KONCEPTUÁLNÍ A TEORETICKÉ ASPEKTY KYBERNETICKÉ BEZPEČNOSTI

Lucie Kadlecová, M.A.
NCKB / Institut mezinárodních studií,
Fakulta sociálních věd, Univerzita Karlova

Národní centrum kybernetické bezpečnosti

Obsah

- **Co je KB? Proč je KB dnes tak významná?**
- **Konceptuální vymezení KB a KO**
- **Tvorba KB politiky**
- **Role a funkce státu v zajištění kybernetické bezpečnosti**

Kybernetický prostor jako doména?

- **USA** jako průkopník:
  - The Department of Defence would „*treat cyberspace as an operational domain to organize, train and equip*“ (2011, DoD Strategy for Operating in Cyberspace)
  - Cyber Strategy DoD z roku 2015 toto stvrzuje a dále prohlašuje, že US Cyber Command „*may conduct cyber operations, in coordination with other US government agencies as appropriate, to deter or defeat strategic threats in other domains*“

Kybernetický prostor jako doména? (pokr.)

- **Francie** definuje kyberprostor jako jeden z „*five environments (earth, air, sea, outerspace and cyberspace)*“
  - 2013 Livre Blanc – White Paper on Defence and National Security Strategy
- **Nizozemí** otevřeně označuje kyberprostor za „*digital domain or cyberspace as the fifth domain for military operations, along with air, sea, land and space*“
  - 2012 Defence Cyber Strategy
- **Velká Británie** popisuje kybernetický prostor jako „an operating environment“
  - 2013 Cyber Primer Ministerstva obrany

Význam kybernetické bezpečnosti

- **Kybernetický prostor** dnes užívá každý (stát, soukromý sektor, jednotlivec)
- **Fenomén provázanosti** a vzrůstající závislosti
  - Positivní efekty: např. ekonomický růst, komunikace
  - Negativní efekty: např. citlivost dat, technologická závislost
- **Závislost** na kybernetickém prostoru ohrožuje bezpečnost státu
- **Státy** se proto začaly v posledních letech v oblasti kybernetické bezpečnosti více angažovat

Bezpečnost jako klíčový pojem

- **Neexistuje jednotná definice** – ať už v zahraničí nebo v ČR
- Např. prof. Miroslav Mareš:
  - *„Bezpečnost* [je] *stav, kdy jsou na nejnižší možnou míru eliminovány hrozby pro objekt (zpravidla národní stát, popř. i mezinárodní organizaci) a jeho zájmy a tento objekt je k eliminaci stávajících i potenciálních hrozeb efektivně vybaven a ochoten při ní spolupracovat.“*

- **Kybernetická bezpečnost** jako podmnožina konceptu bezpečnosti

Kybernetická bezpečnost

- **Opět neexistuje jednotná obecně přijímaná definice**, záleží na aspektech KB
- **Většina definic** přesto sdílí společný znak:
  - připravenost služby či systémů před útokem a jeho následky, spolu s plánováním obnovy funkčnosti při narušení
- **Triády** kybernetické bezpečnosti:
  - **A. předcházet, detekovat, reagovat**
  - **B. lidé, procesy, technologie**
  - **C. důvěrnost, integrita, dostupnost**

Konceptuální vymezení KO vůči KB v chápání ČR

- **Kybernetická bezpečnost**: aktivita státu chránící KII a další informační a komunikační systémy pomocí příslušných bezpečnostních opatření. KB zahrnuje především preventivní opatření a opatření reaktivního charakteru vůči napadeným subjektům v případě kybernetických incidentů.
- **Kybernetická obrana**: jako součást zajištění bezpečnosti ČR, zahrnuje úzce specializované činnosti aktivní povahy směřující k obraně státu, tj. zajištění ochrany před závažným napadením, které již nelze zvládat běžnými prostředky KB. Prostředky KO nasazovány v případech značné významnosti, mohou mít ofenzivní charakter (využití ofenzivních kapacit směrem ke zdroji útoku), ale použity mohou být pouze z defenzivních důvodů.

