Mgr. Nataša Brabcová, LL.M., MBA

PhDr. JUDr. Mgr. Ervín Šimko, LL.M., MBA

INFORMAČNE TECHNOLÓGIE AKO HYBRIDNE HROZBY

Abstrakt: So súčasným dynamicky sa vyvíjajúcim prostredím plným nových a vylepšujúcich sa technológií narastá aj počet nových hybridných hrozieb. Z dôvodu rozsiahleho spektra pôsobnosti sú tieto hrozby stále viac nebezpečné a je ťažšie zaistiť potrebnú ochranu a obranu bezpečnostných záujmov štátu a jeho obyvateľov proti nim. Ohrozenie hybridnými hrozbami je v súčasnosti, vzhľadom na ľahký prístup k moderným technológiám, veľmi reálne. Bezpečnosť je relatívny jav ako aj stav , ktorý môžem sledovať v premenných súvislostiach na dennej baze nášho života. V relatívnom stave pri ideálnych podmienkach môžeme deklarovať, že sa cítime byť v bezpečí no je dnešný stav ideálny je to stav, o ktorom môžeme hovoriť ako o bezpečnosti: či už fyzickej bezpečnosti alebo bezpečnosti dnešného virtuálneho sveta.

Kľúčové slová: bezpečnosť, informačne technológie, online priestor, kybernetická bezpečnosť, verejná správa, analýza

ÚVOD

Informačne technológie ako hybridne hrozby môžeme chápať v širšom slova zmysle ako budovanie systému hrozieb v oblasti napadnutia informačných technológií pôsobiacich v celom priestore Slovenskej Republiky. Priestor kde pôsobia informačne technológie a na nich pôsobiace hybridne hrozby môžeme primárne definovať ako kybernetický priestor. Kybernetickým priestorom sa do nedávna chápalo prostredie, v ktorom prebiehalo spracovanie a prenos digitálne zaznamenanej informácie. V terajšej dobe sa ním už označuje celá informačná a komunikačná infraštruktúra organizácie, štátu, ale aj globálna informačná a komunikačná infraštruktúru. Približne až 97 % všetkých informácií sa už nachádza niekde v kybernetickom priestore. Následkom čoho sme sa stali závislí na jeho stabilite a spoľahlivosti dnes sa dá povedať až životne závislí. Následky hrozieb, ktoré z tohto prostredia môžu pochádzať, môžu mať v niektorých prípadoch veľké devastačné účinky, ktoré pôsobia na životy ľudí, majetok, životné prostredie, kultúrne a sociálne hodnoty. Musíme preto vytvárať podmienky a predpoklady na elimináciu ich tvorby a vnášanie do prostredia, ktoré musíme chrániť.

V príspevku sme sa zamerali na popísanie hybridných hrozieb so zameraním sa na informačné technológie, ich odhaľovanie a dotkneme sa aj postihu za vytváranie hrozieb v trestnoprávnej rovine, kde budeme len simulovať možnosť odhalenia a následného vyvodenia dôsledku čo by trestu v rovine právnej de lege lata ale poukážeme aj na možno úpravu de lege ferenda.

Predikciou tohto článku musí byť pochopenie, že hybridne hrozby sú riziko, ohrozenie , strata rovnováhy systému narušenie primárneho chodu a následne začatie sanovania škôd podľa zistenia reálneho stavu. „ *Riziko predstavuje také javy a procesy, ktoré síce priamo a bezprostredne nepôsobia na ľudstvo, národy, štáty, jednotlivcov, ale ktoré za istého neadekvátneho alebo chybného správania sa, alebo za konkrétnej situácie, za istých konkrétnych podmienok v istej fáze svojho vývoja môžu vyvolať javy a procesy, ktoré sa transformujú na hrozby*“.[1] Hrozba má potenciálnu schopnosť poškodiť záujmy a hodnoty chránené štátom kde s titulu povahy hrozby je nutne rozlíšiť hrozby cielene na jednotlivé subjekt a objekty priamo alebo hrozby pôsobiace vo všeobecnosti s účelom spôsobiť narušenie a pripraviť sa na následný cielený útok. Hrozba pôsobí v konkrétnom čase, mieste a na konkrétne subjekty a objekty.

Na základe rozvoja technológií môžeme priam tvrdiť, že kráčať z reálnou dobou je stav priam nemožný musíme teda hľadať koncepciu ochrany jednotlivých systémovú aby sme vedeli minimálnym spôsobom v stanovenom čase detekovať a následne reagovať na možne hybridne hrozby. Z názvu hybrid môžem vyčítať nekonzistentnú sústavu javov a dejov v stave

[1] VOLNER, Š. Bezpečnosť, riziká a hrozby 21. storočia, Bratislava: IRIS 2012, ISBN: 978-80-8925-674 7

nízkej pripravenosti sa s nimi vysporiadať musíme sa preto zamerať na sanáciu a na jednotlivé fázy takýchto hrozieb , kde deduktívnou ale najmä analytickou činnosťou pripravujeme súbor opatrení na odvrátenie alebo profylaxiu systémov pred hybridnými hrozbami. Ak budeme pátrať po špecifikáciách alebo manuáloch na jednotlivé hybridne hrozby priamo v pôsobení na informačne technológie tak ich nenájdeme ani v tej namodrenejšej literatúre. Je preto nutne skĺbiť viacero defenzívnych prostriedkov ako sme už spomínali na úrovni jednotlivých atribútov, ktoré majú vplyv na obranu schopnosť systémov.

Ak sa pozrieme na platnú legislatívu, ktorá hovorí o jednotlivých stupňoch ochrany potom môžeme povedať že sme „SAFE“ v bezpečí, no reálny stav je že terajšia legislatíva nie je obsiahnutá reflexiou na vyvíjajúcu sa situáciu v oblasti hybridných hrozieb a ak by sme sa chceli cítiť nadpriemerne bezpečný v oblasti, ktorú legislatíva priamo definuje aj tam si musíme povedať, že je nutne novelizovať ju. Tým máme namysli

Zákon o Kybernetickej Bezpečnosti č. 69/2018 Z. z.

