

<https://doi.org/10.5817/RPT2020-1-3>

KYBERNETICKÁ ZBRAŇ: PŘÍSTUPY K JEJÍ DEFINICI¹

IVANA KUDLÁČKOVÁ²

ABSTRAKT

Odhalení počítačového červa Stuxnet v roce 2010 lze označit za zlomový okamžik, který zintenzivnil debaty o kybernetických zbraních. K těm je v odborné literatuře přistupováno různými způsoby, proto si tento příspěvek klade za cíl tyto rozdílné přístupy k definici pojmu kybernetická zbraň zmapovat a následně je aplikovat na reálné kybernetické incidenty.

Právě odhalení Stuxnetu je pro svůj dopad výchozím bodem, od kterého byla prováděna rešerše literatury, která se zabývá pojmem kybernetická zbraň. Za tímto účelem byly analyzovány odborné příspěvky publikované v období let 2010-2019 zařazené v databázích DBLP Computer Science Bibliography Website, Scopus a Web of Science.

Provedená analýza posloužila k představení hlavních přístupů ke kybernetickým zbraním. Definice byly poté podrobeny analýze a byly identifikovány dva hlavní faktory způsobující názorový nesoulad.

KLÍČOVÁ SLOVA

kybernetická zbraň, kybernetický incident, malware, Stuxnet

¹ Tento článek vznikl za podpory projektu "Centrum excelence pro kyberkriminalitu, kyberbezpečnost a ochranu kritických informačních infrastruktur" (CZ.02.1.01/0.0/0.0/16_019/0000822).

² Mgr. Bc. Ivana Kudláčková, výzkumná pracovnice, Ústav práva a technologií, Právnická fakulta, Masarykova univerzita, ivana.kudlackova@mail.muni.cz.

ABSTRACT

Discovery of Stuxnet (a computer worm) in 2010 can be described as a turning point leading to intensification of cyber weapons discussions. This paper aims to map different approaches to the term cyber weapons and apply them to real cyber incidents respectively.

Discovery of Stuxnet is determined as a starting point from which the literature review dealing with the concept of cyber weapons was carried out. Papers published within the period 2010-2019 in DBLP Computer Science Bibliography Website, Scopus and Web of Science databases were analysed.

The analysis helped to introduce three main approaches to cyber weapons. These approaches were then analysed and two main factors causing discrepancy were identified.

KEYWORDS

cyber weapon, cyber incident, Stuxnet, malware

1. ÚVOD

Tým německých expertů v čele s bezpečnostním konzultantem Ralphem Langerem v září 2010 zveřejnil zprávu, která popisovala fungování a dopad počítačového červa jménem Stuxnet.³ Tento den a události po něm následující lze bezesporu chápat jako významný milník možného nasazení a významu kybernetických zbraní. Sám Ralph Langer v r. 2011 uvedl, že „minulý rok znamenal zlom v historii kybernetické bezpečnosti – příchod první kybernetické zbraně známé jako Stuxnet.“⁴ Za klíčový lze tento okamžik označit především ze dvou hlavních důvodů. Zaprvé, Stuxnet byl svojí povahou čistě kybernetickým incidentem, který nebyl doprovázen kinetickými prostředky. Zadruhé, Stuxnet přímo způsobil zničení jaderných

³ V současné chvíli je k dispozici aktualizovaná verze této zprávy. LANGER, Ralph. *To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. [online]. 2013 [cit. 25.10.2019]. Dostupné z: <https://www.langner.com/wp-content/uploads/2017/04/To-kill-a-centrifuge.pdf> .

⁴ LANGER, Ralph. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security Privacy*. 2011, 9(3), str. 49.

centrifug, které musely být nahrazeny za nové a tento incident tedy vyvolal hmotnou škodu, která se projevila ve fyzickém světě. Do té doby probíhající debaty o potenciálu kybernetických zbraní tak získaly reálné obrysy. Poprvé byl explicitně vyřčen názor, že Stuxnet je kybernetickou zbraní, což posléze vedlo k rozproudění dalších debat. Pozornost byla mj. zaměřena na konkrétní parametry, které musí být splněny, aby mohl být určitý nástroj označen za kybernetickou zbraň.

Předkládaný příspěvek mapuje debatu odborné veřejnosti právě od r. 2010, kdy došlo k odhalení Stuxnetu, až do r. 2019. V tomto časovém období se čím dál častěji objevoval termín kybernetická zbraň, jenž doposud nemá normativní zakotvení. Výchozí situací je stav, kdy se termín kybernetická zbraň používá v různých významech, a to s ohledem na zázemí, ze kterého konkrétní autor pochází. Zcela nepřekvapivě pak bude mít odlišnou představu o takové zbraní právník, který rozhoduje o souladu jejího nasazení s právem; voják, jehož cílem je získat vojenskou výhodu; policy-maker, jenž bude uvažovat o možné eskalaci vzájemných vztahů v případě, že k nasazení kybernetické zbraně dojde. Každý z nich tedy sleduje jiné zájmy a klade důraz na jiné prvky. Autor nepovažuje existenci různých přístupů v jednotlivých odvětvích za *a priori* problematické. Z ryze praktické stránky je ale problematická situace, kdy jednotlivci nejsou dostatečně obeznámeni s přístupy ostatních. Pouze prostřednictvím vzájemného pochopení odlišností lze docílit efektivní spolupráce mezi jednotlivými profesemi. Specialisté z jednotlivých oblastí spolu navzájem komunikují, a to např. v rámci kybernetických cvičení, a pokud je používán termín, kterému ovšem jednotlivci připisují odlišný význam a jedinci si těchto odlišných přístupů nejsou vědomi, může to způsobit komplikace. Pokud je kupříkladu politikou konkrétního státu přístup, že nedojde k nasazení kybernetických zbraní, musí si být právník vědom toho, co je považováno za kybernetickou zbraň na politické úrovni, a upozornit na situace, kdy by mohlo příp. k takovému nasazení dojít. Pokud naopak bude mít voják zcela jasno o tom, co je kybernetickou zbraní, tak může nastat situace, kdy její nasazení nebude konzultovat s právníkem (který by její

nasazení mohl nedoporučit, protože z právního úhlu bude za kybernetickou zbraň považovat něco jiného).

Autor si neklade za cíl představit jednotnou a ustálenou definici kybernetické zbraně, neboť taková snaha by se zcela minula účinkem z důvodu jejího nesouladu s běžnou realitou. Autor reaguje na stav, kdy mezi odbornou veřejností doposud chybí zmapování odlišných přístupů a jejich aplikace na konkrétní případy. Z těchto důvodů jsou hlavní cíle tohoto článku následující. Zaprvé, cílem je poskytnout ucelený přehled přístupů k definici pojmu kybernetická zbraň. Tohoto cíle je dosaženo prostřednictvím analýzy odborných článků a výstupů z konferencí publikovaných v letech 2010-2019. Tato analýza následně poslouží i k naplnění druhého cíle, kterým je syntéza těchto přístupů a identifikování slabých míst. Druhý cíl bude naplněn prostřednictvím aplikace jednotlivých definic na reálné kybernetické incidenty, které ve svých příspěvcích zmiňovali sami autoři. Tato analýza tak poslouží k objasnění jednotlivých přístupů a vzájemnému porozumění v případě reálné kybernetické operace.

Za tímto účelem je příspěvek koncipován následujícím způsobem. V první kapitole je vysvětlena metoda sběru a zpracování dat. Dále je pozornost věnována samotným výsledkům. Druhá kapitola představí již proběhlé kybernetické incidenty, jejichž spouštěč může či taktéž nemusí být označen za kybernetickou zbraň. Třetí kapitola se zaměří na autory, již poskytují přímou definici kybernetické zbraně. Čtvrtá kapitola je pak věnována příkladům různých typů kybernetických nástrojů, které autoři přímo či nepřímo za kybernetickou zbraň označují. Pátá kapitola je zaměřena na autory, jejichž přístupy nespádají do žádných předchozích kapitol. Poslední kapitola je pak nejdůležitější, neboť představuje onen diskuzní přínos, kdy dojde k aplikaci definic na konkrétní incidenty a k identifikaci slabých míst.

