ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PEDAGOGICKÁ

KATEDRA VÝPOČETNÍ A DIDAKTICKÉ TECHNIKY

PRINCIPY A PŘÍKLADY HYBRIDNÍCH HROZEB JAKO SOUČÁSTI MEZINÁRODNÍCH SPORŮ

Bakalářská práce

Martin Haváček

Informatika se zaměřením na vzdělávání

Vedoucí práce: PhDr. Zbyněk Filipi, Ph.D.

Plzeň 2021

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně s použitím uvedené literatury a zdrojů informací.

V Plzni 25. června 2021

Martin Haváček *v. r.*

OBSAH

SEZNAM ZKRATEK

CERT	Computer Emergency Response Team
CTHH	Centrum proti terorismu a hybridním hrozbám
COVID-19	Nemoc způsobená virem SARS-CoV-2
CSIRT	Computer Security Incident Response Team
ČLR	Čínská lidová republika
ČR	Česká republika
DIMEFIL	Diplomatic/Political, Information, Military, Economic, Financial, Intelligence, Legal
DoS	Denial of service
DDoS	Distributed Denial of Service
KII	Kritická informační infrastruktura
IMAP	Internet Message Access Protocol
MVČR	Ministerstvo vnitra České republiky
MZČR	Ministerstvo zdravotnictví České republiky
NUKIB	Národní úřad pro kybernetickou a informační bezpečnost
OS	Operační systém
RDP	Remote Desktop Protocol
RF	Ruská federace
SWOT	Strengths, weaknesses, opportunities, threats
ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

ÚVOD

S postupnou digitalizací naší společnosti stojíme před stále novějšími výzvami spojené s tímto postupem doby. Vzhledem ke geopolitické situaci České republiky jsou pravděpodobně největším nebezpečím pocházejíce z cizí země hybridní hrozby – ať už je původce státní či nestátní aktér. Hybridní hrozby pokrývají zejména kyberprostor – proto se bakalářská práce zabývá zejména kybernetickými (hybridními) hrozbami.

V současné době se ukazuje, že hybridní hrozby používají nástroje z celého spektra dimenzí moci známých jako DIMEFIL. Proto se kvalifikační práce věnuje i tomuto frameworku DIMEFIL – jednak vysvětlení použití tohoto frameworku a jednak jeho aplikaci.

Kvalifikační práce si klade za cíl představit možnosti práce s otevřenými relevantními zdroji v oblasti hybridních hrozeb (jako například výroční zprávy orgánů veřejné správy či rozvědek), které jsou součástí mezinárodních sporů, a v oblasti analýzy připravenosti České republiky z veřejně dostupných zdrojů. Následně ověřit možnosti využití dělení dimenzí moci DIMEFIL u hybridních hrozeb, které se odehrávají zejména v kyberprostoru.

Část bakalářské práce se věnuje i uvedení příkladů infiltrací a kybernetických (hybridních) hrozeb. Následně kategorizuje i popsané příklady infiltrací podle přístupové vrstvy – tedy podle úrovně přístupu útočníka.

Poslední část bakalářské práce se věnuje připravenosti České republiky na identifikované hybridní hrozby – k tomu poslouží strategický vládní dokument Audit národní bezpečnosti. Analýza připravenosti se věnuje zejména posouzení plnění doporučení bezpečnostní komunity.

1 HYBRIDNÍ HROZBY A BEZPEČNOSTNÍ PROSTŘEDÍ ČESKÉ REPUBLIKY

Hybridní hrozby představují jednu z reálných ohrožení bezpečnosti České republiky (dále také „ČR“) (Bezpečnostní informační služba, 2019) (Štalmach, 2018). Trend využívání hybridních hrozeb je znatelný z veřejných výročních zpráv Bezpečnostní informační služby, dále je z těchto výročních zpráv patrné, že toto riziko pochází zejména z aktivit Ruské federace (dále také „RF“) a Čínské lidové republiky (dále také „ČLR“), které tím sledují různé aktivity (Bezpečnostní informační služba, 2019).

Definice hybridních hrozeb je nejednotná a velice pružná, což je žádané. (European Commission, 2016). Jedná se o podobnou problematiku jako s definicí terorismu – která je proměnlivá napříč světem. Hybridní hrozby vznikají z podstaty věci pomocí kombinací a křížením různých entit (hrozeb). Těmto hrozbám je složitější čelit, jelikož v konvenční válce bývá jedno spojenectví aktérů proti druhému spojenectví aktérů působící navzájem proti sobě generickými hrozbami, kdežto u hybridních hrozeb je rozeznání samotné hybridní hrozby či dokonce jejího původce složitější (Štalmach, 2018).

Nelze pojímat definici hybridní hrozby podobně jako definici například konvenční války, jelikož pod hybridními hrozbami rozumíme spektrum metod, jakým je konflikt vedený (Ministerstvo vnitra České republiky, 2016).

1.1 VÝVOJ HYBRIDNÍCH HROZEB

Štalmach (2018) předpokládá v budoucnosti větší propojenost státních a nestátních zapojených původců, kteří budou tvořit strategické uskupení; zároveň předpokládá zásadní využívání nekonvenčních činností – viz Tabulka 1.

Minulost	Současnost	Budoucnost
Propojování zájmů zejména nestátních bezpečnostních aktérů	Působení zájmů zejména státních bezpečnostních aktérů	Propojování zájmů státních a nestátních aktérů
Ad hoc propojení bezpečnostních aktérů	Operační aliance bezpečnostních aktérů	Strategické aliance bezpečnostních aktérů
Převaha konvenčních prostředků působení	Rovnováha konvenčních a nevojenských schopností činností	Převaha nemateriálních prostředků působení

Tabulka 1 Trend vývoje hybridních hrozeb, převzato (Štalmach, 2018) a upraveno

V důsledku významné digitalizaci celé společnosti se i mezinárodní spory „digitalizují" – přesouvajíc se na internet. Nejširší definicí mezinárodního sporu můžeme rozumět spor dvou a více aktérů (kteří mohou patřit mezi vládu nebo například i mezi soukromé osoby), přičemž původci se nachází na jiných částech světa, v případě sporu na jednom území či státu se jednání o spory teritoriální. (Merrills, 2019)

1.2 KYBERNETICKÉ HYBRIDNÍ HROZBY

Dle Gerasimovy doktríny je nutné využití součástích inovativních postupů u současných výzev – Gerasimova doktrína je vžitý název hlavní myšlenky uveřejněné v ruském časopisu Vojensko-průmyslový kurýr. Valerij Vasiljevič Gerasimov byl toho času náčelník generálního štábu RF. Asymetrická „válka" probíhá zejména v kybernetickém prostoru, jedná se o nový způsob vedení války, který omezuje rozpoznání, kdy se vede válka; zatímco v konvenční válce je pro obyvatelstvo jednoznačně rozpoznatelné, hybridní válka je optikou obyvatelstvem těžko vnímatelné – jelikož se jich dotýká spíše nepřímo.

Cybernetic security – kybernetická bezpečnost v sobě zahrnuje technické a organizační opatření pro bezpečnost informací, čímž se rozumí „zajištění důvěrnosti, integrity a dostupnosti informací a dat" – jedná se o definici pojmu podle ustanovení § 2 odst. 1. písm. c) zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Problematiku kybernetické bezpečnosti v České republice řeší právě zákon č. 181/2014 Sb., o kybernetické bezpečnosti, který provádí platnou Směrnici Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečností sítí a informačních systémů v Unii.

Kybernetickou bezpečnost nelze brát na lehkou váhu. Kybernetický prostor není již záležitostí pár nadšených jedinců, ale v současné době bez něj těžko obejdeme; internet je nezpochybnitelnou součástí kritické infrastruktury – zejména v oblasti bankovnictví, objednávkové systémy léků, nebo například přibližovací služba řízení letového prostoru. S postupem let se stávají kybernetické útoky mnohem sofistikovanější, v mnoha případech jsou metody obfuskace až tak dokonalé, že není možné původce identifikovat. To je způsobeno evolucí technik a technologií útočníků (Vojenské zpravodajství České republiky, 2020).

1.3 INTERNET JAKO SOUČÁST KRITICKÉ INFRASTRUKTURY ČR

Internet není všeobecně (dle ustanovení zákona č. 240/2000 Sb., zákon o krizovém řízení a o změně některých zákonů (krizový zákon)) součástí kritické infrastruktury – dle § 2 písm. i) je: „*prvek kritické infrastruktury 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*". Prvky kritické infrastruktury jsou stanoveny nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, to určuje průřezová kritéria pro zařazení. Na jistá odvětví kybernetického prostoru lze aplikovat zejména tyto kritéria dle výše zmíněného nařízení vlády: „*ekonomický dopad s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu*" a „*dopad na veřejnost s mezní hodnotou rozsáhlého omezení*

poskytovaných nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob".

Pojem Kritická informační infrastruktura (dále také „KII") zavádí zákon č. 181/2014 Sb., o kybernetické bezpečnosti, který ho definuje jakožto „prvek nebo soubor prvků kritické infrastruktury v odvětví komunikační a informačních systémů v oblasti kybernetické bezpečnosti".

1.4 AUDIT NÁRODNÍ BEZPEČNOSTI

V roce 2016 byl vypracován bezpečnostní komunitou pod záštitou Ministerstva vnitra České republiky (dále také „MVČR") a následně Vládou ČR schválen materiál s názvem Audit národní bezpečnosti, který posuzuje odolnost České republiky vůči bezpečnostním hrozbám. Dokument identifikuje rizika, je provedena SWOT analýza („SWOT" je akronym slov strengths, weaknesses, opportunities threats), jsou uvedena stručná doporučení pro danou oblast k posílení odolnosti a přiřazení odpovědných institucí z rámce bezpečnostního systému ČR a základní nástroje pro snížení či eliminaci rizik a hrozeb. (Ministerstvo vnitra České republiky, 2016)

Audit národní bezpečnosti řeší deset oblastí, které rozdělují identifikovaná rizika do následujících oblastí: antropogenní hrozby, bezpečnostní aspekty migrace, energetická, surovinová a průmyslová bezpečnosti, extremismus, hrozby v kyberprostoru, hybridní hrozby a jejich vliv na bezpečnost občanů ČR, organizovaný zločin, přírodní hrozby, působení cizí moci a terorismus. Z celkových deseti oblastí se tedy hybridním hrozbám a kyberprostoru věnují hned dvě samostatné oblasti. (Ministerstvo vnitra České republiky, 2016)

V oblasti hrozeb kyberprostoru jsou rizika rozdělena do dalších pěti skupin: kybernetická špionáž, kyberterorismus, narušení nebo snížení bezpečnosti eGovernmentu, narušení nebo snížení odolnosti IT infrastruktury a nepřátelské kampaně (Ministerstvo vnitra České republiky, 2016).

