limitovaným využíváním elektronických podatelen.

Následující r. 2010 má být ve znamení realizace výstavby základních registrů státní správy. Jejich záměrem je vytvoření jednotného systému spravování dat veřejné správy ve čtyřech registrech, kdy se má zabránit zejména jejich duplikování. Tyto databáze budou zároveň spolupracovat, takže nebude třeba ze strany občana uvádět stejné informace na různých úřadech. Provázanost těchto registrů se systémem

datových schránek pak také umožní kontrolu občana, kdy a za jakým účelem bylo nakládáno s jeho údaji, které jsou v nich vedeny.

Při sledování zrychleného vývoje a přístupů k zavádění nástrojů e-governmentu v českém prostředí nemůžeme přehlédnout určitou korelaci s vývojem postojů k informační společnosti v rámci EU. Ta uznala ICTs jako hnací sílu svého ekonomického rozvoje na přelomu tisíciletí. Evropská informační společnost je vnímána jako důsledek jednotného trhu, harmonizace pravidel a liberalizace komunikačního trhu. V jejím rámci jsou zdůrazněny informace a potřeba jejich získávání i sdílení, stejně jako jejich ochrany pro rozvoj společnosti.

V rámci víry v ICTs coby základu rozvoje přijalo Společenství několik strategií a iniciativ podporující rozšíření využívání těchto prostředků veřejností. Byly vydány dokumenty *eEurope* zaměřené na dostatečné rozšíření Internetu a jeho využívání v EU, ale také v kandidátských zemích. V r. 2005 pak byla přijata iniciativa *i2010*, která je součástí tzv. Lisabonské strategie a která se zaměřila na zapojení co největšího počtu obyvatelstva do využívání post-moderních ICTs, zejména Internetu v ekonomické oblasti, ale také v komunikaci s veřejnou správou. Součástí těchto iniciativ byla podpora politik a postupů rozšiřování možností e-governmentu v členských, resp. kandidátských zemích EU.

Působení Společenství na své členy skrze výše uvedené strategické dokumenty je motivováno ideou, že evropský prostor a trh je společný pro všechny členské státy a rozvoj služeb v rámci tohoto prostoru nemá znát hranic. V tomto smyslu je zdůrazňován zejména ekonomický aspekt, tedy využívání možností elektronického nakupování či bankovnictví. Nezanedbatelný je také záměr EU zkvalitňovat životy svých „občanů“, a to v tomto ohledu skrze zlepšení fungování státní správy i komunikace s ní. Elektronizace státní správy tak má v rámci EU velkou podporu.

ČR tak svým vstupem do EU dostala jedinečnou možnost jak realizovat své plány v oblasti rozvoje e-governmentu za finanční pomoci strukturálních i komunitárních fondů Společenství. Řada projektů týkajících se efektivizace a elektronizace veřejné správy a jejího přiblížení se občanům je prováděna za výrazné podpory finančních zdrojů EU.

Tímto potvrzujeme svou první hypotézu. Zásadní rozvoj e-governmentu v ČR v první dekádě 21. století byl podpořen EU jak finančně, tak také morálně. Je třeba také zmínit vzájemné ovlivňování jednotlivých států Společenství, kdy jsou sdíleny zkušenosti členských zemí s jejich zaváděním programů e-governmentu. Nezanedbatelný vliv má také technologický rozvoj, který má tendenci se zrychlovat.

Zavádění prostředků e-governmentu je integrálně spjato s vytvářením informačních systémů obsahujících ohromná kvanta dat s různým stupněm citlivosti a utajení. Tato data je třeba chránit před jejich zneužitím, tedy je třeba zajistit dostatečnou informační bezpečnost těchto systémů. E-government tedy v zásadě představuje pozitivní využití ICTs, resp. kybernetického prostoru. Nicméně je třeba si uvědomit také rizika, jež jsou s aplikací těchto prostředků spojena.

Možnosti jak ohrozit informační bezpečnost, tedy snížit důvěryhodnost, integritu a dostupnost informací spravovaných v daném systému jsou různé. Mohou být fyzického charakteru, kdy médium nesoucí na sobě uložené informace může být fyzicky zničeno, ale také technického, kdy je kupříkladu systém infiltrován tzv. hackingem.

Tento text předložil některé přístupy k zajištění informační bezpečnosti v praxi i z teoretického hlediska. ČR od r. 2005 disponuje svou *Národní strategií informační bezpečnosti*, jež vytváří společnou platformu pro zabezpečení informací a dat veřejné správy, ale také subjektů komerční i nekomerční sféry a jednotlivých občanů. Zákon o informačních systémech veřejné správy uvádí, že za bezpečnost těchto systémů je zodpovědný jejich provozovatel, který také přijímá patřičnou bezpečnostní politiku.

Záměrem naší práce bylo, mimo jiné, poukázat na možnost zneužití ICTs proti státu a jeho integritě. Nejde tedy jen o ohrožení dat a informací vedených v informačních systémech veřejné správy, ale také o možnost zneužít určitou závislost současné společnosti na ICTs. Ty, jak už jsme uvedli, jsou nedělitelnou součástí mnoha aktivit soukromého, veřejného i obchodního života post-moderní společnosti. V rámci efektivizace státní správy jednotlivé její složky, a to včetně těch vojenských a obranných, mezi sebou komunikují skrze sofistikované komunikační

kanály. Kritická infrastruktura je řízena na základě současných ICTs. Významná část ekonomického fungování země probíhá v kybernetickém prostoru. Toto vše pak otvírá možnosti, jak státní entitu napadnout, omezit její náležité fungování či přímo hrozit její existenci.

Motivace k útokům v kybernetickém prostoru je různá. Může být ekonomická, politická, ale také náboženská či jiná. Motiv ekonomický se pak vyskytuje nejčastěji. Jedná se o různá finanční obohacení skrze proniknutí do systému elektronického bankovnictví či průmyslová špionáž a mohli bychom přidat další. Nás však předně zajímají politické stimuly kybernetických útoků.

Nejčastěji dochází k jakémusi politickému aktivismu skrze využití možností kybernetického prostoru, tedy k tzv. hacktivismu. V jeho rámci se útočník snaží vyjádřit svůj názor a postoj. Využívá různé prostředky a metody (hlavně Internetu), jak svoje vnímání situace rozšířit v co největším prostoru. Nejčastější technikou hacktivistů je pak defacement, kdy jsou oficiální stránky státní správy, ale také politických stran či firem a médií obsahově změněny či přesměrovány na jiný server.

Tato podoba kybernetických útoků v zásadě nepatří k nejzávažnějším. Nicméně může souviset s kybernetickou propagandou, a tím nežádoucně působit na morálku obyvatel. Internet také umožňuje přístup do širokého okruhu domácností, a tím pádem možnost ovlivnit vnímání či postoje velkého počtu lidí.

Spravování informací v rámci elektronických databází i elektronická komunikace dávají prostor k aplikování tzv. kybernetické špionáže. Internet také může tuto metodu výzvědné činnosti zefektivnit a zlevnit. Proto můžeme očekávat její rozšíření do praxe mnoha států, které budou disponovat patřičnou technologickou základnou. Již v současnosti jsou za nejaktivnější hráče v této oblasti považováni Číňané, Američané, ale také např. Německo či Švédsko. Nebezpečnost tohoto typu kybernetických útoků je srovnatelná s nebezpečností klasické špionáže, nicméně kybernetický prostor dává možnost zapojení většího počtu jakýchsi rozvědčíků z široké, patrioticky laděné populace disponující dostatečným technologickým vybavením, kdy často stačí jen připojení k Internetu.

Kybernetický terorismus je vnímán jako extenze klasického terorismu do prostředí kybernetického prostoru, resp. s využitím post-moderních ICTs. Cílem těchto kybernetických útoků se tak stávají kritické infrastruktury států, což může mít zásadní vliv na morálku jeho obyvatelstva, ale také na zajištění jeho správného fungování. V současnosti, kdy teroristické skupiny spíše představují globální sítě, pak kybernetický prostor dává možnost snadnější komunikace mezi jednotlivými členy i koordinace případných teroristických útoků. Nebezpečnost metody kybernetického terorismu je pak závislá na technologické vybavenosti a zručnosti dané teroristické skupiny.

V nedávné době jsme mohli být svědky několika závažných kybernetických útoků či série útoků, jež jsou obecně odborníky hodnocené jako významné pro omezení bezpečnosti státu. Na tomto místě bychom uvedli zejména kybernetické útoky proti Estonsku na jaře r. 2007 a zapojení kybernetického hacktivismu během gruzínsko-ruské války v srpnu 2008.