2. METODA SBĚRU A ZPRACOVÁNÍ DAT

K získání prvotního setu všech relevantních zdrojů byly využity databáze DBLP computer science bibliography (dále jen „DBLP“), Scopus a Web of

Science. Za klíčová slova byla zvolena slovní spojení cyber weapon nebo též cyberweapon. V časovém rozmezí let 2010-2019 bylo celkově napříč databázemi identifikováno 124 výsledků v následujícím rozložení: DBLP (34 výstupů), Scopus (47 výstupů) a Web of Science (43 výstupů). Následně byl počet výstupů redukován, a to na základě následujících parametrů. Nejdříve byly odstraněny výstupy, které se opakovaly napříč databázemi, ojediněle byl některý výstup několikrát i ve stejné databázi. V této chvíli počet výstupů klesl na 76, s rozložením DBLP (33 výstupů), Scopus (27 výstupů), Web of Science (16 výstupů). Toto rozložení výsledků je dáno postupem, kterým došlo k vyřazení opakujících se výstupů. Za výchozí databázi byla určena databáze DBLP, vůči které pak byly porovnávány výstupy databáze Scopus (proto počet originálních děl klesl v databázi Scopus tak razantním způsobem). Následně byla databáze Web of Science porovnána s databázemi DBLP a Scopus, proto je počet výstupů v databázi Web of Science nejnižší.

Následně probíhala další selekce, která se skládala ze tří kroků. Cílem prvního kroku bylo určit výstupy, které je možné označit za článek odborného časopisu či článek vznikající v návaznosti na konferenci. Tento postup byl zvolen z důvodu prvku recenzního řízení, které je právě u těchto dvou typů žádaným standardem. Cíleně tak nebylo pracováno s kapitoly knížek nebo jejich pouhými recenzemi. Vyřazeno bylo 21 výstupů. Druhý krok je možné označit za subjektivní kritérium, neboť jeho cílem bylo určit, zda je daný článek či výstup z konference v souladu se stanoveným cílem zmapování přístupů k definici kybernetické zbraně. Vyřazeny tak byly takové výstupy, kde jediná zmínka o kybernetických zbraních byla např. v seznamu literatury, či jediná spojitost s tématem spočívala v názvu časopisu, který obsahoval slovo kybernetický. Tímto krokem neprošlo 11 výstupů. Poslední krok je nutné jednoznačně označit za limit výzkumu. Některé výstupy, který by pravděpodobně prošly výše zmíněnými kritérii, totiž nebyly k dispozici v kompletním znění, neboť nebyla k dispozici licence Masarykovy univerzity, která by umožnila přístup. Celkově tedy nebyl umožněn přístup k 10 výstupům.

Na první pohled byl vcelku rozsáhlý set 124 výsledků redukován na pouhých 34 výstupů, a to s rozložením DBLP (18), Scopus (14) a Web of Science (2). Přestože se může na první pohled jevit, že je problematika již dopodrobna zpracována a existuje dostatek zdrojů, spousta otázek doposud zůstává nezodpovězených. S výstupy je až na výjimku v kapitole *Ostatní přístupy* pracováno v chronologickém pořadí, kdy rozhodující je rok, ve kterém došlo k publikaci. Tento přístup byl zvolen z důvodu snahy reflektovat změnu též s ohledem na postupující čas.

3. KYBERNETICKÉ INCIDENTY

Analýza již proběhlých kybernetických incidentů poskytuje vhodný rámec, skrze něhož lze uceleně přistoupit ke kybernetickým zbraním. Přestože tento přístup není nejjednodušší a je vyžadována nejenom znalost průběhu, ale mnohdy i technických detailů samotných incidentů, umožní komplexní pochopení celé problematiky. V této kapitole je dán prostor k seznámení se s fakty jednotlivých případů, pozornost ale nebude záměrně věnována případu testování nového systému s cílem vyřadit navigaci GPS mimo provoz, neboť v tomto případě se jedná o pouhé podezření.⁵

Nejčastěji zmiňovaným incidentem je bezesporu počítačový červ Stuxnet, jehož cílem bylo obohacovací uranové středisko v Íránu (v Natanz). Samotný Stuxnet způsobil, že se jednotlivé centrifugy začaly točit příliš rychle nebo naopak pomalu, což v některých případech vedlo k jejich explozi a vzniku materiální škody. Poškozené centrifugy musely být vyměněny za nové. Jednalo se o „světově první kybernetickou zbraň zaměřenou na kritické průmyslové kontrolní systémy.“⁶ Zároveň je Stuxnet označován za „nejúspěšnější kybernetickou zbraň“⁷, která změnila „pravidla hry, a to vzhledem k její složitosti, účelu a výkonu.“⁸ Jiní autoři se podrobněji

⁵ HAMBLING, David. Hints of a new cyberweapon: GPS spoofing may have thrown vessels off course in the Black Sea. *New Scientist*. 2017, 235(3139), str. 6.

⁶ BARZASZKA, Ivanka. Are cyber-weapons effective? *The RUSI Journal*. 2013, 158(2), str. 48.

⁷ KOBLENTZ, Gregory D.; MAZANEC, Brian M. Viral Warfare: The Security Implications of Cyber and Biological Weapons. *Comparative Strategy*. 2013, 32(5), str. 423.

⁸ MAITRA, Amit K. Offensive cyber-weapons: technical, legal, and strategic aspects. *Environment Systems and Decisions*. 2015, 35(1), str. 173.

věnovali technické stránce Stuxnetu a popisovali proces, který vedl k požadovanému výsledku⁹, našli se ovšem i tací, kteří na Stuxnet odkázali bez dalšího.¹⁰

Tento počítačový červ ale není jediným incidentem, se kterým autoři pracují. Dále se lze obeznámit s průběhem výbuchu transsibiřského plynovodu v roce 1982,^{11,12} který je třeba zasadit do kontextu Studené války. Pro bezchybný chod plynovodu potřeboval Sovětský svaz získat speciální software obdobný dnešním SCADA systémům. Existuje podezření, že dodaný software CIA úmyslně pozměnila takovým způsobem, aby došlo k vytvoření přetlaku v potrubí, a to prostřednictvím manipulace s regulačními ventily. Samotný výbuch tedy nebyl způsoben výpadkem systému, ale právě příliš silným tlakem. Odpůrci této teorie naopak tvrdí, že chyba byla na straně pracovníka, který rostoucí tlak i nadále udržoval, aby nedošlo k přerušení toku zemního plynu.¹³

Jak již z názvu vypovídá, v případě experimentu Aurora se nejednalo o reálný útok, neboť se uskutečnil jako pouhý pokus v energetickém oddělení národní laboratoře ve státě Idaho. Cílem experimentu bylo zjistit, zda by hacker mohl zasáhnout do řídicího systému provozujícího generátor

⁹ Srovnej RID, Thomas; McBURNEY, Peter. Cyber-Weapons. *The RUSI Journal*. 2012, 157(1), str. 9. PETERSON, Dale. Offensive Cyber Weapons: Construction, Development, and Employment. *Journal of Strategic Studies*. 2013, 36(1), str. 121. CARR, Jeffrey. The misunderstood acronym: Why cyber weapons aren't WMD. *Bulletin of the Atomic Scientists*. 2013, 69(5), str. 34. BELLOVIN, Steven M.; LANDAU, Susan; LIN, Herbert S. Limiting the undesired impact of cyber weapons: technical requirements and policy implications. *Journal of Cybersecurity*. 2017, 3(1), str. 60.

¹⁰ Srovnej TYUGU, Enn. Situation awareness and control errors of cyber weapons. In: *IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*. 2013, str. 143.