V oblasti hybridních hrozeb jsou rozvedeny sféry moci DIMEFIL („DIMEFIL" je akronym slov Diplomatic, Information, Military, Economic, Financial, Intelligence, Legal), kterým je také věnována kapitola v této bakalářské

práci. Identifikovaná rizika jsou rozdělena v této oblasti podle předpokládaného zacílení proti pilířům České republiky: bezpečnost a obrana, fungující ekonomika a soudržná společnost a její ztotožnění se s ideově-hodnotovým zakotvením státu. V pilíři bezpečnost a obrana se hybridní hrozby prolínají s oblastí hrozeb v kyberprostoru. (Ministerstvo vnitra České republiky, 2016)

1.5 BEZPEČNOSTNÍ PROSTŘEDÍ ČESKÉ REPUBLIKY

Pro vypořádání se s kyberkriminalitou, která je zásadně odlišná od „konvenční" kriminality – zejména latentností, obtížnou identifikací pachatele a lhostejností společnosti, vznikají bezpečnostní týmy a infrastruktura týmů Computer Emergency Response Team (dále také „CERT") a Computer Security Incident Response Team (dále také „CSIRT"). Význam zkratek CERT/CSIRT se liší zejména v názvu a historickém kontextu. V dnešní době můžeme pod těmito zkratkami rozumět tým, který se věnuje kybernetickým hrozbám a bezpečnostním incidentům. V agendě CERT/CSIRT týmů je i spolupráce s jinými obdobnými týmy při řešení bezpečnostních incidentů. Státy si zřizují vlastní CERT/CSIRT, které vzhledem k omezené možnosti vstupu do fyzické infrastruktury fungují jako tzv. poslední instance (last resort), kdy jejich primární úkol je zprostředkování kontraktu a případné koordinaci jednotlivých aktérů při řešení problému – zejména tedy při útoku. (Kolouch & Bašta, 2019)

Národní CERT je ustanoven dle § 17 zákona č. 181/2014 Sb. o kybernetické bezpečnosti, kde je ustanovena činnost Národního CERT, a je provozován korporací CZ.NIC, z. s. p. o. na základě veřejnoprávní smlouvy uzavřené s Českou republikou. (Kolouch & Bašta, 2019)

Český Vládní CERT je ustanoven dle § 20 zákona č. 181/2014 Sb. o kybernetické bezpečnosti, tento paragraf poskytuje rámec činností, kterými se Vládní CERT ČR zabývá – jeho činnost je zejména v oblasti státních správ, samospráv a kritické infrastruktury. Vládní CERT je ze zákona o kybernetické bezpečnosti součástí Národního úřadu pro kybernetickou a informační bezpečnost. (Kolouch & Bašta, 2019)

V České republice také působí Centrum proti terorismu a hybridním hrozbám (dále také „CTHH“), což je vedeno jako oddělení pod Odborem bezpečnostní politiky Sekce vnitřní bezpečnosti a policejního vzdělávání (Ministerstva vnitra České republiky, 2021). Pomocí ustanovení zákona č. 106/1999 Sb. o svobodném přístupu k informacím bylo zjištěno, že CTHH neřeší oblast kybernetické bezpečnosti – jedná se o malý odbor s 12 osobami ve služebním poměru a 1 osobou v pracovním poměru; nepodařilo se získat vyhodnocení činnosti CTHH, odpověď na dotaz ohledně vyhodnocení roční činnosti zní: „*sděluji, že vyhodnocení činnosti CTHH probíhá neformálně a není zpracováváno ve formě, kterou je možné poskytnout jako přílohu tohoto dopisu. Jako ředitel odboru, pod nějž CTHH spadá, mohu uvést, že toto oddělení plní svěřené úkoly zcela uspokojivě.*“ (Ministerstvo vnitra České republiky, 2021).

2 TAXONOMIE NARUŠENÍ BEZPEČNOSTI INFORMACÍ

Při výkladu definice „bezpečnosti informací“, která již byla uvedena v první kapitole, uvažujeme společně v kontextu s narušením bezpečnosti informací zejména narušením důvěrnosti, integrity či dostupnosti informací.

Infiltrací můžeme mimo jiné rozumět průnik do cizího prostředí, pro účely této kvalifikační práce se pod pojmem infiltrace rozumí zejména počítačová infiltrace, tedy průnik do počítačové sítě či způsob narušení počítačové sítě.

Pro snazší přehlednost typických příkladů možných infiltrací v podobě napadení počítačové sítě, je nutné definovat základná taxonomii. Tato bakalářská práce si neklade za cíl popsat kompletní metody počítačových útoků, ale s uvedenými typovými příklady se pracuje v následujících kapitolách.

V rámci taxonomie počítačových útoků lze rozlišovat tři úrovně, které se od sebe liší úrovní přístupových práv uživatele. První úroveň nevyžaduje žádná přístupová práva útočníka, aby se infiltroval do sítě; druhá úroveň již vyžaduje běžná „uživatelská“ práv pro přístup do počítačové sítě, aby bylo možné provést její narušení. Poslední tedy třetí úroveň již vyžaduje „root“ přístup, tedy uživatelský přístup na úrovni administrátora. (Chapman, et al., 2011)

Pakliže jsou v síti a počítačích nastaveny přístupová práva špatně – tedy například „basic“ uživatelé mají práva k instalacím software, když to jejich běžná činnost s počítačem nevyžaduje, pak následující taxonomii nelze použít. Zejména dojde k promísení druhé a třetí přístupové úrovně.

2.1 PRVNÍ ÚROVEŇ: BEZ PŘÍSTUPOVÝCH PRÁV

V této úrovni se zejména využívá povahy počítačových sítí, která je z již z podstaty fungování velice otevřená. (Chapman, et al., 2011)

Útoky na této úrovni v kontextu mezinárodních sporů mohou mít dva cíle – zdiskreditovat poskytovatele služby (nedostupností, únikem dat etc.) a získat

přístup k útoku na druhé úrovni (výjimečně na třetí úrovni – ale to předpokládá zásadní pochybení odborníka s administrátorským přístupem).

2.1.1 DoS ÚTOKY

Zkratka DoS pochází z anglického sousloví denial of sevice; v doslovném překladu „odmítnutí služby". Cíle tohoto útoku, je zahlcení služby požadavky, aby služba již nebyla schopna přijmout další požadavky. Útok je zprostředkován požadavky na úkony, které má služba vykonat. Základní dělení těchto útoků je na DoS a DDoS (Distributed Denial of Service). (Kolouch, 2016)

Rozdíl mezi DoS a DDoS je v tom, že DoS je veden z jednoho počítače a DDoS je veden z více jak jednoho počítače – většinou obrovského počtu počítačů. Útoku DoS se lze jednodušeji bránit – zablokování přístupu ke službě jednomu počítači je jednoduší než filtrovat reálné uživatele od fiktivních uživatelů, kteří se podílejí na DDoS útoku. Větší počet počítačů, které jsou ovládány z jednoho místa, se nazývá „botnet" – počítače, které jsou takto ovládány, byly napadeny většinou v dřívějším čase. Určení původce útoku DDoS je náročné, jelikož je schován za „botnet" a jelikož se objevuje i praxe, že se „botnet" pronajímá k útoku ad hoc. (Kolouch, 2016) (Chapman, et al., 2011)

Jeden z významnějších případů útoků DDoS na území Evropské unie v poslední době byl útok provedený na poskytovatele internetových služeb, přičemž útokem došlo k ochromení vlakové sítě ve Švédsku. (European Union Agency for Law Enforcement Cooperation, 2019)

DDoS útoky jsou v rámci Evropské unie označeny jako nejčastější kybernetický útok – v roce 2018 to bylo 65 % všech hlášených případů. Hlavním faktorem zvyšujícího se trendu využívání DDoS útoků má být zvýšení dostupnosti těchto útoků nabízených jako service as a product. (European Union Agency for Law Enforcement Cooperation, 2019)

2.1.2 PHISHING

Phishing je zaběhnutý termín pro klamné a podvodné jednání, které si klade za cíl vylákat od uživatele jeho citlivé údaje – ty jsou pak často útočníkem zneužity k získání majetkového či jiného prospěchu (např. odčerpání finančních prostředků z internetového bankovnictví). Samotnou podstatou phishingového útoku je získání důvěry uživatele a donucení vyplnit své citlivé údaje (např. falešná urgence od banky, že je nutné změnit si své heslo k internetovému bankovnictví a přivedení na podvodnou stránku která se vydává za přihlašovací stránku internetového bankovnictví. Phishingové útoky lze rozdělit na cílené a necílené. Necílené útoky fungují na principu kobercových náletů, kdy je například rozeslán email vypadaje jako od bankovního domu co největšímu okruhu uživatelů – návratnost je poměrné nízká. Cílené útoky pracují již s jistými údaji o uživateli – tedy například jméno, zaměstnavatel a pracovní pozice; phishingový útok je pak vytvořen na míru uživateli a je tedy důvěryhodnější – ergo efektivnější. (Kolouch, 2016) (Chapman, et al., 2011)

2.2 DRUHÁ ÚROVEŇ: S OMEZENÝMI PŘÍSTUPOVÝMI PRÁVY

Na této úrovni se předpokládá, že útočník má základní uživatelská práva, které mohl získat vzdáleným přístupem do sítě, či fyzickým přístupem do sítě. Ačkoliv se jedná o uživatelská – tedy omezená přístupová práva, útočníkovi jsou již poskytnuty podpory ve formě uživatelského přístupu. Po získání přístupu na druhé úrovni typicky následuje „nainstalování“ zadních vrátek, kterými se může útočník vrátit v případě omezení původního přístupu (např. při změně hesla etc.). (Chapman, et al., 2011)

V kontextu mezinárodních sporů jsou útoky v této úrovni primárně prostředkem k získání přístupu k třetí úrovni (s administrátorským přístupem).

