Rizika a hrozby v kyberprostoru z hlediska bezpečnosti státu

Ing. Dušan Navrátil

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.

Cíle kybernetického působení

- **Narušení infrastruktury**
- **Narušení funkčnosti vojenské techniky**
- **Vytěžení informací v kyberprostoru**
- **Informační vlivové operace**
- **Hybridní působeni**

Narušení infrastruktury

Útoky na kritickou infrastrukturu a další infrastrukturu mající 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.

Kritickou infrastrukturou (KI) se dle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) rozumí prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.

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.

Prvkem KI je zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle **průřezových a odvětvových kritérií** (je-li prvek kritické infrastruktury součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury). Tato kritéria jsou obsažena v nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. Prvky kritické infrastruktury mohoubýt v oblasti veřejné i soukromé.

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.

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 (zasáhlo i země mimo Ukrajinu)
- útoky na energetiku - útoky na SCADA systémy
- útoky na komunikační systémy Viasat, Kyistar

2021 – Colonial Pipeline

Česká republika

Úspěšný útok na narušení kritické infrastruktury – Nemocnice Bohunice Brno

Útoky na zbraňové systémy

Kybernetický útok na systém Patriot

Problém dodavatelkých řetězců

Falšování GPS

Ovládání dronů

Vytěžení informací v kyberprostoru

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**

Využití kyberprostoru pro tyto oblasti získávání informací je velmi efektivní.

Kybernetická špionáž

Kybernetická špionáž začala již v roce 1996, kdy se rozmohlo rozsáhlé zavádění internetového připojení do vládních a podnikových 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.

Kybernetická špionáž provádí kybernetické útoky za účelem získání politických, obchodních 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.

Přisouzení (atribuce)

Atribuce kybernetického útoku je určení identity útočníka včetně kontextuálních informací, jako jsou motivace, fyzické umístění či detailní informace o způsobu provedení útoku. Vhledem ke specifickým vlastnostem kybernetického prostoru je atribuce složitější než v případě útoků konvenčními prostředky. Kybernetický prostor umožňuje cíleně a velmi dobře kamuflovat identitu, lokaci a další aspekty, běžně vedoucí k určení pachatele. Rozeznat, zda útočníkem je *ad hoc* sdružená skupina hackerů s kriminálním zájmem, či státní aktér s institualizovaným rámcem pro vedení ofenzivních operací v kybernetickém prostoru, je obtížné. O to více, pokud útočníci disponují štědrým rozpočtem a vydávají se skrze své jednání a nástroje jeden za druhého. Působení útočníků pod falešnou vlajkou, maskujících, své aktivity za nástroje užívané jiným aktérem, či využívání cizí infrastruktury, je jednou z největších výzev.

Rukopis ATP (Advanced Threat Protection) skupin.

Informační vlivové operace

Informačních vlivové operace lze definovat například jako „akce směřující k ovlivňování osob druhé strany odpovědných za rozhodování v zájmu politických a vojenských cílů.

Cizími mocnostmi do oběhu pokoutně vypouštěné klamné informace za účelem podkopávání základních demokratických procesů, kontroly veřejného dialogu a ovlivňování rozhodování. Informační vlivové operace podkopávají důvěru veřejnosti v důležité instituce, izolují zranitelné komunity a přispívají ke společenské a politické polarizaci.

Autoritářské režimy stále častěji využívají kybernetické vlivové operace k ovlivňování veřejného mínění, diskreditaci protivníků, podněcování strachu, podpoře konfliktů a překrucování reality.

Při Informační operaci je často využíváno informací získaných kybernetickým útokem a kyberprostorem jsou tyto také efektivně šířeny a cíleny na publikum.

Působení Ruské federace v České republice.

- podrývání důvěry v demokracii a demokratické instituce;
- diskreditace Západu, právního státu a vytvoření nedůvěry občanů ve stát;
- ovlivňování politických představitelů, politických rozhodnutí a veřejné správy;
- polarizace, rozdělení společnosti a zvýšení napětí; • prosazování pozitivního obrazu Ruska a propagace proruských postojů.

Působení Číny v České republice.

Techniky informačního ovlivňování

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 – reklamy nebo příspěvky s přizpůsobeným obsahem, vytvořeným prostřednictvím psychografického profilování, zobrazované pouze vybraným členům cílové demografické skupiny za účelem ovlivnění jejich názorů nebo chování.**

- **Stádový efekt – psychologický jev, kdy se lidé chovají určitým způsobem primárně proto, že se tak chovají ostatní. Lidé, kteří se domnívají, že patří k většině, sdílí své názory a projevují své chování s větší ochotou. Čím více jsou myšlenky a trendy obecně akceptovány, tím snadněji se dále šíří.**

- **Spirála mlčení – psychologický jev, kdy lidé, jejichž názor je nepopulární, raději mlčí, protože se bojí izolace nebo zesměšňování. Čím méně představitelé názorové menšiny sdílí své postoje, tím méně je budou sdílet i ostatní, kteří tyto názory také zastávají.**