¹¹ RID, Thomas; McBURNEY, Peter. Cyber-Weapons. *The RUSI Journal*. 2012, 157(1), str. 9.

¹² CARR, Jeffrey. The misunderstood acronym: Why cyber weapons aren't WMD. *Bulletin of the Atomic Scientists*. 2013, 69(5), str. 33.

¹³ Srovnej CARR, Jeffrey. The misunderstood acronym: Why cyber weapons aren't WMD. *Bulletin of the Atomic Scientists*. 2013, 69(5), str. 34.

a způsobit tak jeho poškození.¹⁴ Video poukazující na zranitelnost těchto systémů je k dispozici v několika verzích na YouTube.¹⁵

Skutečným incidentem pak byly DDoS útoky v Estonsku v r. 2007, jež byly s největší pravděpodobností reakcí na přesunutí sochy vojáka představující sovětský válečný památník 2. světové války. Pouliční nepokoje byly doprovázeny sérií DDoS útoků trvajících tři týdny. Zároveň bylo mimo provoz 58 estonských webových stránek, v součtu více než dvě hodiny byly též nefunkční online služby největší estonské banky.¹⁶

Útok uskutečněný Izraelem na syrský vzdušný obranný systém v r. 2007 byl naopak pouhým prostředkem, který posloužil k efektivnějšímu útoku na syrský jaderný objekt. Cílem kybernetického útoku bylo přimět obranný systém k tomu, aby po určitý časový úsek nezobrazoval žádná přibližující se letadla a umožnil tak provést útok kinetickými prostředky na fyzický objekt, což se i zdárně podařilo.¹⁷

Posledním z incidentů je nasazení počítačového viru Shamoon proti saudskoarabské ropné společnosti Saudi Aramco. Shamoon způsobil zničení pevných disků a též došlo k vymazání dokumentů, které byly nahrazeny obrázkem hořící americké vlajky.¹⁸

Někteří autoři tedy cíleně s kybernetickými incidenty pracují, nejasná situace ale nastává v případech, kdy autoři na tyto incidenty pouze bez dalšího odkazují a neprovádí podrobnější zhodnocení. Slabinou tohoto přístupu je fakt, že může docházet k nežádoucímu zjednodušení celé situace tím, že budou tyto incidenty plošně a bez další analýzy označeny přívlastkem kybernetický a jejich spouštěč pak bude považován za kybernetickou zbraň. V případech, kdy autor cíleně neodpovídá na otázku, zda zmínka o kybernetickém incidentu je zároveň odpovědí na to, zda je

¹⁴ CARR, Jeffrey. The misunderstood acronym: Why cyber weapons aren't WMD. *Bulletin of the Atomic Scientists*. 2013, 69(5), str. 34.

¹⁵ Například Staged cyber attack reveals vulnerability in power grid. Dostupné z: <https://www.youtube.com/watch?v=fJyWngDco3g> [vid. 5. února 2020].

¹⁶ RID, Thomas; McBURNEY, Peter. Cyber-Weapons. *The RUSI Journal*. 2012, 157(1), str. 8.

¹⁷ Tamtéž, str. 9.

¹⁸ CARR, Jeffrey. The misunderstood acronym: Why cyber weapons aren't WMD. *Bulletin of the Atomic Scientists*. 2013, 69(5), str. 34.

její spouštěč bez další považován za kybernetickou zbraň, je nutné pracovat s oběma variantami (tedy, že se může, ale nemusí jednat o kybernetickou zbraň) a přistupovat k hodnocení situace kriticky. K tomuto kritického zhodnocení se přiklání i autor článku, jenž cíleně využije výše uvedené incidenty k samotné analýze v kapitole *Diskuze*.

4. DEFINICE KYBERNETICKÉ ZBRANĚ

V této kapitole jsou zmíněni autoři, již cíleně představují definici kybernetické zbraně. Prvním z nich je dvojice autorů Lorents a Ottis, již svůj výzkum založili na formální logice s matematicky prokazatelnými výsledky a představili tři vzájemně provázané koncepty, a to zbraň, zbraň informačních technologií (zbraň IT) a kybernetickou zbraň. Za zbraň označují „*system, který je navržen tak, aby poškodil strukturu nebo operace jiného systému.*“¹⁹ Pro účely tohoto příspěvku je rozhodující pochopení rozdílů mezi zbraní IT a kybernetickou zbraní. Zatímco obě tyto zbraně jsou založeny na informačních technologiích, liší se ve svých cílech. Zbraň IT má širší záběr a je navržena tak, aby „*poškodila strukturu nebo operace jiného systému.*“²⁰ Lze si představit systém sloužící k přesné lokalizaci vojenského cíle, kterým může být např. budova, která bude posléze zničena pozemní silou. Podmnožinou zbraní IT je kybernetická zbraň, jež má sloužit k „*poškození struktury nebo provozu některých jiných systémů založených na informačních technologiích.*“²¹ Tito autoři tedy vnímají kybernetickou zbraň z pohledu cíle, kterým má být prvek obsahující informační technologii.

Obdobně poukazují na souvislost mezi zbraní jako nadřazeným termínem a kybernetickou zbraní jako její množinou autoři Rid a McBurney, svou pozornost ale zaměřili na cíl, kterého má kybernetická zbraň dosáhnout. Takováto zbraň je pak „*počítačový kód, který je používán nebo navržen tak, aby byl používán s cílem ohrožovat nebo způsobovat fyzické,*

¹⁹ LORENTS, Peeter; OTTIS, Rain. Knowledge based framework for cyber weapons and conflict. In: *Conference on Cyber Conflict Proceedings 2010*. Tallinn: CCD COE Publications, 2010, str. 139.

²⁰ Tamtéž.

²¹ Tamtéž.

*funkční nebo duševní poškození struktur, systémů nebo živých bytostí.*²² Cílem kybernetické zbraně tedy nemusí být pouze systém založený na informační technologii, ale utrpět újmu mohou i jiné objekty. Zároveň představují dělení zbraní na tzv. obecné s nízkým potenciálem (používají připodobnění k paintballovým zbraním, v kybernetickém světě pak odkazují na malware) nebo takové, které jsou specifické a disponují vysokým potenciálem (ty připodobňují k antiradarovým střelám, či k malware, který je schopen proniknout do chráněných a fyzicky izolovaných systémů a je schopen autonomně ovlivnit výstupy systému tak, aby spáchal přímou újmu)²³. Autoři také upozorňují na nepatrný rozdíl mezi tím, co lze ještě označit za kybernetickou zbraň a co již ne. Určení této hranice má své bezpečnostní, politické a právní důsledky. V této souvislosti zmiňují nezbytný prvek úmyslu, neboť *“ani vysoce sofistikovaný malware, který je vyvíjen a používán pouze za účelem skryté exfiltrace dat ze sítě nebo stroje, není zbraní.”*²⁴

S prvkem úmyslu pracuje i L. Arimatsu, jež tvrdí, že pouze pokud je prokázáno, že malware má *„útočné schopnosti a existuje úmysl jej používat způsobem, který odpovídá jeho útočné schopnosti, může být považován za kybernetickou zbraň.“*²⁵

Myšlenku dělení zbraní dle jejich potenciálu nevědomky rozvíjí E. Tyugu. Pozornost věnuje sice pouze pokročilým malwarům (bez bližší specifikace), zároveň ale kybernetické zbraně definuje velmi široce či až vágně, kdy uvádí, že se jedná o *„agenty působící v kyberprostoru, (...) skládající se ze všech výpočetních zařízení, dat a softwaru přístupných prostřednictvím sítě (internet, mobilní sítě atd.).“*²⁶ Odkazuje sice na Stuxnet

²² RID, Thomas; McBURNEY, Peter. Cyber-Weapons. *The RUSI Journal*. 2012, 157(1), str. 7.

²³ Tamtéž, str. 7 a 8.

²⁴ Tamtéž, str. 11.

