

KYBERNETICKÁ KRIMINALITA

ÚVOD DO STUDIA PŘEDMĚTU

MGR. RADIM VIČAR

UNIVERZITA OBRANY, FAKULTA EKONOMIKY A MANAGEMENTU

radim.vicar@unob.cz

Operační program Vzdělávání pro konkurenceschopnost

Projekt: ***Vzdělávání pro bezpečnostní systém státu***

(reg. č.: CZ.1.01/2.2.00/15.0070)



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Úvod do studia předmětu Kybernetická kriminalita – základní pojmy

- **Kybernetická kriminalita (počítačová kriminalita, Cybercrime)** = obecně ji lze vymezit jako trestnou činnost, která směřuje k narušení nebo zneužití počítače, jejich hardwaru, softwaru, dat, sítí apod., tedy trestnou činnost zaměřenou na vyspělou techniku a prostředí, kde počítač může být předmětem trestné činnosti, ale zároveň i nástrojem pachatele trestného činu.
- **Kybernetická kriminalita** jako obecnější, širší a sjednocující pojem, který zahrnuje veškeré zločinné, neetické, nežádoucí či jinak pro bezpečnost státu a společnost rizikové jednání, související s fungováním informačních a komunikačních technologií, vedle počítačové a informační kriminality jako jednání pokrytá konkrétními skutkovými podstatami trestního zákoníku, kybernetická kriminalita zahrnuje kybernetický terorismus, hospodářskou špionáž apod.

Úvod do studia předmětu Kybernetická kriminalita – základní pojmy

- **Kyberprostor** = virtuální svět, který je vytvářen prostřednictvím rozvoje informačních a telekomunikačních technologií, fenomén moderní společnosti, který lze charakterizovat jako prostor s globálním pokrytím, decentralizací, otevřeností, kdy připojením na komunikační a informační služby vytváří uživatelé určitý druh společného prostoru.
- **Počítačové právo** = mezioborová disciplína, která zahrnuje informatiku obohacenou o vybrané aspekty z právních odvětví soukromého práva (občanské, obchodní právo) a veřejného práva (trestní právo hmotné a trestní právo procesní, ústavní právo, správní právo, finanční právo).
- Zdroj: JIROVSKÝ, V. *Kybernetická kriminalita*. Praha: Grada Publishing, a. s. 2007. 288 s. ISBN 978-80-247-1561-2.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

Úvod do studia předmětu Kybernetická kriminalita – základní pojmy

- **Formální prameny práva** = formy, ve kterých je objektivní právo obsaženo (např. trestní zákoník).
- **Materiální prameny práva** = zdroje obsahu práva, např. stav dané společnosti, technologická, ekonomická a kulturní úroveň, úroveň IT technologií.
- **Právní odvětví** = souhrn právních norem, které upravují určitou skupinu právních vztahů (např. tradiční trestní právo, či méně tradiční počítačové právo či právo bezpečnosti a obrany).
- **Právní řád** = systém pramenů práva, obsahujících právní normy určitého státu, tedy souhrn pramenů práva platných v daném státě.

Úvod do studia předmětu Kybernetická kriminalita – základní pojmy

- **Právo** = můžeme jej definovat jako soubor pravidel chování, vytvořených státem v určité zvláštní formě, a státem též vynutitelný.
- **Právo v objektivním slova smyslu** = tvořeno a představováno souborem obecně závazných pravidel chování, tedy právních norem.
- **Právo v subjektivním slova smyslu** = soubor oprávnění toho kterého subjektu právního vztahu, vedle jeho povinností.
- **Právní norma** = pravidlo chování, které je vyjádřeno zvláštní, státem uznanou formou, tj. má podobu některého z pramenů práva, a jeho zachování je vynutitelné státní mocí.