Zákon o Informačných technológiách vo verejnej správe č. 95/2019 Z. z.

Zákon o kritickej infraštruktúre č. 45/2011 Z. z.

Vybrali sme nosné legislatívne pramene, ktoré by mohli byť na pretrase v oblasti ochrany pred hybridnými hrozbami v oblasti informačných technológií a nehovoriac o tom že v demokratickom štáte musíme mať nastroj aj na sankcie voči spáchaniu škôd , ujmy , či nebodaj nejakej katastrofe tak namieste je položiť si otázku kde v priestupkovom zákone alebo trestnom zákone nájdeme priamu definíciu, že za pôsobenie hybridnými hrozbami nám hrozí taký alebo onaký postih

Preto musíme povedať, je nutne definovať hybridne hrozby aj v týchto legislatívnych normách

Trestný zákon č. 300/2005 Z. z.

Zákon o priestupkoch č. 372/1990 Z. z.

Definovať hybridne hrozby môžeme nasledovne : hybridná hrozba sa vzťahuje na činnosť vykonávanú štátnymi alebo neštátnymi subjektmi, ktorej cieľom je poškodiť cieľ ovplyvňovaním jeho rozhodovania na miestnej, regionálnej, štátnej alebo inštitucionálnej úrovni.

Hybridné nástroje definujeme ako: nástroje alebo technológie kombinujúce viacero rôznych technologických prístupov alebo metód na riešenie konkrétneho problému. Hybridným nástrojom je napríklad kombinácia umelej inteligencie a strojového učenia s ľudskou interakciou. Táto kombinácia umožňuje nástroju učiť sa z ľudských interakcií a následne využívať tieto informácie na zlepšovanie svojej funkčnosti a poskytovanie efektívnejších riešení. Hybridné nástroje sa často používajú v oblastiach, ako sú napríklad medicína, financie, priemysel alebo výroba. Ich výhodou je, že umožňujú využívať najlepšie vlastnosti viacerých technológií a zároveň minimalizovať ich nedostatky.

Podstatou hybridných hrozieb je: vedenie boja, ktoré v sebe spája rôzne formy a stratégie. Slovenská republika sa najčastejšie stretáva s pokusmi o ovplyvňovanie verejnej mienky v kybernetickom priestore, ktorý má sám o sebe hybridnú povahu. Nie je totiž vlastnený ani prevádzkovaný výlučne verejnými alebo súkromnými subjektmi. Pokrok v boji proti hybridným hrozbám si preto vyžaduje úzku spoluprácu medzi verejným a súkromným sektorom, ako aj civilno-vojenskú interakciu, pričom sa musí prijať celospoločenský prístup k problému.

Hybridne hrozby vnímame na každodennom prístupe k informáciam a ich prejavy považujeme za samozrejmosť k následkom sa často krát dostávame až keď je neskoro. Niektoré ďalšie príklady hybridných nástrojov zahŕňajú kombináciu softvéru a hardvéru, kombináciu rôznych typov dátových úložísk alebo kombináciu tradičných a moderných technológií v informačných technológiach. No treba brať na zreteľ, že všetko to, čo dokáže ľudstvo posunúť vo vývoji vpred, sa dá naopak využiť, respektíve presnejšie zneužiť na nekalé účely s cieľom dosiahnuť výhody, ktoré mu neprináležia.

Hybridné hrozby sú kombináciou viacerých typov hrozieb, ktoré sa prelínajú a navzájom podporujú. Ide o spojenie rôznych metód útoku, ktoré zahŕňajú nebezpečenstvo v oblasti kybernetickej bezpečnosti, informačnej bezpečnosti, ale aj hybridnej vojny a terorizmu. Hybridné hrozby sú rôznorodé a pôsobia naprieč doménami infraštruktúry, kybernetického priestoru, vesmíru, ekonomiky, obrany, kultúry, spoločnosti, verejnej správy, práva, spravodajských služieb, diplomacie, politiky a informácií. Majú pritom tendenciu byť zložitejšie a čoraz viac sofistikovanejšie. Môžu byť vyvolané rôznymi faktormi, vrátane politickej motivácie hospodárskeho zisku alebo túžbou po moci a kontrole. Ich cieľom je zvyčajne narušenie politických procesov, hospodárskej stability alebo destabilizácia určitej oblasti. Európske centrum na boj proti hybridným hrozbám (Hybrid CoE) definuje ciele hybridných hrozieb nasledovne: „*Hybridné hrozby sú metódy a aktivity namierené voči zraniteľným miestam oponenta. Zraniteľné miesta môžu byť vytvorené mnohými vecami, vrátane historickej pamäte, legislatívy, starých praktík, geostrategických faktorov, silnej polarizácie spoločnosti, technologickými nevýhodami či ideologickými rozdielmi. Ak záujmy a ciele toho, čo využíva hybridné metódy a aktivity, nie sú dosiahnuté, situácia môže vyústiť do hybridnej vojny, kde značne narastie úloha armády a násilia“.* [2]

Základne charakteristiky hybridných hrozieb: Základným prvkom, ktorý odlišuje hybridné spôsoby vedenia vojny od hybridných hrozieb, je využitie vojenských síl a kapacít, ako aj hrozba silou alebo priame použitie ozbrojených síl skrytým či otvoreným spôsobom na dosiahnutie politických cieľov. Hybridné hrozby nemožno jednoznačne definovať vzhľadom na ich premenlivosť a nestálosť, definičným znakom je zneužívanie zraniteľnosti cieľa a vytváranie neprehľadných situácií s cieľom narušiť rozhodovacie procesy.