²⁵ ARIMATSU, Louise. A treaty for governing cyber-weapons: Potential benefits and practical limitations. In: *Conference on Cyber Conflict Proceedings 2012*. Tallinn: CCD COE Publications, 2012, str. 98.

²⁶ TYUGU, Enn. Situation awareness and control errors of cyber weapons. In: *IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*. 2013, str. 144.

a též na malware Flame²⁷, ale oproti předchozím autorům tato definice vyvolává více otázek, než nabízí odpovědí.

Více odpovědí naopak nabízí A. K. Maitra, jenž je zároveň prvním autorem pracujícím s vícero definicemi. S ohledem na v té době již existující Tallinský manuál²⁸ představuje kybernetické zbraně jako „*kybernetické prostředky k válčení, které jsou svým designem, použitím či zamýšleným použitím schopné způsobit zranění či smrt osob.*“²⁹ Tento přístup je třeba chápat v kontextu Tallinnského manuálu, jehož první vydání je zaměřeno na aplikaci mezinárodního práva v kontextu kybernetické války. Tato definice už tak nereflktuje stav, kdy může být kybernetická zbraň nasazena i v situacích, které nelze označit za kybernetickou válku. Dále se inspiruje přístupem autorů Rid a McBurney a zaměřuje se na cíl, kterým má být „*poškození počítačového nebo telekomunikačního systému mající povahu kritické infrastruktury.*“³⁰ Svoji roli tak nehraje pouze schopnost samotné zbraně, ale též i to, vůči čemu nebo komu je nasazena. Zároveň A. K. Maitra hodnotí možný budoucí vývoj situace a absenci definice kybernetické zbraně označuje za mezeru v právu.³¹

Na problém absence globální definice naráží i autoři Maathuis, Pieters a Berg a předkládají myšlenku, že kybernetickou zbraní je „*počítačový kód vytvořený a/nebo používaný k pozměnění či poškození systému (resp. komponentu informační a komunikační technologie) s cílem dosáhnout (vojenských) cílů proti protivníkům uvnitř a/nebo mimo kyberprostor.*“³² Nad to se autoři dále věnují jednotlivým složkám této definice a blíže vysvětlují

²⁷ Tamtéž, str. 143.

²⁸ Tady je ovšem odkazováno na jeho první verzi publikovanou v r. 2013, druhá verze vyšla v r. 2017.

²⁹ MAITRA, Amit K. Offensive cyber-weapons: technical, legal, and strategic aspects. *Environment Systems and Decisions*. 2015, 35(1), str. 179.

³⁰ Tamtéž, str. 179.

³¹ Tamtéž, str. 176.

³² Cyber weapons: a profiling framework - Clara Maathuis, Wolter Pieters, Jan van den Berg, 2016, s. 4. MATHIUS, Clara; PIETERS, Wolter; BERG, Jan van den. Cyber weapons: a profiling framework. In: *2016 IEEE International Conference on Cyber Conflict (CyCon U.S.) Proceedings*. USA: IEEE eXpress Conference Publishing. 2016, str. 97.

jejich význam. Jejich přístup lze označit za unikátní, jdoucí do hloubky a nevyhýbající se obtížným prvkům celé definice.

Žádoucího efektu na systém může být docíleno různými způsoby, proto se za kybernetickou zbraň dá označit též software, jenž „*může způsobit destruktivní, škodlivé nebo znehodnocující účinky na systém nebo síť, proti které je namířen.*”³³ Žádný z těchto autorů už ale neposkytuje bližší vysvětlení či nenabízí příklady, které by napomohly lepší představě o tom, jakými způsoby mohou tyto účinky nastat. Vodítko nabízejí až Kushwaha a Watson, již si kladou tuto otázku a poskytují na ni odpověď. Pokud tedy kybernetické zbraně mají „*způsobit zranění nebo smrt osob nebo poškození či zničení předmětů, musí kompromitovat systémy, které mají dopad na lidský život; tedy systémy spravující kritickou infrastrukturu včetně jaderných nebo vojenských zařízení, vládní infrastrukturu apod.*”³⁴

Schopnost způsobit újmu je tak klíčovým prvkem kybernetických zbraní. V souvislosti se vzájemným vztahem mezi pojmy kybernetická zbraň a malware na to upozorňují autoři Eggenschwiler a Silomon. Nestačí tyto pojmy nějak mechanicky rozlišovat, je nezbytné zaměřit se na znaky, které konkrétní malware vykazuje. Do množiny kybernetických zbraní bude malware spadat pouze za předpokladu, že vykazuje schopnost způsobit újmu, pouhé „*nasazení malwaru za účelem skryté exfiltrace dat ze sítě*”³⁵ tak není dostačující. Na schopnost kybernetické zbraně způsobit újmu nelze nahlížet optikou konvenčních zbraní, a to z toho důvodu, že kybernetické zbraně mají kratší životnost, resp. mají pouze dočasnou schopnost způsobit újmu, a to do té doby, než je chyba v konkrétním systému opravena.

S postupujícím časem lze sledovat nejnovější trend přejímání definic, které představily buď státy nebo organizace, konkrétně NATO. Ustupuje tak snaha autorů přicházet s inovativními způsoby, kterak uchopit pojem

³³ BELLOVIN, Steven M.; LANDAU, Susan; LIN, Herbert S. Limiting the undesired impact of cyber weapons: technical requirements and policy implications. *Journal of Cybersecurity*. 2017, 3(1), str. 60.

³⁴ KUSHWAHA, Neal; WATSON, Bruce William. Cyber weapons and the U.S. In: *Proceedings of the 17th European Conference on Cyber Warfare and Security*. 2018, str. 1.

³⁵ EGGENSCHWILLER, Jacqueline; SILOMON, Jantje. Challenges and opportunities in cyber weapon norm construction. *Computer Fraud & Security*. 2018, 12, str. 12.

kybernetická zbraň. Autoři se tak například inspirovali definicí, kterou představilo Centrum excelence při Severoatlantické alianci (NATO CCD COE), jež za kybernetickou zbraň označuje „*software, firmware nebo hardware navržený nebo použitý tak, abych způsobil škodu v počítačové doméně.*“³⁶ Ze stanovisek států je často zmiňována definice Ministerstva obrany Spojených států amerických, které za kybernetickou zbraň považují „*zařízení, počítačový program nebo techniku, včetně jakékoli kombinace softwaru, firmwaru nebo hardwaru, určené k vytvoření efektu v nebo prostřednictvím kyberprostoru.*“³⁷

Jakkoli doposud zmíněné přístupy k definici kybernetické zbraně mohou působit konstruktivně, opačný názor zastává F. B. Hare, jenž se vymezil vůči dosavadním autorům, kteří do centra pozornosti umístili počítačový kód a jím zamýšlený účinek, který je schopen vyvolat. Hare zpochybnil tento přístup a označil ho za „*dostačující v diskuzi o počítačové kriminalitě, ale již znemožňující produktivní diskuzi o vojenské aplikaci kybernetické síly.*“³⁸ K tomuto závěru dospěl z důvodu požadavku přísného hodnotícího procesu, který se uplatňuje při vývoji konvenčních zbraní. V případě počítačového kódu si nelze představit situaci, kdy by armádní složky jednoduše nasadily takovýto kód, aniž by ho před tím nepodrobily přísnému hodnotícímu procesu.³⁹ Přestože s touto myšlenkou kritizovaní autoři cíleně nepracují, je na zvážení, zda jimi zastávané přístupy jsou v rozporu s požadavkem, který prezentuje Hare.

³⁶ YAMIN, Muhammad Mudassar; KATT, Basel; KIANPOUR, Mazaher. Cyber Weapons Storage Mechanisms. In: *Security, Privacy, and Anonymity in Computation, Communication, and Storage*. 2019, str. 354. KALLBERG, Jan. The Second Amendment and Cyber Weapons: Constitutional Relevance of Digital Gun Rights. *IEEE Technology and Society Magazine*. 2019, 38(2), str. 73.