Kybernetické hrozby

- Kybernetické hrozby jsou trvalé, všudypřítomné, latentní i zjevné. Informační technologie přitom vystupují jako předpoklad ekonomického růstu státu.
- Počet kybernetických útoků narůstá, přičemž vykazují vysokou míru latence. České republice se tyto útoky nevyhýbají.
- Odhalování trestné činnosti v oblasti kybernetické kriminality a její stíhání není příliš časté.
- Kybernetické útoky mohou s sebou nést riziko ztráty na životech, ochromení dodávek elektrické energie, vody, tepla, finančních služeb, počítačových sítí apod.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

Kyberprostor a typické útoky

- **Mezi typické útoky v kyberprostoru patří:**
- **1. Útoky proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů, kam lze zařadit zejména**
 - průnik do počítačového systému (např. překonáním hesla s pomocí prolamovače hesel),
 - vzdálené řízení cílového počítače (např. prostřednictvím backdoors),
 - získávání informací o cílových počítačích a o informačním systému (např. prostřednictvím skenerů),
 - sniffing (odposlech datové komunikace),
 - potlačení služby (útok na spojovací cesty), patří sem tzv. DDoS (distributed denial of service, zahlcení odesíláním paketů z více strojů),
 - oklamání uživatelů (malware, trojské koně),
 - phishing (vylákání informací pomocí podvodné emailové zpráva),
 - pharming (získání informací prostřednictvím přesměrování klienta na falešné stránky internetbankingu),
 - spamming a další.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

Kyberprostor a typické útoky

- **2. Útoky spočívající v šíření závadného (nelegálního či nežádoucího) obsahu, kam patří např.**
 - dětská pornografie,
 - rasistické, extremistické, xenofobní či jiné projevy nenávisti,
 - tzv. cyber grooming, tedy komunikace prostřednictvím komunikačních prostředků (facebook, chat, ICQ, skype) pod jinou identitou s cílem sexuálně či jinak zneužít a obtěžovat nezletilé),
 - cyberbullying (kybernetická šikana) jako druh šikany, který využívá elektronické prostředky (jako jsou e-maily, internet, blogy, mobilní telefony a podobně, např. zasílání obtěžujících mailů, vytváření urážejících stránek a blogů, nahrání scény na mobil a následného rozeslání či vystavení na internetu.
 - zasílání tzv. hoaxů (poplašných a podvodných zpráv a řetězových e-mailů) apod.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

Kyberprostor a typické útoky

- **3. Útoky spočívající v porušování práv duševního vlastnictví**
 - šíření tzv. pirátských dat (uveřejňování nelegálních warez kopií uměleckých děl, programů),
 - neoprávněné nakládání s počítačovými programy,
 - neoprávněná reprodukce a užití hudby, filmů, databází a knih.
- **4. Další formy trestné činnosti v kyberprostoru**
 - neoprávněné nakládání s osobními údaji, podvodná jednání (např. nabídka zboží prostřednictvím Internetu), provozování hazardních her bez povolení apod.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

Východiska kybernetické kriminality v Úmluvě o kybernetické kriminalitě

- Koncem roku 2001 byla Radou Evropy přijata **Úmluva o kybernetické kriminalitě** (Convention on Cybercrime, Budapest, 23.XI.2001).
- Dohoda je prvním mezinárodněprávním instrumentem, určeným speciálně pro řešení problémů spojených s mezinárodním charakterem počítačového zločinu.
- Dohoda zejména požaduje, aby signatářské země kriminalizovaly určitá jednání, které je možné zařadit do oblasti počítačového zločinu, a dále požaduje, aby tyto země přijaly procesní normy, umožňující tuto trestnou činnost postihovat.

Východiska kybernetické kriminality v Úmluvě o kybernetické kriminalitě

- Česká republika podepsala Úmluvu dne 9. února 2005.
- 48 článků, preambule, 4 kapitoly (používání pojmů, opatření přijímaná na národní úrovni, závazky na poli mezinárodní spolupráce, závěrečná ustanovení)
- Charakterizuje znaky 9 trestných činů, úpravu základů trestní odpovědnosti, požadavky na sankce apod.
- Dále byl přijat Dodatkový protokol (kriminalizace činů rasistické a xenofobní povahy spáchané prostřednictvím počítačového systému) z roku 2003.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

Východiska kybernetické kriminality v Úmluvě o kybernetické kriminalitě

- **Úmluva o kybernetické kriminalitě** (Convention on Cybercrime) neobsahuje jednotnou definici kybernetické kriminality, vymezuje ovšem souhrn aktivit, které by smluvní strany měly v rámci svého právního řádu postihovat jako trestný čin. Jedná se o tyto delikty:
- A/ delikty proti důvěrnosti, integritě a dosažitelnosti počítačových dat a systémů, kam dále patří
 - protiprávní přístup,
 - protiprávní zachycení informací,
 - narušování dat,
 - narušování systému,
 - zneužití zařízení.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

Východiska kybernetické kriminality v Úmluvě o kybernetické kriminalitě

- B/ delikty se vztahem k počítači, které se dále dělí na:
 - padělání (falšování) údajů souvisejících s počítači,
 - podvod související s počítači,
 - C/ delikty se vztahem k obsahu počítače, především související s dětskou pornografií,
 - D/ delikty související s porušením autorského práva a práv příbuzných autorskému právu.
-
- Tato úmluva se v České republice stala podkladem pro odpovídající vymezení skutkových podstat trestných činů v trestním zákoníku z roku 2009.