Estonský případ představuje první příklad dočasné paralýzy země, kdy série koordinovaných kybernetických útoků proti kritickým infrastrukturám znamenala významné omezení náležitého fungování země. Tato zkušenost otevřela debatu o možné kybernetické válce, nicméně incident samotný představuje spíše příklad tzv. hacktivismu, kdy se jednalo spíše o vyjádření nesouhlasu ruské populace žijící v Estonsku a pro-ruských aktivistů (hacktivistů) v zahraničí s přemístěním pomníku Rudé armády z centra Tallinnu. Kybernetické útoky byly ukončeny po několika dnech, resp. týdnech. Nebyly také spojeny s dalším vojenským či bezpečnost ohrožujícím aktem.

Závažnost estonského kybernetického zásahu však spočívá v tom, že stát jako entita přestal načas správně fungovat a nemohl zajistit svým občanům služby, které jim z jeho strany náleží. Možnost kybernetické války a otázky kybernetické bezpečnosti se tak staly součástí debat o současných bezpečnostních hrozbách v rámci vojensko-obranné, politické, ale i vědecké obce. Přijímání strategií ohledně zajištění dostatečné kybernetické bezpečnosti, tedy zajištění vlastního kybernetického prostoru proti jeho zneužití či napadení, tak získalo na důležitosti. Nejde již jen o

zajištění bezpečnosti informací, ale o zamezení zneužití ICTs proti bezpečnosti státu a jeho občanů.

Příklad gruzínsko-ruské války a zapojení pro-rusky orientovaných hacktivistů pak představuje možnou novou strategii ve vedení války. U konfliktů současnosti můžeme očekávat, že alespoň některá z jejich částí bude vedena v kybernetickém prostoru, který pak mimo jiné umožňuje zapojení individuálních aktivistů vedených patriotickým postojem k podpoře vojenské operace své země.

EU se v otázce kybernetické bezpečnosti tradičně zaměřuje na její finanční aspekty a dopady. Vnímání ICTs a jejich využívání k obchodování coby pozitivní příspěvek do evropského ekonomického rozvoje vede k podpoře posilování kybernetických prostorů proti zneužití zejména v oblasti tzv. kybernetické kriminality. Ve svém působení se zaměřuje na vytvoření jakési obecné *kultury kybernetické bezpečnosti*, kdy si jak státy, tak soukromé subjekty, firmy i individuální uživatelé ICTs uvědomí vzájemnou propojenost v rámci kybernetického prostoru napříč těmito sektory a že tento prostor není omezen hranicemi států.

Již teroristické útoky 11. září 2001 znamenaly přehodnocení pohledu na ochranu kritických infrastruktur, a to nejen v rámci EU. Její bezpečnostně-strategické dokumenty a iniciativy označují informační sítě jako součást těchto kritických infrastruktur, jako kritické informační infrastruktury. Na jejich zabezpečení se Společenství zaměřilo jak v oblastech svého výzkumu, tak také v rámci působení na své členské státy (např. *Strategie pro bezpečnou informační společnost* s podtitulem *Dialog, partnerství a posílení*). Podporován je zejména dialog, sdílení zkušeností a mezinárodní spolupráce v této oblasti.

Kybernetické útoky na Estonsko, pak byly jedním ze stěžejních důvodů vedoucích k přehodnocení globálních bezpečnostních hrozeb ze strany EU a kybernetická bezpečnost se stala součástí seznamu současných bezpečnostních výzev, kterým Evropa čelí. To potvrdila *Zpráva o implementaci Evropské bezpečnostní strategie* vydaná v prosinci 2008, která také poukazuje na to, že tato oblast a přístup k ní potřebuje další rozvoj a práci. Komisařka pro média a informační společnost V. Reding pak na jaře 2009 uvedla, že současná bezpečnostní situace v rámci

kybernetického prostoru potřebuje přijetí jednotného postupu a založení jakéhosi exekutivního orgánu v rámci EU, který by se věnoval zajištění kybernetické bezpečnosti ve Společenství.

Tímto potvrzujeme svou druhou hypotézu, kdy kybernetické útoky se v současnosti staly reálným ohrožením bezpečnosti státu, jak bylo možné pozorovat na příkladu Estonska. Zároveň se stávají součástí klasických vojenských operací, což se událo během gruzínsko-ruské války v srpnu 2008. Ukázali jsme si také, že EU přistupuje k těmto skutečnostem s obezřetností a kybernetickou bezpečnost přijala do svých strategicko-bezpečnostních dokumentů i aktivit. Je také možné sledovat pozitivní přístup vyspělých států k vytváření svých kyberneticko-bezpečnostních strategií.

S určitou zvědavostí pak můžeme pozorovat další vývoj přístupu EU ke kybernetické bezpečnosti své i svých členských států v souvislosti s prohlášením komisařky V. Reding z jara 2009. Postoj NATO coby vojensko-obranné entity k otázkám kybernetické bezpečnosti jsme do této práce již nezahrnuli. Nicméně věnovali jsme se jí již dříve ve studii o kybernetické bezpečnosti a přístupech NATO a EU.[421] V této diplomové práci jsme chtěli zmapovat zejména pozici EU a její působení na rozvoj politik a strategií týkajících se rozvoje ICTs i jejich neužitelnosti v jejích členských státech, ale také v rámci mezinárodní spolupráce. Postoj EU jako mezinárodního tělesa k otázkám informační a kybernetické bezpečnosti nás zajímal také z důvodu její do jisté míry v současnosti teprve se rodící obranně-bezpečnostní identity. Dalšímu bádání tak tedy přenecháváme budoucí strategické přístupy EU k problematice kybernetické bezpečnosti.

Podobně tak jsme nevyčerpali tematickou oblast e-governmentu v ČR. Návrhem pro další analýzy může být možnost elektronického hlasování a voleb (tzv. e-voting). Zajímavé jistě bude sledovat také další vývoj projektů e-governmentu, které již byly spuštěny či jejich začátek teprve očekáváme. Jedná se zejména o systém datových schránek a centrální registry státní správy. Atraktivním tématem výzkumu může být také způsob propagace e-governmentu mezi občany ze strany státu.

[421] ŠTOLFOVÁ, R.: c.d.

ANOTACE

Autor: Bc. Renata Štolfová

Název katedry a fakulty: Katedra politologie a evropských studií
Filozofická fakulta Univerzity Palackého v Olomouci

Název práce: E-government a rizika plynoucí z využívání současných ICTs ve státní správě. Rozvoj e-governmentu v ČR. Informační a kybernetická bezpečnost aneb Je třeba se obávat kybernetické války?

Vedoucí práce: Mgr. Eva Lebedová

Počet znaků: 139 283

Počet titulů použitých pramenů a literatury: 252

Klíčová slova: e-government, elektronický podpis, elektronické doručování a podání, CzechPOINT, datové schránky, informační bezpečnost, kybernetická bezpečnost, kybernetické útoky, Česká republika, Evropská unie.

Krátký popis: Práce sleduje vývoj e-governmentu v ČR od počátku 90. let do současnosti. Zájem je obrácen k vlivu EU coby významné entity stojící za zintenzivněním rozvoje elektronizace české státní právy v polovině první dekády 21. století, a to z důvodu finanční i morální podpory Společenství. Druhá část studie je věnovaná problematice informační a kybernetické bezpečnosti. Široké využití ICTs prostředků otevírá další možnost, jak společnost a stát napadnout. Příklady neužitelnosti ICTs vedou k pojetí kybernetických hrozeb coby reálných bezpečnostně-strategických výzev současnosti.

ANNOTATION

Author: Bc. Renata Štolfová

Submitted at: Department of Politics and European Studies
Philosophical Faculty, Palacky University Olomouc

Entitled: E-government and Its Risks Concerning Contemporary ICTs Use within the Public Administration. Development of E-government in the Czech Republic. Information and Cyber Security – Shall We Be Afraid of Cyberwar?

Supervised by: Mgr. Eva Lebedová

Word count: 139 283

Number of references: 252

Key words: e-government, electronic signature, electronic delivering and administrative action, CzechPOINT, data mail boxes, information security, cyber security, cyber attacks, Czech Republic, European Union.

Short description: The work is focused on e-government development in the Czech Republic from the beginning of 1990s. It follows the influence of EU on an intensification of e-government development within the Czech public administration in mid-2000s due to Community´s financial and moral support. The second part of the study is dedicated to information and cyber security. A wide range of ICTs use opens other opportunities how to attack society and state. Examples of ICTs misuse lead to accepting the cyber threats as real contemporary strategic and security challenges.