³⁷ KALLBERG, Jan. The Second Amendment and Cyber Weapons: Constitutional Relevance of Digital Gun Rights. *IEEE Technology and Society Magazine*. 2019, 38(2), str. 73.

³⁸ HARE, Forrest B. Precision cyber weapon systems: An important component of a responsible national security strategy? *Contemporary Security Policy*. 2019, 40(2), str. 195.

³⁹ Tamtéž, str. 195.

5. VÝČET PŘÍKLADŮ KYBERNETICKÝCH ZBRANÍ

Zcela odlišný přístup k definici kybernetické zbraně zaujímají autoři, kteří se ve svých příspěvcích neuchylují k přímé definici. Naopak využívají obecné technické termíny a mnohdy je pouze z kontextu samotného příspěvku možné usoudit, zda autor má sklon určitý technický pojem využít jako prostředek k vyjádření toho, co je to kybernetická zbraň.

Při tomto přístupu narážíme na dva problémy. Prvním z nich je nejasný vztah mezi pojmem malware a kybernetická zbraň. Autor se tak mnohdy zaměřuje na jejich vývoj a možný budoucí potenciál bez toho, aby poskytl řádné teoretické ukotvení. Lze se tak dozvědět, že malware a kybernetické zbraně se „stávají sofistikovanějšími, nezávislejšími a inteligentnějšími“⁴⁰, ale již není řečeno, co to malware a kybernetická zbraň znamená. Tento přístup bohužel není ojedinělý.⁴¹ Pokud není primárním cílem autorů mluvit o kybernetických zbraních, ale zaměřují svoji pozornost na nějaké související či specifitější téma, tak lze sledovat tendenci opomíjení představení alespoň nějaké pracovní definice. Příkladem může být výzkum zkoumající prvek kontroly kybernetických zbraní z důvodu zamezení kolaterálních škod, autoři ovšem vzápětí poukazují na nejstarší malwary, které v sobě nějaké kontrolní prvky měly zakomponovány.⁴² Jak autoři vnímají vztah mezi kybernetickou zbraní a malwarem zůstává nejasné.

Druhým problémem je specifikace jednotlivých druhů malwaru bez uvedení spojitosti mezi kybernetickou zbraní, malwarem a jejich jednotlivými druhy. Je otázkou, zda „software, který poškozuje uživatele, počítač nebo síť, lze považovat za malware včetně virů, trojských koní, červů, rootkitů a spywaru“⁴³, už také nenaplnuje definici kybernetické zbraně. Autoři se k této otázce nevyjadřují. V některých případech lze nalézt

⁴⁰ TYUGU, Enn. Command and control of cyber weapons. In: *Conference on Cyber Conflict Proceedings 2012*. Tallinn: CCD COE Publications, 2012, str. 334.

⁴¹ Srovnej KIRAVUO, Timo; SÄRELÄ, Mikko; MANNER, Jukka. Weapons against Cyber-Physical Targets. In: *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops Proceedings*. USA: IEEE Computer Society Conference Publishing Services, 2013, str. 321.

⁴² Srovnej RAYMOND, David; CONTI, Gregory J.; CROSS, Tom; FANELLI, Robert. A control measure framework to limit collateral damage and propagation of cyber weapons. In: *Conference on Cyber Conflict Proceedings 2013*. Tallinn: CCD COE Publications, 2013, str. 182.

odpověď na tuto otázku v kontextu konkrétního příspěvku, kdy autor například uvede, že „kombinací ransomware s červí technologií a zranitelnostmi nultého dne dohromady vzniká nová ransomware kybernetická zbraň.“⁴⁴ Přestože tento výše uvedený přístup není tak frekventovaný jako možnost představení přímé definice, nachází i přesto několik zastánců.

6. OSTATNÍ PŘÍSTUPY

Tato kapitola představuje značně složité a nejméně uchopitelné pojetí kybernetických zbraní, protože se pouze s velkými obtížemi daří nalézt indikátory, které by odpovídaly na otázku, co je to kybernetická zbraň.

Jedním z přístupů je snaha autorů nalézt inspiraci v právních úpravách jiných zbraní. Je tedy možné se například inspirovat Úmluvou o chemických zbraních a uvažovat o vhodnosti aplikace této úpravy na právní regulaci kybernetických zbraní.⁴⁵ Jiní autoři vedle sebe naopak pokládají biologické a kybernetické zbraně, ale již bez toho, aby osvětlili jejich podobu a vzájemný vztah.⁴⁶ Lze se také setkat s polemikou, zda lze kybernetické zbraně označit za zbraně hromadného ničení či nikoli. Přestože J. Carr představuje definici zbraní hromadného ničení, již tak nečiní v případě kybernetických zbraní a klade tak více otázek, než nabízí odpovědi.⁴⁷ Jiný přístup zastává B. B. Hatch, jenž uvádí, že pokud by bylo kybernetickou operací způsobeno „přehřátí jaderné elektrárny, došlo by k otevření přehradní hráze nad obydlenu oblastí či by bylo způsobeno zničení či deaktivace služeb řízení letového provozu s následkem leteckých havárií“⁴⁸,

⁴³ ZHIOUA, Sami. The Middle East under Malware Attack Dissecting Cyber Weapons. In: *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops Proceedings*. USA: IEEE Computer Society Conference Publishing Services. 2013, str. 11.

⁴⁴ WELSH, Thomas. A Cybersecurity Threat Model for the Detection of a Ransomware Cyberweapon in a Networked Computing Environment. In: *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*. 2019, str. 212.

⁴⁵ Srovnej GEERS, Kenneth. Cyber Weapons Convention. *Computer Law & Security Review*. 2010, 26(5), str. 549-550.

⁴⁶ Srovnej KOBLENTZ, Gregory D.; MAZANEC, Brian M. Viral Warfare: The Security Implications of Cyber and Biological Weapons. *Comparative Strategy*. 2013, 32(5), str. 419-421.

⁴⁷ Srovnej CARR, Jeffrey. The misunderstood acronym: Why cyber weapons aren't WMD. *Bulletin of the Atomic Scientists*. 2013, 69(5), str. 33.

tak by byla způsobena škoda takového rozsahu, aby jejího původce bylo možné označit za zbraň hromadného ničení.

Další přístup spočívá v určení limitů, které jsou na kybernetické zbraně kladeny. Může se jednat o limity ekonomické, etické či technologické.

Autoři Mezzour, Carley a Carley se jako jedni z mála zabývají otázkou, kdo stojí za financováním kybernetických zbraní. Ekonomický aspekt se dostává do popředí v případě, kdy je kybernetická zbraň sponzorována státem, pak je její nasazení považováno za „*sofistikovaný, politicky motivovaný kybernetický útok*.“⁴⁹ Ekonomickou stránkou věci lze chápat i připodobnění „*velikosti kybernetické kriminality k obchodování se zbraněmi či drogami*.“⁵⁰ Už ale není zřejmé, zda je třeba kybernetickou kriminalitu a obchod s kybernetickými zbraněmi chápat odděleně či nikoli. Jiní řeší etické meze, které je třeba brát v potaz, pokud by kybernetické zbraně mohly být použity „*k útoku anonymně na dálku a způsobovaly by velký chaos*.“⁵¹ Technickým aspektům se věnují autoři Pavur a Martinovič, již uvažují o možnosti nasazení kybernetických protisatelitních zbraní⁵² či autoři Kim a Eon, již se snaží nastavit parametry, které musí kybernetická zbraň splňovat, aby co nejúčinněji detekovala svůj cíl a zasáhla nejzranitelnější místo cílového systému.⁵³ Naprosto odlišným případem je situace, kdy autor v úvodu deklaruje, že kybernetické kapacity (bez bližšího vysvětlení vztahu kybernetických kapacit a kybernetických zbraní) nejsou

⁴⁸ HATCH, Benjamin B. Defining a Class of Cyber Weapons as WMD: An Examination of the Merits. *Journal of Strategic Security*. 2018, 11(1), str. 47.

