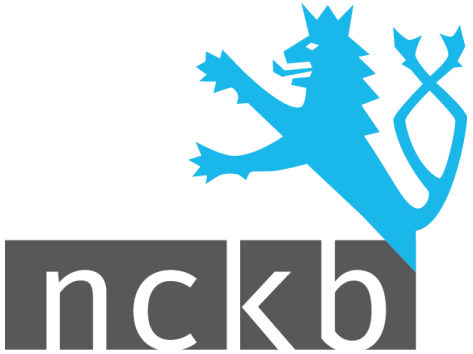
PRÁVO A KYBERPROSTOR



Taťána Jančárková
NBÚ/NCKB

Národní centrum
kybernetické
bezpečnosti

Jak definujete kyberprostor?

KYBERPROSTOR – OBSAH POJMU

- *konsenzuální halucinace prožívaná denně miliardami legitimních operátorů, v každém národě, dětmi, které se učí matematickým pojmům…grafické zobrazení dat abstrahovaných z pamětí každého počítače v lidské společnosti. Nepředstavitelná komplexita. Linie světla rozprostírající se v neprostoru mysli, klastry a konstelace dat. (Gibbson, 1984)*
- *globální doména v rámci informačního prostředí, jejíž odlišující a unikátní charakter je ohraničen použitím elektroniky a elektromagnetického spektra k vytvoření, uchovávání, modifikování, výměny a využití informací skrze závislé a propojené sítě využívající informační a komunikační technologie (Kuehl, 2009)*
- *propojené informační technologie (Healey, 2013)*
- *digitální prostředí umožňující vznik, zpracování a výměnu informací, tvoření informačními systémy a službami a sítěmi elektronických komunikací (ZKB, 2014)*

KYBERPROSTOR – PRÁVNÍ DIMENZE

- kyberprostor nezná hranice – teritorialita? suverenita státu?
- rychlost technologického vývoje – normy obsoletní v okamžiku vzniku?
- přičitatelnost – kdo je adresátem norem, jak je vymáhat?

Dimenze kyberprostoru

- technická – IT infrastruktura
- sociální – mezilidské vztahy, sdílení a přijímání informací
- politická – prosazování/ochrana zájmů státu
- právní – ochrana infrastruktury, regulace činností v kyberprostoru, otázky jurisdikce a vymahatelnosti

KYBERPROSTOR – PRÁVNÍ DIMENZE

- hrozby – špionáž, kriminalita, terorismus, válka
- rostoucí dopad na offline svět - regulace nevyhnutelná?
- autoregulace x vnucená úprava chování
- demokratické x autoritativní režimy
- centrem práva jednotlivec x společnost/stát
  - regulace infrastruktury x regulace obsahu x regulace jednání
  - snaha o prosazení teritoriálního prvku

NSKB 2015-2020

- *Kybernetická bezpečnost představuje **souhrn organizačních, politických, právních, technických a vzdělávacích opatření** a nástrojů směřujících k zajištění **zabezpečeného, chráněného a odolného kyberprostoru** v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost. Kybernetická bezpečnost pomáhá **identifikovat, hodnotit a řešit hrozby** v kyberprostoru, **snižovat** kybernetická **rizika** a **eliminovat dopady** kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže ve smyslu **posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury**. Hlavním smyslem kybernetické bezpečnosti je pak ochrana prostředí k **realizaci informačních práv** člověka.*

Kybernetická bezpečnost

- kybernetická bezpečnost v úzkém smyslu – Zákon č.181/2014 Sb., o kybernetické bezpečnosti (+ prováděcí předpisy)
- kybernetická bezpečnost v širším smyslu
  - normy ústavního, občanského, trestního, správního, autorského práva aj.
    - Ústava, LZPS, ústavní zákon o bezpečnosti ČR
    - ZEK, TZ, TŘ, zákon o zajišťování obrany ČR, o mezinárodní justiční spolupráci, o ochraně osobních údajů, správní řád …
  - kyberkriminalita x mezinárodně protiprávní jednání států
    - Charta OSN (čl. 2(4) x čl. 39 a 51), obyčejové MP
    - užití síly, odpovědnost státu, IHL

ZÁKON O KYBERNETICKÉ BEZPEČNOSTI - ÚČEL

- komplexní zajištění **bezpečnosti kritické informační infrastruktury** státu
- zavést základní **opatření** kybernetické bezpečnosti
- zlepšit **detekci a hlášení** kybernetických bezpečnostních **incidentů**
- zavést systém opatření k **zvládání incidentů**
- upravit činnost **národního** a **vládního CERT**

ZÁKON O KYBERNETICKÉ BEZPEČNOSTI – ZÁSADY

- ukládá povinnosti **veřejnoprávním i soukromoprávním** subjektům
- dělí kybernetický prostor na oblast působnosti **vládního CERT** a **národního CERT**
- **odpovědnost provozovatele** sítě za její bezpečnost
- technologická **neutralita**
- **minimalizace** zásahu do práv soukromoprávních subjektů (standardizace, nikoli certifikace)

Zákon o kybernetické bezpečnosti – povinné osoby

- Kritická informační infrastruktura (KII)
  - prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti (zákon č. 240/2000 Sb., vyhl. 315/2014 Sb.)
- Odvětvová kritéria
- Dopadová kritéria: dopad na důvěrnost, integritu nebo dostupnost (CIA)
  - Přes 250 obětí nebo 2500 osob s následnou hospitalizací delší než 24 hodin
  - Hospodářská ztráta nad 0,5% HDP (2013 – 19,4 mld Kč)
  - Omezení základních služeb nebo jiné vážné narušení dopadající na více než 125 000 osob