Nástrojom hybridných hrozieb môžu byť masívne dezinformačné kampane, ako aj využívanie sociálnych médií na propagandu alebo radikalizáciu, nábor a priame ovládanie svojich priaznivcov. Hybridné hrozby predstavujú súbor nátlakových a podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód, ktoré môžu štátne aj neštátne subjekty koordinovaným spôsobom využívať na dosiahnutie konkrétnych cieľov bez formálneho vyhlásenia vojny a pod prahom zvyčajnej reakcie. Ohrozujú fungovanie demokratických spoločností a pokúšajú sa ich oslabovať zvnútra s využitím ich zraniteľností, ale aj ich hlavných výdobytkov, vrátane slobody prejavu a vyjadrovania, nezávislosti médií, právneho štátu, verejnej kontroly inštitúcií a demokratickej politickej súťaže, ako aj otvorenosti trhovej ekonomiky.

V prostredí Slovenskej republiky, hybridné hrozby dlhú dobu neboli identifikované ako bezprostredná hrozba. Tento pojem sa prvýkrát objavil v roku 2016, a to v Bielej knihe o obrane Slovenskej republiky z dielne Ministerstva obrany SR. V bode 56. tohto strategického dokumentu je uvedené: *„Z hľadiska spôsobu vedenia konfliktov v meniacom sa bezpečnostnom prostredí je vážnou bezpečnostnou hrozbou najmä propaganda na strategickej úrovni ako súčasť informačného a psychologického pôsobenia na vybrané cieľové skupiny spoločnosti v rámci tzv. informačnej vojny a špecifické operačné postupy, ktoré sú najlepšie charakterizované pojmom ‚hybridný spôsob vedenia bojových činností'.* [3] Koncepcie Slovenskej republiky na boj proti hybridným hrozbám, ich definuje nasledovne: „*Súčasne pôsobiace aktivity, ktoré ohrozujú základné atribúty štátu alebo ich funkčnosť, sa označujú ako hybridné hrozby. Hybridná hrozba je definovaná ako súbor nátlakových a podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód, ktoré môžu štátne aj neštátne subjekty koordinovaným spôsobom využívať na dosiahnutie konkrétnych cieľov bez formálneho vyhlásenia vojny a pod prahom zvyčajnej reakcie.“ Sú realizované aktivitami charakterizovanými centrálne riadeným spravodajským a informačným pôsobením, pôsobením neštátnych aktérov, vrátane polovojenských skupín, či nasadením ozbrojených síl štátneho aktéra bez označenia. Takéto aktivity sa môžu začať skôr, než dôjde k otvorene deklarovaným vojenským operáciám. Polarizujú spoločnosť, vnášajú neistotu, a tým podkopávajú legitimitu, dôveryhodnosť, akcieschopnosť štátnych inštitúcií*

[2] Hybrid CoE 2018, podľa Milo 2018
[3] Ministerstvo obrany SR 2016

a demokratický ústavný poriadok a majú tak negatívny vplyv na realizáciu bezpečnostných záujmov štátov, ktoré sú im vystavené" [4]Základnými indikátormi hybridných hrozieb sú:

- externý alebo interný politický nátlak na najvyšších štátnych predstaviteľov a štátne inštitúcie;
- ekonomický alebo energetický nátlak ako rozšírenie politického nátlaku
- rozsiahle sabotáže proti kľúčovej infraštruktúre;
- kybernetické útoky s potenciálom spôsobiť škody veľkého rozsahu;
- informačné a propagandistické operácie s cieľom podkopať dôveru v štátne inštitúcie, vyvolať spoločenské nepokoje a vážne destabilizovať politickú a bezpečnostnú situáciu;
- ovplyvňovanie etnických, náboženských a kultúrnych menšín a ich manipulácia na politické účely; hrozba použitia vojenskej sily.

Uvedené indikátory sami o sebe sú známymi a dlhodobými hrozbami, ale ich individuálny výskyt nemožno ešte považovať za hybridnú hrozbu. Hybridnou hrozbou sa rozumie až kombinované použitie niekoľkých, najmenej troch vyššie uvedených indikátorov v širšej kampani so zjavnou snahou aktéra útoku zasahovať do situácie v SR, pričom samotný aktér nie je známy alebo popiera svoju účasť na organizovaní a realizácii útoku/kampane.[5] (Definícia hybridných hrozieb by mala však zostať dostatočne pružná, aby primerane reflektovala na vývoj hrozieb. Vo svojej podstate je to však súbor koordinovaných činností alebo metód ktoré pôsobia destabilizačne a oslabujúco voči svojim protivníkom resp. aktérom proti ktorým majú byť využité bez jednoznačného vyhlásenia vojny v "de jure" kontexte. [6]

KOMPARÁCIA A PRÍSTUP ČESKEJ REPUBLIKY PROTI HYBRIDNÝM HROZBÁM

Prvé explicitné zmienky o prístupe Českej republiky k čeleniu hybridným hrozbám (všeobecne hybridnému pôsobeniu) možno časovo zasadiť do obdobia formulácie obsahu strategického dokumentu Audit národnej bezpečnosti z roku 2016, kde do širšieho spektra najvýznamnejších aktuálnych hrozieb pre Českú republiku boli zakomponované konkrétne aj vplyv na bezpečnosť občanov Českej republiky.[7].

Audit ukázal, že bezpečnostný systém je dobre pripravený na tzv. tradičné hrozby. Štát dokáže bojovať s kriminalitou, azylová a migračná politika je nastavená dobre a zvláda otázky spojené s migráciou, aj keď vždy je priestor na spresňovanie legislatívy aj nelegislatívnych opatrení. Audit však potvrdil, že tzv. moderné hrozby a najmä ich kombinácie vyžadujú oveľa zásadnejšiu pozornosť, než tomu bolo v minulosti. Schopnosť štátu detekovať a koordinovane riešiť prepojené útoky musí byť podľa auditu posilnená. Preto zintenzívni monitoring, spoluprácu medzi rezortmi a cvičenia aj spoluprácu so zahraničím a považuje za zodpovedné zapojiť do príprav aj verejnosť. Oveľa komplexnejšie potom sa musí tiež riešiť oblasť tzv. hybridných hrozieb a s nimi spojenými dezinformačnými útokmi.