⁴⁹ Srovnej MEZZOUR, Ghita; CARLEY, Kathleen M.; CARLEY, L. Richard. Remote assessment of countries' cyber weapon capabilities. *Social Network Analysis and Mining*. 2018, 8(1), str. 3.

⁵⁰ FILSHTINSKIY, Stas. Privacy and security: Cybercrime, Cyberweapons, Cyber Wars: Is There Too Much of It in the Air? *Communications of the ACM*. 2013, 56(6), str. 28.

⁵¹ LIN, Patrick; ALLHOFF, Fritz; ROWE, Neil C. Computing Ethics: War 2.0 Cyberweapons and Ethics. *Communications of the ACM*. 2012, 55(3), str. 24.

⁵² Srovnej PAVUR, James; MARTINOVIC, Ivan. The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space. In: *Conference on Cyber Conflict Proceedings 2019*. Tallinn: CCD COE Publications, 2019, str. 213-230.

⁵³ Srovnej KIM, Ki Hoon; EOM, Jung Ho. Modeling of Cyber Target Selection for Effective Acquisition of Cyber Weapon Systems. *International Journal of Security and Its Applications*. 2016, 10(11), str. 301.

cílem příspěvku⁵⁴ a zaměří se na jejich vlastnosti, kterou mohou vzbuzovat humanitární obavy natolik, aby vedly k zákazu těchto technologií. Je diskutabilní, nakolik je vhodným přístupem zamýšlet se nad limity, jež by mohly být kladeny na technologie, když tyto technologie nejsou řádně popsány.

Závěrem lze uvést několik až překvapivých přístupů. Singer již v úvodu upozorňuje, že „*přesná kvalifikace kybernetického nástroje (...) není pro právní problém, který je v příspěvku diskutován, rozhodující.*“⁵⁵ Dokud tedy představa autorů o kybernetické zbrani spadá do mezí jejich výzkumu, tak nepovažují za důležité se tomuto aspektu věnovat. Zcela okrajovým a značně bizarním přístupem je pak bez dalšího použití termínu kybernetická zbraň pouze v názvu článku.⁵⁶

7. DISKUZE

Výše uvedené přístupy ke kybernetickým zbraním jsou nyní v této kapitole aplikovány na reálné kybernetické incidenty, jejichž fakta byla již popsána ve druhé kapitole. Tento krok poslouží k naplnění druhého cíle tohoto článku, kterým je syntéza těchto přístupů a nalezení slabých míst. Z tohoto důvodu je pozornost věnována identifikaci jednotlivých faktorů, které ve svém souhrnu vedou k fragmentaci názorů nejenom napříč obory, ale i mezi specialisty v jednom konkrétním odvětví. Pro analýzu nebyly použity přístupy všech výše zmíněných autorů, ale pouze těch, jež poskytli definici, kterou bylo možné na kybernetický incident aplikovat. Pokud tedy autor ve své práci žádnou definici neuvedl, nebyl do této analýzy zařazen.

⁵⁴ Srovnej BAER, Merritt. *Toward Criteria for International Cyber Weapons Bans*. In: *2013 World Cyberspace Cooperation Summit IV (WCC4) Proceedings*. IEEE Explore. 2013, str. 1.

⁵⁵ SINGER, Tassilo V. P. *Update to revolving door 2.0: The extension of the period for direct participation in hostilities due to autonomous cyber weapons*. In: *Conference on Cyber Conflict Proceedings 2017*. Tallinn: CCD COE Publications, 2017, str. 125.

⁵⁶ Srovnej KARLSSON, Marcus; LARSSON, Erik G. *Massive MIMO as a cyber-weapon*. In: *2014 48th Asilomar Conference on Signals, Systems and Computers Proceedings*. 2014, str. 661-665. NGUYEN, Nam-Phong; NGO, Hien Quoc; DUONG, Trung Quang; TUAN, Hoang Duong; COSTA, Daniel Benevides da. *Full-Duplex Cyber-Weapon With Massive Arrays*. *IEEE Transactions on Communications*. 2017, 65(12), str. 5544-5558.

Pro analýzu byl zvolen následující postup. Rozhodujícím indikátorem bylo profesní zaměření každého autora. Autoři tak byli rozřazeni do následujících skupin – IT, matematika, policy-making, politologie, právo, filozofie a armáda. Následně byla každá definice aplikována na kybernetický incident a byla položena otázka, zda konkrétní incident byl příkladem nasazení kybernetické zbraně či nikoli. Výstupem této analýzy je tabulka uvedená níže.

	STUXNET	TRANSSIBIŘSKÝ PLYNOVOD	DDOS ÚTOKY V ESTONSKU	SYRSKÝ VZDUŠNÝ OBRANNÝ SYSTÉM	SHAMOON A SAUDI ARAMCO
RAIN OTTIS (IT)	ANO	ANO	ANO	ANO	ANO
PETER MCBURNEY (IT)	ANO	ANO	ANO	ANO	ANO
ENN TYUGU (IT)	ANO	ANO	ANO	ANO	ANO
MAATHUIS A PIETERS (IT)	ANO	ANO	ANO	ANO	ANO
BELLOVIN, LANDAU A LIN (IT)	ANO	ANO	ANO	ANO	ANO
KUSHWAHA, WATSON (IT)	ANO	ANO	ANO	ANO	ANO
YAMIN, KATT A KIANPOUR (IT)	ANO	ANO	NE	ANO	ANO
ZHIOUA (IT)	ANO	ANO	NE	ANO	ANO
SILOMON (IT)	ANO	NE	NE	NE	ANO
MEZZOUR, CARLEY A CARLEY (IT)	NE	NE	NE	ANO	NE
ROWE (IT)	NE	NE	NE	NE	NE
WELSH (IT)	NE	NE	NE	NE	NE
LORENTS (MATEMATIKA)	ANO	ANO	ANO	ANO	ANO
BERG (MATEMATIKA)	ANO	ANO	ANO	ANO	ANO

KALLBERG (POLICY- MAKING)	ANO	ANO	ANO	ANO	ANO
EGGENSCHWILER (POLICY- MAKING)	ANO	NE	NE	NE	ANO
MAITRA (POLICY- MAKING)	NE	NE	NE	NE	NE
RID (POLITOLOGIE)	ANO	ANO	ANO	ANO	ANO
ARIMATSU (PRÁVO)	ANO	NE	NE	NE	ANO
LIN A ALLHOFF (FILOZOFIE)	NE	NE	NE	NE	NE
HATCH (ARMÁDA)	NE	NE	NE	NE	NE

Již na první pohled je zřejmé, že dosažení shody ohledně přístupu ke kybernetickým zbraním je obtížné nejenom napříč všemi profesemi, ale i v rámci konkrétního odvětví.

Mezi autory pocházejícími z IT prostředí bylo možné nalézt shodu pouze v případě, kdy používali pro kybernetickou zbraň obecný termín počítačový kód a zaměřili svoji pozornost na účinek spočívající ve schopnosti kybernetické zbraně vyvolat poškození určité struktury. V tomto případě jsou pak všechny incidenty příkladem kybernetické zbraně. Situace již ale není jednoznačná v případě, kdy autoři používají specifitější termíny. Příkladem jsou autoři Yamin, Katt a Kianpour a taktéž Zhioua, již za kybernetickou zbraň označují určitý software. V tomto případě nelze za kybernetickou zbraň označit DDoS útoky v Estonsku. Silomon se přiklonila ke specifitějšímu termínu malware, který okruh možných kybernetických zbraní dále zúžil, neboť malware byl použit pouze v případě Stuxnetu a Shamoon proti Saudi Aramco. K větší specifikaci přistoupil Welsh, jenž se zaměřil pouze na ransomware, který nebyl nasazen v žádném z incidentů. Někteří autoři do svých úvah zahrnuly i prvky netechnického charakteru.