2.2.1 SNIFFING

Metoda nazývaná Sniffing představuje nelegální odposlech dat proudící přes danou počítačovou síť. Sniffing dělíme na dva typy – první předpokládá napadení počítače a zavedení škodlivého programu, který na pozadí „odposlouchává“ dění na PC, tyto data jsou pak přenášena k útočníkovi

k vyhodnocení (lze získat například zadané přístupové údaje, či citlivé informace), druhý typ je odposlech na přenosové vrstvě sítě, kdy se uvažuje odposlech dat, které jsou skrze síť přijímány a odesílány (efektivní útok nastane pouze za předpokladu porušení hned několika bezpečnostních pravidel jako například nezabezpečená síť a nevyužívání zabezpečených protokolů). (Kolouch, 2016) (Chapman, et al., 2011)

2.2.2 PROLOMENÍ HESLA

Takzvaný „password cracking" je způsob získání hesla uživatele. Útočník může při pokusu o prolomení hesla použít automatizovanou hrubou sílu – tedy použití slovníků s potenciálními hesly metodou pokus-omyl; skript zadává jedno heslo po druhém, dokud není heslo prolomeno. Při prvotních pokusech o prolomení lze útok personifikovat na konkrétního uživatele díky tzv. sociálnímu inženýrství či získání veřejně dostupných informací o uživateli, které mohou být nápomocné k uhádnutí hesla (datum svatby, jméno mazlíčka etc.). Další metodou prolomení hesla, je využití postupu „zapomenutého hesla" - v tomto případě velmi závisí na bezpečnostních opatřeních poskytovatele služby. (Chapman, et al., 2011)

2.3 TŘETÍ ÚROVEŇ: S ADMINISTRÁTORSKÝM PŘÍSTUPEM

Třetí úroveň je spjatá s přístupem na úrovni tzv. root (což je název pro správcovské účty na administrátorské úrovni u Linux/Unix operačních systémů). Na třetí úrovni má útočník téměř neomezenou volnost pro nakládání s počítači a sítí. Tato úroveň je spjatá s celou řadou a škálou škodlivých útoků, které útočník může provést.

2.3.1 RANSOMWARE

Ransomware je tzv. vyděračský, který po svých obětech žádá zaplacení výkupného za uzamčená data. Tento malware můžeme dělit na dva typy – první typ ransomware celý počítač uzamkne a požaduje zaplacení určitě částky pro zpřístupnění počítače; druhý typ ransomware typicky uzamkne jen data uživatele, které má uložena na svém počítači. V současné době převažuje druhý typ ransomware, jelikož vytváří větší nátlak na uživatele tím, že umožňuje základní práci s počítačem. (Kolouch, 2016)

Historicky se ve světě i v ČR objevoval „policejní" ransomware, který uživateli říkal, že policií byl nalezen v uživatelově počítači materiál, který vykazuje známky trestné činnosti. Důvěřivý uživatel neznalý postupů orgánů činných v trestním řízení mohl snadno uvěřit, že se jedná opravdovou o sankci. Tato šablona ransomware byla v průběhu často medializována mass médii, což působilo jako silné preventivní opatření. (Kolouch, 2016)

Ransomware je zmiňován jako jeden ze základních modus operandi kybernetických útoků na kritickou infrastrukturu. Všeobecně mají tyto útoky málo společného, avšak tento modus operandi je většinou spojuje. (European Union Agency for Law Enforcement Cooperation, 2019).

2.4 SOCIÁLNÍ INŽENÝRSTVÍ

Sociální inženýrství či sociotechnika je soubor metod, které počítač přímo nenapadají, avšak útočí na jeho uživatele. Tyto metody cílí na slabé stránky uživatele – těmi mohou být ochota pomoci, strach, lehkověrnost, lenost či nerozumnost. Základní prostředek sociálního inženýrství je schopnost manipulovat lidmi a ošálit jejich úsudek; bez tohoto prostředku nelze předpokládat úspěšný útok. Zaměření na lidský prvek v systému je logické – uživatel bude vždy nejslabší článek celého systému; zatím nejsou dispozici počítačové systémy, které by byly kompletně nezávislé na lidském prvku (nepoužití takzvaného „human plugin" alespoň v jedné části procesu). (Kolouch, 2016)

Sociální inženýrství je základem použití infiltrace do počítačových systémů při využití speciálně upravených útoků pro osobu, organizaci či odvětví hospodářství. Útoky nevyžadují přílišnou osobní personalizaci a postačí, pakliže jsou upraveny pro odvětví hospodářství – teoretickým příkladem může být rozeslání phishing útoků na nemocnice či organizace v přímé působnosti Ministerstva zdravotnictví České republiky (dále také „MZČR"), který byl vydáván za přihlašovací stránku MZČR, tento typ útoku by měl vysoký počet potenciálních obětí.

3 PŘÍKLADY HYBRIDNÍCH HROZEB

V následující kapitole jsou uvedeny významné hybridní hrozby, při nichž byly poškozeny něčí zájmy. Nutno dodat, že hybridní hrozby, i když se mohou jevit jako neúspěšné, mohou poškodit něčí zájmy pouhým zveřejněním informace ohledně pokusu o nějaký čin, jež má mít charakter hybridní hrozby.

Bezpečnostní informační služba se ve svých veřejných výročních zprávách za roky 2017-20219 (Bezpečnostní informační služba, 2020) (Bezpečnostní informační služba, 2019) (Bezpečnostní informační služba, 2018) zmiňuje zejména o zpravodajských aktivitách Čínské lidové republiky a Ruské federace. Cíle těchto aktérů jsou často odlišné, Výroční zprávy Bezpečnostní informační služby za rok 2020 (2020, pp. 8-9) uvádí: „*[…] Rusko usiluje o destabilizaci a rozklad svých protihráčů, zatímco čínský cílem je vybudovat sinocentrickou globální komunitu, kde ostatní národy uznají legitimitu čínských zájmů a přiznají Číně respekt, který jí (dle čínského mínění) náleží.*“. Ovšem informace o těchto aktivitách bývají zejména z důvodu uvedeného v předchozím odstavci nezveřejněné v utajovaném režimu.

3.1 KOMPROMITACE SOUKROMÝCH EMAILŮ PŘÍSLUŠNÍKŮ ARMÁDY ČESKÉ REPUBLIKY

Bezpečnostní informační služba ve své veřejné výroční zprávě za rok 2018 upozornila na případ, kdy mělo dojít kompromitaci soukromých emailových schránek příslušníků Armády České republiky. Zpráva dále dodává, že nedošlo k vyzrazení žádné informace podléhající ustanovení zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti; uniknout měly „pouze“ informace osobního charakteru (citlivé informace zahrnující například informace o bydlišti, dovolených, rodinném zázemí a kontaktní údaje). Tyto emailové schránky měly být vytěžovány pomocí protokolu IMAP (IMAP je akronym slov Internet Message Access Protocol, tedy protokolu přístupu k emailové schránce) – oběť neměla šanci tento útok rozpoznat, jelikož poskytovatelé inkriminovaných emailových schránek neumožňují nahlížet na IP adresy, ze kterých je proveden přístup k emailové schránce. (Bezpečnostní informační služba, 2019)

Skupina APT28 (známá také jako Sofacy či Fancy Bear), která kyberšpionáž provedla, má napojení na Ruskou federaci. Některé zdroje uvádí, že se jedná o součást ruské vojenské rozvědky GRU, jiné uvádí, že se jedná o skupinu, která je financována ruskou vládou – napojení na oficiální ruské státní orgány je tedy nezpochybnitelné. (Välisluureamet, 2019) (Wintour, 2018) (Bezpečnostní informační služba, 2019)

Tyto informace samy o sobě nemají příliš velkou hodnotu, jelikož údajně nedošlo k úniku dat, která by stát označil za utajované. Nicméně tato osobní data poskytují dobrý podklad k přesnému zacílení sociálního inženýrství a získání informací, které jsou označeny jako utajované. Ministerstvo obrany České republiky na svých webových stránkách uveřejnilo upřesnění: „*Pravděpodobná kompromitace soukromých e-mailových účtů ruskou kybernetickou kampaní APT28/Sofacy se netýkala žádných významných funkcionářů MO nebo AČR a nezpůsobila žádnou újmu směrem k úniku utajovaných informací.*“ (Pejšek, 2019).

Vzhledem k tomu, že se kompromitace týkala pouze základních a nižších velitelských funkcí, je případný únik informací vyššího stupně utajení spíše nepravděpodobný.

Nebyly zveřejněny podrobnosti, jakým způsobem proběhlo získání přístupu k emailovým schránkám, avšak pravděpodobně se příslušníci stali obětí phisingového útoku. Z veřejně dostupných zdrojů nebylo možné zjistit, jakým způsobem je podobným útokům předcházeno (nebyl zjištěn stav před útokem ani po útoku).

3.2 HUAWEI A ZTE

Týden před Vánoci roku 2018 vydal Národní úřad pro kybernetickou a informační bezpečnost (dále také „NÚKIB“) varování dle zákona č. 181/2014 Sb. o kybernetické bezpečnosti před zařízeními společností HUAWEI a ZTE, kterým zásadně ovlivnil postavení těchto výrobců na českém trhu (de iure byla omezena účast těchto společností v hospodářských soutěží státních

institucí; bezesporu tyto společnosti utrpěly újmu na vnímání prestiže značky. Bylo to poprvé, co NÚKIB vydal varování od svého založení v roce 2017.

