Informační bezpečnost a vznik kyberprostoru Rizika a hrozby v kyberprostoru z hlediska bezpečnosti státu

Ing. Dušan Navrátil

Kybernetická bezpečnost naší země a společnosti nikdy nebude absolutní, ale naší povinností je, se k tomu stavu co nejvíce přiblížit.

Kybernetickou bezpečnost nelze chápat úzce technicky, ale je nutné ji vnímat v souvislostech.

Nelze strojem porazit kybernetické útočníky. Ani AI není plně schopna nahradit kreativního člověka.

Pokud se někdo rozhodne, že bude útočit a destruovat a má dostatek financí, tak uspěje.

V kybernetickém světě neexistují hranice, nelze použít klasické řešení

Informační bezpečnost

- **Informační bezpečnost** je komplex opatření, které mají zaručit ochranu informací. Předmětem ochrany z pohledu informační bezpečnosti jsou informace bez ohledu na to, zda jsou uloženy **v informačním systému, vytištěny na papíře, existují pouze v něčí mysli** a na dalších médiích.

- **Kybernetická bezpečnost** je zajištění **informační bezpečnost v kyberprostoru**. Je to komplex opatření, který zahrnuje proces navrhování, schvalování a implementaci **softwarových, hardwarových, technických a personálních ochranných opatření** spojených s minimalizací možných ohrožení informací, vzniklých v důsledku poškození, zničení nebo zneužití informačních systémů.

Petr Jirásek, Luděk Novák, Josef Požár - *Výkladový slovník kybernetické bezpečnosti (2025)*

https://www.cybersecurity.cz/data/Slovnik_610_el.pdf

Informační bezpečnost

Cíle informační bezpečnosti:

- **důvěrnost (confidentiality)**: k informacím má přístup pouze oprávněná osoba nebo osoby.
- **integrita (integrity)**: jsou jasně stanovena práva pro pozměňování a případné zničení informací.
- **dostupnost (vailability)**: zajištění dostupnosti informací.

V **praxi** je důležité zajistit také:

- autentizaci (ověření, že subjekt je tím, za koho se vydává).
- autorizaci (omezení dostupnosti operací, jakými jsou například čtení nebo zápis informací, jen pro oprávněné uživatele).
- **nepopiratelnost** (vyloučení možnosti popřít dřívější provedení nějaké operace).

Dálkový přenos informací – jeho fyzické jeho narušení

- přeprava člověkem nebo zvířetem - běžec, kurýr, holub, kurýrní služba, kurýrní plavidlo, letadlo, pošta atd.
- optickým signálem – oheň, dým, optický telegraf
- akustickým signálem - siréna, tam-tam, systém sirén
- **kabelem (pozemním, podmořským)** – telegraf, telefon, rozhlas, **internet**
- **bezdrátové spojení v rámci sítě pozemních stanic** – bezdrátový telegraf, radiofonie, rozhlas, televize, telefon, **internet**
- **satelitní přenos** – telefon, televize, **internet**

Zajištění informační bezpečnosti před využíváním kyberprostoru (před rokem 1995)

Zajištění důvěrnosti

- pečetění
- zamykání do schránek
- důvěra v přepravce
- využívání holubů
- steganografie - ukrývání zprávy jako takové: neviditelné inkousty, vyrývání zprávy do dřevěné tabulky, která se zalije voskem apod.
- **šifrování** – substituční, aditivní šifry, šifrování pomocí transpoziční tabulky, symetrická a asymetrická šifra
- **využívání vlastní kabelové sítě**

Zajištění informační bezpečnosti před využíváním kyberprostoru (před rokem 1995)

- **Zajištění integrity**

- **podpis**
- datování s podpisem svědků
- odborná expertiza
- využívání vlastní kabelové sítě

Zajištění informační bezpečnosti před využíváním kyberprostoru (před rokem 1995)

Zajištění dostupnosti

- možnost dopravy zprávy pozemní, námořní a vzdušnou cestou
- možnost dopravy zprávy **kabelem**
- možnost dopravy zprávy **elektromagnetického vlněním sítí pozemních stanic nebo satelitem**

Vznik kyberprostoru

Datum vzniku kyberprostoru je diskutabilní – názory se liší – důvody pro rok 1995

- přechod Internetu na plně komerční fungování
- objevila se globální síť - Microsoft Network

Definice kyberprostoru – existuje mnoho definic

Dle Zákona o kybernetické bezpečnosti (ZKB)

Kybernetickým prostorem se rozumí soubor sítí elektronických komunikací a dalších technologií, ve kterém dochází ke zpracování informací a dat v elektronické podobě.