Prameny a literatura

Prameny

Bezpečnostní strategie České republiky. Praha 2003. In: Ministerstvo zahraničních věcí ČR, http://www.mzv.cz/jnp/cz/zahranicni_vztahy/bezpecnostni_politika/bezpecnostni_strategie_ceske_republiky.html (10. listopadu 2009)

Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards. In: Portál EU, http://eur-lex.europa.eu/Notice.do?val=117475:cs&lang=en&list=120608:cs,120607:cs,120606:cs,117958:cs,117475:cs,&pos=5&page=2&nbl=15&pgs=10&hwords=&checktexte=checkbox&visu=#texte (11. listopadu 2009)

Critical Information Infrastructure Protection – a new initiative in 2009. In: European Commission, Europe's Information Society, http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm (7. října 2009)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. In: Portál Evropské unie, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (20. října 2009)

eEurope 2002: An Information Society for All. In: European Commission, Europe's Information Society, Before i2010: eEurope initiative, http://ec.europa.eu/information_society/eeurope/2002/documents/archiv_eEurope2002/actionplan_en.pdf (7. října 2009)

eEurope 2005: An Information Society for All. In: European Commission, Europe's Information Society, Before i2010: eEurope initiative, http://ec.europa.eu/information_society/eeurope/2002/news_library/documents/eeurope2005/eeurope2005_en.pdf (7. října 2009)

Efektivní veřejná správa a přátelské veřejné služby. Strategie realizace Smart Administration v období 2007-2015. In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/odbor-reformy-a-regulace-kvality-verejne-spravy-smart-administration.aspx (12. září 2009)

i2010 - A European Information Society for growth and employment. In: Portál Evropské unie http://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:CS:PDF (12. srpna 2009)

Informatizace územních orgánů VS. In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/informatizace-uzemnich-organu-vs.aspx (28. října 2009)

Integrovaný operační program pro období 2007-2013. In: Ministerstvo vnitra ČR, EU, Strukturální fondy, http://www.mvcr.cz/clanek/strukturalni-fondy-integrovany-operacni-program.aspx (16. října 2009)

Měsíční monitorovací zpráva o průběhu čerpání strukturálních fondů, fondu soudržnosti a národních zdrojů v programovém období 2007-2013. Srpen 2009. In: Fondy Evropské unie, http://www.strukturalni-fondy.cz/Narodni-organ-pro-koordinaci/Dokumenty/Zpravy-2/MMZ/FileList/2009/MMZ---srpen-2009 (16. října 2009)

Ministerial Declaration. In: 4th Ministerial eGovernment Conference, http://www.egov2007.gov.pt/images/stories/ministerial_declaration_final_version_180907.pdf (22. listopadu 2009)

Ministerial Declaration on eGovernment. In: Swedish Presidency of the EU, http://www.se2009.eu/polopoly_fs/1.24306!menu/standard/file/Ministerial%20Declaration%20on%20eGovernment.pdf (21. listopadu 2009)

Národní politika pro vysokorychlostní internet - broadband strategie. In: Archiv stránek bývalého Ministerstva informatiky, http://web.mvcr.cz/archiv2008/micr/scripts/detail.php_id_3157.html (12. srpna 2009)

Národní strategie informační bezpečnosti ČR. In: Archiv stránek bývalého Ministerstva informatiky, http://web.mvcr.cz/archiv2008/micr/scripts/detail.php_id_2705.html (9. září 2009).

Národní strategie informační bezpečnosti ČR. Příloha 1. In: Archiv stránek bývalého Ministerstva informatika, http://web.mvcr.cz/archiv2008/micr/scripts/detail.php_id_2705.html (19 . září 2009)

Národní strategie informační bezpečnosti ČR. Příloha 2: Standardy a doporučení. In: Archiv stránek bývalého Ministerstva informatiky, http://web.mvcr.cz/archiv2008/micr/files/2705/06_nsib_cr_priloha_2_v0_8__2_.pdf (1. února 2009)

Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů. In:

Ministerstvo vnitra ČR, eGovernment, http://www.mvcr.cz/clanek/narizeni-vlady-c-495-2004-sb-kterym-se-provadi-zakon-c-227-2000-sb-o-elektronickem-podpisu-a-o-zmene-nekterych-dalsich-zakonu.aspx (5. července 2009)

Network and Information Society: Proposal for a European Policy Approach. In: Portál Evropské unie, http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf (6. října2009)

OECD Guidelines for the Security of Information Systems. Towards a Culture of Security. In: Organisation for Economic Cooperation and Development (OECD), http://www.oecd.org/dataoecd/16/22/15582260.pdf (3. října 2009)

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. In: Organisation for Economic Cooperation and Development (OECD), http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (20. října 2009)

Operační program lidské zdroje a zaměstnanost 2007-2013. In: Ministerstvo vnitra ČR, EU, Strukturální fondy, http://www.mvcr.cz/clanek/operacni-program-lidske-zdroje-a-zamestnanost-500016.aspx (16. října 2009)

Presidency Conclusions. Lisbon European Council 23 and 24 March 2000. In: Rada EU, http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/00100-r1.en0.htm (11. listopadu 2009)

Prioritní osy IOP. In: Centrum pro regionální rozvoj ČR, http://www.crr.cz/index.php?did=828 (16. října 2009)

Programové prohlášení vlády (srpen 1998). In: Vláda ČR, http://www.vlada.cz/assets/clenove-vlady/historie-minulych-vlad/prehled-vlad-cr/1993-2007-cr/milos-zeman/Programove-prohlaseni-vlady_1.pdf (28. října 2009)

Programové prohlášení vlády (2002). In: Vláda ČR, http://www.vlada.cz/assets/clenove-vlady/historie-minulych-vlad/prehled-vlad-cr/1993-2007-cr/vladimir-spidla/Programove-prohlaseni-vlady_1.pdf (12. srpna 2009)

Programové prohlášení vlády (2004). In: Vláda ČR, http://www.vlada.cz/assets/clenove-vlady/historie-minulych-

vlad/prehled-vlad-cr/1993-2007-cr/stanislav-gross/Programove-prohlaseni-vlady-Ceske-republiky_1.pdf (28. října 2009)

Programové prohlášení vlády (2005). In: Vláda ČR, http://www.vlada.cz/assets/clenove-vlady/historie-minulych-vlad/prehled-vlad-cr/1993-2007-cr/jiri-paroubek/Programove-prohlaseni-vlady-Jiriho-Paroubka_1.pdf (28. října 2009)

Programové prohlášení vlády (2007). In: Vláda České republiky, http://www.vlada.cz/scripts/detail.php?id=20780 (11. srpna 2009)

Programové prohlášení vlády (2009). In: Vláda České republiky, http://www.vlada.cz/cz/jednani-vlady/programove-prohlaseni/programove-prohlaseni-vlady-cr-58369/ (11. srpna 2009)

Report on the Implementation of the European Security Strategy – Providing Security in a Changing World. In: The European Council, http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf (8. října 2009)

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 narušení: zvyšujeme připravenost, bezpečnost a odolnost. In: Portál Evropské unie, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:CS:PDF (10. října 2009)

Seznam záměrů strategických projektů pro čerpání prostředků ze Strukturálních fondů EU v rámci Smart Administration. In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/odbor-reformy-a-regulace-kvality-verejne-spravy-smart-administration.aspx (16. října 2009)

Směrnice Evropského parlamentu a rady 1999/93/EC o zásadách Společenství pro elektronické podpisy. In: Portál Evropské unie, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:24:31999L0093:CS:PDF (14. října 2009)

Směrnice OECD pro bezpečnost informačních systémů a sítí. Směrem ke kultuře bezpečnosti. In: Archiv stránek bývalého Ministerstva informatiky, http://web.mvcr.cz/archiv2008/micr/images/dokumenty/cz_security_guidelines_4_3__03.pdf (19. září 2009)

Statistiky vydaných výstupů v rámci projektu CzechPOINT k 18. 10. 2009. In: CzechPOINT, http://www.czechpoint.cz/web/?q=statistiky_aktualni (20. října 2009)

Státní informační politika – cesta k informační společnosti. In: Britské listy, 5. září 2006, http://blisty.cz/2006/9/5/art30127.html (10. listopadu 2009)

Státní informační a komunikační politika. e-Česko 2006. In: Národní knihovna ČR, http://knihovnam.nkp.cz/docs/SIKP_def.pdf (12. srpna 2009)

Strategy for a Secure Information Society. Dialogue, Partnership and Empowerment. In: Portál Evropské unie, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:EN:PDF (10. října 2009),

The European Programme for Critical Infrastructure Protection. In: ProAdrias, http://www.proadrias.isig.it/Documenti/EPCIP%20memo.pdf (7. října 2009)

Usnesení Vlády České republiky k budování registrů veřejné správy. In: Vláda ČR, http://racek.vlada.cz/usneseni/usneseni_webtest.nsf/web/cs?Open&2004&12-22 (20. října 2009).