Konceptuální vymezení KO vůči KB v chápání ČR (pokr.)

- **Typy kybernetických incidentů řešených pomocí KO:**
  - Útoky masivního charakteru, které se nedají zvládnout běžnými prostředky KB
  - Útoky mající vliv na strategická aktiva a zájmy státu
  - Útoky ovlivňující obranyschopnost státu či řízení a koordinaci vojenských sil

- **Gesce KO a KB v ČR:**
  - Gestorem KB – Národní bezpečnostní úřad
  - Gestorem KO – Ministerstvo obrany / Vojenské zpravodajství

Funkce státu při zajištění KB

- **Vnitřní funkce státu:**
  - Právní
  - Bezpečnostní
  - Sociální a kulturní
- **Vnější funkce státu:**
  - Obranná
  - Hospodářská
  - Mezinárodně vztahová

Kybernetická bezpečnostní politika ČR

- **Nejvýznamnější dokumenty:**
  - Bezpečnostní strategie ČR
  - Národní strategie KB ČR pro období let 2015-2020
  - Akční plán NSKB 2015-2020
  - Zákon č. 181/2014 Sb., o KB a o změně souvisejících zákonů (tzv. Zákon o KB)
  - Vyhláška o bezpečnostních opatřeních, KB incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti KB (tzv. Vyhláška o KB)
  - Vyhláška o významných informačních systémech a jejich určujících kritériích.

Role státu v zajištění KB

- **4 základní oblasti:**
  - 1. Policejní složky (vymáhání práva)
  - 2. Zpravodajské služby
  - 3. Vojenské složky (kybernetická obrana)
  - 4. Ochrana KII

1. Policejní složky (vymáhání práva)

- **Informační kriminalita**: trestná činnost vztahující se k softwaru, datům/informacím, obecně činnostem, jejichž cílem je neautorizované čtení, vymazání, zneužití nebo jiné protiprávní nakládání s daty
- Pojmy:
  - **Digitální forenzní analýza**
  - **OSINT (Open Source Intelligence)**
  - **Wiretapping**
  - **Anonymizace**

2. Zpravodajské služby

- **Kybernetická špionáž:** Získávání strategicky citlivých či strategicky důležitých informací od jednotlivců nebo organizací za použití či cílení prostředků IT. Používá se nejčastěji v kontextu získávání politické, ekonomické nebo vojenské převahy.
- **Špionáž dle cíleného objektu**:
  - Špionáž proti státním aktérům
  - Průmyslová špionáž
  - Špionáž proti obyvatelstvu
- Edward **Snowden** (2013)
- Pojem **data mining**

3. Vojenské složky (kybernetická obrana)

- Kybernetický prostor jako **pátá doména válčení?**
- Využívání kybernetického prostoru pro **vojenské účely** v souvislosti s: Estonsko (2007), Gruzie (2008), Ukrajina (2014/2015)
- **Budoucí trend**: vojenské operace v kyberprostoru součástí konvenčního válčení → **budování vojenských obranných kapacit** (např. ČR Národní centrum kybernetických sil)
- **3 základní rysy KO**:
  - Zajištění KO v reálném čase
  - Schopnost aktivní identifikace a rekognoskace nepřítele
  - Schopnost provádět odvetné a preemptivní kybernetické útoky

4. Ochrana kritické informační infrastruktury (KII)

- **Definice KII (ČR)**: Komplex informačních a komunikačních systémů (naplňující stanovená průřezová kritéria a odvětvová kritéria v oblasti KB), jejichž nefunkčnost by mohla způsobit závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.
- **4 pilíře KII**:
  - Prevence
  - Detekce
  - Reakce
  - Krizový management

Děkuji za pozornost

Lucie Kadlecová, M.A.

Lucie.Kadlecova@nbu.cz