Problematika čelenia hybridnému pôsobeniu a hybridným hrozbám či oblasť hybridného boja je veľmi rozsiahla. Často záleží na perspektíve a konkrétnom postoji jednotlivých expertov, akademikov či politických autorít, akým pohľadom na danú problematiku nazerať. Významnú a určujúcu úlohu hrá v tejto súvislosti voľba a identifikácia referenčného objektu a neopomenuteľne taktiež určitá reflexia na vlastné umiestnenie.

---

[4] Vláda SR 2018
[5] Vláda SR 2018
[6] Európska komisia 2016
[7] Vojenské rozhledy [online]. 2023. [cit. 2023-04-06]. Dostupné z:https://www.vojenskerozhledy.cz/kategorie-clanku/bezpecnostni-a-obranna-politika/aktualni-pristupy-hybridni-hrozby

V Českej republike je za oblasť čelenia hybridnému pôsobeniu zodpovedná vláda, ktorá by mala v ideálnom prípade prijímať zodpovedajúce opatrenia reagujúce na konkrétne hybridné hrozby a prejavy hybridného pôsobenia. Za čelenie jednotlivým aktivitám a prejavom hybridného pôsobenia sú v rámci svojich pôsobností následne zodpovedné jednotlivé rezorty (ministerstvá).

Hoci je vymenované celé spektrum zodpovedných subjektov, v Českej republike doposiaľ neexistuje spoločný koordinačný a spolupôsobiaci prvok, ktorý by komplexne zastrešil predmetnú problematiku.

Slovenská republika je členským štátom Európskej únie (EÚ) aj Severoatlantickej aliancie (NATO). V posledných rokoch sa začala aj v týchto organizáciách dostávať do popredia téma hybridných hrozieb a hybridnej vojny. Z toho dôvodu boli vytvorené aj špecializované inštitúcie, niektoré zamerané na špecifické oblasti spadajúce pod tento koncept a iné pokrývajúce hybridné hrozby ako celok. V záujme prevencie a boja proti hybridným hrozbám vznikli špecifické štruktúry patriace pod EÚ: Stredisko EÚ pre hybridné hrozby (EU Hybrid fusion cell) zriadené v rámci Centra EÚ pre analýzu spravodajských informácií (EU INTCEN) a rovnako aj The European Centre of excellence for Countering Hybrid Threats. V rámci NATO vznikol celý rad špecializovaných centier excelentnosti, z ktorých viaceré majú priamy vzťah k problematike hybridných hrozieb. Asi najvýznamnejšie z nich sú NATO StratCom CoE (Centrum excelentnosti NATO na strategickú komunikáciu) a NATO Cooperative Cyber Defence Centre of Excellence (Spoločné centrum excelentnosti NATO na kybernetickú obranu). Z pohľadu európskych inštitúcii, je jeden z najrelevantnejších bodov konceptu hybridných hrozieb pomenovaný v dokumente Spoločný rámec EÚ pre boj proti hybridným hrozbám ktorý uvádza: *„Definície hybridných hrozieb sú síce rôzne a musia zostať flexibilné, aby mohli reagovať na premenlivú povahu týchto hrozieb".* [8] Táto definícia si uvedomuje nejednoznačnosť pojmu, ktorý sa môže meniť v závislosti od krajiny, času, alebo situácie. Komisia rovnako považuje za dôležitý koordinovaný postup v boji proti hybridným hrozbám, no dodáva, že každá krajina má svoje vlastné slabé miesta, na ktoré sa musí pri obrane zamerať.

Hybridné hrozby informačných technológií vo verejnej správe predstavujú nový typ bezpečnostnej hrozby, ktorá kombinuje tradičné metódy s modernými technológiami a sociálnymi médiami a ktoré môžu ohroziť systémy a služby, ktoré poskytuje verejná správa. Nesú so sebou veľkú strategickú a bezpečnostnú hrozbu pre verejné inštitúcie, a preto by mali byť zvlášť zvažované aj v kontexte kybernetickej bezpečnosti.

V dnešnej dobe je informačná technológia (IT) kľúčovým prvkom pre fungovanie verejnej správy. Zahŕňa všetky informačné a komunikačné technológie používané na podporu a zlepšenie výkonu verejnej správy. Tieto technológie umožňujú vládam a iným verejným inštitúciám rýchlejšie a efektívnejšie poskytovať verejné služby a zlepšiť interakciu s občanmi. Zahŕňa širokú škálu technológií a aplikácií, vrátane webových stránok, mobilných aplikácií, softvéru pre správu záznamov, inteligentných systémov pre podporu rozhodovania elektronických služieb a online komunikačných nástrojov. Zároveň je to aj oblasť, kde môžu hybridné hrozby spôsobiť vážne problémy. Môžu mať za následok zneužitie informácií, stratu dát, či narušenie kritických systémov.

V kontexte verejnej správy sa môžu prejaviť napríklad cez:

- *dezinformačné kampane* – sú zamerané na zavádzanie verejnosti prostredníctvom falošných informácií, s cieľom ovplyvniť verejnú mienku, posilniť určité názory, oslabiť dôveru v médiá a demokratické inštitúcie alebo destabilizovať spoločnosť. Môžu sa šíriť rôznymi spôsobmi, vrátane sociálnych sietí, internetových fór, blogov alebo tradičných médií. V praxi sa realizujú prostredníctvom falošných alebo útočných informačných kampani. V hybridnej hrozbe môžu byť využité techniky dezinformácie na poskytnutie nepravdivých informácií, ktoré môžu spôsobiť rozkol alebo spochybniť legitimitu určitej inštitúcie. Môžu byť tiež využité na šírenie počítačových vírusov alebo zavádzať odkaz na falošné webové stránky.