Usnesení Vlády České republiky o Postupu a hlavních směrech reformy a modernizace ústřední státní správy. In: Vláda ČR, http://racek.vlada.cz/usneseni/usneseni_webtest.nsf/0/4D45F2283205A4F2C12571B6006D669A (20. října 2009)

Ústava České republiky. In: www.hrad.cz, http://www.hrad.cz/cz/ustava_cr/index.shtml (12. září 2009)

Vyhláška č. 194/2009, o stanovení podrobností užívání a provozování informačního systému datových schránek. In: Sagit, http://www.sagit.cz/pages/sbirkatxt.asp?cd=76&typ=r&zdroj=sb09194 (6. září 2009)

Vyhlášky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb. In: Ministerstvo vnitra ČR, eGovernment, http://www.mvcr.cz/clanek/vyhlaska-c-378-2006-sb-o-postupech-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb.aspx (4. srpna 2009)

Vyhláška č. 496/2004 Sb. k elektronickým podatelnám. In: Ministerstvo vnitra ČR, eGovernment, http://www.mvcr.cz/clanek/vyhlaska-c-496-2004-sb-k-elektronickym-podatelnam.aspx (5. července 2009)

Vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy. In: Ministerstvo vnitra ČR, eGovernment, http://www.mvcr.cz/clanek/vyhlaska-c-529-2006-sb-o-dlouhodobem-rizeni-informacnich-systemu-verejne-spravy.aspx (19. září 2009)

Zákon č. 22/1997 Sb., o technických požadavcích na výrobky. In: Portál veřejné správy ČR, http://portal.gov.cz/wps/portal/_s.155/701?kam=zakon&c=22/1997 (19. září 2009)

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: Sagit, http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00101&cd=76&typ=r (19. září 2009)

Zákon č. 227/2000 Sb., o elektronickém podpisu. In: Ministerstvo vnitra ČR, eGovernment, http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx (8. září 2009).

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. In: Sagit, http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb08300&cd=76&typ=r (6. září 2009)

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy. In: Ministerstvo vnitra ČR, eGovernment, http://www.mvcr.cz/clanek/legislativa-zakon-c-365-2000-sb-o-informacnich-systemech-verejne-spravy.aspx (9. září 2009).

Zákon č. 440/2004 Sb., kterým se mění zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů. In: Sbírka zákonů, roč. 2004, 26. července 2004, http://web.mvcr.cz/archiv2008/sbirka/2004/sb144-04.pdf (9. září 2009)

Literatura

5 telecom priorities for Belgian Presidency. In: Euractive.com, http://www.euractiv.com/en/general/5-telecom-priorities-belgian-eu-presidency/article-116150# (21. Listopadu 2009)

A working definition of e-government. In: State University of New York, Center for Technology in Government, The Future of eGovernment, http://www.ctg.albany.edu/publications/reports/future_of_egov?chapter=2 (8. července 2009)

Activities. In: European Network and Information Security Agency (ENISA), http://www.enisa.europa.eu/about-enisa/activities (8. října 2009)

Aktivovaná je teprve každá desátá datová schránka. In: Informační systémy veřejné správy, http://www.isvs.cz/e-government/aktivovana-je-teprve-kazda-desata-datova-schranka.html (12. října 2009)

ALLEN, Patrick D. – DEMCHAK, Chris C.: *The Palestinian – Israeli Cyberwar*. Military Review, březen-duben 2003, s. 52-59. (http://web.ebscohost.com)

At the Dawn of e-Government: The Citizen as Customer. In: Government Finance Review, říjen 2000, http://www.entrepreneur.com/tradejournals/article/67323089_1.html (6. července 2009)

Audit informačního systému. In: Vydavatelství VŠCHT Praha, http://vydavatelstvi.vscht.cz/knihy/uid_es-005/hesla/audit_informaCnIho_systEmu.html (4. října 2009)

BARBER, Richard: *Hacking Techniques. The tools that hackers use, and how they are evolving to become more sophisticated.* Computer. Fraud and Security. 1. března 2003, č. 3, s. 9-12. (http://web.ebscohost.com)

BARBER, Richard: *Hackers Profiled – Who Are They and What Are Their Motivations?* In: Computer Fraud and Security, únor 2001, č.2. (http:// web.ebscohost.com), s. 14-17.

BASTL, Martin: *Budoucnost nekonvečních forem boje*. In: Rexter, 2008, č. 2, http://www.rexter.cz/budoucnost-nekonvencnich-forem-boje/2008/11/01/ (11. září 2009)

Before i2010: Eeurope Initiative. In: European Commission, Europe´s Information Society, http://ec.europa.eu/information_society/eeurope/2002/index_en.htm (12. srpna 2009)

Bezpečnost IS – co to znamená? In: Informační systémy veřejné správy, http://www.isvs.cz/bezpecnost/bezpecnost-is-co-to-znamena-1-dil-.html (19. září 2009)

BINDER, Jean Carlo: *Public Key Infractructures (PKIs): What are they?*. In: VACCA, John R. (ed.): *Public Key Infrastructure: building trusted applications and Web services*. Auerbach, 2004.(http://books.google.com)

BONI, William – KOWACICH, Gerald L.: Netspionage: The Global Threat to Information. Woburn, Butterworth-Heinemann 2000. (http://books.google.com)

BRUNNER, Elgin M. – SUTER, Manuel: *International CIIP Book 2008/2009. An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*. In: Crisis and Risk Network, http://www.crn.ethz.ch/index.cfm (12. října 2009)

CERT. In: ENISA, http://www.enisa.europa.eu/act/cert (8. října 2009)

Co je Czech POINT. In: CzechPOINT, http://www.czechpoint.cz/web/?q=node/22 (5. července 2009)

Co je a co není ISVS. In: Informační systémy veřejné správy, http://www.isvs.cz/atestace/co-je-a-co-neni-isvs.html (12. srpna 2009)

Co je to outsourcing a kdy jej využít. In: ASI informační technologie, http://www.asi.cz/Podpora/OdbornéčlánkyzesvětaIT/tabid/54/articleType/ArticleView/articleId/91/Co-je-to-outsourcing-a-kdy-jej-vyuzit.aspx (4. října 2009).

CURRAN, Kevin – CONCANNON, Kevin – McKEEVER, Sean: *Cyber Terrorism Attacks*. In: Igi Global, http://www.igi-global.com/downloads/excerpts/reference/IGR4726_WbOBBAVgQ2.pdf (14. září 2009)

CURTIN, Gregory G. – SOMMER, Michael H. – VIS-SOMMER, Veronika (eds.): *The World of E-government*. Binghamton (NY), Haworth Press 2003. (http://books.google.com)

Cyber Wars between Pakistan and India. In: Articlebase, http://www.articlesbase.com/internet-articles/cyber-wars-between-pakistan-and-india-373872.html (14. září 2009)

CzechPOINT. In: www.ostrava.cz, http://www.ostrava.cz/jahia/Jahia/site/ostrava/cache/offonce/ostrava/obcan/czech-point;jsessionid=127A1344E2E4A6C7EC167E5945311CDB (11. srpna 2009)

CzechPOINT@home. In: Asseco Czech Republic, http://www.eobec.eu/egovernment/czechpoint-home/ (6. září 2009)

CzechPOINT@office - Agendy pro vnitřní použití na úřadech. In: CzechPOINT, http://www.czechpoint.cz/web/?q=node/382 (6. září 2009)

DANCHEV, Dancho: *Cyber Intelligence – CYBERINT*. In: Dancho Danchev' s Blog, http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html (18. září 2009)

Datové schránky v poločase – dva měsíce po startu a dva měsíce před plným provozem. In: datoveschranky.info, http://www.datoveschranky.info/clanek/233 (6. září 2009)

Datové schránky. Typový postup implementace. Občan. In: datoveschranky.info, http://www.datoveschranky.info/obcan/?PHPSESSID=187b6fefcb77aa068914df2363f6eba3 (5. září 2009)

Datový trezor a jiné služby. In: datoveschranky.info, http://www.datoveschranky.info/aditivni-sluzby/ (12. září 2009)

Definition of E-Government. In: The World Bank (WB), http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/EXTEGOVERNMENT/0,,contentMDK:20507153~menuPK:702592~pagePK:148956~piPK:216618~theSitePK:702586,00.html (8. července 2009)