ZÁKON O KYBERNETICKÉ BEZPEČNOSTI – POVINNÉ OSOBY (2)

- Významné informační systémy (VIS)
  - informační systém provozovaný orgánem veřejné moci/krajem, který není KII a jehož úplná nebo částečná nefunkčnost způsobená narušením bezpečnosti informací by mohla mít negativní vliv na výkon veřejné moci, na prvek KII, případně naplnit jiná z určených dopadových kritérií (§ 4 vyhlášky č. 317/2014 Sb.)
- Oblastní kritéria
  - Orgán veřejné moci x kraje v přenesené působnosti (x obce)

ZÁKON O KYBERNETICKÉ BEZPEČNOSTI – POVINNOSTI

- Vést bezpečnostní dokumentaci
- Hlásit kybernetické bezpečnostní incidenty
- Zavést bezpečnostní opatření (standardizace)
- Provádět bezpečnostní opatření uložená NBÚ
- Hlásit kontaktní údaje/kontaktní osoby

- (pokuta do výše 100 000 Kč)

ZKB – STAV KYBERNETICKÉHO NEBEZPEČÍ (§ 21)

- stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost a integrita služeb nebo sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací*

***Zájem ČR:** zachování její ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života nebo zdraví fyzických osob

(zákon 412/2005 Sb.. § 2 písm. b))

ZKB – STAV KYBERNETICKÉHO NEBEZPEČÍ (§ 21)

- vyhlašuje Ř/NBÚ, zveřejnění v rozhlase a TV, informování vlády o postupech při řešení a o aktuálním stavu hrozeb
- max. 7, resp. 30 dnů
- vztahuje se na subjekty a vztahy upravené ZKB, rozhodnutí a opatření obecné povahy
- Ř/NBÚ požádá vládu o vyhlášení stavu nouze, pokud situaci nelze zvládnout v rámci stavu kybernetického nebezpečí

Mezinárodní úroveň

- stále větší provázanost činností v kyberprostoru s mezinárodními vztahy (viz hrozby) x hlavním subjektem mezinárodního práva tradičně stát, zatímco v kyberprostoru původně jen doplňková úloha – jaké normy pro kyberprostor?
- i na mezinárodní úrovni vícero dimenzí
  - politicko-vojenská – užití síly, kyberválka
  - ekonomicko-bezpečnostní – bezpečnost sítí a systémů, kyberkriminalita
  - rozvojová – internet governance, informační společnost

Ekonomicko-bezpečnostní rozměr

- 2013 – návrh směrnice o bezpečnosti sítí a informací (NIS směrnice)
  - poskytovatelé základních služeb a digitální platformy
- 2013 - směrnice EP a Rady 2013/40/EU o útocích na informační systémy
  - kriminalizace vybraného jednání, přísnější sankce, spolupráce
- 2001 - Úmluva Rady Evropy o počítačové kriminalitě (Budapešťská úmluva) (CZ 2013)
  - státy Rady Evropy i mimo (vč. USA)

POLITICKO-VOJENSKÝ ROZMĚR

- 1998 – RF návrh rezoluce o vývoji na poli ICT v kontextu mezinárodní bezpečnosti
- 2011, 2015 – RF/CN (ŠOS) – International Code of Conduct
  - kontrola států nad internetem (mezivládní x multistakeholder přístup)
  - respektování suverenity států
  - zákaz „informačních zbraní“ (kyberšpionáž)
  - povinnost států stíhat činnosti jako „terorismus, separatismus a extremismus, které narušují politickou, ekonomickou a sociální stabilitu jiných států, stejně jako jejich duchovní a kulturní prostředí

Politicko-vojenský rozměr (2)

- 2004 – 2015 – 4 skupiny vládních expertů (UN GGE)
  - normy mezinárodního práva platí i v kyberprostoru
  - státy mj. musí respektovat zásady suverenity, pokojného řešení sporů a nevměšování se do vnitřních záležitostí jiných států
  - státy musí dodržovat závazky k dodržování lidských práv a základních svobod
  - státy nesmí využívat prostředníky k mezinárodně protiprávnímu chování
- 2013 – Talinský manuál

POLITICKO-VOJENSKÝ ROZMĚR (3)

- 2013 - Talinský manuál
  - skupina expertů pod egidou CCDCoE
  - aplikace *ius ad bellum* a *ius in bello* na kyberprostor – stejné normy (pátá doména?)
  - otázka přičitatelnosti
  - mezinárodní právo platí i v kyberprostoru (UN GGE 2013)
  - užití síly ve smyslu čl. 2(4) Charty OSN
  - právo sebeobrany podle čl. 51 Charty
- 2016? – Talinský manuál 2.0

Politicko-vojenský rozměr (4)

- Hard law x soft law
  - výhody x nevýhody
  - doporučení UN GGE (A/70/174)
  - 2013 - OBSE - opatření na budování důvěry (CBMs) – rozhodnutí PC č. 1106

ROZVOJOVÝ ROZMĚR

- 2005 – World Summit on Information Society
- 2010 - Internet Governance Forum
- 2015 – WSIS+10 review
- IANA/ICANN – intergovernmental x multistakeholder approach

ZÁVĚR

- konflikt hodnot a chráněných zájmů
- mezinárodní normy pro kyberprostor stále ve fázi formování
- mezinárodní právo se dokázalo s technickými výzvami vypořádat již v minulosti (radiové vlny, vesmír)

t.jancarkova@nbu.cz

nckb@nbu.cz