[8] Európska komisia 2016

Často sú podporované alebo šírené politickými, podnikateľskými alebo inými záujmovými skupinami s cieľom dosiahnuť svoje ciele. Niektoré príklady dezinformačných kampaní zahŕňajú zavádzajúce informácie o voľbách, dezinformácie o klimatických zmenách, falošné správy o zdravotných témach, alebo propagovanie nenávisti a diskriminácie na základe rasy, pohlavia alebo sexuálnej orientácie. Je dôležité si uvedomiť, že dezinformačné kampane môžu mať vážne následky na spoločnosť a demokratické inštitúcie. Dôležité je preto kriticky sa pozerať na informácie, ktoré dostávame, a overiť ich pravdivosť pomocou spoľahlivých zdrojov a faktov.

- *kybernetické útoky* – vo verejnej správe, a nielen v nej, predstavujú vážne bezpečnostné riziko pre vládne inštitúcie, organizácie a občanov. Tieto útoky môžu zahrňovať pokusy o získanie citlivých informácií, úmyselné narušenie systémov alebo poškodenie infraštruktúry a majetku, môžu viesť ku krádeži citlivých údajov, porušeniu súkromia, ba dokonca môžu až paralyzovať fungovanie kritických systémov. Zahŕňajú pokusy o zneužitie firemných sieti, slúžiacich na poskytovanie verejnej služby. Môžu to byť napríklad útoky na databázy s cennými dátami, ktorej účelom môže byť vymôcť si výkupné alebo ukradnúť informácie. Niektoré príklady kybernetických útokov na verejnú správu zahŕňajú:
- *Phishing:* Tento typ útoku sa snaží získať citlivé informácie od používateľov prostredníctvom zavádzajúcich e-mailov alebo webových stránok.
- *Malware:* Tento typ útoku sa snaží infikovať počítače alebo siete škodlivým softvérom s cieľom získať prístup k informáciám alebo narušiť systémy.
- *Ransomware:* Tento typ útoku sa snaží blokovať prístup k dôležitým informáciám alebo systémom a následne požaduje výkupné za ich odblokovanie.
- *DDoS útoky:* Tieto útoky sa snažia preťažiť webové stránky alebo sieťové systémy prostredníctvom veľkého počtu požiadaviek, čo môže spôsobiť výpadky a straty dát.
- *sociálne inžinierstvo* – hybridné hrozby môžu byť jeho produktom. Ide o formu kybernetického útoku, ktorý sa snaží zneužiť dôveru a ochotu pomôcť ostatným. Sociálne inžinierstvo je technika, ktorou útočníci využívajú sociálne interakcie a psychologické vplyvy na ľudí s cieľom získať citlivé informácie alebo zaviesť obeť do niečoho nebezpečného. Je predstavované šírením nezmyslov s cieľom získať citlivé informácie o inštitúciách verejnej správy alebo jednotlivých zamestnancov, získať prístup do životných údajov používateľa alebo prevziať kontrolu nad jeho účtom. Príklady sociálneho inžinierstva zahŕňajú *phishing* (získavanie citlivých informácií prostredníctvom zavádzajúcich e-mailov alebo webových stránok), *pretexting* (falošné tvrdenie, že útočník má oprávnenie na určité akcie) alebo *baiting* (zavádzajúce ponuky alebo príležitosti na získanie informácií alebo prístupu k systémom).Sociálne inžinierstvo sa často využíva ako prvá fáza útoku na organizácie alebo jednotlivcov, keďže môže byť účinnejšie a menej nákladné ako pokusy o prelomenie technickej ochrany. Často sa zameriava na zamestnancov organizácií, ktorí môžu byť vnímaní ako slabé miesto v systéme ochrany.

Boj proti hybridným hrozbám vychádza z nutnosti kooperácie zainteresovaných subjektov založenej na realizácií opatrení, ďalej pružnej výmene informácií, a koordinácií postupov. Ide teda o koordinovaný a komplexný prístup. Boj proti hybridným hrozbám v informačných technológiách vo verejnej správe vyžaduje kombináciu technologických a organizačných opatrení. Niektoré z možných krokov, ktoré by mohli byť účinné pri boji proti hybridným hrozbám na informačné technológie vo verejnej správe, sú:

Vyspelé technologické riešenia: Verejná správa by mala mať k dispozícii vyspelé technologické riešenia na detekciu, monitorovanie a prevenciu kybernetických útokov a iných hybridných hrozieb. Tieto technológie by mali byť prispôsobené špecifickým potrebám a rizikám verejnej správy a mali by identifikovať a rýchlo reagovať na prípadné hrozby a anomálie.