- **Komnaty ozvěn a sociální bubliny – přirozeně utvářená skupina lidí, kteří sdílejí stejné názory a postoje, a kteří komunikují především v rámci této skupiny (v online i offline prostředí).**

Techniky informačního ovlivňování

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 – nezávislým dojmem působící mluvčí, který však ve skutečnosti jedná na základě spolupráce (i placené) s někým jiným**

- **Podvodné jednání - - podvodná osoba se vydává za někoho, kým není, a s úmyslem klamat imituje osobní či profesní identitu jiného člověka**

- **Podvrh - falzifikace oficiálních dokumentů nebo fotografií.**

- **Potěmkinovy vesnice – falešné společnosti, výzkumné instituce nebo think-tanky, vytvořené za účelem dodání důvěryhodnosti dezinformacím.**

- **Falešná média – podvodné zpravodajské entity (servery) imitující jejich skutečné předlohy.**

Techniky informačního 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 – počítačové programy, který provádí automatizované, opakované úlohy. Mohou však také být použiti pro zvýraznění konkrétních zpráv, pro spamování diskusních fór, pro navyšování počtu liků a sdílení příspěvků na sociálních médiích.**

- **Falešné „loutkové“ účty - falešné účty spravované někým, kdo neodhaluje svou skutečnou identitu nebo záměry, se označují jako tzv. sockpuppet účty. Takové falešné identity jsou používány ke vstupu do online komunit a účastní se dění se záměrem vnést do debat nepravdivé či kontroverzní informace.** Dva nebo více sockpuppet účtů může skrytě spolupracovat a uměle simulovat obě strany debaty.

- **Deepfake videa -pokročilé algoritmy strojového učení dnes umožňují takovou manipulaci s audio a video záznamem, jejíž výsledek vypadá velice přesvědčivě.**

- **Phishing – oklamání uživatelů internetu za účelem získání jejich přístupových hesel nebo jiných citlivých informací.**

Techniky informačního 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 ¨- informace bez faktického základu publikované způsobem, který má vzbuzovat zdání legitimity.**

- **Manipulace - přidání prvku, odstranění části nebo změna obsahu textu, fotografie, videa nebo zvukového záznamu za účelem změny sdělení zprávy.**

- **Nerelevantní obsah - Zavádějící využití věcně správného obsahu v rámci prezentace nesouvisející problematiky, události či osoby. Například článek obsahující fake news může použít fotografie vztahující se k jiné události pro navození dojmu autenticity.**

- **Satira a parodie - Satira a parodie jsou obvykle neškodné formy zábavy. I humor však lze využít agresivně k šíření zavádějících informací a zesměšňování či kritizování jednotlivců, názorů nebo narativů.**

Techniky informačního 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 - argumenty, které namísto soustředění se na předmět diskuse, útočí, diskreditují nebo zesměšňují osobu oponenta, označujeme termínem ad hominem. Tento řečnický faul je používán k umlčení, odrazení nebo zastrašení oponenta.**

- **Whataboutismus - odvrácení kritiky vytvořením falešné paralely s podobným, ale pro diskusi irelevantním jevem.**

- **Zahlcení - zahlcení oponenta záplavou argumentů, faktů a zdrojů, z nichž mnohé jsou pochybné nebo nesouvisí s předmětem diskuse.**

- **Slaměný panák - snaha zdiskreditovat oponenta tím, že mu jsou přisuzovány postoje či názory, které nezastává a následná argumentace proti těmto postojům.**

- **Zmocnění se tématu - Převzetí stávající debaty a změna jejího účelu či tématu.**

Techniky informačního ovlivňování

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 - Únik informací zde chápeme jako zveřejnění informací, které byly získány nelegitimními prostředky. Má obvykle silný symbolický význam, jelikož může odhalit nepravosti a před veřejností zamlčované skutečnosti. Pokud jsou však úniky informací využívány jako prostředek informačních vlivových aktivit, informace bývají vyňaty z kontextu a jsou použity k diskreditaci aktérů a rozostření informačního prostředí.**

- **Hacking - Termínem hacking označujeme získání neoprávněného přístupu k počítači nebo síti, jedná se o trestný čin. Pokud je hacking součástí informačního ovlivňování, může sloužit jako symbolický akt, kdy je samotný zásah podružný. V těchto případech bývá skutečným cílem vyvolat nejistotu, zda je systém bezpečný nebo kompromitovaný, tak aby byla podkopána důvěra v dotyčný systém nebo v subjekt za tento systém odpovědný.**

- **Veřejné demonstrace - Legitimní demonstrace jsou symbolické akty vyjádření podpory určité politické otázce nebo pozice. Představují důležitý prvek demokratického dialogu. Nepřátelští aktéři však mohou demonstrace organizovat uměle, aby vzbudili dojem silné podpory nebo naopak odporu k určité otázce.**

SLABINY MEDIÁLNÍHO SYSTÉMU

Moderní mediální systém má řadu slabých míst, zejména rychlý vývoj technologií, změny v novinářském obchodním modelu a rozšíření alternativních zdrojů. Podvržené zprávy, upravené fotografie, algoritmy, boti a konkurenční boj o prokliky na sociálních sítích – to vše činí mediální systém zranitelným vůči těm, kteří ho chtějí využít pro svůj vlastní prospěch, pro politický či ekonomický zisk nebo jen proto, aby viděli, zda je to možné.