Department of Defence Dictionary of Military Terms. Washington D.C. 2001

Digital Europe – Europe's Fast Track to Economic Recovery. In: Europa Press Releases, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/09/336&format=HTML&aged=0&language=EN&guiLanguage=en (12. září 2009)

DiMARIA, Eleonora – MICELLI, Stefano (eds.): *Online Citizenship. Emerging Technologies for European Cities*. New York, Springer Science and Business Media, Inc. 2005. (http://books.google.com)

eEurope – An Information Society for All. In: Euractive.com, http://www.euractiv.com/en/infosociety/eeurope-information-society/article-117472# (6. října 2009)

E-governance and Access to Information. In: Organizace spojených národů (OSN), Democratic Governance, http://ictd.undp.org/e-gov/ (31. října 2009)

eGovernment. In: European Commission, Europe´s Information Society, http://ec.europa.eu/information_society/activities/egovernment/index_en.htm (11. listopadu 2009)

eGovernment: Commission calls for Ambitious Objectives in EU for 2010. In: European Commission, Europe´s Information Society, http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2601 (12. září 2009)

Egovernment Act – zákon o egovernmentu. In: Egovernment, http://egovernment.cz/best/PDF%2007/EgovAct.pdf (10. srpna 2009)

E-government. Veřejná správa jako živý organismus. In: CzechPOINT, http://www.czechpoint.cz/web/?q=node/18 (5. července 2009)

Echelon. In: Federation of American Scientists (FAS), http://www.fas.org/irp/program/process/echelon.htm (23. září 2009)

eJustice. In: Justice.cz, http://obcanskyzakonik.justice.cz/ejustice/index.html (4. srpna 2009)

Elektronický podpis a jeho využití. In: businessinfo.cz, http://www.businessinfo.cz/cz/clanek/podnikatelske-prostredi/elektronicky-podpis-a-jeho-vyuziti/1001234/2984/ (5. září 2009)

Elektronický portál územních samospráv. In: Ministerstvo vnitra ČR, eGovernment, http://www.mvcr.cz/clanek/elektronicky-portal-uzemnich-samosprav.aspx (5. července 2009)

EU Commissioner Reding Calls for Preventive Action to Make the EU Resilient against Cyber Attacks. In: Portál Evropské unie, Press Releases Rapid, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/199 (10. října 2009)

EU: Como Conference: Interoperability is key, says European Commissioner. In: ePractice.eu, http://www.epractice.eu/en/news/283954 (22. listopadu 2009)

EU cyber security and defence body proposed. In: Secpoint, http://www.secpoint.com/eu-cybersecurity-superbody-proposed.html (8. října 2009)

European Social Fund. In: European Commission, http://ec.europa.eu/employment_social/esf/index_en.htm (12. září 2009)

European Union. In: BRUNNER, Elgin M. – SUTER, Manuel: *International CIIP Book 2008/2009*. Zurich, http://e-collection.ethbib.ethz.ch/eserv/eth:31095/eth-31095-01.pdf (8. října 2009), p. 465-484.

European Union plugging the gaps in the fight against terrorism. In: European Commission, Justice and Home Affairs, http://ec.europa.eu/justice_home/fsj/criminal/terrorism/fsj_criminal_terrorism_en.htm (22. září 2009)

EVERARD, Paul: *NATO and Cyber Terrorism*. In: *Response to Cyber Terrorism*. Amsterdam, IOS Press 2008 (http://books.google.com)

Full Blown Cyber War: An Information Age War in the Making. *Cyber War: The Third World War*. In: Cyberoam, http://newsletters.cyberoam.com/072008/images/FullBlownCyberWar.pdf (17. září 2009)

GATTIKER, Urs E.: *The Internet as a Diverse Community: cultural, organizational, and political issues*. Mahwah (NJ), Lawrence Erlbaum 2001. (http://books.google.com)

GEERS, Kenneth: *Cyberspace and the changing nature of warfare*. In: SC Magazine, 27. srpna 2008, http://www.scmagazineus.com/Cyberspace-and-the-changing-nature-of-warfare/article/115929/ (9. září 2009)

GIBSON, William: *Neuromancer*. Plzeň, Laser-books 1998.

GRAHAM, Bradley: *U.S. Studies a New Threat: Cyber Attack*. In: The Washington Post, 24. května 1998, http://www.washingtonpost.com/wp-srv/washtech/daily/may98/cyberattack052498.htm (14. září 2009)

GRAMLICH, Ludwig: *Recent Developments Relating to Electronic Government*. In: POLČÁK, Radim - ŠKOP, Martin - ŠMAHEL, David (eds.): *Cyberspace 2005*. Brno, Masarykova univerzita 2006, s. 81-97.

GRIFFIN, David – TREVORROW, Philippa – HALPIN, Edward F.: *Development in E-government: a Critical Analysis*. Amsterdam, IOS Press 2007, (http://books.google.com)

HASTEDT, Glenn: *Espionage: a reference handbook*. Santa Barbara, ABC-CLIO Inc. 2003. (http://books.google.com)

HINES, Matt: *Cyber-espionage moves into B2B*. In: InfoWorld, http://www.infoworld.com/t/business/cyber-espionage-moves-b2b-546 (15. září 2009)

HINKELBEIN, Oliver: *'Digital literacy': the central cultural technique of the 21st century*. In: European Commission, http://ec.europa.eu/education/archive/elearning/doc/workshops/digital_literacy/position_papers/hinkelbein_oliver.pdf (12. září 2009)

HRAJNOCHA, Luděk: *Projekty MI v oblasti e-governmentu*. In: Institut mikroelektronických aplikací (IMA), http://www.ima.cz/download/cz/aktuality/platformai2010/seminare/S5_i2010_Hrajnoha.pdf (12. září 2009)

HUBER, Jordana: *Cyber Attacks „Grossly Underestimated". Industries lack technology and skill to counter dangerous hackers, security expert says*. In: Financial Post, 26. června 2009, http://www.financialpost.com/m/story.html?id=1731010 (29. října 2009)

CHÝLEK, Jaroslav – STIEGLER, Petr: *Dva týdny ostrého provozu*. In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/dva-tydny-ostreho-provozu-informacniho-systemu-datovych-schranek.aspx (21. listopadu 2009)

ICT Trust and Security Research. In: Portál Evropské unie, Information and Communication Technologies, http://cordis.europa.eu/fp7/ict/security/home_en.html (7. října 2009)

Implementing e-government in OECD countries: experience and challenges. In: Organisation for Economic Cooperation and Development (OECD), http://www.oecd.org/dataoecd/35/6/36853121.pdf (6. července 2009)

Informace o zřízení elektronických podatelen u orgánů veřejné moci. In: Ministerstvo vnitra ČR, eGovernment, http://www.mvcr.cz/clanek/informace-o-zrizeni-elektronickych-podatelen-u-organu-verejne-moci.aspx (4. srpna 2009)

Informační politika MPO. In: Ministerstvo průmyslu a obchodu ČR, http://www.mpo.cz/dokument495-strana1.html (1. února 2009)

Informační systém datových schránek se rozběhl naplno. In: datoveschranky.info, http://www.datoveschranky.info/clanek/284 (21. listopadu 2009)

Informační systém datových schránek. Základní informace. In: datoveschranky.info, http://www.datoveschranky.info/clanek/84/ (12. září 2009),

Informační systémy veřejné správy. In: Ministerstvo vnitra ČR, eGovernment, http://www.mvcr.cz/clanek/informacni-systemy-verejne-spravy.aspx (1. února 2009)

Information Security. In: BusinessDictionary.com, http://www.businessdictionary.com/definition/information-security.html (20. září 2009)

Information Security and Privacy. In: Organisation for Economic Cooperation and Development (OECD), http://www.oecd.org/department/0,3355,en_2649_34255_1_1_1_1_1,00.html (19. září 2009).

JANOUŠEK, Michal: *Kybernetický terorismus: terorismus informační společnosti*. In: Obrana a strategie, 2006, č. 2, http://www.defenceandstrategy.eu/cs/archiv/rocnik-2006/2-2006/kyberterorismus-terorismus-informacni-spolecnosti.html (22. září 2009), 60-66.

JAŠEK, Roman: *Informační a datová bezpečnost*. Zlín, Univerzita Tomáše Bati 2006.