Kroky české státní správy proti HUAWEI a ZTE nebyly v rámci světa ojedinělé. Z dalších významných restrikcí proti těmto společnostem lze uvést například reakci americké společnosti Google, která omezila možnosti prodávat mobilní telefony těchto společností s operačním systémem (dále také „OS") Android, který je i byl jeden ze dvou majoritních OS pro mobilní telefony. (Nadeem & Lily, 2019)

Geneze tohoto případu se údajně dle tehdejšího ředitele Ing. Dušana Navrátila datuje k létu 2018, kdy údajně tehdejší premiér Ing. Andrej Babiš prohlásil „že vnímá jako problém, že Huawei zvítězil v zakázce na datová centra pro ČEZ.". Bezpečnostní komunita tento problém začala řešit v září 2018. (Zelenka, 2020)

Jedno z odůvodnění varování NÚKIB je mimo jiné, že ČLR na území ČR prosazuje své zájmy prostřednictvím zpravodajských aktivit špionážních technik s odkazem na Výroční zprávu BIS za rok 2019 (Národní úřad pro kybernetickou a informační bezpečnost, 2018).

3.3 ÚTOK NA FAKULTNÍ NEMOCNICI V BRNĚ V PRŮBĚHU PANDEMIE COVID-19

Následující den po 13. březnu 2020 – kdy proběhlo k vyhlášení nouzového stavu Vládou České republiky kvůli pandemii onemocnění COVID-19 způsobené SARS-CoV-2, došlo ke kybernetickému útoku na Fakultní nemocnici Brno. Vedení nemocnice oficiálně neuveřejnilo podrobnosti o útoku, avšak dle dostupných informací se nejspíše jednalo o ransomware. Útok byl natolik rozsáhlý, že vedení Fakultní nemocnice Brno muselo odříct i urgentní chirurgické zákroky a nové pacienty přesměrovat do Fakultní nemocnice u svaté Anny – nemocniční personál zasažené nemocnice měl pokyn vypnout a ponechat vypnuté všechny počítače; zasažená byla celá počítačová síť nemocnice. (Cimpanu, 2020)

Zasažená Fakultní nemocnice v Brně toho času měla na starost i testování pacientů s onemocněním COVID-19 – kybernetický útok negativně ovlivnil i

toto testování – následkem bylo významné regionální zpoždění diagnostiky nemocných s onemocněním COVID-19. Útok na Fakultní nemocnici v Brně byl na světě první kybernetický útok na nemocnici v průběhu pandemie onemocnění COVID-19, který byl nahlášený a který způsobil rozsáhlejší škodu. (Muthuppalaniappan & Stevenson, 2020)

Dle článku Muthuppalaniappan & Stevenson (2020) byl tento útok ojedinělý, jelikož útočil přímo na nemocnici, jiné útoky byly namířeny proti nestátním institucím, národním autoritám, akademickým institucím etc. Autoři článku upozorňují, že ve zdravotnických a akademických institucí nesmí být zanedbávána kybernetický bezpečnost, i přes to, že dané instituce v průběhu pandemie COVID-19 primárně řešily jiné záležitosti s pandemií spojené.

Dne 16. dubna 2020 vydal NÚKIB v pořadí své druhé varování dle zákona č. 181/2014 Sb. o kybernetické bezpečnosti před hrozbou spočívající v rozsáhlých útocích zejména vůči zdravotnickým zařízením. Předmětem varování bylo zejména upozornění na spear-phishing (tedy cílený phishing), omezení možnosti kompromitace systému pomocí maker v MS Office, zablokování otevřených vzdálených přístupů a jejich kompletní prověření, zálohování a další základní opatření – všechny tyto opatření by dle názoru autora měly být pravidlem počítačové bezpečnosti v organizaci. Dne 20. května 2020 téměř po pěti týdnech NÚKIB ukončil účinnost svého varování. (Národní úřad pro kybernetickou a informační bezpečnost, 2020)

Auditem národní bezpečnosti bylo v oblasti hrozeb v kyberprostoru stanoveno jako jedno z doporučení: „Zahrnout důležité sektory jako chemický průmysl, zdravotnická zařízení a další strategická odvětví do soustavy KII skrze […] novelizaci krizového zákona a nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, jež by umožnilo zahrnutí důležitých sektorů mezi sektory KI, pomocí kterého je KII určována.“. (Ministerstvo vnitra České republiky, 2016) Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury byl od jeho vyhlášení v roce 2010 novelizováno celkem dvakrát. Při první novelizaci

v roce 2014 nedošlo ke změně ustanovení týkající se zdravotnictví a jako odvětvové kritérium u nemocnic stále zůstal celkový počet akutních lůžek alespoň 2 500. Při druhé novelizaci v roce 2020 (pozn. účinné znění od 09/04/2020) přibylo do odvětvových kritérií pro oblast zdravotnictví kritéria pro činnosti spojené s výrobou léčivých přípravků a podobných činností; odvětvové kritérium bylo zachováno na úrovni alespoň 2 500 akutních lůžek. Dle ustanovení § 9 zákona č. 372/2011 Sb. Zákon o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) je lůžková péče rozdělena na akutní lůžkovou péči standardní, akutní lůžkovou péči intenzivní, následnou lůžkovou péči a dlouhodobou lůžkovou péči; lze tedy dovozovat, že se odvětvové kritérium vztahuje pouze na lůžka, které jsou zahrnuta do akutní lůžkové péče standardní a intenzivní.

Pro kontext – Fakultní nemocnice v Motole, která se profiluje dle svých webových stránek (Fakultní nemocnice v Motole, 2021) jako největší zdravotnické zařízení v České republice, má celkem 2199 lůžek pro pacienty, přičemž lze předpokládat, že se jedná o souhrn všech lůžek, která jsou zahrnuta i do následné lůžkové péče a dlouhodobé lůžkové péče.

Napadená Fakultní nemocnice Brno na svých webových stránkách (Fakultní nemocnice Brno, 2021) uvádí, že po celý rok 2020 měla celkem stále 1889 lůžek, přičemž opět není uvedeno rozdělení lůžkového fondu na lůžka akutní péče standardní a intenzivní, následné lůžkové péče a dlouhodobé péče, lze tedy předpokládat, že akutních lůžek je méně.

Nelze predikovat, jaký vliv by mělo zařazení informačního systému Fakultní nemocnice Brno do soustavy kritické informační infastruktury, avšak vzhledem k povinnostem, které plynou pro správce informačního systému kritické informační infrastruktury z ustanovení zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) lze předpokládat jiný průběh útoku na nemocnici.

3.4 ÚTOK NA MAGISTRÁT MĚSTA OLOMOUC

Dne 6. dubna 2021 se ocitl olomoucký magistrát pod kybernetickým útokem. Den po útoku zveřejnil zpravodajský server Olomoucký deník.cz informace (Kovář & Auberová, 2021), že byly napadeny datové systémy a z bezpečnostních důvodů byly odpojeny jednotlivé subsystémy. Z článku není patrné, o jaký typ útoku se jednalo. O týden později se objevila zpráva (Vránová, 2021), že útočník požaduje výkupné 100 000 dolarů za dešifrování soborů, je tedy zřejmé, že se jedná o útok typu ransomware – nejsou známé předběžné informace, jaké soubory a data byly zašifrovány; údajně však magistrát přišel jen o soubory z jednoho dne před útokem, ostatní data jsou obnovena či budou brzy obnovena.

Dne 26. dubna 2021 zaznamenaly webové stránky magistrátu výpadek – pravděpodobně šlo o DDoS. Dle dostupných informací je DDoS útok pomstou za to, že město Olomouc neuhradilo výkupné 100 000 dolarů a data si obnovila svojí cestou. Hackerská skupina Avaddon ransomware upozorňuje, že pokud do sedmi dnů nezačne město spolupracovat, bude následovat únik dat – na svých webových stránkách mimo jiné uvádí (přeloženo z anglického jazyka): „Společnost pravděpodobně nechápe, že máme všechny jejich důvěrné dokumenty, a pokud nebudou spolupracovat, skončí to únikem cenných dat, myslíme si, že by pak mohli mít opravdu zábavné dny. Tak jim popřejme hodně štěstí.“. (Čížek, 2021) (Avaddon ransomware, 2021)

Ani na výzvu o výkupné ze dne 26. dubna 2021 olomoucký magistrát s veřejnou pohrůžkou únikem dat nereaguje. A tak se následně na webových stránkách hackerské skupiny Avaddon ransomware objevuje zhruba 23 gibibyte souborů volně dostupných ke stažení. Mezi nimi jsou i již veřejně dostupné soubory – jako jsou například usnesení Vlády České republiky, nebo nevýznamné soubory jako Informace o zpracování osobních údajů při provádění testování na onemocnění COVID-19 či Čestné prohlášení zaměstnance – samotestování. Některé soubory obsahují i osobní údaje (jako například hodnocení kompetencí strážníka TA, kde je jeho výkon

uváděn jako dobré – z pochopitelných důvodů nejsou uváděny osobní údaje jako celé jméno, datum narození, datum nástupu do funkce či identifikační číslo, ačkoliv jsou tyto osobní údaje uváděny. (Avaddon ransomware, 2021)

Vzhledem pouze ke kusým informacím, které jsou zatím veřejně dostupné – nelze vyhodnotit připravenost či vyhodnotit pochybení. Dle nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury magistrát sám o sobě není začleněn jako prvek kritické infrastruktury.

Hackerská skupina Avaddon ransomware nevykazuje známky přímého napojení na cizí moc, dle všeho se jedná o konvenční hackerskou skupinou, která sice působí po celém svět – může však poskytovat službu jako produkt (tedy nabízet útok typu ransomware jako službu) Avšak nejedná se o první útok na území České republiky této hackerské skupiny – již dříve publikovala soubory české společnosti ASBIS CZ, spol. s r.o., která se na svých webových stránkách profiluje jako distributor ICT řešení a velkoobchod s počítačovými komponentami s obratem za rok 2019 téměř 2 miliardy dolarů (ASBIS CZ spol. s r.o., 2021); nebo soubory společnosti MEDUNA vakuová kalírna s.r.o.