Jiná definice

Kyberprostor je globální a vyvíjející se doména popisovaná užíváním elektrických sítí a elektromagnetického spektra, jejíž smysl je vytvářet, uchovávat, upravovat, vyměňovat, sdílet, vybírat, používat či vymazávat informace.

Co zahrnuje kyberprostor

- fyzická i telekomunikační zařízení, která umožňují spojení technologií a komunikaci sítí systému, chápáno obecně (SCADA zařízení, smartphony/tablety, počítače, servery atd..)
- počítačové systémy a komplementární software, který zaručuje spojení a funkčnost systému
- spojení počítačových sítí,
- uživatelské vstupy a uzly zprostředkovatelů spojení,
- informace – uživatelská data.

Kybernetický prostor - kyberprostor

V současném století je kyberprostor považován za **základní prvek v životech milionů lidí** na celém světě. Prostřednictvím a v rámci kyberprostoru se provádějí operace nezbytné pro ekonomický rozvoj, společensko-politickou činnost, bezpečnost, průmyslovou výrobu, demokratickou praxi a ochranu kritické infrastruktury státu.

Kyberprostor je výsledným produktem **aktivního spojení ICT s jejich uživateli**. Fyzicky neexistuje, ale má jasně daný začátek a konec, např. zapnutím a vypnutím počítače. Uživatelské rozhraní je zlomem mezi světem reálným a světem virtuálním.

Kybernetický prostor - kyberprostor

- Původně byly do kyberprostoru vkládány velké naděje, **byl vnímán jako prostor přátelství**, míru a prosperity.
- **Stal se však prostorem** dominance, soutěžení a nástrojem a médiem pro nezákonné aktivity, s určitou mírou beztrestnosti, kvůli nedostatečné regulaci násilných a válečných činů páchaných prostřednictvím kyberprostoru.
- Stal se také velmi výhodným prostorem pro **kyberkriminalitu** páchanou soukromými, polostátními a státními aktéry.

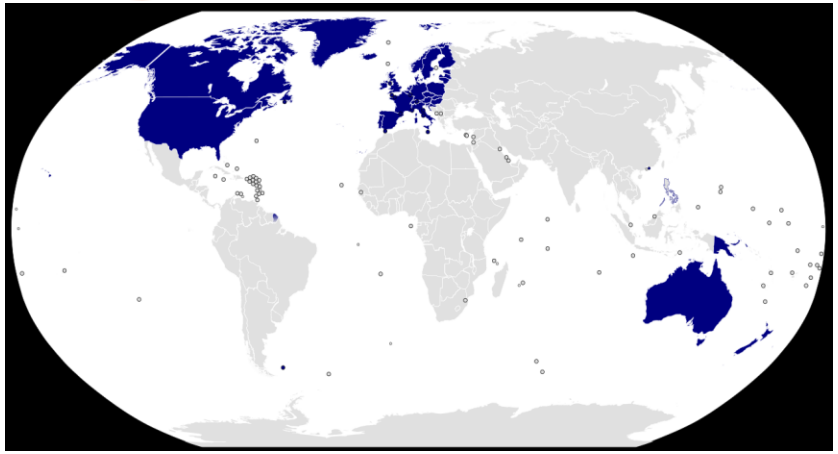
Několik základních charakteristik kybernetického prostoru