Prameny právní úpravy v boji s kybernetickou kriminalitou

- Mezi základní prameny právní úpravy v boji s kybernetickou kriminalitou v českém právním řádu patří:
- zákon č. 40/2009, trestní zákoník, ve znění pozdějších předpisů,
- zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů,
- zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů,
- zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů,



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

Prameny právní úpravy v boji s kybernetickou kriminalitou

- zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů,
- zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů,
- zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů,
- zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví, ve znění pozdějších předpisů,
- zákon č. 441/2003 Sb., o ochranných známkách a o změně zákona č. 6/2002 Sb., o soudech, soudcích, přísedících a státní správě soudů a o změně některých dalších zákonů (zákon o soudech a soudcích), ve znění pozdějších předpisů, (zákon o ochranných známkách), ve znění pozdějších předpisů,

Prameny právní úpravy v boji s kybernetickou kriminalitou

- zákon 527/1990 Sb., o vynálezech a zlepšovacích návrzích, ve znění pozdějších předpisů,
- zákon č. 40/1995 Sb., o regulaci reklamy a o změně a doplnění zákona č. 468/1991 Sb., o provozování rozhlasového a televizního vysílání, ve znění pozdějších předpisů,
- zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů,
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů,
- zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů,
- Občanský zákoník, ve znění pozdějších předpisů a další.

Strategické nástroje v boji s kybernetickou kriminalitou v České republice

- Dne 20. července 2011 schválila Vláda České republiky Strategii pro oblast kybernetické bezpečnosti ČR na období 2011 - 2015.
- Strategie stanovuje tyto hlavní prioritní oblasti v budování kybernetické bezpečnosti v České republice, kterými jsou:
- I. Koordinace a řízení rizik kybernetické bezpečnosti ČR.
- II. Podpora mezinárodní spolupráce v oblasti kybernetické bezpečnosti ČR.
- III. Národní spolupráce v oblasti kybernetické bezpečnosti (veřejné, soukromé a akademické).
- IV. Vytvoření legislativního rámce k posílení kybernetické bezpečnosti ČR, podpora a ochrana lidských práv a svobod.
- V. Zvyšování povědomí a znalostí o kybernetické bezpečnosti ČR.
- VI. Posilování kybernetické bezpečnosti v ICT veřejné správy a komunikační infrastruktury ČR.
- VII. Posilování odolnosti proti narušení ICT systémů a proti kybernetickým útokům.

Závěr

- Rozvoj informačních a telekomunikačních technologií spolu s připojením na komunikační a informační služby vede k vytváření zvláštního prostoru, který se nazývá kyberprostor.
- Kyberprostor s sebou nutně nese riziko jeho zneužití pro společensky nebezpečné aktivity nového typu – kybernetickou kriminalita.
- Tento rozvoj technologií a služeb spolu s rozmachem kyberprostoru vystupuje jako materiální pramen práva a je nutno na tento vývoj reagovat i v rovině práva, zejména pak trestního práva.
- Kybernetická kriminalita je jev poměrně nový, útoky můžou vést ke značným škoda a ztrátám, je pro ni typická rychlost výměny dat a též jistá míra anonymity.

Závěr

- Úmluva o kybernetické kriminalitě (Convention on Cybercrime), ač neobsahuje definici kybernetické kriminality, se v ČR stala podkladem pro odpovídající vymezení skutkových podstat trestných činů v trestním zákoníku a pro jejich stíhání a trestání.
- V roce 2011 schválila Vláda ČR Strategii pro oblast kybernetické bezpečnosti ČR na období 2011 – 2015 jako důležitý strategický a koncepční materiál v oblasti kybernetické bezpečnosti a potírání kybernetické kriminality.