SLABINY VEŘEJNÉHO MÍNĚNÍ

Veřejné mínění bylo vždy ovlivnitelné určitými jevy, jako je např. sociální schválení - tzn. kopírování takového chování druhých, které je interpretováno jako správné nebo žádoucí. V dnešním informačním prostředí, kde mohou být účty na sociálních médiích falešné a armády trollů znepřehledňují internetové diskuse, je však snazší než kdy jindy vytvořit „fakta", „důkazy", vzbudit hněv a pobouření. To vše činí veřejné mínění zranitelným vůči úmyslné manipulaci.

KOGNITIVNÍ LIMITY

Některé zranitelnosti vychází přímo z fungování lidského mozku. Kognitivní schopnosti člověka nestačí na to, abychom se dokázali vypořádat se všemi informacemi, které nás v moderním světě obklopují. Naproti tomu naše osobní údaje mohou být podrobeny psychografické analýze, schopné zjistit o nás více než víme sami. Na každého jednotlivce, jenž používá sociální média, existuje dle odhadů více než 800 datových údajů, které mohou být použity k předvídání širokého spektra chování. Informační vlivové operace využívají naše myšlenkové vzorce k ovlivňování našeho vnímání, chování a rozhodování.

Využívání slabin společnosti

SLABINY MEDIÁLNÍHO SYSTÉMU

Moderní mediální systém má řadu slabých míst, zejména rychlý vývoj technologií, změny v novinářském obchodním modelu a rozšíření alternativních zdrojů. Podvržené zprávy, upravené fotografie, algoritmy, boti a konkurenční boj o prokliky na sociálních sítích – to vše činí mediální systém zranitelným vůči těm, kteří ho chtějí využít pro svůj vlastní prospěch, pro politický či ekonomický zisk nebo jen proto, aby viděli, zda je to možné.

SLABINY VEŘEJNÉHO MÍNĚNÍ

Veřejné mínění bylo vždy ovlivnitelné určitými jevy, jako je např. sociální schválení - tzn. kopírování takového chování druhých, které je interpretováno jako správné nebo žádoucí. V dnešním informačním prostředí, kde mohou být účty na sociálních médiích falešné a armády trollů znepřehledňují internetové diskuse, je však snazší než kdy jindy vytvořit „fakta", „důkazy", vzbudit hněv a pobouření. To vše činí veřejné mínění zranitelným vůči úmyslné manipulaci.

KOGNITIVNÍ LIMITY

Některé zranitelnosti vychází přímo z fungování lidského mozku. Kognitivní schopnosti člověka nestačí na to, abychom se dokázali vypořádat se všemi informacemi, které nás v moderním světě obklopují. Naproti tomu naše osobní údaje mohou být podrobeny psychografické analýze, schopné zjistit o nás více než víme sami. Na každého jednotlivce, jenž používá sociální média, existuje dle odhadů více než 800 datových údajů, které mohou být použity k předvídání širokého spektra chování. Informační vlivové operace využívají naše myšlenkové vzorce k ovlivňování našeho vnímání, chování a rozhodování.

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.

Kyberprostor 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.

Problém „kapitalismu dozoru“ v kyberprostoru

Big Tech, také známý jako Tech Giants, jsou největší společnosti v oblasti informačních technologií. Termín nejčastěji odkazuje na Big Five – velká pětka technologických společností ve Spojených státech: Alphabet (Google), Amazon, Apple, Meta a Microsoft. V Číně to je BATX, což jsou Baidu, Alibaba, Tencent a Xiaomi.

Společnosti Velké pětky jsou dominantními hráči ve svých příslušných oblastech technologií: umělá inteligence, cloud computing, spotřební elektronika, e-commerce, domácí automatizace, online reklama, samořídící auta, sociální sítě, software a streamovací média.

Velká pětka jsou silné korporace ve strukturálním a vztahovém smyslu. Jako takoví jsou kritizováni za vytvoření nového ekonomického řádu zvaného „kapitalismus dozoru“. Obsluhují miliardy uživatelů, a jsou schopny ovlivňovat chování uživatelů a kontrolovat velké množství uživatelských dat.

„Kapitalismus dozoru“ je využíván při lepším cílení reklamy, ale byl a je využíván pro politické kampaně. Osobní údaje získané tzv. těžaři dat mohou umožnit různým společnostem (nejznámější Cambridge Analytica) zlepšit cílení *politické* reklamy, což je krok za komerčními cíli předchozích sledovacích reklamních operací. Tímto způsobem spolu s využitím umělé inteligence politické strany budou schopny produkovat mnohem přesněji cílenou politickou reklamu, aby maximalizovaly svůj dopad na voliče.

Dotazy?

Diskuze.

Co by jste se chtěli ještě dozvědět?