- **anonymita** – identita uživatele není jasně prokazatelná a garantovaná žádnou autoritou
- **asymetričnost** – činnost v kybernetickém prostoru může mít významný dopad na ostatní uživatele sítě bez ohledu na význam a důvěryhodnost uživatele, který tuto aktivitu vyvinul
- **neexistence hranic** – aktivity v kybernetickém prostoru nejsou omezovány žádnou jurisdikcí nebo suverenitou, právním systémem nebo kulturou
- **okamžitost** – akce provedená v kybernetickém prostoru může mít okamžitě celosvětový dopad
- **volný vstup i ukončení pobytu v něm** – kdokoliv, kdykoliv může do kybernetického prostoru vstoupit, ale také v něm může ukončit svoji aktivitu
- **interakce** – interaktivní činnosti v něm mohou vytvářet znalosti a mohou též vézt k významnému ovlivnění ostatních uživatelů
- **nízké náklady** – finanční náklady na působení v

Různé vnímání kyberprostoru

- Význačnou a charakteristickou vlastností kyberprostoru je, že **žádná jediná centrální moc nekontroluje všechny sítě**, které tvoří tuto doménu, tudíž nekontroluje kyberprostor.
- Stejně jako v reálném světě neexistuje světová vláda, ani kyberprostor postrádá institucionálně předem definované **hierarchické centrum**.
- Západ, Čína a Rusko vnímají kyberprostor jinak. Proto v současné době obtížné, až nemožné vytvořit mezinárodní dohody a standarty.
- Všichni tři aktéři se shodují na tom, že kyberprostor (či prostředky, které nabízí) lze využít ke **kybernetickým útokům, kybernetické válce, nebo jako prostředek pro použití psychologických zbraní, a to v obdobích války a míru**.

Vnímání kyberprostor u Západem



Západ vychází ze svých základních hodnot, kterými jsou **demokracie, lidská práva, právní stát, svoboda projevu, přístup k informacím, právo na soukromí** (rozdílné pojetí USA a EU). Lidská práva a základní svobody jednotlivců musí být respektovány a dodržovány stejným způsobem on-line i off-line. Západ kyberprostor vnímá **jako nástroj liberalizace.**

Poznámka:

Co je to vlastně Západ?

O Západě, západní filosofii, západní kultuře nebo civilizaci se často a běžně hovoří, aniž bychom dokázali vysvětlit, co to vlastně je.

Označení Západ vlastně nikdy nebylo zcela geografické – vzniklo před 25 stoletími, kdy Řekové sami sebe pokládali za západní, nikoliv orientální Peršany. Západ nesouvisí s žádným kontinentem, konkrétním národem či náboženstvím.

Vnímání kyberprostoru Čínskou lidovou republikou

Čínané vás okouzlí, když Vás chtějí okouzlit, Číňané vás zmáčknou, když vás chtějí zmáčknout.

Nejlépe charakterizuje postoj Číny interní dokument Komunistické strany Číny č. 9, který unikl na veřejnost v roce 2013.

Sedm „západních hodnot“, které jsou pro Čínu nebezpečné:

- ústavní demokracie,
- universální hodnoty,
- občanská společnost,
- ekonomický neoliberalismus,
- svoboda médií,
- historický nihilismus (zpochybňování oficiální verze historie)
- zpochybňování politiky otevírání se světu a reforem.

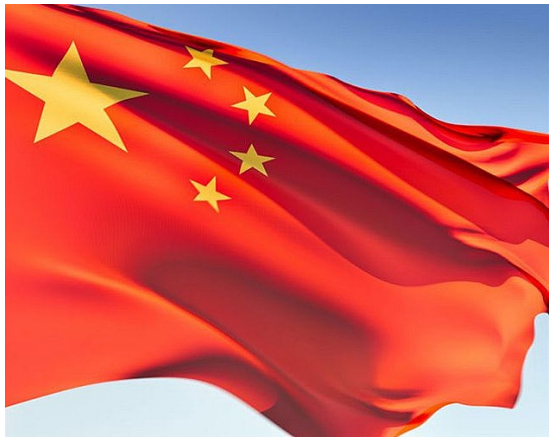
Vnímání kyberprostoru Čínskou lidovou republikou

V rámci mezinárodního prostředí Čína vnímá kyberprostor jako nové citlivé místo u svých soupeřů (nikoliv však u sebe) – **hrozba pro Čínu samotnou je odlišná, přichází zevnitř,** ze společnosti). To znamená, že není vnímán, jak ho vnímá Západ, **jako nástroj liberalizace**.