3.5 ÚTOKY NA VYSOKÉ ŠKOLY V ČESKÉ REPUBLICE

Dle Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2018 (Národní úřad pro kybernetickou a informační bezpečnost, 2019, pp. 37-38) je patrný nárůst kybernetických útoků na české vysoké školy a zvyšující se zájem útočníků o tuto skupinu. Útočníci jsou zejména konvenční kyberzločinci (skupiny či jednotlivci) a státem sponzorované skupiny, přičemž využívají zejména phishing, podvodné e-maily a DDoS útoky. Akademické obci zejména hrozí zcizení duševního vlastnictví, nemožnost provádět výzkum z důvodu nedostupnosti počítačové techniky či kompromitace doposud nepublikovaných výsledků vědy a výzkumu. Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019 (Národní úřad pro kybernetickou a informační bezpečnost, 2020, pp. 19-20) výše uvedená tvrzení potvrzuje – tato zpráva zmiňuje zejména nárůst sofistikovanosti (i. e.

detailní znalost českého univerzitního prostředí, používání vizuálních stylů univerzit a čeština rodilého mluvčího – nikoliv strojový překlad bez kontroly).

Nejen Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2018 (Národní úřad pro kybernetickou a informační bezpečnost, 2019, pp. 37-38) se zmiňuje o české akademické obce jako o možném cíli útoků, ale na jiné riziko upozorňuje Bezpečnostní informační služba ve své Výroční zprávě určené veřejnosti za rok 2019 (Bezpečnostní informační služba, 2020) – v české akademické sféře se údajně angažovaly zejména zpravodajské služby Čínské lidové republiky (primárně v navazování kontaktů a využívání získaných kontaktů). Tato výroční zpráva nezmiňuje souvislost kybernetických útoků na české vysoké školy a zájem zpravodajských služeb Čínské lidové republiky, avšak explicitně uvádí, že do kyberšpionážních aktivit byla zapojena nejen Ruská federace ale i Čínská lidová republika – ke které není přiřazen jediný kyberútok (Bezpečnostní informační služba, 2020, p. 11) (je nutné mít na paměti, že se jedná o veřejnou zprávu o činnosti, která z podstaty věci nesmí být příliš konkrétní).

Pomocí zákona č. 106/1999 Sb. o svobodném přístupu k informacím bylo provedeno šetření aktuálního stavu kybernetických útoků na vybraných vysokých školách. Prostřednictvím datových zpráv byly dotázány následující vysoké školy univerzitního typu:

- Západočeská univerzita v Plzni,
- Univerzita Hradec Králové,
- Univerzita Karlova,
- Vysoké učení technické v Brně a
- Masarykova univerzita.

Předmětem dotazování byl stav kybernetických útoků proti počítačovým sítím ve správě, případné zjištění původců těchto útoků, spolupráce s jinými bezpečnostními týmy a případný únik citlivých dat za poslední dva roky.

Západočeská univerzita v Plzni se setkává zejména s phishing útoky, DoS a DDoS útoky a také pokusy o prolení hesel počítačových systémů. Univerzita se setkala i s instalací ransomware či zneužití RDP (Remote Desktop Protocol, vzdálené ovládání počítače). Dále uvedla, že nezjišťovala původce útoků; spolupracuje s NÚKIB (jelikož je správce významných informačních systémů) a s bezpečnostními týmy CESNET. Univerzita si není vědoma úniku žádných citlivých dat, s výjimkou následků úspěšných phishing útoků. (Západočeská univerzita v Plzni, 2021)

Univerzita Hradec Králové uvedla, že se pravidelně setkává s útoky typu phishing, malware, social engineering. Původce útoků nebyl zjištěn, avšak byl detekován a zablokován zdroj útoků. Univerzita spolupracuje při s bezpečnostními týmy CESNET a NÚKIB. Údajně na univerzitě v posledních dvou letech nedošlo k ztrátě citlivých dat. (Univerzita Hradec Králové, 2021)

Masarykova univerzita uvedla, že se v roce 2019 setkala s 111 317 pokusy o kybernetický útok a v roce 2020 s 121 387 pokusy o kybernetický útok. Nejčastěji se univerzita setkává s pokusy o zneužití zranitelností, phishing, spear-phishing, ransomware či malware; sporadicky se setkává i s neoprávněnou těžbou kryptoměn. Při zjišťování původců útoků se univerzita spíše zaměřuje na dohledání úrovně IP adres či e-mailových adres, ze kterých byl útok veden pro účely jejich mitigace. Univerzita spolupracuje s bezpečnostními týmy CESNET a NÚKIB; uvedla také, že s organizací CESNET spolupracuje i na bázi projektů vědy a výzkumu v oblasti kybernetické bezpečnosti. Údajně došlo ke ztrátě vědeckých dat, které byly zašifrovány pomocí ransomware. (Masarykova univerzita, 2021)

Vysoké učení technické v Brně se setkává s kybernetickými útoky téměř denně – jde zejména o phishing, ransomware a DDoS. Univerzita většinou nezjišťuje původce útoků, avšak uvedla, že v případně závažného útoku by se o zjištění původce pokusily. Dále univerzita uvedla, že se spolupracuje s bezpečnostními týmy CESNET a NÚKIB. Údajně jí nebyla zcizena žádná citlivá data. (Vysoké učení technické v Brně, 2021)

Univerzita Karlova v zákonné lhůtě nedopověděla na dotaz zaslaný via datová schránka dle zákona č. 106/1999 Sb. o svobodném přístupu k informacím.

3.6 PŘEVZETÍ KONTROLY NAD OVLÁDACÍM SYSTÉMEM ÚPRAVY PITNÉ VODY

Americký magazín Wired v únoru roku 2021 upozornil na případ, kdy se pachatel pomocí aplikace TeamViewer připojil do objektu čističky vody a více jak sto násobně zvýšil koncentraci nebezpečného hydroxidu sodného. V počátku si dozor ničeho nevšiml, jelikož jeho nadřízený se pomocí aplikace TeamViewer připojoval pravidelně, aby zkontroloval stav vody. Jakmile byla aktivita pachatele nápadná (úroveň koncentrace hydroxidu sodného byla nad povolenou mezí), dozor zasáhl. Daná čistička vody je zdrojem vody pro floridské město Oldsmar, kde žije přibližně 15 000 obyvatel (Greenberg, 2021).

Obdobná čistička vody by se v Česku nepovažovala za prvek kritické infrastruktury, jelikož nesplňuje hlediska průřezových kritérií dle ustanovení bodu II/b přílohy k nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury se za prvek kritické infrastruktury považuje úpravna vody o výkonu 3000 l/s. Článek v magazínu neuvádí výkon čističky, avšak použitelné průřezové kritérium stanovuje závažný zásah do života více jak 125 000 osobám – proto lze předpokládat, že by čistička pro 15 000 obyvatel toto kritérium nesplňovala.

4 DIMEFIL

Rozlišuje se celkem sedm sfér vlivu Diplomatic/Political, Information, Military, Economic, Financial, Intelligence, Legal (český překlad sedmi dimenzí mocí je diplomacie/politika, informace, ozbrojené síly, ekonomika, finančnictví, zpravodajství a právo). Těchto sedm dimenzí moci lze využít k prosazování politických zájmů – přičemž počet uplatněných dimenzí moci může být variabilní u různých politických zájmů s ohledem na původce zájmu, který může být státní ale i nestátní a který se svým účelným jednáním může dostat do konfliktu s mezinárodním právem. (Ministerstvo vnitra České republiky, 2016).

4.1 DIPLOMATIC/POLITICAL

Osoby ve veřejných funkcích (vykonavatelé moci soudní, moci výkonné či moci zákonodárné) mohou uplatnit nátlak svými proklamacemi či svým jednáním (Ministerstvo vnitra České republiky, 2016).

Příkladem této sféry vlivu může být 184. usnesení Poslanecké sněmovny ze dne 25. března 2014: „[…] odmítá násilnou anexi části území Ukrajiny – Krymu ze strany Ruské federace. Tento postup je porušením mezinárodního práva.“ (Poslanecká sněmovna, 2014). Tato proklamace vytváří z hlediska mezinárodních vztahů jistý tlak.

4.2 INFORMATION

Do informační sféry vlivu patří moc získání prostoru ve sdělovacích prostředích či sociálních sítí. Tuto moc lze využít k manipulacím a propagandě. (Ministerstvo vnitra České republiky, 2016).

Moc nad masmédii a moc získání prostoru v masmédiích se sobě nerovnají – moc nad masmédii poskytuje komfortnější ovlivňování prostoru v masmédiích, ale v jistých případech postačí i poskytnutí prostoru pro oponentní názor, který kombinuje lži a pravdu. Lež se šíří mnohonásobně rychleji než pravda (Soroush, et al., 2018), proto uvádět dezinformace na pravou míru je velice neefektivní, náročný a složitý boj. Zejména sociální sítě už z podstaty své existence spojují podobné sociální bubliny, což v těchto

kruzích výrazně napomáhá k šíření komfortních informací – jde zejména o efekt utvrzování se navzájem v našem názoru.

Dle Výroční zprávy Bezpečnostní informační služby za rok 2017 (2018) je jeden z nástrojů Ruské hybridní strategie takzvané Overtonovo okno – tím se rozumí postupný názorový posun společnosti (neustálou obhajobou nepřijatelných témat se témata stávají společností přijímaná – je nutné mít namysli, že historie zná nespočet témat, která přišila z okraje společnosti, až byla nakonec legislativně ukotvena, jako byl například holocaust). Bezpečnostní informační služba v této výroční zprávě (2018) uvádí přirovnání: „Dveřmi vyhodíte internacionalistu a oknem se vám vrátí bojovník proti migraci, islamizaci, dekadentnímu chaosu a obhájce tradičních křesťanských hodnot.“.