Autoři Mezzour, Carley a Carley nevědomky poukazují na problém přičitatelnosti, neboť svoji pozornost zaměřili na státem sponzorovanou kybernetickou zbraň. V tomto případě by bylo možné za kybernetickou zbraň označit pouze útok na syrský vzdušný obranný systém. Rowe se zaměřil na schopnost způsobení velkého chaosu, který ovšem nebyl dosažen ani v jednom z incidentů.

Absolutní shody bylo dosaženo mezi matematiky, již se zaměřili na faktor vyvolání určitého poškození systému a za použití kybernetické zbraně tak lze označit všechny incidenty. V neprospěch ale hovoří minimální vzorek.

Výraznější rozkol lze sledovat mezi autory zabývající se policy-making. Zatímco Kallberg se při popisu kybernetické zbraně přiklonil k obecnějšímu termínu technika, Eggenschwiller zvolila konkrétnější termín malware. Maitra se naopak zaměřil na konkrétnost účinku, který spatřoval v zapříčinění zranění či úmrtí osob.

Zbývající obory politologie, právo, filozofie a armáda měly každý pouze jednoho představitele, možnost nějakých zobecnitelných závěrů je tedy značně omezená. Politolog Rid se přiklonil k široce pojatému účinku spočívajícím v poškození struktury, proto jsou příkladem kybernetických zbraní všechny incidenty. Na účinek v úzkém pojetí se zaměřili filozofové Lin a Allhoff a představitel armádního prostředí Hatch. Naopak Arimatsu při právní analýze pracovala s termínem malware.

Závěrem této analýzy lze vyvodit dva základní faktory vedoucí k názorové fragmentaci napříč či v rámci jednotlivých oblastí. Prvním z nich je obecnost či naopak konkrétnost technického parametru, kdy lze vyvodit závěr, že s větší mírou konkrétnosti se zmenšuje pravděpodobnost označit kybernetický incident za příklad nasazení kybernetické zbraně. Za nejobecnější termín vyvolávající nejmenší rozpory lze označit spojení počítačový kód, konkrétnější je poté termín software a následně malware. Pokud je tedy v diskuzi použit obecný termín počítačový kód, dovoluje tento termín označit incident za kybernetickou zbraň s větší pravděpodobností, než pokud je použit termín software či malware.

Druhý faktor je zaměřen na konkrétnost samotného účinku. Opětovně lze dovodit stejný závěr, že čím konkrétněji je uchopen účinek, tím méně pravděpodobné je, že bude původce kybernetického incidentu označen za kybernetickou zbraň. Příklad lze najít v obecném termínu poškození, nebo naopak v konkrétním účinku chaosu nebo zranění či úmrtí osob.

8. ZÁVĚR

Tento článek si vytyčil dva hlavní cíle. Prvním cílem bylo poskytnout ucelený přehled přístupů k definici pojmu kybernetická zbraň. Za tímto účelem byla zmapována odborná literatura (resp. odborné články a příspěvky z konferencí), které byly v letech 2010-2019 zařazeny v databázích DBLP Computer Science Bibliography Website, Scopus a Web of Science. V rámci druhého cíle došlo k aplikaci jednotlivých definic na reálné kybernetické incidenty a též došlo k identifikaci dvou hlavních faktorů způsobujících názorovou odlišnost.

První kapitola byla věnována metodě sběru a zpracování dat, kdy bylo vysvětleno, jakými kroky bylo docíleno stavu, kdy z původního počtu 124 výstupů bylo v tomto výzkumu pracováno s pouhými 34 výstupy. Přestože se při zběžném seznámení s touto problematikou může zdát, že relevantní literatury je dostatek, tento výzkum prokázal opak. Dosavadní výzkumy neposkytují odpovědi na všechny otázky a některým otázkám se autoři cíleně vyhýbají.

Druhá kapitola se věnovala kybernetickým incidentům a otázce, zda je jejich spouštěč kybernetickou zbraní či nikoli. Nejčastěji zmiňovaným incidentem byl počítačový červ Stuxnet, jehož cílem bylo uranové obohacovací středisko v Íránu. Jakkoli se na první pohled může zdát tento přístup nápomocný, skrývá v sobě jedno zásadní riziko. Pokud nebude zřetelně vyjasněn vztah mezi kybernetickou zbraní a konkrétním kybernetickým incidentem, může docházet bez dalšího k označení kybernetického incidentu za případ nasazení kybernetické zbraně bez ohledu na to, zda bylo naplněno například zmíněné kritérium úmyslu.

Třetí kapitola se zaměřila na autory, kteří ve svých dílech pracují s přímou definicí kybernetické zbraně. Často zmiňovaným prvkem byl

úmysl, se kterým je zbraň konstruována a následně i nasazena. Proto lze za kybernetickou zbraň označit takový kybernetický nástroj, který má útočné schopnosti a je schopen způsobit újmu nejenom jinému kybernetickému nástroji, ale též živým bytostem. Dalším častěji zmiňovaným kritériem pak byl určitý stupeň technologické dokonalosti kybernetické zbraně, který je definován jejím potenciálem dosáhnout stanoveného cíle. S postupujícím časem reagovali autoři na situaci, kdy státy nebo mezinárodní organizace představily své vlastní definice. Přejata tak byla například definice Spojených států amerických či NATO CCD COE.

Čtvrtá kapitola se zaměřila na příklady různých typů kybernetických nástrojů, které autoři výjimečně přímo, ale ve většině případů nepřímo označili za kybernetickou zbraň. Tento přístup v sobě skrýval dvě hlavní úskalí. Prvním z nich byl nevyjasněný vztah mezi pojmy malware a kybernetická zbraň. Druhým problémem byly odkazy na různé druhy malware, a to opětovně bez bližšího vysvětlení vzájemného vztahu. Především tito autoři nereflektovali například prvek úmyslu, který by ovlivnil to, zda je některý malware možné označit za kybernetickou zbraň.

Pátá kapitola pak reflektovala zbývající přístupy, které nebylo možné zařadit do předchozích kapitol. Autoři se tak kupříkladu uchylují k úvahám, zda lze najít možnou inspiraci pro právní regulaci kybernetických zbraní v právní úpravě chemických či biologických zbraní, nebo zbraní hromadného ničení. K těmto úvahám dochází opětovně bez vysvětlení, co je považováno za kybernetickou zbraň. Jiní autoři se zaměřili na představení ekonomických, etických či technologických limitů, které jsou na kybernetické zbraně kladeny.

V rámci poslední kapitoly došlo k aplikaci jednotlivých přístupů na reálné kybernetické incidenty. Tato analýza posloužila k identifikaci dvou hlavních faktorů vedoucích k názorové odlišnosti. První z nich spočívá v technickém parametru, kdy lze shrnout, že s větší mírou konkrétnosti technického parametru se zmenšuje pravděpodobnost označit kybernetický incident za příklad nasazení kybernetické zbraně. Druhý faktor se týká účinku, kdy lze dovodit, že čím konkrétnější účinek, tím méně

pravděpodobné je, že bude původce kybernetického incidentu označen za kybernetickou zbraň.

Závěrem lze uvést, že zkoumaná problematika kybernetických zbraní není vyčerpaným tématem a představuje pouze první krok v obsáhlé analýze možných dopadů jejich nasazení. Při konkrétním zkoumání přístupů k definici by bylo vhodné věnovat pozornost nejenom odborné literatuře, ale též stanoviskům států.