Z vojenského hlediska je kyberprostor Čínou považován za **nové bojiště a skvělý nástroj pro armádu**. Kyberprostor umožňuje mnohonásobně důslednější kontrolu obyvatelstva která povede k **digitální diktatuře**.

Čína se dlouhodobě zabývá **kyberšpionáží**, sbírá a ukládá veškerá data, politická, vojenská, technologická, sociální, zdravotní a další, svých možných protivníků. Bude schopna díky své rozvinuté umělé inteligence (AI), **je zpracovat, analyzovat a využít ve svých politických a vojenských akcích.**

Využívání kyberprostoru Čínskou lidovou republikou



Přístup ke kyberprostoru je **útočný** a jako hrozba č. 1 jsou vnímány USA. Zásadním je snaha o dosažení kontroly sítí a technologická převaha.

Čína přemýšlí v **dlouhodobém horizontu**, uvažuje o převzetí iniciativy, zahrnuje kyberprostor do svého vojenského přemýšlení. Její přístup se zaměřuje spíše na **ovlivnění protivníkova rozhodování** (v duchu čínského strategického myšlení, které má svoje počátky u Sun-C - Umění války), je kladem větší důraz na přemýšlení, než na bojování. Záměrně nepoužívá slovo cyber, ale slovo informationization (informační technologie), aby zdůraznila jiné pojetí.

Čína se snaží o **kybernetickou suverenitu**. Mít pod technologickou kontrolou všechny vlastní zásadní systémy, včetně výroby čipů.

Využívání kyberprostoru Čínskou lidovou republikou - Zlatý štít

Čína pro kontrolu internetu vytvořila projekt **Zlatý štít** (čínsky: 金盾工程 ťin-tun kung-čcheng, anglicky: The Golden Shield Project). Je to projekt **internetové cenzury a bezpečnosti informačních systémů** vyvíjený Čínskou lidovou republikou. Jedná se v současnosti o **nejkomplexnější projekt svého druhu na světě**. Ke spouštění docházelo ve vlnách. Obecně lze říci, že projekt byl postupně realizován od roku 2000.

Projekt Zlatý štít zahrnuje rozsáhlé systémy určené ke **kontrole občanů, k monitorování a zabezpečení telekomunikačních sítí.** Název projektu bývá často považován za synonymum pro **Velký čínský firewall**, to je ale pouze jedna z dílčích částí celého projektu. Další důležitou součásti je například národní informační centrum pro kriminalitu. Nejedná se tedy jen o pouhý firewall, ale o **komplexní sledovací systém, který vládě mimo jiné umožňuje cenzurovat a blokovat specifické výsledky vyhledávání na internetu a monitorovat aktivitu jeho uživatelů.**

Vvyužívání kyberprostoru Čínskou lidovou republikou – systém kreditů

Systém sociálního kreditu či **systém společenského kreditu** (čínsky 社會信用體系) je zatím částečně fungující státní systém hodnocení obyvatel Čínské lidové republiky na základě různých aspektů jejich ekonomického a společenského chování (společenské důvěryhodnosti), na jehož základě jsou jednotlivým občanům poskytována **různá úroveň přístupu k veřejným službám**.

Vliv na získání kreditů bude mít vliv:

- dodržování legislativy (snížení v případě dopravních přestupků, jízdy na černo nebo kouření na zakázaných místech)
- ekonomického chování (úprava podle struktury nákupů a řádného placení účtů a daní)
- sociálního chování (úprava v závislosti od kreditu lidí, s nimiž občan komunikuje, snížení v případě odmítnutí vojenské služby)
- způsobu využívání digitálních technologií (úprava s přihlédnutím k míře hraní počítačových her, času strávenému na sociálních sítích, sdílení nevhodného obsahu nebo šíření “fake news“.

Využívání kyberprostoru Čínskou lidovou republikou – systém Sociálního kreditů

Systém sociálního kreditu či **systém společenského kreditu** (čínsky 社會信用體系) je připravovaný státní systém hodnocení obyvatel Čínské lidové republiky na základě různých aspektů jejich ekonomického a společenského chování (společenské důvěryhodnosti), na jehož základě se bude jednotlivým občanům poskytovat různá úroveň přístupu k veřejným službám.