Zabezpečenie kritických systémov: Kritické systémy a informačné systémy verejnej správy by mali byť chránené pomocou vyspelých technologických riešení na detekciu a prevenciu kybernetických útokov a iných hybridných hrozieb. K tomu slúžia napr.: *antivírusový softvér*, ktorý je základnou technológiou pre detekciu a prevenciu kybernetických útokov. Pomáha chrániť počítače a siete pred škodlivým softvérom a vírusmi; *firewall* pomáha chrániť počítače a siete pred neoprávneným prístupom tým, že kontrolovať tok dát medzi sieťami a zariadeniami; *Intrusion Detection System (IDS)*, sleduje sieťovú aktivitu a hľadá neobvyklé vzory správania, ktoré by mohli naznačovať kybernetický útok; *Intrusion Prevention System (IPS),* ktorý sa podobá na IDS, ale namiesto toho, aby iba identifikoval neobvyklé vzory správania, sa pokúsi zabrániť kybernetickému útoku ešte predtým, ako sa stane; *SIEM (Security Information and Event Management)*, zabezpečuje monitorovanie, správu a analýzu rôznych udalostí v systéme na detekciu neobvyklých vzorov a varovných signálov, ktoré by mohli naznačovať kybernetický útok. Ďalej to môžu byť bežné siete ako *Virtual Private Network (VPN)*, ktorý umožňuje šifrovanú a bezpečnú komunikáciu medzi zariadeniami a sieťami, v ktorých sú dáta prenášané.; *Advanced Threat Protection (ATP)* je technológia, ktorá používa rôzne metódy na detekciu a prevenciu pokročilých hrozieb, ako sú napríklad zero-day útoky alebo APT útoky [9] ; *Data Loss Prevention (DLP)* pomáha chrániť dôverné a citlivé dáta pred únikom alebo zneužitím. Pomáha monitorovať a riadiť tok dát, čím sa minimalizuje riziko straty alebo zneužitia dát.

Školenie zamestnancov: Zamestnanci verejnej správy by mali byť pravidelne školení v oblasti kybernetickej bezpečnosti a v rámci toho by mali byť informovaní o najnovších hrozbách a o tom, ako sa im vyhnúť alebo ich odvrátiť. Mali by byť obozretní pri otváraní príloh e-mailov, návšteve nebezpečných webových stránok a používaní verejných Wi-Fi sietí.

Prísna kontrola prístupov: Prístup k informačným systémom by mal byť prísne kontrolovaný a overovaný, aby sa minimalizovalo riziko zneužitia prístupov. V praxi to možno realizovať napr. zavádzaním silných hesiel a autentifikačných mechanizmov, viacúrovňovým overovaním totožnosti, ad hoc vytvoreným a časovo obmedzeným prístupovým kódom.

Zabezpečená komunikácia: Komunikácia medzi informačnými systémami by mala byť zabezpečená pomocou šifrovania a iných technológií na ochranu dát.

Spolupráca a koordinácia: Boj proti hybridným hrozbám by mal byť koordinovaný a spolupracujúci a malo by ho charakterizovať úsilie medzi rôznymi orgánmi verejnej správy, ako aj súkromným sektorom a občianskou spoločnosťou.

---

[9] Zero-day útoky sú kybernetické útoky, ktoré využívajú zraniteľnosti v softvérových systémoch, ktoré sú zatiaľ neznáme alebo nemajú opravu. Tento typ útoku môže byť veľmi nebezpečný, pretože táto zraniteľnosť ešte nebola odhalená a neexistuje žiadna obrana alebo náprava, ktorá by ju chránila. Zero-day útoky sú často používané k šíreniu škodlivého softvéru alebo na získanie neoprávnenej prístupu k cenným dátam. Využívajú sa na útoky na rôzne ciele, vrátane podnikov, vládnych inštitúcií, bankových systémov a ďalších kritických infraštruktúr. Vývojári softvéru sa snažia minimalizovať riziko zero-day útokov tým, že systematicky vyhľadávajú zraniteľnosti a aktualizujú softvér s opravami bezpečnostných chýb. Bezpečnostné aktualizácie sú však často oneskorené alebo sa nedostanú ku všetkým používateľom, takže je dôležité, aby používatelia boli obozretní a mali aktuálny antivírusový softvér a firewally. Existujú aj špeciálne nástroje a technológie, ktoré sa používajú na detekciu zero-day útokov. Tieto nástroje monitorujú sieťovú prevádzku a vyhľadávajú neobvyklé vzory, ktoré by mohli naznačovať pokus o zero-day útok. V prípade zistenia podozrivých aktivít môžu tieto nástroje automaticky reagovať a obmedziť prístup počítača alebo používateľa. Vzhľadom na neustále sa meniace hrozby v kybernetickom priestore je dôležité mať nielen správne nástroje na detekciu a prevenciu zero-day útokov, ale aj pripravenosť a schopnosť rýchlo reagovať a minimalizovať škody v prípade, že sa takýto útok stane.
Advanced Persistent Threat (APT) útoky sú sofistikované kybernetické útoky, ktoré sú zamerané na dlhodobú infiltráciu cieľového systému alebo siete a získanie neoprávnenej prístupu k citlivým údajom alebo zdrojom. Útoky APT sa od bežných kybernetických útokov líšia tým, že sú plánované, cielené a vytrvalé, pričom útočníci používajú rôzne techniky, aby sa vyhli detekcii a zabránili zisteniu svojej identity.

Pravidelné aktualizácie a overenia: Informačné systémy a technologické riešenia by mali byť pravidelne aktualizované a overované, aby sa zabezpečilo, že sú stále účinné proti najnovším hrozbám. Tieto opatrenia môžu zahŕňať pravidelné aktualizácie softvéru, zálohovanie dôležitých dát.

Vytvorenie protokolov a postupov pre rýchlu a účinnú reakciu : Je dôležité mať pripravené plány a protokoly na rýchlu a efektívnu reakciu na hybridné hrozby. Organizácie verejnej správy by mali mať zostavené tzv. bezpečnostné plány. Na ochranu proti hybridným hrozbám existuje niekoľko protokolov a postupov, ktoré pomáhajú identifikovať a eliminovať hrozbu. Spomenúť možno napr. tzv. *Hybrid Threat Response (HTR) framework*, ktorý bol vyvinutý NATO a EÚ. Tento rámec poskytuje štruktúrovaný postup na reakciu na hybridné hrozby, ktorý zahŕňa detekciu hrozby, analýzu, hodnotenie a plánovanie reakcie. HTR rámec sa zameriava na koordinovanú reakciu a spoluprácu medzi rôznymi inštitúciami a organizáciami. Ďalším protokolom je tzv. *Cyber Incident Response Plan (CIRP)*, ktorý sa zameriava na reakciu na kybernetické útoky, ktoré môžu byť súčasťou hybridných hrozieb. CIRP zahŕňa definíciu zodpovednosti a úloh, koordináciu, plánovanie, analýzu a správu kybernetických incidentov. Okrem týchto protokolov existujú aj ďalšie postupy a nástroje, ktoré sa používajú na reakciu na hybridné hrozby. Patrí sem napríklad pripravenosť a plánovanie, ktoré zahŕňajú predbežné opatrenia a pravidelné cvičenia a simulácie, aby sa zvýšila efektivita a rýchlosť reakcie. Dôležitou súčasťou protokolov na reakciu na hybridné hrozby je tiež spolupráca medzi rôznymi inštitúciami a organizáciami. Spolupráca umožňuje zdieľanie informácií a skúseností, koordináciu a lepšiu efektivitu pri riešení hrozby.