4.3 MILITARY

Sféra ozbrojených sil má dvě roviny: přímou a nepřímou. Přímá rovina využívá veřejné zastrašování či ukázání moci (vojenské jednotky u hranic, vojenská přehlídka etc.). Nepřímá rovina v sobě nese tajné operace, participace na asymetrických útocích či infiltrace. (Ministerstvo vnitra České republiky, 2016)

4.4 ECONOMIC

Země mohou pomocí uvalování různých podob ekonomických nátlaků – například pomocí uvalování cel či embarga na zboží, omezení používání dopravních cest či destabilizaci určitých odvětí, které daná země ovládá. (Ministerstvo vnitra České republiky, 2016)

Tato dimenze může být také uplatněna zejména při nedokonalé konkurenci u klíčových surovin; příkladem můžou být suroviny ropa a plyn z Ruské federace dovážené na území Evropské unie. V jistých případech může být tato dimenze použita při nátlaku státními aktéry.

4.5 FINANCIAL

Instrumenty finančního trhu představují silný nástroj, avšak jejich ovlivnění vyžaduje značné množství prostředků či jiného vynaloženého úsilí. Segment finančního trhu (kapitálový, peněžní a komoditní) může být využit zejména

k destabilizaci určitých instrumentů finančního trhu. Do této skupiny patří zejména destabilizace měny, bankovních domů či ovlivňování hlavních finančních instancí. Současný svět je silně propojený a setkáváme se častěji s otevřenými ekonomikami zemí v porovnání s počátkem minulého století. Proto destabilizovat například měnu v malé či uzavřené ekonomice je proveditelné, avšak u velkých otevřených ekonomik je to neproveditelné či velice náročně proveditelné. (Ministerstvo vnitra České republiky, 2016).

4.6 INTELLIGENCE

Zásadní roli v rozhodování hrají informace získané pomocí činnosti zpravodajských služeb – tím se rozumí celé spektrum technik analytických či operativních činností (například získání spolupracujících osob pro protistátní činnost). (Ministerstvo vnitra České republiky, 2016)

4.7 LEGAL

Subverze se může zejména v demokratických společnostech pohybovat v poli legální činnosti, avšak existuje i činnost nelegální a podvratná, která nese známky další kriminální činnosti (např. únosy). Útočeno je vždy na hodnotové či právní uspořádání společnosti. Avšak je nutné rozeznávat rozvratnou činnosti v demokratických společnostech a obyčejnou kritiku systému v nedemokratickém uspořádání. (Ministerstvo vnitra České republiky, 2016)

5 POROVNÁNÍ HYBRIDNÍCH HROZEB Z HLEDISKA DISTRIBUCE MOCI DIMEFIL

Na základě analýzy příkladů hybridních hrozeb bylo možné provést začlenění jednotlivých použitých dimenzí moci. V následujících podkapitolách jsou uvedena odůvodnění začlenění a jednotlivá začlenění v tabulkách.

5.1 KOMPROMITACE SOUKROMÝCH EMAILŮ PŘÍSLUŠNÍKŮ ARMÁDY ČESKÉ REPUBLIKY

Při tomto útoku existuje jednoznačně zásah do dimenze Military a Intelligence, jelikož dle dostupných informací se jednalo to původce útoku, který byl napojen na orgán cizí moci a lze jej charakterizovat jako zpravodajskou aktivitu.

Dimenze moci	Použito v tomto případě
Diplomatic/Political	Ne
Information	Ne
Military	Ano
Economic	Ne
Financial	Ne
Intelligence	Ano
Legal	Ne

Tabulka 2 DIMEFIL: Kompromitace soukromých emailů příslušníků Armády České republiky

5.2 HUAWEI A ZTE

V tomto případě není známo příliš informací – varování NÚKIB bylo vydáno zejména na základě právního a politického prostředí ČLR a prosazování svých zájmů i pomocí aktivit zpravodajských služeb ČLR (Národní úřad pro kybernetickou a informační bezpečnost, 2018). Proto lze jednoznačně říci, že v tomto případě bylo vydáno varování NÚKIB zejména kvůli potenciálnímu

použití dimenze Intelligence. Vzhledem k silné diplomatické reakci lze začlenit i dimenzi Diplomatic/Political.

Dimenze moci	Použito v tomto případě
Diplomatic/Political	Ano
Information	Ne
Military	Ne
Economic	Ne
Financial	Ne
Intelligence	Ano
Legal	Ne

Tabulka 3 DIMEFIL: HUAWEI a ZTE

5.3 ÚTOK NA FAKULTNÍ NEMOCNICI V BRNĚ V PRŮBĚHU PANDEMIE COVID-19

V tomto případě měl útok zásadní dopad na nemocnici, která byla de facto vyřazena z provozu – což společně s náklady zajištění akutní péče, jistě znamenalo nemalé finanční škody, ale to nelze považovat za destabilizaci klíčového odvětví, aby mohla být uplatněna dimenze Economic. Avšak jednalo se o cílený útok za účelem nemocnici paralyzovat, proto lze říci, že byla použita dimenze Legal – ačkoliv vzhledem k místním poměrům je ohrožení veřejného pořádku či drastické snížení důvěry ve státní instituce spíše nepravděpodobné.

Dimenze moci	Použito v tomto případě
Diplomatic/Political	Ne
Information	Ne

Dimenze moci	Použito v tomto případě
Military	Ne
Economic	Ne
Financial	Ne
Intelligence	Ne
Legal	Ano

Tabulka 4 DIMEFIL: Útok na Fakultní nemocnici v Brně v průběhu pandemie COVID-19

5.4 ÚTOK NA MAGISTRÁT MĚSTA OLOMOUC

Jeden z atributů útoku byla hrozba zveřejnění získaných dat, což v případě orgánu veřejné moci může mít za následek snížení důvěry obyvatel k orgánům veřejné moci. Proto lze říci, že byla použita dimenze Legal. Pro začlenění do dimenze Economic nebylo prokázáno, že by měl útok charakter destabilizace daného odvětví (státní správy).

Dimenze moci	Použito v tomto případě
Diplomatic/Political	Ne
Information	Ne
Military	Ne
Economic	Ne
Financial	Ne
Intelligence	Ne
Legal	Ano

Tabulka 5 DIMEFIL: Útok na magistrát města Olomouc

5.5 ÚTOKY NA AKADEMICKOU OBEC V ČESKÉ REPUBLICE

Jelikož část spektra původců útoků jsou státem sponzorované skupiny – lze předpokládat, že prostředkem k útokům jsou dimenze Intelligence a Legal. Ani v tomto případě nejsou veřejně dostupná všechna data o útocích, které by umožnovaly přesně začlenění útoků.

Dimenze moci	Použito v tomto případě
Diplomatic/Political	Ne
Information	Ne
Military	Ne
Economic	Ne
Financial	Ne
Intelligence	Ano
Legal	Ano

Tabulka 6 DIMEFIL: Útoky na akademickou obec v České republice

5.6 PŘEVZETÍ KONTROLY NAD OVLÁDACÍM SYSTÉMEM ÚPRAVY PITNÉ VODY

Útok měl potenciál způsobit značně ekonomické škody pro větší skupinu obyvatel, proto lze začlenit dimenzi Economic. Útok lze bezesporu označit jako subverzi, proto je možné útok začlenit k dimenzi Legal.

Dimenze moci	Použito v tomto případě
Diplomatic/Political	Ne
Information	Ne
Military	Ne
Economic	Ano

Dimenze moci	Použito v tomto případě
Financial	Ne
Intelligence	Ne
Legal	Ano

Tabulka 7 DIMEFIL: Převzetí kontroly nad ovládacím systémem úpravy pitné vody

6 PLNĚNÍ DOPORUČENÍ AUDITU NÁRODNÍ BEZPEČNOSTI K POSÍLENÍ ODOLNOSTI

Audit národní bezpečnosti byl již představen v podkapitole 1.4 Audit národní bezpečnosti. Tato kapitola se bude věnovat vyhodnocení plnění podkapitol Doporučení k posílení odolnosti v Auditu národní bezpečnosti v kapitolách Hrozby v kyberprostoru a Hybridní hrozby a jejich vliv na bezpečnost občanů ČR. Pro posouzení plnění byly použity pouze veřejně dostupná data.

6.1 HROZBY V KYBERPROSTORU A HYBRIDNÍ HROZBY A JEJICH VLIV NA BEZPEČNOST OBČANŮ ČR

Z celkem 13 doporučení byla vybrána tři doporučení, jejíž aplikaci lze snadno ověřit z veřejně dostupných zdrojů. Nelze předpokládat, že například posouzení možnosti nasazení ozbrojených sil v kontextu hybridních hrozeb bude veřejně dostupné.

Vybrané doporučení a jejich vyhodnocení:

- „*Vytvořit v rámci bezpečnostního systému ČR platformu pro sdílení informací, v níž se budou sbíhat informace a indikace, na základě kterých bude schopna identifikovat potenciální hybridní kampaň. Nemusí jít nutně o zřizování nové instituce, ale o vytvoření specifické kapacity lidí s požadovanou odborností v rámci již existujících institucí a jejich působností v rámci stávající legislativy.*“ (Ministerstvo vnitra České republiky, 2016)

Toto doporučení bylo splněno – bylo zřízeno Centrum proti terorismu a hybridním hrozbám, které je vedeno jako oddělení pod Odborem bezpečnostní politiky Sekce vnitřní bezpečnosti a policejního vzdělávání (Ministerstva vnitra České republiky, 2021).

- „*Definovat strategický přístup ČR, jak čelit hybridní kampani vedené proti ní nebo proti jinému státu NATO či EU (může být součástí Bezpečnostní strategie ČR nebo samostatným strategickým dokumentem). Přitom vycházet z analýzy přínosů, které nabízí mezinárodní spolupráce, primárně v rámci EU a NATO.*“ (Ministerstvo vnitra České republiky, 2016)

Toto doporučení bylo splněno – dne 19. dubna 2021 byla schválena Národní strategie pro čelení hybridnímu působení a usnesením Vlády České republiky bylo uloženo členům vlády a vedoucím ostatních ústředních správních orgánů realizovat strategické cíle této strategie (Vláda České republiky, 2021). Národní strategie pro čelení hybridnímu působení se v první kapitole zmiňuje, že vypracování této strategie bylo zadáno Auditem národní bezpečnosti a vychází z dokumentů Organizace Severoatlantické smlouvy a Evropské unie (Ministerstvo obrany České republiky , 2021).