Vliv na získání kreditů bude mít vliv:

- dodržování zákonů (snížení v případě dopravních přestupků, jízdy na černo nebo kouření na zakázaných místech)
- ekonomického chování (úprava podle struktury nákupů a řádného placení účtů a daní)
- sociálního chování (úprava v závislosti od kreditu lidí, s nimiž občan komunikuje, s kým je příbuzný, snížení v případě odmítnutí vojenské služby)
- způsobu využívání digitálních technologií (úprava s přihlédnutím k míře hraní počítačových her, času strávenému na sociálních sítích, sdílení nevhodného obsahu nebo šíření "fake news".

V roce 2015 vláda pověřila 8 soukromých technologických společností vývojem algoritmů a vytvořením menších zkušebních systémů; k těmto firmám patřila například China Rapid Finance, partner konglomerátu Tencent (provozovatel největší čínské sociální sítě WeChat) nebo firma Ant Financial ze skupiny Alibaba Group (provozovatel platebního systému Alipay), jež vytvořila kreditní systém Sesame Credit, který využívá dat uživatelů jednotlivých služeb skupiny

Využívání kyberprostoru Čínskou lidovou republikou – systém Sociálního kreditů

Dosažený **počet kreditů ovlivní**:

- míru sociálního zabezpečení daného obyvatele,
- dostupnost a podmínky úvěrových finančních produktů (úvěr, hypotéka, kreditní karta),
- úroveň přístupu do stravovacích podniků,
- kvalitu ubytování a turistických služeb,
- dostupnost jednotlivých způsobů přepravy
- rychlost internetového připojení
- rozhodne například o přístupu k lepšímu vzdělání nebo zaměstnání (manažerské pozice v státních podnicích nebo velkých bankách) atd.

Nízký kredit může způsobit i úplné zamezení přístupu k některým službám – například s platností od 1. května 2018 ztratilo 9 milionů občanů možnost zakoupit si letenky na vnitrostátní lety a 3 miliony možnost cestovat v byznys třídě ve vlacích, a to po dobu až jednoho roku.

Vláda ČLR nyní disponuje největším počtem na **veřejnosti umístěných kamer**, které permanentně sledují obyvatelstvo. Tyto kamery navíc dokáží rozpoznat obličej a přiřadit jej ke konkrétní osobně v databázi. Čínská vláda plánuje kamerový systém ještě více rozšířit a **napojit ho na Sociální kredit**.

Vnímání kyberprostoru Ruskou federací

• Rusko přistupuje ke kyberprostoru zejména ze svého vnímání **pocitu ohrožení**. Podobně jako Čína vidí Rusko kyberprostor jako určitou hrozbu pro svoji vnitřní stabilitu.

• Kyberprostor využívá ke **kybernetické špionáži,** k **destruktivním kybernetickým útokům** a úspěšným **dezinformačním kampaním**. Nemůže soupeřit na poli technologií. Kinetické vojenské operace předcházejí a doprovázejí destrukční kybernetické útoky. (Gruzie, Ukrajina). Dokonale zvládá **hybridní válčení**.

Různé vnímání kyberprostoru

- **Jiné vnímání kyberprostoru** Čínou a Ruskem je zásadní globální problém. Nejsou stejně vnímány některé pojmy. Např. pojem válka je vnímán podobně, což umožňuje mezinárodní dohody. Ale různý výklad pojmu demokratické volby v dohodě v Jaltě (1945) byl jedním z důvodů Studené války. Nejednotnost vnímání kyberprostoru přináší problém v uzavírání mezinárodní dohod.

- Dnes je důležitá kybernetická diplomacie. Probíhá boj o rozvojové země, kam se přikloní v chápání a standardů kyberprostoru. Nutnost pravidel např. z hlediska kyberkriminality, řešení anonymity atd. řeší OSN.

