Kybernetická bezpečnost v kontextu hybridní a informační války

Ing. Dušan Navrátil
Ředitel

Národní úřad
pro kybernetickou
a informační bezpečnost

Kyberprostor slouží k provádění informačních a hybridních operací

- velká míra anonymizace, s tím spjaté výzvy atribuce (přisouditelnosti)
- relativně nízké vstupní náklady

V rámci tohoto tématu lze identifikovat dvě základní roviny:

- Obsah komunikace
- Způsob využití informačních a komunikačních technologií (ICT) / kyberprostoru

Role NÚKIB v oblasti informačních / hybridních operací

- Agenda NÚKIB se nezaměřuje na obsahovou stránku (udržování povědomí a sledování i obsahové stránky je však nedílnou součástí)
- Zaměřuje se na sledování vývoje škodlivého využívání ICT/kyberprostoru v rámci informačních operací
- Primární je zajištění důvěrnosti, integrity a dostupnosti IS a KS, resp. významné infrastruktury, která přenáší důležité informace a data pro chod a prosperitu státu

  => NÚKIB hlavní role, jakožto gestor kybernetické bezpečnosti v ČR
- Při podcenění kybernetických hrozeb by mohlo docházet k ohrožení schopnosti ochrany kriticky důležité infrastruktury státu. Možnost extenzivního zneužívání k provádění nejrůznějších informačních a jiných hybridních operací
- Důvěra obyvatelstva v informace komunikované státními institucemi je zásadní

Nejpoužívanější kybernetické útoky v rámci InfoOps/HybridOps

- Hacking / neautorizovaný přístup k informačním systémům
- False flag kybernetické operace (útoky) různého druhu
- DoS/DDoS útoky
- Website defacement
- Doxing

Příklad využití ICT: Automatizované nástroje

- Využívání automatizovaných nástrojů online propagandy, neboli robotizovaných účtů (či tzv. botů)
- Může mít závažné konsekvence: ovlivnění výsledků voleb nebo dalších rozhodovacích procesů.
- Vývoj směřuje k využívání umělé inteligence a strojovému učení
- Využívají je státní aktéři, politická uskupení, hackeři, státem sponzorované skupiny, nevládní organizace či teroristická uskupení.
- Ve středoevropském regionu se nejvíce diskutuje o hrozbě ruské internetové propagandy. Využívání botů v robotizované propagandě ale není pouze doménou Ruska.

Protiopatření

- Účinné zajišťování kybernetické bezpečnosti, zejména u subjektů KII a veřejného sektoru
- Budování kultury kybernetické bezpečnosti ve společnosti
- Efektivní spolupráce na národní úrovni napříč všemi relevantními subjekty (tzv. whole-of-government přístup), a to i v otázce spolupráce civilního a vojenského sektoru
- Kontinuální aktualizace a prověřování krizového managementu ve vztahu k novým trendům a výzvám
- Podpora mediální gramotnosti, kritického myšlení, kybernetické hygieny a celkové odolnosti společnosti proti jakýmkoliv škodlivým vlivovým kampaním.

DĚKUJI ZA POZORNOST!

Ing. Dušan Navrátil
Ředitel NÚKIB

Národní úřad
pro kybernetickou
a informační bezpečnost