JIROVSKÝ, Václav – HNÍK, Václav – KRULÍK, Oldřich: *Základní definice, vztahující se k tématu kybernetických hrozeb*. In: Ministerstvo vnitra ČR,

http://web.mvcr.cz/archiv2008/bezpecnost/informacni/zakladni_info.pdf (20. října 2009)

Jiří Peterka se zamýšlí nad zánikem Ministerstva informatiky. In: Informační systémy veřejné správy, http://www.isvs.cz/e-government/jiri-peterka-se-zamysli-nad-zanikem-ministerstva-informatiky.html (12. srpna 2009)

JONES, Andy – KOVACICH, Gerald L. – LUZWICK, Perry G.: *Global Information Warfare. How Businesses, Governments and Others Achieve Objectives and Attain Competitive Advantages*. Boca Raton, Auerbach 2002 (htto://books.google.com)

JRC History. In: European Commission, Joint Research Centre, http://ec.europa.eu/dgs/jrc/index.cfm?id=2260 (7. října 2009)

KALDOR, Mary: *New and Old Wars. Organised Violence in a Global Era*. 2. vydání. Cambridge, Polity Press 2006. (http://books.google.com)

KARATZOGIANNI, Athina (ed.): *Cyber-conflict and Global Politics*. Oxon, Routledge 2009. (http://books.google.com)

KHOSROWPOURE, Mehdi (ed.): *Practising E-Government. A Global Perspective*. Hersey, Idea Group Publishing 2005. (http://books.google.com)

Komunitární programy. In: Euractive.cz, http://www.euractiv.cz/komunitarni-programy (16. října 2009)

Komunitární programy v oblasti informační společnosti. In: Ministerstvo vnitra ČR, Komunitární programy, http://www.mvcr.cz/clanek/komunitarni-programy-v-oblasti-informacni-spolecnosti.aspx (16. října 2009)

Koncepce budování informačních systémů veřejné správy. In: Informační systémy veřejné správy, http://www.isvs.cz/user_data/dokumenty/UVIS-Koncepce-ISVS-1999.pdf (12. srpna 2009)

Koncepce informatizace Plzeňského kraje. In: Portál Plzeňského kraje, http://www.kr-plzensky.cz/article.asp?itm=10322 (5. září 2009)

Konec úřední počty? Datové schránky má jen desetina povinných uživatelů. In: ihned.cz, 5. října 2009, http://domaci.ihned.cz/c1-38539250-konec-uredni-posty-datove-schranky-ma-jen-desetina-povinnych-uzivatelu (12. října 2009)

KONOPA, Prokop: *Rozvoj e-governmentu z pohledu Asociace krajů ČR*. Veřejná správa online, 2009, č. 3, http://vsol.obce.cz/clanek.asp?id=2009316 (4. října 2009)

KREBS, Brian: *Report: Russian Hacker Forums Fuelled Georgia Cyber Attacks*. In: The Washington Post, 16. října 2008,

http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html (15. září 2009)

KREJČÍ, Oskar: *Mezinárodní politika*. Praha, Victoria Publishing 1997.

KŘEPELKOVÁ, Helena: *Úvodní slovo k novému seriálu o informační bezpečnosti ze všech úhlů*. In: ICT Security, 3. června 2009, http://www.ictsecurity.cz/serial-o-informacni-bezpecnosti/uvodni-slovo-k-novemu-serialu-o-informacni-bezpecnosti-ze-vsech-uhlu.html (19. září 2009)

KUSÁK, Martin*: CIP - Program pro podporu ICT*. In: Euroskop.cz, http://euroskop.cz/gallery/39/11821-cip_ict_psp.pdf (16. října 2009)

LEDVINKA, Robert a kol.: *Technologická centra krajů a obcí s rozšířenou působností, včetně spisových služeb. Koncept a východiska*. In: Ministerstvo vnitra ČR, http://www.mvcr.cz/soubor/koncept-a-vychodiska-projekt-tc.aspx (6. září 2009)

Legislativa. In: Ministerstvo vnitra ČR, eGovernment, http://www.mvcr.cz/clanek/legislativa-zakon-c-365-2000-sb-o-informacnich-systemech-verejne-spravy.aspx (1. 2. 2009)

LIDÍNSKÝ, Vít a kol.: *eGovernment bezpečně*. Praha, Grada 2008.

LOWERY, Liza M.*: Developing a Successful E-Government Strategy*. In: United Nations (UN), http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN000343.pdf (8. července 2009)

MAIWALD, Eric: *Network Security. A Beginner's Guide*. 2. vydání. Emeryville McGraw-Hill 2003. (http.//books.google.com)

Majitelům datových schránek hrozí, že by mohli přijít o hesla. In: Ihned.cz, 18. listopadu 2009, http://ihned.cz/?s1=0&m=frommail&article[id]=39115690 (21. listopadu 2009)

MANNES, Aaron - HENDLER, James: *Profile of a Real Cyberware*. In: The Washington Times, 5. srpna 2009, http://www.washingtontimes.com/news/2009/aug/05/profile-of-a-real-cyberwar/ (14. září 2009)

MARSAN, Carolyn Duffy: *How close is World War 3.0?* Network World, 24, 27. srpna 2007, č. 33, s. 21-25 (http://web.ebscohost.com)

MATES, Pavel – SMEJKAL, Vladimír: *E-government v českém právu*. Praha, Linde 2006

MELOTÍKOVÁ, Petra: *Vybrané právní nástroje Rady Evropy v oblasti ochrany osobních údajů*. In: Právnická fakulta Masarykovy univerzity, http://www.law.muni.cz/edicni/sborniky/cofola2008/files/pdf/sprava/melotikova_petra.pdf (19. října 2008)

MERKOW, Mark: *Growing a Tree of Trust*. In: VACCA, John R. (ed.): *Public Key Infrastructure: building trusted applications and Web services*. Auerbach, 2004 s. 33-50.(http://books.google.com)

MESERVE, Jeanne: *Study Warns of Cyberwarfare during Military Conflicts*. In: cnn.com/US, 17. srpna 2009, http://www.cnn.com/2009/US/08/17/cyber.warfare/index.html (15. září 2009)

Ministerial eGovernment Conference 2005, 24-25 November in Manchester, UK. In: European Commission, Europe´s Information Society, http://ec.europa.eu/information_society/activities/egovernment/conferences/past/2005/index_en.htm (22. listopadu 2009)

Ministerstvo. In: Ministerstvo pro místní rozvoj ČR, http://www.mmr.cz/ministerstvo (2. 2. 2009)

MIHAILA, Viorel: *NATO's Strategic Communication in Combating Terrorism*. In: North Atlantic Treaty Organization (NATO), http://ftp.rta.nato.int/public//PubFullText/RTO/MP/RTO-MP-IST-086///MP-IST-086-01.pdf (22. září 2009)

MOORE, Malcolm: *China's global cyber-espionage network GhostNet penetrates 103 countries*. In: telegraph.co.uk, 29. března 2009, http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html (21. září 2009)

NAGESH, Gautham: *Latest Security Threat Lies in Trusted Software and Hardware*. In: Nextgov, http://www.nextgov.com/nextgov/ng_20080825_7185.php (18. září 2009)

Národní projekt počítačové gramotnosti. In: Archiv stránek bývalého Ministerstva informatiky, http://web.mvcr.cz/archiv2008/micr/nppg.html (12. září 2009)

Naše cesta k e-governmentu je pro Unii inspirativní. In: Ministerstvo vnitra ČR, Informační servis, http://www.mvcr.cz/clanek/nase-cesta-k-egovernmentu-je-pro-unii-inspirativni.aspx (9. září 2009)

New Approach to technical harmonization and standardization. In: Portál EU, Summaries of EU Legislation, http://europa.eu/legislation_summaries/internal_market/single_market_for_goods/technical_harmonisation/l21001a_en.htm (11. listopadu 2009)

Nové přípustné formáty datové zprávy. In: datoveschranky.info, http://www.datoveschranky.info/clanek/243/ (13. září 2009)

Nový přístup k evropské harmonizaci. In: MM Průmyslové spektrum, http://www.mmspektrum.com/clanek/novy-pristup-k-evropske-harmonizaci (19. září 2009)

O datových schránkách. In: datoveschranky.info, http://www.datoveschranky.info/o-datovych-schrankach-text/ (12. září 2009)

O radě vlády pro informační společnost. In: Ministerstvo vnitra ČR, eGovernment, http://www.mvcr.cz/clanek/egovernment-rada-vlady-pro-informacni-spolecnost-o-rade-vlady-pro-informacni-spolecnost.aspx (11. srpna 2009)

ODS chce první volby přes internet už v roce 2013. In: ihned.cz, 25. srpna 2009, http://domaci.ihned.cz/c1-38142850-ods-chce-prvni-volby-pres-internet-uz-v-roce-2013 (7. září 2009)