Zlepšenie legislatívy a regulácie: Zavedenie a presadzovanie prísnych noriem a nariadení na ochranu informačných systémov, kritických infraštruktúr a sietí. Ochrana informačných systémov verejnej správy je kritickou otázkou pre bezpečnosť štátu a občanov. Preto existujú právne predpisy, ktoré upravujú ochranu informačných systémov verejnej správy. V Európskej únii sú najdôležitejšie smernice o kybernetickej bezpečnosti, ktoré sa týkajú aj ochrany informačných systémov verejnej správy. *Smernica NIS (Network and Information Systems Directive)* [10] stanovuje minimálne bezpečnostné požiadavky pre prevádzkovateľov kritických služieb a digitálne služby, vrátane verejnej správy. Ďalšou smernicou, ktorá sa týka ochrany informačných systémov verejnej správy, je *GDPR (General Data Protection Regulation)*. Táto smernica stanovuje pravidlá na ochranu osobných údajov a ich spracovávanie. GDPR tiež ukladá povinnosť poskytovať bezpečnostné opatrenia na ochranu osobných údajov a informačných systémov. V rámci Slovenskej republiky existuje zákon č. 69/ 2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, ktorý sa zameriava na ochranu informačných systémov a kybernetickú bezpečnosť. Tento zákon stanovuje povinnosť prevádzkovateľov kritických informačných infraštruktúr a digitálnych služieb na poskytovanie informácií o kybernetickej bezpečnosti a oznámenie bezpečnostných incidentov. Ďalší zákon, ktorý sa týka ochrany informačných systémov verejnej správy, je zákon č. 18/2018 o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Tento zákon stanovuje pravidlá na ochranu osobných údajov a ich spracovávanie a ukladá povinnosť zabezpečiť bezpečnostné opatrenia na ochranu osobných údajov.

Okrem toho existujú aj iné právne predpisy a smernice, ktoré sa týkajú ochrany informačných systémov verejnej správy. Ich cieľom je zabezpečiť vysokú úroveň kybernetickej bezpečnosti a ochrany osobných údajov, čo prispieva k ochrane štátu a občanov pred kybernetickými hrozbami. Hoci sa legislatíva na ochranu informačných systémov verejnej správy neustále vyvíja a aktualizuje, vzhľadom na rastúce množstvo kybernetických hrozieb je nutné venovať jej väčšiu a dôslednejšiu pozornosť. De lege ferenda by sme navrhli v rámci legislatívnej úpravy:

- *zvýšenie sankcií a trestov za kybernetické útoky a zneužívanie osobných údajov* – zákony by mali byť prísnejšie a vynucovanie by malo byť dôraznejšie na tých, ktorí porušujú zákony;

[10] Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii

- *zabezpečenie vyšších národných štandardov kybernetickej bezpečnosti* – štát by mal stanoviť minimálne bezpečnostné požiadavky pre informačné systémy verejnej správy a definovať postupy na identifikáciu a odstránenie bezpečnostných slabín;
- zavedenie kontroly na dodávateľov a dodávateľské reťazce – je dôležité, aby dodávatelia boli skúmaní z hľadiska bezpečnosti ich produktov a služieb, ktoré dodávajú verejnej správe.

Celkovo by zlepšenie legislatívy na ochranu informačných systémov verejnej správy malo prispieť k väčšej ochrane kritických informačných infraštruktúr, osobných údajov a kybernetickej bezpečnosti, čo by malo mať pozitívny vplyv na bezpečnosť štátu a občanov.

Celkový prístup k boju proti hybridným hrozbám by mal byť založený na spolupráci a koordinácii rôznych orgánov a sektorov a mal by byť prispôsobený aktuálnym hrozbám a trendom. Úspešná ochrana proti hybridným hrozbám by mala byť založená na komplexnom a dobre koordinovanom prístupe, ktorý zahŕňa kombináciu technických, organizačných a ľudských opatrení.

Na záver konštatujeme, že za jednu z najviac zraniteľných oblastí, ktorá výraznou mierou prispieva k tomu, že riziko hybridnej hrozby aj v oblasti informačných technológií vo verejnej správe je veľmi vysoké, považujeme nízke povedomie spoločnosti ako takej o kybernetickej bezpečnosti. Z tohto dôvodu je zvýšenie povedomia o tomto fenoméne mimoriadne dôležité. Veríme , že tento článok k tomu prispel.