- „*Přizpůsobit právní rámec pro umožnění aktivního zapojení zpravodajských služeb ČR do realizace opatření na obranu proti hybridní kampani vedené proti ČR nebo státům NATO a EU.*“ (Ministerstvo vnitra České republiky, 2016)

Toto doporučení bylo pravděpodobně nesplněno – od vydání Auditu národní bezpečnosti a jeho schválení Vládou České republiky byly zákony řešící právní rámec pro možnost zapojení zpravodajských služeb České republiky několikrát novelizovány (jedná se o zákony č. 153/1994 Sb. o zpravodajských službách České republiky, č. 154/1994 Sb. o bezpečnostní informační službě a č. 181/2014 Sb. o kybernetické bezpečnosti). Avšak ani jednou nebyl předmětem novelizace úpravy činnosti zpravodajských služeb České republiky.

6.2 HROZBY V KYBERPROSTORU

Z celkem deseti cílů a dílčích podcílů či prostředků k dosažení bylo vyhodnoceno pět, které je možné ověřit z veřejně dostupných zdrojů. Podobně jako u předchozí podkapitoly u některých cílů a dílčích podcílů či prostředků nelze provést ověřitelné zjištění stavu plnění.

- „*Provést některé novelizace platné právní úpravy v oblasti potírání kybernetické kriminality. Zejména je nutné se zaměřit na otázku anonymity uživatelů internetu a s tím spojené pátrání po pachatelích protiprávních skutků skrze možné doplnění dalších nástrojů do zákona o Policii ČR.*“ (Ministerstvo vnitra České republiky, 2016)

Toto doporučení bylo pravděpodobně nesplněno – od vydání Auditu národní bezpečnosti byl zákon č. 273/2008 Sb. o Policii ČR několikrát novelizován, avšak předmětem novelizací nebylo rozšíření pravomocí či nástrojů pro zjištění identity uživatelů internetu při pátrání po pachatelích protiprávní činnosti.

- „*Zamezit nedostatku kvalifikovaných pracovníků v oboru kybernetické bezpečnosti skrze: […]*

  b. novelizaci zákona č. 234/2014 Sb. o státní službě takovým způsobem, aby bylo zjednodušeno přijímání kvalitních odborníků na ICT a kybernetickou bezpečnost ve státní správě. […]" (Ministerstvo vnitra České republiky, 2016)

Nelze plně posoudit splnění tohoto doporučení – od vydání Auditu národní bezpečnosti došlo k úpravě nařízení vlády č. 304/2014 Sb. o platových poměrech státních zaměstnanců, které bylo změněno nařízením vlády č. 327/2016 Sb. nařízení vlády, kterým se mění nařízení vlády č. 304/2014 Sb., o platových poměrech státních zaměstnanců, ve znění nařízení vlády č. 279/2015 Sb. Dle novelizovaného nařízení vlády lze klíčovým zaměstnancům přiznat až dvojnásobek platového tarifu – stání správa již má v rukou lepší nástroj, kterým může udržet schopné zaměstnance ve služebním poměru. Jedna z uvedených hrozeb v Auditu národní bezpečnosti bylo v oblasti hrozeb v kyberprostoru: „*Nedostatek kvalifikovaných specialistů na problematiku ICT a kybernetické bezpečnosti a neschopnost tyto odborníky řádně finančně ohodnotit*." (Ministerstvo vnitra České republiky, 2016). Lze předpokládat, že tato hrozba byla částečně eliminována.

- „*Zahrnout důležité sektory jako chemický průmysl, zdravotnická zařízení a další strategická odvětví do soustavy KII skrze:*

  a. novelizaci krizového zákona a nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, jež by umožnilo zahrnutí důležitých sektorů mezi sektory KI, pomocí kterého je KII určována." (Ministerstvo vnitra České republiky, 2016)

Toto doporučení bylo nesplněno – neproběhla novelizace nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, která by toto doporučení splnila. Podrobněji je tato oblast popsána v podkapitole 3.3 Útok na Fakultní nemocnici v Brně v průběhu pandemie COVID-19.

- „*Dostatečně upravit vztahy mezi správci KII a VIS na straně jedné a dodavateli a subdodavateli ICT služeb na straně druhé.*

  a. K řešení tohoto problému již navrhl NBÚ, v rámci mezirezortního připomínkového řízení k návrhu zákona, kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, a některé další zákony, předkládaný nyní MV (MV-165721/LG-2015) k dalšímu legislativnímu procesu do Legislativní rady vlády, změnu v této oblasti a současně navrhl změnu zákona č. 181/2014 Sb.“ (Ministerstvo vnitra České republiky, 2016)

Toto doporučení bylo splněno – jak je napsáno v Auditu národní bezpečnosti – Národní bezpečnostní úřad v rámci mezirezortního připomínkového řízení navrhl úpravu, která byla přijata. Zákon byl následně vyhlášen 5. 4. 2017 ve Sbírce zákonů pod číslem 104/2017 Sb.

- „*Ošetřit problematiku zákona o svobodném přístupu k informacím (č. 106/1999 Sb.) ve vztahu ke kybernetické bezpečnosti, buďto:*

  a. novelizací rozsahu zákona č. 106/1999 Sb., nebo

  b. rozšířením povinnosti zachovávat mlčenlivost upravenou v ZKB i o vybrané aspekty bezpečnostních opatření, a stanovit tuto povinnost i správcům a provozovatelům informačních systémů a sítí ve věcné působnosti tohoto zákona (nyní se mlčenlivost týká jen evidence incidentů vedené vládním CERT). Tím by bylo dosaženo efektu vynětí bezpečnostně exponovaných informací z rozsahu zákona č. 106/1999 Sb. bez toho, aby bylo třeba zasahovat do jeho struktury.“ (Ministerstvo vnitra České republiky, 2016)

Toto doporučení bylo splněno – byl vydán zákon č. 205/2017 Sb. zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony – ze bylo zrušeno ustanovení § 11 odst. 4 písm. f zákona č. 106/1999 Sb. o svobodném přístupu k informacím *"Povinné subjekty dále neposkytnou informace o […] údajích vedených v evidenci incidentů podle zákona o kybernetické bezpečnosti, ze kterých bylo možné identifikovat orgán nebo osobu, která kybernetický bezpečnostní incident ohlásila nebo jejichž poskytnutí by ohrozilo účinnost reaktivního nebo ochranného opatření podle zákona o kybernetické bezpečnosti*." a toto ustanovení bylo nahrazeno novým paragrafem 10a v zákoně č. 181/2014 Sb. o kybernetické bezpečnosti: „*Informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost opatření vydaného podle tohoto zákona, nebo informace, které jsou vedené v evidenci incidentů, ze kterých by bylo možné identifikovat orgán nebo osobu, která kybernetický bezpečnostní incident ohlásila, se podle předpisů upravujících svobodný přístup k informacím neposkytují.*"

Zkratkou ZKB se rozumí zákon č. 181/2014 Sb., o kybernetické bezpečnosti.

ZÁVĚR

Cílem této kvalifikační práce bylo představit možnosti práce s otevřenými zdroji v oblasti hybridních hrozeb, které jsou součástí mezinárodních sporů, a v oblasti analýzy připravenosti České republiky z veřejně dostupných zdrojů. Druhým cílem bylo ověření možnosti využití dělení dimenzí moci DIMEFIL u hybridních hrozeb, které se odehrávají zejména v kyberprostoru.

Pro možnost splnění výše uvedených cílů bylo nutné analyzovat některé hybridní hrozby (zejména v oblasti kyberprostoru), popsat některé způsoby kybernetických útoků či infiltrací a uvést základy dimenzí moci DIMEFIL. Těmto třem mezikrokům se věnují druhá, třetí a čtvrtá kapitola.

Při ověřování připravenosti České republiky byl využit Audit národní bezpečnosti, který poskytl základní registr rizik v oblasti kyberprostoru a hybridních hrozeb. Poměrná část analyzovaných rizik v těchto dvou oblastech byla podrobena ověření, jakým způsobem probíhá plnění. Bylo zjištěno, že ani po pěti letech od publikování tohoto strategického dokumentu, nebyly ve výše zmíněných dvou oblastech realizována všechna doporučení. Bezesporu probíhá i oficiální vyhodnocování Auditu národní bezpečnosti, avšak závěry těchto vyhodnocení nejsou publikovány.

Bylo zjištěno, že aplikace frameworku dimenzí moci DIMEFIL na hybridní hrozby v kyberprostoru je komplikovaná a jeho aplikace je méně vypovídající než u prosazování cizích zájmů konvenčních sporů (či válek). Z aplikace je zejména patrné prolínání dimenzí moci u jednotlivých hybridních hrozeb a nerovnoměrné zapojení jednotlivých dimenzí moci.

Budoucí rozšíření této kvalifikační práce by mohlo být zejména zaměření na hybridní hrozby útočící na kritickou infrastrukturu České republiky – zejména revizi aktuálních legislativních požadavků a stanovení konkrétních doporučení pro úpravu legislativy a případně i zaběhlých postupů v oblasti kybernetické bezpečnosti.

RESUMÉ

Tato bakalářská práce pojednává o hybridních hrozbách v kyberprostoru, připravenosti České republiky na (hybridní) hrozby v kyberprostoru a zejména pak čerpání informací z veřejně dostupných zdrojů.

Bakalářská práce obsahuje podpůrné kapitoly, které analyzují některé hybridní hrozby, popisují způsoby infiltrací a framework dimenzí moci. Dále se v bakalářské práci nachází dvě kapitoly spíše praktického charakteru – jedna aplikuje framework DIMEFIL na analyzované hybridní hrozby v kyberprostoru, další se zaměřuje na vyhodnocení plnění doporučení z Auditu národní bezpečnosti.

Při aplikaci frameworku DIMEFIL na analyzované hybridní hrozby bylo zjištěno, že jeho použití je v této oblasti komplikované a hůře vypovídající. Pomocí analýzy plnění doporučení z Auditu národní bezpečnosti bylo zjištěno, že část doporučení zůstávají nerealizovaná a jejich realizace není v dohlednu.