9. SEZNAM LITERATURY

- [1] ARIMATSU, Louise. A treaty for governing cyber-weapons: Potential benefits and practical limitations. In: *Conference on Cyber Conflict Proceedings 2012*. Tallinn: CCD COE Publications, 2012, str. 91-109. ISBN 978-9949-9040-9-9.
- [2] BAER, Merritt. Toward Criteria for International Cyber Weapons Bans. In: *2013 World Cyberspace Cooperation Summit IV (WCC4) Proceedings*. IEEE Explore. 2013, str. 1-3.
- [3] BARZASZKA, Ivanka. Are cyber-weapons effective? *The RUSI Journal*. 2013, 158(2), str. 48-56.
- [4] BELLOVIN, Steven M.; LANDAU, Susan; LIN, Herbert S. Limiting the undesired impact of cyber weapons: technical requirements and policy implications. *Journal of Cybersecurity*. 2017, 3(1), str. 59-68.
- [5] CARR, Jeffrey. The misunderstood acronym: Why cyber weapons aren't WMD. *Bulletin of the Atomic Scientists*. 2013, 69(5), str. 32-37.
- [6] EGGENSCHWILLER, Jacqueline; SILOMON, Jantje. Challenges and opportunities in cyber weapon norm construction. *Computer Fraud & Security*. 2018, 12, str. 11-18.
- [7] FILSHTINSKIY, Stas. Privacy and security: Cybercrime, Cyberweapons, Cyber Wars: Is There Too Much of It in the Air? *Communications of the ACM*. 2013, 56(6), 28-30.
- [8] GEERS, Kenneth. Cyber Weapons Convention. *Computer Law & Security Review*. 2010, 26(5), str. 547-551.
- [9] HAMBLING, David. Hints of a new cyberweapon: GPS spoofing may have thrown vessels off course in the Black Sea. *New Scientist*. 2017, 235(3139), str. 6.
- [10] HARE, Forrest B. Precision cyber weapon systems: An important component of a responsible national security strategy? *Contemporary Security Policy*. 2019, 40(2), str. 193-213.
- [11] HATCH, Benjamin B. Defining a Class of Cyber Weapons as WMD: An Examination of the Merits. *Journal of Strategic Security*. 2018, 11(1), str. 43-61.
- [12] KALLBERG, Jan. The Second Amendment and Cyber Weapons: Constitutional Relevance of Digital Gun Rights. *IEEE Technology and Society Magazine*. 2019, 38(2), str. 71-77.

- [13] KARLSSON, Marcus; LARSSON, Erik G. Massive MIMO as a cyber-weapon. In: *2014 48th Asilomar Conference on Signals, Systems and Computers Proceedings*. 2014, str. 661-665. ISBN 978-1-4799-8297-4.
- [14] KIM, Ki Hoon; EOM, Jung Ho. Modeling of Cyber Target Selection for Effective Acquisition of Cyber Weapon Systems. *International Journal of Security and Its Applications*. 2016, 10(11), str. 293-302.
- [15] KIRAVUO, Timo; SÄRELÄ, Mikko; MANNER, Jukka. Weapons against Cyber-Physical Targets. In: *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops Proceedings*. USA: IEEE Computer Society Conference Publishing Services. 2013, str. 321-326. ISBN 978-0-7685-5023-7.
- [16] KOBLENTZ, Gregory D.; MAZANEC, Brian M. Viral Warfare: The Security Implications of Cyber and Biological Weapons. *Comparative Strategy*. 2013, 32(5), str. 418-434.
- [17] KUSHWAHA, Neal; WATSON, Bruce William. Cyber weapons and the U.S. In: *Proceedings of the 17th European Conference on Cyber Warfare and Security*. 2018, str. 1-11. ISBN: 978-1-911218-85-2.
- [18] LANGER, Ralph. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security Privacy*. 2011, 9(3), str. 49-51.
- [19] LANGER, Ralph. To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve. [online]. 2013 [cit. 25. 10. 2019]. Dostupné z: <https://www.langner.com/wp-content/uploads/2017/04/To-kill-a-centrifuge.pdf>.
- [20] LIN, Patrick; ALLHOFF, Fritz; ROWE, Neil C. Computing Ethics: War 2.0 Cyberweapons and Ethics. *Communications of the ACM*. 2012, 55(3), str. 24-26.
- [21] LORENTS, Peeter; OTTIS, Rain. Knowledge based framework for cyber weapons and conflict. In: *Conference on Cyber Conflict Proceedings 2010*. Tallinn: CCD COE Publications, 2010, str. 129-142. ISBN: 978-9949-9040-1-3.
- [22] MAITRA, Amit K. Offensive cyber-weapons: technical, legal, and strategic aspects. *Environment Systems and Decisions*. 2015, 35(1), str. 169-182.
- [23] MATHIUS, Clara; PIETERS, Wolter; BERG, Jan van den. Cyber weapons: a profiling framework. In: *2016 IEEE International Conference on Cyber Conflict (CyCon U.S.) Proceedings*. USA: IEEE eXpress Conference Publishing. 2016, str. 94-101. ISBN 978-1-5090-5258-5.
- [24] MEZZOUR, Ghita; CARLEY, Kathleen M.; CARLEY, L. Richard. Remote assessment of countries' cyber weapon capabilities. *Social Network Analysis and Mining*. 2018, 8(1), str. 1-15.
- [25] NGUYEN, Nam-Phong; NGO, Hien Quoc; DUONG, Trung Quang; TUAN, Hoang Duong; COSTA, Daniel Benevides da. Full-Duplex Cyber-Weapon With Massive Arrays. *IEEE Transactions on Communications*. 2017, 65(12), str. 5544-5558.
- [26] PAVUR, James; MARTINOVIC, Ivan. The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space. In: *Conference on Cyber Conflict Proceedings 2019*. Tallinn: CCD COE Publications, 2019, str. 213-230. ISBN 978-9949-9904-5-0.

- [27] PETERSON, Dale. Offensive Cyber Weapons: Construction, Development, and Employment. *Journal of Strategic Studies*. 2013, 36(1), str. 120-124.
- [28] RAYMOND, David; CONTI, Gregory J.; CROSS, Tom; FANELLI, Robert. A control measure framework to limit collateral damage and propagation of cyber weapons. In: *Conference on Cyber Conflict Proceedings 2013*. Tallinn: CCD COE Publications, 2013, str. 181-196. ISBN 978-9949-9211-5-7.
- [29] RID, Thomas; McBURNEY, Peter. Cyber-Weapons. *The RUSI Journal*. 2012, 157(1), str. 613.
- [30] SINGER, Tassilo V. P. Update to revolving door 2.0: The extension of the period for direct participation in hostilities due to autonomous cyber weapons. In: *Conference on Cyber Conflict Proceedings 2017*. Tallinn: CCD COE Publications, 2017, str. 121-133. ISBN 978-9949-9904-1-2.
- [31] TYUGU, Enn. Command and control of cyber weapons. In: *Conference on Cyber Conflict Proceedings 2012*. Tallinn: CCD COE Publications, 2012, str. 333-343. ISBN 978-9949-9040-9-9.
- [32] TYUGU, Enn. Situation awareness and control errors of cyber weapons. In: *IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*. 2013, str. 143-148. ISBN 9781467324366.
- [33] WELSH, Thomas. A Cybersecurity Threat Model for the Detection of a Ransomware Cyberweapon in a Networked Computing Environment. In: *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*. 2019, str. 212. ISBN 9781538670026.
- [34] YAMIN, Muhammad Mudassar; KATT, Basel; KIANPOUR, Mazaher. Cyber Weapons Storage Mechanisms. In: *Security, Privacy, and Anonymity in Computation, Communication, and Storage*. 2019, str. 354-367. ISBN 9783030249076.
- [35] ZHIOUA, Sami. The Middle East under Malware Attack Dissecting Cyber Weapons. In: *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops Proceedings*. USA: IEEE Computer Society Conference Publishing Services. 2013, str. 11-16. ISBN 978-0-7685-5023-7.
- [36] Staged cyber attack reveals vulnerability in power grid. Dostupné z: <https://www.youtube.com/watch?v=fJyWngDco3g> [vid. 5. února 2020]

Toto dílo lze užít v souladu s licenčními podmínkami Creative Commons BY-SA 4.0 International (<http://creativecommons.org/licenses/by-sa/4.0/legalcode>).