Odbor rozvoje služeb a projektů eGovernmentu. In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/odbor-rozvoje-sluzeb-a-projektu-egovernment.aspx (19. září 2009)

Operační program lidské zdroje a zaměstnanost. In: Ministerstvo vnitra ČR, Strukturální fondy, http://www.mvcr.cz/clanek/operacni-program-lidske-zdroje-a-zamestnanost-500016.aspx (16. října 2009)

Outsourcing. In: Adaptic, http://www.adaptic.cz/znalosti/slovnicek/outsourcing.htm (4. října 2009)

PARKER, Tom: *Cyber Adversary Characterization: auditing the hacker mind*. Rockland (MA), Syngress Publishing Inc. 2004. (http://books.google.com)

PETERKA, Jiří: *i2010 místo eEurope 2005*. In: Archiv článků a přednášek Jiřího Peterky, http://www.earchiv.cz/b05/b0607001.php3 (12. srpna 2009)

PETERKA, Jiří*: Ohlédnutí za zanikajícím Ministerstvem informatiky*. In: Živě, http://www.zive.cz/clanky/ohlednuti-za-zanikajicim-ministerstvem-informatiky/sc-3-a-135620/default.aspx (12. srpna 2009)

PETERKA, Jiří: *Osm priorit státní informační politiky*. In: Archiv článků a přednášek Jiřího Peterky, http://www.earchiv.cz/anovinky/ai2364.php3 (12. srpna 2008)

POŽÁR, Josef a kol.: *Základy teorie informační bezpečnosti*. Praha, Vydavatelství Policejní akademie ČR 2007

POŽÁR, Josef: *Informační bezpečnost*. Plzeň, Vydavatelství a nakladatelství Aleš Čeněk, s.r.o. 2005.

Právní předpisy k datovým schránkám. In: Ministerstvo vnitra ČR, Legislativa, http://www.mvcr.cz/clanek/navrhy-provadecich-pravnich-predpisu-k-datovym-schrankam.aspx (9. září 2009)

Protection and Security of Networked Critical Infrastructures (SCNI). In: Euroepan Commission, JRC, Institute for the Protection and Security of the Citizen, http://ipsc.jrc.ec.europa.eu/showaction.php?id=22 (7. října 2009)

PROTIVOVÁ, Ivana a kol.: *Analýza dopadu zákona č. 300/2008 Sb. a návrh zajištění implementace tohoto zákona pro Krajský úřad Plzeňského kraje*. In: Egovernment, http://egovernment.cz/schranky/anal%C3%BDza/anal%C3%BDza%20komplet.pdf (6. září 2009)

Prováděcí právní předpisy k datovým schránkám. In: datoveschranky.info, http://www.datoveschranky.info/vyhlasky/?PHPSESSID=780cc31f7eb987e497fbfdc5478bdcb3 (14. července 2009)

První pracovní setkání Výboru pro informační bezpečnost ČR. In: Archiv stránek bývalého Ministerstva informatiky, http://web.mvcr.cz/archiv2008/micr/scripts/detail.php_id_3090.html (27. října 2009)

Přehled dodavatelů řešení informační bezpečnosti. In: SystemOnLine, http://www.systemonline.cz/dodavatele-it-sluzeb-a-reseni/informacni-bezpecnost/ (4. října 2009)

Přehled udělených akreditací. In: Ministerstvo vnitra ČR, eGovernment, http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx (4. srpna 2009)

PTAŠNIK, Adam: *Cyberspace in Public Administration*. In: POLČÁK, Radim - ŠKOP, Martin - ŠMAHEL, David (eds.): *Cyberspace 2005*. Brno, Masarykova univerzita 2006, s. 113-116.

Putting Citizens First. In: European Commission, Europe's Information Society, http://ec.europa.eu/information_society/tl/soccul/egov/index_en.htm (8. září 2009)

Rada vlády pro informační společnost. In: Ministerstvo vnitra ČR, eGovernment, http://www.mvcr.cz/egovernment-rada-vlady-pro-informacni-spolecnost.aspx (31. října 2009)

Rada vlády pro informační společnost schválila Strategii rozvoje služeb pro informační společnost. In: businessinfo.cz, http://www.businessinfo.cz/cz/clanek/koncepce-a-politiky/informacni-spolecnost-strategiie-rozvoje/1000502/48353/ (11. srpna 2009)

RANNENBERG, Kai: *Recent Development in Information Technology Security Evaluation – The Need for Evaluation Criteria for multilateral Security*. In: Institut für Wirtschaftsinformatik, http://www.is-frankfurt.de/publikationenNeu/RecentDevelopmentinInformation.pdf (11. listopadu 2009)

Regulation in the Information Society. In: European Commission, Europe's Information Society, http://ec.europa.eu/information_society/tl/policy/regulate/index_en.htm (5. října 2009)

RIS – Regionální informační servis. In: Agentura regionálního rozvoje, http://www.arr-nisa.cz/iware_cz/?D=21 (19. 10. 2008)

ROTSCHILD, Michael: *The Threat from within: the evolution of cyber attacks*. Computer Technology Review, březen-duben 2006. (http://findarticles.com)

SAMUEL, Alexandra Whitney: *Hacktivism and the Future of Political Participation*. Massachusetts, Harvard University Cambridge 2004, http://www.alexandrasamuel.com/dissertation/pdfs/index.html (15. října 2009)

Seznam záměrů strategických projektů pro čerpání prostředků ze Strukturálních fondů EU v rámci Smart Administration. In: Ministerstvo vnitra ČR, http://www.mvcr.cz/clanek/odbor-reformy-a-regulace-kvality-verejne-spravy-smart-administration.aspx (16. října 2009)

SMEJKAL, Vladimír: *Datové schránky nastupují*. In: ihned.cz, 22. července 2009, http://pravniradce.ihned.cz/c4-10078260-37865170-F00000_d-datove-schranky-nastupuji (12. října 2009)

Social inclusion, better public services and quality of life. In: European Commission, Europe´s Information Society,

http://ec.europa.eu/information_society/eeurope/i2010/inclusion/index_en.htm (12. září 2009)

Strategie rozvoje služeb pro informační společnost. In: businessinfo.cz, http://www.businessinfo.cz/cz/clanek/koncepce-a-politiky/informacni-spolecnost-strategiie-rozvoje/1000502/48353/ (11. srpna 2009)

Světové počítače v září nejvíce trápil červ Conficker, ty naše reklamní software. In: ihned.cz, 9. října 2009, http://digiweb.ihned.cz/c1-38595350-svetove-pocitace-v-zari-nejvice-trapil-cerv-conficker-ty-nase-reklamni-software (9. října 2009)

Symantec Global Internet Security Threat Report. Trends for 2008. In: Symantec, duben 2009, http://www.symantec.com/content/en/us/about/media/Symantec2009AnnualReport_Proxy_10-K.pdf (11. září 2009)

ŠTĚDROŇ, Bohumír: *Úvod do eGovernmentu.* Praha, Úřad vlády ČR 2007.

ŠTOLFOVÁ, Renata: *Contemporary Security Threats within Cyberspace. NATO and EU Approaches to Cybersecurity*. Maria Enzersdorf, AIES 2009.

The e-government imperative: main findings. In: Organisation for Economic Cooperation and Development (OECD), Policy Brief, březen 2003, http://www.oecd.org/dataoecd/60/60/2502539.pdf (6. července 2009)

The „Lisbon Strategy" in Short. In: Výbor regionů, http://portal.cor.europa.eu/lisbon/Profiles/Pages/welcome.aspx (11. listopadu 2009)

There Is No UN Definition on Terrorism. In: Eye on the UN, http://www.eyeontheun.org/facts.asp?1=1&p=61 (22. září 2009)

Tracking GhostNet: Investigating a Cyber Espionage Network. In: F-Secure, http://www.f-secure.com/weblog/archives/ghostnet.pdf (21. září 2009)

TUŠEROVÁ, Lenka: *E-government a jeho projevy v českém právu.* Právnická fakulta Masarykovy univerzity, http://www.law.muni.cz/edicni/dp08/files/pdf/sprava/tuserova.pdf (6. července 2009)

Updated Work Programme 2009 and Work Programme 2010. Cooperation. Theme 3. ICT – Information and Communications Technologies. In: European Commission, Community Research and Development Information Service (CORDIS), Information and Communication Technologies, FP7, ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/ict-wp-2009-10_en.pdf (7. října 2009)

VANČURA, Jan: *Outsourcing bezpečnostních služeb v IT*. In: Moderní řízení, modernirizeni.ihned.cz, 12. září 2003, http://modernirizeni.ihned.cz/c4-10007700-13346250-600000_detail-outsourcing-bezpecnostnich-sluzeb-v-it (4. října 2009)