NATO vnímá kyberprostor jako vojenskou doménu

vojenské domény:

- země
- moře
- vzduch
- vesmír
- **kyberprostor**

- Kybernetický prostor byl vyhlášen jako 5. doména na Varšavském summitu NATO (červen 2016). Ve 4 tradičních doménách konfliktu je hranice a limity jasně dané, v **kybernetického prostoru však veškeré hranice absentují a limity jsou nejasné**. Kybernetický prostor a ICT dnes propojují všechny oblasti boje, zajišťují její funkčnost, a zároveň jsou na něm i kriticky závislé.

Aktéři působící v kyberprostoru

- **státní aktéři a státem sponzorované skupiny**

Jsou to nejsofistikovanější a nejnebezpečnější útočníci z hlediska jejich působení a náročnosti jejich odhalení. Tito útočníci disponují zdroji, intelektuálnějšími i finančními pro dlouhodobé, vytrvalé a vysoce sofistikované kampaně. Většinou se jedná o precizně cílené operace ve snaze získat přístup k politicky, vojensky či diplomaticky významným informacím, nebo kompromitovat aktivity oponenta, zničit informace nebo narušit schopnost např. komunikace. Státní aktéři mohou být reprezentováni příslušníky zpravodajských služeb cizí moci, vojenskými složkami, ale také „volnou“ skupinou, která je neprovázána se státním aparátem, aby bylo možno odmítnout zodpovědnost v případě prozrazení.

- **kyberzločinci**

Motivem je zejména osobní obohacení. Nejpoužívanější způsob kybernetického útokuje Ransomware. Ale existuje i mnoho dalších způsobů kyberkriminality, kdy k páchání trestné činnosti je využíván kyberprostor. Využívají dělbu práce a jejich služby je možno si objednat, včetně

Aktéři působící v kyberprostoru

- **bývalí i současní zaměstnanci a dodavatelé**

Tito mají přístup k sítím datům, či autentizačním informacím. Jedná se o hrozby zevnitř, tzv, Insider threat, vědomě zneužívající informací či zranitelností. Motivací je obvykle snaha se obohatit, pomstít či např. poukázat na domnělé neetické chování zaměstnavatele.

- **hactivisté**

Jsou většinou politicky, nábožensky nebo sociálně motivovaní aktéři. Jejich cílem je zlepšení reputace nebo změna, které nejsou schopni docílit běžnými dostupnými a legálními prostředky. Obvykle používají DDoS útoky, kompromitaci webových stránek s podtextem zobrazeným pro uživatele nebo zveřejňování dat za účelem kompromitace nebo odhalení, tzv. *doxing*.

- **teroristické skupiny**

Které jsou v kybernetickém prostoru aktivní v rovině rekrutace, šíření propagandy, výcviku, získávání finančních prostředků. Týkají se spíše snahy o exfiltraci informací a následné snahy o demoralizaci nepřítele či vyhledávání cílů pro kinetické útoky. Projevy kyberterorismu ve smyslu destruktivního působení jsou vzácné.

Kybernetická hrozba a ryziko

- **Kybernetická hrozba** (Cyber Treat) je hrozba, která se nachází v kybernetickém prostoru.

- **Kybernetické riziko** (Cyber ¨Risk) je způsobené kybernetickou hrozbou. Je to pravděpodobnost škodlivých následků vyplývajících z hrozby.

Hrozby z pohledu využívání kyberprostoru

- **Cyber-dependent** (kyberneticky závislá) je hrozba, kterou lze realizovat pouze pomocí počítačů, počítačových sítí nebo jiných forem informačních komunikačních technologií (ICT). V podstatě bez internetu by tyto hrozby nemohly být realizovány.
- **Cyber-enabled** (kyberneticky umožněná) je tradiční hrozba, která je ve vnějším fyzickém světě, kterou lze realizovat bez použití počítače. Realizace této hrozby, se však vynálezem a používáním internetu přeneslo na zcela novou úroveň. Její rozsah a dosah se zvýšil pomocí ICT nebo informačních komunikačních technologií.
- **Cyber-supported** (kyberneticky podporovaná) je hrozba která je realizovaná ve fyzickém světě. Při realizaci hrozby, kromě realizace v reálném světě je využíván i kyberprostor.