Hybridne hrozby v rovine priestupkov by mohli podľa nášho názoru byť definovane ako základná forma zneužitia technologických ale verejne prístupných nástrojov alebo prostriedkov na šírenie hoaxov, dezinformácií a iných hybridných hrozieb, ktoré sme v predošlých častiach vymenovali a definovali. Zároveň môžeme zaviesť aj inú metriku rozdelenia a povahy vzhľadom na spôsobenú škodu kde sa budeme opierať najmä o podstatu identifikovania hybridnej hrozby kde predikovať je ich ťažké ale následne po pôsobení na systém inštitúcií, ekonomiku , subjekt a i... , môžeme vytvoriť škálu priestupkov a k nim vyšpecifikovať určite sankcie. Tu by však mala existovať funkčnosť právneho systému na úrovni prejednavania takýchto priestupkov. Je nutne ich vedieť správne posúdiť a v prípade nutnosti požadovať aj o odborne stanovisko pre následne udelenie sankcie čo značne predražuje a komplikuje prejedanie priestupku samotného s ohľadom na hospodárnosť a účelnosť konania samotného. Následne na uvedené je na zvážení zákonodarcu či v legislatívnej norme ako je zákon o priestupkoch by našiel odvahu definovať hybridné hrozby ako priestupok.

Hybridne hrozby v rovine trestnoprávnej: ak sme sa zaoberali ako vyšpecifikovať alebo vydefinovať v oblasti zákona o priestupkoch hybridne hrozby tak v trestnoprávnej rovine by sme ich mohli definovať jednoduchým spôsobom a to jedeným paragrafovým znením a zaradiť ho do trestného zákona, ale ak uvažujeme nad spôsobom ako ho paragrafovom znení nazvať, napadá nám myšlienka skôr kde ho zaradiť a to najmä do oblasti spôsobenia škody na majetku. Pozor! Bude to postačujúce? Preto sa nám vynorila v mysli myšlienka definovať v trestnom kódexe slovenskej republiky hybridne hrozby viac širšie a následne sa s nimi vysporiadať čo do jednotlivých presahov jednotlivých druhov trestného práva. Napríklad v rovine majetkovej, rovine duševného vlastníctva alebo rovine hospodárskej, rovine šírenia poplašnej správy ako aj iných mnohých. Navrhli by sme aby v tejto oblasti jednali a tvorili základ rozdelenia odborne skupiny kde by sa definovala nielen miera spôsobenej škody ale aj spôsob akým by boli vytvorené a aký účel mali splniť a najmä čo nimi páchateľ sledoval. Potom by predpokladáme vznikla škála na ich ukotvenie v právnych kódexoch slovenskej republiky, ktorými sa dnes riadi celá naša vyspela spoločnosť. Upriamujúc na rastúcu sa mieru digitalizácie a presahu informačných technológií do nášho každodenného života, konštatujeme : „Bezpečnosť je život a život musí byť bezpečný aj s ohľadom na spejúcu dobu informatizácie“.

ZÁVER

Bez ohľadu na definíciu pojmu hybridných hrozieb je nevyhnutné, aby každý štát vedel dostatočne reagovať na hybridné útoky konané proti svojim občanom. Legislatíva je nutným základom, mala by zabezpečiť aby bezpečnostné zložky mohli reagovať v čo najkratšom, reálnom čase. Obrana musí byt najefektívnejšia, ktorá je spôsobilá útoku zabrániť, odvrátiť alebo zmenšovať škody, či už na národnej úrovni, alebo v rámci medzinárodnej spolupráce . Veľmi účinnou a lacnou zbraňou proti hybridným hrozbám je vzdelaná, sebavedomá demokratická spoločnosť, ktorá je ochotná brániť demokratické hodnoty aj svoju národnú identitu.

LITERATÚRA:

MARCHEVKA, P., NÉMETH, Ľ., 2010. *Diskusia k základným pojmom krízového riadenia.* (http://fsi.umiza.sk.).

MILO, D. 2018. *Mapovanie zraniteľnosti SR v oblasti hybridných hrozieb*. GLOBSEC. Bratislava (https://www.globsec.org/wpcontent/uploads/2018/08/Zranitelnost-SR-v-oblasti-hybridnychhrozieb-web.pdf).

VOLNER, Š. 2009. *Bezpečnosť, riziká a hrozby 21. storočí.* Bratislava: IRIS, ISBN 978-80-8925-636 5.

VOLNER, Š. 2012. *Bezpečnosť, riziká a hrozby 21. storočí*, Bratislava: IRIS, ISBN: 978-80-8925-674 7.

Ministerstvo obrany SR. 2016. *Biela kniha o obrane SR. Ministerstvo obrany: Bratislava* (https://www.mod.gov.sk/data/BKO2016_LQ.pdf).

Vláda SR. 2018. Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám. *Bratislava* (https://rokovania.gov.sk/RVL/Material/23100/1).

Európska komisia. 2016. *Spoločné oznámenie Európskemu parlamentu a rade: Spoločný rámec pre boj proti hybridným hrozbám - reakcia Európskej únie. Brusel.* (https://eurlex.europa.eu/legalcontent/SK/TXT/PDF/?uri=CELEX:52016JC0018&from=EN)

INTERNETOVÉ ZDROJE:

Vojenské rozhledy [online]. 2023. [cit. 2023-04-06]. *Dostupnéz:https://www.vojenskerozhledy.cz/kategorie-clanku/bezpecnostni-a-obranna-politika/aktualni-pristupy-hybridni-hrozby*

PRÁVNE PREDPISY:

Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii

Trestný zákon č. 300/2005 Z. z.

Zákon o priestupkoch č 372/1990 Z. z.

KONTAKT NA AUTOROV:

Mgr. Nataša Brabcová, LL.M., MBA
externý doktorand, vedoucí odborných předmětu
TRIVIS – SŠV A VOŠ PK a KŘ Praha, s.r.o.,
Hovorčovická 281/11, 182 00 Praha 8
tel: + 420 773 658 103
e-mail: natašabrabcova@gmail.com

PhDr. JUDr. Mgr. Ervín Šimko, LL.M
externý doktorand
Katedra verejnej správy a krízového manažmentu
Akademia Policajného zboru v Bratislave

Sklabinská 1, 835 17 Bratislava 35
tel: + 421 917 113 038
e-mail: simko.ervin@gmail.com