Veřejná správa. In: Český statistický úřad, Informační společnost v číslech 2009, http://www.czso.cz/csu/redakce.nsf/i/e_verejna_sprava_is2009/$File/is09_e.pdf (12. října 2009)

Virtual Criminology Report – Cybercrime: The Next Wave. In: McAfee, http://www.mcafee.com/us/research/criminology_report/default.html (14. září 2009)

Vláda schválila zákon o e-governmentu. In: Portál veřejné správy ČR, http://portal.gov.cz/wps/portal/_s.155/708/_ps.1272/M/_s.155/8414?docid=114412 (9. září 2009)

WALTERS, Conrad: *Cyber cold war a threat to all*. The Sydney Morning Herald, 24. prosince 2007, http://www.smh.com.au/articles/2007/12/23/1198344874193.html (5. března 2008)

WEISE, Joel: *Public Key Infrastructure Overview*. In: Sun Blueprints Online, srpen 2001, http://www.sun.com/blueprints/0801/publickey.pdf (8. září 2009)

What is Cyberspace? In: Wisegeek, http://www.wisegeek.com/what-is-cyberspace.htm. (10. září 2009)

What is cyberspace? In: Iwebtool, http://www.iwebtool.com/what_is_cyberspace.html (10. září 2009)

What is eGovernment? In: Manchester University, Institute for Development Policy and Management, eGovernment for Development, http://www.egov4dev.org/success/definitions.shtml#eAdmin (8. července 2009)

What is PKI? In: SearchSecurity.com, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214299,00.html (8. září 2009)

WHITTAKER, Jason: *The cyberspace handbook*. London, Routledge 2004. (http://books.google.com)

Zákon o základních registrech prošel třetím čtením. In: Ministerstvo vnitra ČR, Informační servis, http://www.mvcr.cz/clanek/zakon-o-zakladnich-registrech-prosel-tretim-ctenim.aspx (4. srpna 2009)

Základní definice vztahující se k tématu kybernetické bezpečnosti. In: Ministerstvo vnitra ČR, Informační servis, www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx (20. září 2009),

Zákon o základních registrech schválil Senát Parlamentu ČR. In: Portál veřejné správy ČR, http://portal.gov.cz/wps/portal/_s.155/7226/_s.155/10202?docid=120601 (4. srpna 2009)

Internetové odkazy

Administrativní registr ekonomických subjektů: http://wwwinfo.mfcr.cz/ares/ares.html

Critical Information Infrastructure Research Co-ordination Project: http://www.ci2rco.org

Český institut Manažerů informační bezpečnosti: http://www.cimib.cz

CzechPOINT: www.czechpoint.cz

Datové schránky: http://www.datovéschranky.info

Egoncentrum: http://egoncentrum.cz/

eIdentity, a. s.: http://www.eidentity.cz/

Elektronická vlídná administrativa: http://www.naseeva.cz/

Evropská informační společnost: http://ec.europa.eu/information_society/

Evropský sociální fond: http://ec.europa.eu/employment_social/esf/index_en.htm

ePusa: http://www.epusa.cz/

Federace amerických vědců (FAS): http://www.fas.org/

ICT Security: http://www.ictsecurity.cz/

Informační systémy veřejné správy: http://www.isvs.cz/

Information Warfare Monitor: http://www.infowar-monitor.net/

Integrovaný operační program: http://www.strukturalni-fondy.cz/getdoc/ae5865d4-be4a-403d-9461-7ee797397a20/Integrovany-operacni-program

Jiří Peterka (osobní stránky): http://jiri.peterka.cz/

Komisařka Viviane Reding: http://ec.europa.eu/commission_barroso/reding/index_en.htm

Land Parcel Information System: http://www.lpis.cz/

Ministerstvo vnitra ČR: http://www.mvcr.cz

Operační program lidské zdroje a zaměstnanost: http://www.strukturalni-fondy.cz/getdoc/d26c8d6a-821b-45df-9c9c-29a8a55f7e1e/OP-Lidske-zdroje-a-zamestnanost
Portál Evropské unie: http://europa.eu
Portál veřejné správy ČR: http://portal.gov.cz/
PostSignum OCA (Česká pošta, s. p.): https://qca.postsignum.cz/
PrimeLife: http://www.primelife.eu
První certifikační autorita, a.s.: http://www.ica.cz/
Sagit: http://www.sagit.cz
Senát Parlamentu České republiky: http://www.senat.cz/
Veřejná správa online: http://www.mool.cz
Vláda České republiky: http://www.vlada.cz/

ABSTRAKT

Inspirací pro napsání této diplomové práce byly kybernetické útoky na Estonsko na jaře 2007, jež způsobily dočasnou paralýzu země, a stát nemohl poskytovat náležité služby svým občanům. Tato pobaltská republika je známá svou vyspělou aplikací post-moderních ICTs do různých odvětví života své populace. Relevantní bylo pro autorku zejména využívání nástrojů e-governmentu.

Cílem této studie se tak stalo zmapování a zhodnocení vývoje zavádění metod e-governmentu v ČR s přihlédnutím k vlivu EU na tento proces. První hypotézou této studie je právě vnímání EU coby stěžejní entity stojící za zintenzivněním rozvoje e-governmentu v ČR, který je možné sledovat kolem poloviny první dekády 21. století, tedy v korelaci se vstupem země do Společenství v r. 2004. Ukázalo se, že strukturální a komunitární fondy EU představují významný finanční zdroj pro realizaci elektronizace a efektivizace veřejné správy. Nezanedbatelná je také možnost sdílení zkušeností v této oblasti mezi jednotlivými členskými státy v rámci Unie.

Zranitelnost současné společnosti pramenící ze závislosti na post-moderních ICTs, jež jsou využívány v široké škále našich činností, může být zneužita ke kybernetickým útokům proti státu. Druhým předpokladem této diplomové práce je tak vnímání kybernetické bezpečnosti a kybernetických útoků coby relevantních strategických a bezpečnostních výzev současnosti. Zkušenost Estonska i jiných zemí vskutku vedla k přehodnocení pojetí kybernetických hrozeb a jejich přítomnost je zahrnována do strategicko-bezpečnostních koncepcí jednotlivých států, ale i mezinárodních organizací, např. EU.

Text sleduje též motivace, prostředky i nejčastější typy kybernetických útoků. Pozornost je věnovaná rovněž teorii a praxi informační bezpečnosti tedy zajištění ochrany informačních systémů, neboť praxe e-governmentu je s nimi úzce spojena a současné fungování státu je charakteristické spravováním ohromných objemů dat o svých občanech právě v těchto informačních systémech a zaručení jejich náležitého zabezpečení před zneužitím či narušením jejich integrity a důvěryhodnosti se tak stává zásadní.

Klíčová slova: e-government, elektronický podpis, elektronické doručování a podání, CzechPOINT, datové schránky, informační bezpečnost, kybernetická bezpečnost, kybernetické útoky, Česká republika, Evropská unie.

ABSTRACT

The topic of this thesis was inspired by cyber attacks against Estonia in spring 2007. They paralyzed the country temporarily to provide appropriate services to its citizens. This Baltic state is known for its sophisticated use of post-modern ICTs within a wide range of its population‘s life. Especially the use of e-government tools was relevant for the author of the thesis.

The objective of this study is to present and analyse a development of e-government methods application in the Czech Republic with regard to the EU influence on this process. Our first hypothesis is therefore an acknowledgement of the Community as a driving force of more intensive development within the e-government tools application in the Czech Republic visible from mid-2000s. There can be seen certain correlation with the EU accession in 2004. It has been shown that structural and communitarian funds are an important financial source for electronic and effective public administration implementation. Indispensable is also an opportunity to share experience within this field among the Member states.

Contemporary society has become dependent on post-modern ICTs that are used in a wide range of our activities (e.g. e-banking, e-commerce, e-government etc.). This dependency causes its vulnerability that can be misused for cyber attacks against the state. Next presumption of this thesis is thus acknowledgement of cyber security and cyber attacks as relevant strategic and security challenges of today. The experience of Estonia but also other countries has led to revaluation of an approach to cyber threats and they have become present in strategic and security concepts of particular states as well as international organizations such as the EU.

The text also presents motivations, tools and the most common types of cyber attacks. The theory and practise of information security is also taken into consideration. Contemporary state functioning is characterized by huge amount of personal data storing. Their secure administration is therefore crucial.

Key words: e-government, electronic signature, electronic delivering and administrative action, CzechPOINT, data mail boxes, information security, cyber security, cyber attacks, Czech Republic, European Union.