Cíle kybernetického působení

- Vytěžení informací v kyberprostoru (kyberšpionáž)
- Narušení infrastruktury státu
- Narušení funkčnosti vojenské techniky
- Informační vlivové operace
- Hybridní působeni
- Získání finančního prospěchu (kyberkriminalita)

Vytěžení informací

Klasické získávání informací

- **HUMINT** (Human intelligence) - lidské zpravodajství - informace shromažďované a poskytované lidskými zdroji
- **SIGINT** (Signals intelligence) - signálové zpravodajství - informace shromažďované zachycením signálů
- **IMINT** (Imagery intelligence) - obrazové zpravodajství
- **MASINT** (Measurement and signature)– měření charakteristických vlastností
- **GEOINT** (Geospatial Intelligence) – geoprostorové zpravodajství
- **OSINT** (Open-source intelligence) – vytěžování otevřených zdrojů
- **FININT** (Financial intelligence) - finanční zpravodajství
- **MEDINT** (Medical Intelligence)

Využití kyberprostoru pro tyto oblasti získávání informací je velmi efektivní.

Kybernetická špionáž - kyberšpionáž

- Kybernetická špionáž začala již v roce 1996, kdy se rozmohlo rozsáhlé zavádění internetového připojení do vládních a firemních systémů. Od té doby došlo k mnoha případům takové činnosti.
- **Kybernetická špionáž** zahrnuje:
  - neoprávněný přístup k systémům nebo zařízením za účelem získání informací,
  - sociální inženýrství pro osoby, které mají oprávněný přístup k systémům nebo zařízením, za účelem získání informací
  - útoky na dodavatelské řetězce a další
- Kybernetická špionáž provádí kybernetické útoky za účelem získání politických, obchodních finančních, techonologických a vojenských informací.
- Kybernetická špionáž a tradiční špionáž mají podobné nebo stejné konečné cíle. Kybernetická špionáž využívá anonymitu, globální dosah, rozptýlenou povahu, propojenost informačních sítí, příležitosti ke klamání, které nabízejí hodnověrné popření.

Narušení infrastruktury státu

Kybernetické útoky na kritickou infrastrukturu a další infrastrukturu státu mají vliv na chod státu.

Kritická infrastruktura je klíčovým prvkem pro stabilitu státu a společnosti. Pokud dojde k výpadku nebo poruše této infrastruktury, mohou nastat závažné následky, jako jsou hospodářské škody, ztráty lidských životů, ekonomické kolapsy nebo narušení bezpečnosti státu. Je důležité, aby byla kritická infrastruktura chráněna a zabezpečena před možnými hrozbami a riziky, aby mohla plnit svou klíčovou roli v životě a fungování společnosti.

Evropskou kritickou infrastrukturou (EKI) se rozumí kritická infrastruktura na území České republiky, jejíž narušení by mělo závažný dopad i na další členský stát Evropské unie.

Narušení infrastruktury státu

V České republice bylo vyčleněno 9 odvětví **kritické infrastruktury**:

- energetika,
- vodní hospodářství,
- potravinářství a zemědělství,
- zdravotní péče,
- doprava,
- komunikační a informační systémy,
- bankovní a finanční sektor
- nouzové služby
- veřejná správa.

Ve všech odvětvích se využívají informační systémy a dokonce dnes na nich plně závisí a navíc velká většina je napojena na internet. Tím je přímo ohrožují rizika a hrozby z kyberprostoru. Riziko se zvyšuje kybernetickým útokem na část dodavatelského řetězce.

Příklady úspěšných útoků na narušení kritické infrastruktury v zahraničí (destruktivní nebo znehodnocení dat)

- 2007 Stuxnet
- 2012 Saudi Aramco
- 2017 WannaCry
- 2014 – 2024 ruské útoky na Ukrajinu (zasáhly i země mimo Ukrajinu)
- útoky na energetiku - útoky na SCADA systémy
- útok na dodavatelský řetězec prostřednictvím aktualizace účetního software MeDoc
- útoky na komunikační systémy Viasat, Kyistar
- 2021 – Colonial Pipeline

Informační vlivové operace – techniky ovlivňování

- **DEZINFORMACE -** Dezinformace jsou mylné, zmanipulované či zavádějící informace, které jsou záměrně šířeny za účelem uvést v omyl. Představují základní kámen klasické propagandy i současného fenoménu fake news. Záměrné využití nepravdivých informací za účelem manipulace není nic nového, digitální platformy však zásadně změnily povahu dezinformací, (fabulace, manipulace, nerelevantní obsah, satira parodie).