SUMMARY

This bachelor thesis deals with hybrid threats in cyberspace, the Czech Republic's preparedness for (hybrid) threats in cyberspace, and especially the use of information from publicly available sources.

The bachelor thesis contains supporting chapters that analyse some hybrid threats, describe infiltration methods and the power dimension framework. In addition, there are two chapters of a more practical nature – one applies the DIMEFIL framework to the hybrid threats analyzed in cyberspace, and the other focuses on evaluating the implementation of recommendations from the National Security Audit.

In applying the DIMEFIL framework to the hybrid threats analyzed, it was found that its use in this area is complicated and less telling. Through the analysis of the implementation of the recommendations from the National Security Audit, it was found that some of the recommendations remain unimplemented and their implementation is not in sight.

BIBLIOGRAFIE

ASBIS CZ spol. s r.o., 2021. *ASBIS CZ.* [Online]
Dostupné na: https://www.asbis.cz/
[Citováno dne 30. května 2021].

Avaddon ransomware, 2021. *Avaddon ransomware.* [Online]
Dostupné na: Tor website
[Citováno dne 30. května 2021].

Bezpečnostní informační služba, 2018. *Výroční zpráva Bezpečnostní informační služby za rok 2017.* [Online]
Dostupné na: https://www.bis.cz/vyrocni-zpravy/vyrocni-zprava-bezpecnostni-informacni-sluzby-za-rok-2017-d85907e6.html
[Citováno dne 7. března 2021].

Bezpečnostní informační služba, 2019. *Výroční zpráva Bezpečnostní informační služby za rok 2018.* [Online]
Dostupné na: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2018-vz-cz.pdf.pdf
[Citováno dne 7. března 2021].

Bezpečnostní informační služba, 2020. *Výroční zpráva Bezpečnostní informační služby za rok 2019.* [Online]
Dostupné na: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf
[Citováno dne 2. června 2021].

Chapman, I. M., Sylvain, L. P. & Andrew, P., 2011. Taxonomy of Cyber Attacks and Simulation of Their Effects. p. 73–80.

Cimpanu, C., 2020. *Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak.* [Online]
Dostupné na: https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/
[Citováno dne 17. dubna 2021].

Čížek, J., 2021. *Oficiální web Olomouce nejede a my tušíme proč. Může za to opět ransomware.* [Online]
[Citováno dne 30. května 2021].

European Commission, 2016. *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats a European Union response.* Brussels: EUR-Lex.

European Union Agency for Law Enforcement Cooperation, 2019. *Internet Organised Crime Threat Assessment (IOCTA) 2018.* Haag: Euroopol.

Fakultní nemocnice Brno, 2021. *Lůžkový fond FN Brno.* [Online]
Dostupné na: https://www.fnbrno.cz/luzkovy-fond-fn-brno/t1027
[Citováno dne 28. dubna 2021].

Fakultní nemocnice v Motole, 2021. *Fakultní nemocnice v Motole v číslech.* [Online]
Dostupné na: https://www.fnmotol.cz/o-nas/historie-a-soucasnost/fakultni-nemocnice-v-motole-v-cislech/
[Citováno dne 28. dubna 2021].

Greenberg, A., 2021. *Wired.* [Online]
Dostupné na: https://www.wired.com/story/oldsmar-florida-water-utility-hack/
[Citováno dne 6. března 2021].

Kolouch, J., 2016. *CyberCrime.* CZ.NIC editor Praha: CZ.NIC, z.s.p.o..

Kolouch, J. & Bašta, P., 2019. *CyberSecurity.* Praha: CZ.NIC, z.s.p.o..

Kovář, M. & Auberová, D., 2021. *Kyberútok na olomoucký magistrát, agendy úřadů jsou mimo provoz.* [Online]
Dostupné na: https://olomoucky.denik.cz/zpravy_region/kyberutok-magistrat-olomouc-hacker-napadeni-2021.html
[Citováno dne 30. května 2021].

Masarykova univerzita, 2021. *Poskytnutí informace podle zákona č. 106/1999 Sb., osvobodném přístupu k informacím, ve znění pozdějších předpisů,* Brno: autor neznámý

Merrills, J. G., 2019. *International dispute settlement.* Cambridge: Cambridge University Press.

Ministerstva vnitra České republiky, 2021. *Organizační struktura Ministerstva vnitra.* [Online]
Dostupné na: https://www.mvcr.cz/clanek/organizacni-struktura-362751.aspx
[Citováno dne 2. června 2021].

Ministerstvo obrany České republiky , 2021. *Národní strategie pro čelení hybridnímu působení.* [Online]
Dostupné na: https://www.mocr.army.cz/informacni-servis/zpravodajstvi/vlada-schvalila-narodni-strategii-pro-celeni-hybridnimu-pusobeni-227120/
[Citováno dne 1. června 2021].

Ministerstvo vnitra České republiky, 2016. *Audit národní bezpečnosti,* Praha: Ministerstvo vnitra České republiky, odbor bezpečnostní politiky a prevence kriminality.

Ministerstvo vnitra České republiky, 2021. *Poskytnutí informace podle zákona č. 106/1999 Sb., osvobodném přístupu k informacím, ve znění pozdějších předpisů,* Praha: autor neznámý

Muthuppalaniappan, M. & Stevenson, K., 2020. Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal for Quality in Health Care*, 27 September, Issue 1.

Nadeem, B. & Lily, K., 2019. *Google blocks Huawei access to Android updates after blacklisting.* [Online]
Dostupné na: https://www.theguardian.com/technology/2019/may/19/google-huawei-trump-blacklist-report
[Citováno dne 3. června 2021].

Národní úřad pro kybernetickou a informační bezpečnost, 2018. *Varování NÚKIB ze dne 17. prosince 2018.* [Online]
Dostupné na:
https://nukib.cz/download/uredni_deska/Varovani_NUKIB_2018-122-17.pdf
[Citováno dne 17. ledna 2021].

Národní úřad pro kybernetickou a informační bezpečnost, 2019. *Zpráva o stavu kybernetické bezpečnosti ČR - 2018,* Praha: autor neznámý

Národní úřad pro kybernetickou a informační bezpečnost, 2020. *Doporučená bezpečnostní opatření k varování ze dne 16. dubna 2020,* Praha: autor neznámý

Národní úřad pro kybernetickou a informační bezpečnost, 2020. *Zpráva o stavu kybernetické bezpečnosti ČR - 2019,* Praha: autor neznámý

Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

Nařízení vlády č. 304/2014 Sb. o platových poměrech státních zaměstnanců

Nařízení vlády č. 327/2016 Sb. nařízení vlády, kterým se mění nařízení vlády č. 304/2014 Sb., o platových poměrech státních zaměstnanců, ve znění nařízení vlády č. 279/2015 Sb.

Pejšek, J., 2019. *Upřesnění k výroční zprávě BIS za rok 2018.* [Online] [Citováno dne 15. května 2021].

Poslanecká sněmovna, 2014. *Digitální repozitář Poslanecká sněmovna Parlamentu České republiky.* [Online]
Dostupné na: https://www.psp.cz/sqw/text/text2.sqw?idd=97551
[Citováno dne 7. března 2021].

Soroush, V., Roy, D. & Aral, S., 2018. The spread of true and false news online. *Science*, 359(6380), pp. 1146-1151.

Štalmach, P., 2018. Hybridní hrozby – včera, dnes a zítra - pohled z Prahy. *Czech Industry,* Issue 3, pp. 40-41.

Univerzita Hradec Králové, 2021. *Poskytnutí informace podle zákona č. 106/1999 Sb., osvobodném přístupu k informacím, ve znění pozdějších předpisů,* Hradec Králové: autor neznámý

Välisluureamet, 2019. *Estonian Foreign Intelligence Service public report 2018,* Tallinn: autor neznámý

Vláda České republiky, 2021. *Usnesení Vlády České republiky ze dne 19. dubna č. 384.* [Online]
Dostupné na: https://apps.odok.cz/attachment/-/down/IHOAC2AATLMK
[Citováno dne 1. června 2021].

Vojenské zpravodajství České republiky, 2020. *Výroční zpráva o činnosti Vojenského zpravodajství za rok 2019.* [Online].

Vránová, M., 2021. *Na magistrátu zachrání většinu dat, obnova potrvá. Hacker chce 100 tisíc dolarů.* [Online]
Dostupné na: https://olomoucky.denik.cz/zpravy_region/kyberutok-radnice-magistrat-olomouc-hacker-130421.html
[Citováno dne 30. května 2021].

Vysoké učení technické v Brně, 2021. *Poskytnutí informace podle zákona č. 106/1999 Sb., osvobodném přístupu k informacím, ve znění pozdějších předpisů,* Brno: autor neznámý

Wintour, P., 2018. *UK accuses Kremlin of ordering series of 'reckless' cyber-attacks.* [Online]
Dostupné na: https://www.theguardian.com/technology/2018/oct/04/uk-accuses-kremlin-of-ordering-series-of-reckless-cyber-attacks
[Citováno dne 25. května 2021].

Zákon č. 153/1994 Sb., o zpravodajských službách České republiky

Zákon č. 154/1994 Sb., o bezpečnostní informační službě

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím

Zákon č. 240/2000 Sb., zákon o krizovém řízení a o změně některých zákonů (krizový zákon)

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

Zákon č. 273/2008 Sb., o Policii ČR

Zákon č. 372/2011 Sb., Zákon o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách)

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Zákon č. 104/2017 Sb. zákon, kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony

Zákon č. 205/2017 Sb. zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony

Západočeská univerzita v Plzni, 2021. *Poskytnutí informace podle zákona č. 106/1999 Sb., osvobodném přístupu k informacím, ve znění pozdějších předpisů,* Plzeň: autor neznámý

Zelenka, J., 2020. Sledovali mě Číňané, abych dostal strach. Hrad od nás chtěl získat tajné informace, popsal muž, který varoval před Huawei. *Deník N*, 21. prosince, pp. 4-5.

SEZNAM TABULEK