- **SOCIÁLNÍ A KOGNITIVNÍ HACKING -** Sociální a kognitivní hacking se týká činností, které využívají našich společenských vztahů a myšlenkových procesů. Podobně, jako při hackování počítače, se nepřátelští aktéři snaží nekalým způsobem využít zranitelnosti subjektu (temná reklama, stádový efekt, spirála mlčení, komnaty ozvěn a sociální bubliny)

Informační vlivové operace – techniky ovlivňování

- **ZÁKEŘNÁ KOMUNIKACE - Je** hojně se vyskytujícím prostředkem negativní komunikace online tzv. troll. Trollové jsou uživatelé sociálních sítí, kteří prostřednictvím svých komentářů a chování online záměrně provokují ostatní. Jejich činnost přispívá k prohloubení polarizace, umlčuje nesouhlasné názory a dusí legitimní diskusi. Jednání trollů může vycházet z osobních pohnutek nebo, jako v případě *hybridních trollů*, pracují pod vedením někoho jiného (útok ad hominem, whataboutismus, zahlcení, slaměný panák, zmocnění se tématu).

- **PODVODNÉ IDENTITY -** Důvěryhodnost informací často hodnotíme dle jejich zdroje. Kdo se mnou komunikuje a proč? Co ví o dané problematice? A je skutečně tím, za koho/co se vydává? Nepřátelští aktéři, kteří se podílí na informačním ovlivňování, využívají „kapitál důvěry“ tím, že prostřednictvím podvodných identit napodobují legitimní zdroje informací (shilling, podvodné jednání, podvrh, potěmkinovy vesnice, falešná média).

Informační vlivové operace – techniky ovlivňování

- **Technologické manipulace -** Informační vlivové aktivity často využívají nejnovější technologie. Nepřátelští aktéři používají pokročilé technické dovednosti pro manipulaci online toků informací – automatizované účty, algoritmy nebo kombinace lidských a technologických prvků (boti, falešné „loutkové“ účty, deepfake videa, hishing).

- **Symbolické akty -** Činy jsou mocnější než slova. Někdy skutečným účelem nějaké akce nemusí být ani tak dosažení určitého cíle, ale spíše demonstrace nějakého sdělení. V takových případech lze akci označit za symbolickou. Příkladem velmi surových symbolických aktů může být terorismus a to, jak teroristé využívají všeobecně sdílený strach z nahodilého násilí (únik informací, hacking, veřejné demonstrace).

Informační vlivové operace – cílové skupiny

- **Široká veřejnost:** největší možné publikum Informační vlivové aktivity zaměřené na společnost jako celek, a to prostřednictvím obecně přijímaných narativů.
- **Sociodemografické zacílení:** specifické skupiny Rozdělení publika na základě demografických faktorů (jako je věk, příjem, vzdělání a etnický původ) umožní přizpůsobit sdělení tak, aby působila na konkrétní skupinu.
- **Psychografické zacílení:** jednotlivci Analýzou a kategorizací velkých objemů dat lze informační vlivové aktivity zaměřit na jedince s určitými osobnostními rysy, politickými preferencemi, vzorci chování nebo jinými charakteristikami.

Kybernetický prostor umožňuje velmi zefektivnit, zlevnit a globalizovat vlivové působení. Vlivové operace kombinují vlivové techniky. Další velké zefektivnění přináší umělá inteligence jak již ve vytváření dezinformací, tak i lepším cílením na skupiny nebo jednotlivce. Kam dospějeme, není možno dnes dohlédnout

Nové technologie v kyberprostoru – nové hrozby a rizika

- umělá inteligence
- kvantová výpočetní technika
- biotechnologie
- ?
- ?

Dotazy?

Diskuze.

Co by jste se chtěli ještě dozvědět?