466—477

Kybernetická zbraň a právo: kybernetické útoky proti nemocnicím

Jakub Vostoupal* – Ivana Kudláčková**

Abstrakt: **V daném článku se autoři věnují potenciálnímu významu a normativnímu uchopení pojmu kybernetická zbraň, který byl použit ve veřejném prostoru v kontextu kybernetického útoku na Nemocnici Rudolfa a Stefanie v Benešově. V tomto ohledu analyzují detaily daného kybernetického incidentu za účelem identifikace konstitučních prvků kybernetické zbraně a možnosti následné subsumpce a aplikace daného pojmu v českém právním prostředí. V rámci právní analýzy, ve které se pokoušejí vyrovnat se situací, kdy český právní systém daný pojem nejen nezná, ale ani s ním nepočítá a ve velké části případů neumožňuje aplikaci ani prostřednictvím extenzivního výkladu, se nakonec zaměřují na problematiku trestního práva jakožto nejrelevantnějšího odvětví pro danou problematiku. V tomto prostředí pak hodnotí, zda je trestněprávní zohlednění pokročilých malwarů žádoucí, a nabízejí několik směrů, ve kterých je možné o dané subsumpci a aplikaci uvažovat, přičemž se především zaměřují na problematiku kvalifikačního rozšíření a regulatorního dotvoření kvalifikované skutkové podstaty neoprávněného přístupu k počítačovému systému a na možnosti, které nabízí právní úprava přitěžujících okolností. Celé pojednání uzavírají vyhodnocením a doporučením pro další vývoj.**

Klíčová slova: **kybernetická zbraň, zbraň, benešovský kybernetický incident, trestní právo, kyberkriminalita**

Úvod

Na konci roku 2019 došlo ke kybernetickému útoku, který tvrdě zasáhl systémy Nemocnice Rudolfa a Stefanie v Benešově (dále též jako „nemocnice Benešov“ nebo „benešovská nemocnice“), přičemž danou nemocnici vyřadil na bezmála tři týdny z normálního provozu a škody byly vyčísleny na více než 50 milionů korun.[1] Když se tehdejší premiér Andrej Babiš setkal v únoru 2020 se svým estonským protějškem Jürim Ratasem, prohlásil mimo jiné následující:

> *„Kybernetická bezpečnost je pro nás velké téma. Kybernetické zbraně jsou dnes mnohem nebezpečnější než zbraně konvenční. Například to, co se stalo v benešovské nemocnici. Nemůže se nám stát, aby byla nemocnice mimo provoz. Je to pro nás velké ponaučení.“*[2]

Toto konkrétní prohlášení potvrdilo důležitost způsobu používání termínů politickými představiteli ve veřejném prostoru, a to zvláště pokud mají dané pojmy určité právní

* Mgr. Jakub Vostoupal, Ústav práva a technologií, Právnická fakulta Masarykovy univerzity. E-mail: jakub.vostoupal@law.muni.cz. ORCID: https://orcid.org/0000-0002-1669-9931. 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). Autoři děkují anonymním recenzentům za cennou zpětnou vazbu.

** Ivana Kudláčková, Ústav práva a technologií, Právnická fakulta Masarykovy univerzity. E-mail: 420533@mail.muni.cz. 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).

1 NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019*. 2020. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/.

2 Vláda ČR. Premiér Babiš jednal v Estonsku o spolupráci v oblasti kyberbezpečnosti či digitalizace. In: *Vláda České republiky* [online]. 18. 2. 2020 [cit. 2023-02-04]. Dostupné z: https://www.vlada.cz/cz/media-centrum/aktualne/premier-babis-jednal-v-estonsku-o-spolupraci-v-oblasti-kyberbezpecnosti-ci-digitalizace-179679/tmplid-47/.

konotace. Problém pak přichází především ve chvíli, kdy se pojmosloví nedodržuje a pojmy se objevují ve veřejném prostoru bez uvážení či ohledu na fakt, že doposud nebyl vyjasněn jejich význam, s čímž se bohužel často lze setkat u pojmů souvisejících s kyberprostorem a IT tematikou obecně. Takový přístup pak do jednání, aplikace práva, mediálních reportů i diplomatických vztahů vnáší nejistotu ohledně významu daného termínu a toho, co jeho použitím autor zamýšlel a jaké implikace z toho plynou.

V současném rapidně se proměňujícím světě čelí společnost širokému spektru dopadů moderních technologií, které ve svém souhrnu společnost nejenom rozvíjí, ale představují pro ni i možné hrozby. Své specifické dopady to má i v oblasti právní regulace. S ohledem na vývoj na poli technologického pokroku a s tím související proměny bezpečnostních hrozeb je z důvodu zachování vysokého standardu ochrany společnosti nezbytné rozšířit a přizpůsobit stávající výklad právních norem tak, aby právě dopady těchto změn byly dostatečně reflektovány právním řádem. Pokud není jasné, co daný pojem (tedy kybernetická zbraň) znamená a ve kterých oblastech se uplatní, zásadně to ztěžuje nejen regulaci daného fenoménu, ale také aplikaci potenciálně relevantních právních norem, jejich vymáhání a zajišťování efektivního naplňování politiky, která se dané tematiky týká. Pokud daný pojem nemá jasné ukotvení a společnost tak pouze podvědomě tuší, co daný pojem znamená, právo oslabuje svoji regulatorní roli. Filipec a Plášil v této souvislosti upozorňují na tzv. *efekt černé labutě*.[3]

Nabízí se tak nepříliš překvapivé otázky. Pokud při kybernetickém útoku na benešovskou nemocnici došlo k použití kybernetické zbraně, co to přesně znamená? Jaké následky s použitím kybernetických zbraní právo spojuje a zná vůbec právo pojem kybernetická zbraň?

Cílem tohoto příspěvku je analyzovat pojem kybernetická zbraň v kontextu kybernetického útoku na benešovskou nemocnici a zasadit tento pojem do systému již existující právní regulace. Autoři představí možné konstituční znaky kybernetické zbraně a s nimi spojené právní dopady. Vzhledem k tomu, že pojem kybernetická zbraň již byl podroben analýze z pohledu mezinárodního práva,[4] bude následující příspěvek věnován české právní úpravě.

1. Benešovský kybernetický incident

Abychom mohli odpovědět na výše položené otázky, představíme nejdříve relevantní fakta benešovského kybernetického incidentu.[5] Benešovská nemocnice je spádovou nemocnicí pro přibližně 120 000 lidí, v letních měsících se ovšem toto číslo může vyšplhat až na 400 000, neboť se jedná o vyhledávanou rekreační oblast.[6] Jedná se tak o nemocnici, jejíž dopad na poskytování zdravotnických služeb je bez pochyb nezanedbatelný, nejednalo se ovšem o povinný subjekt ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti

3 FILIPEC, O. – PLÁŠIL, D. Poučení z případu benešovské nemocnice napadené ransomwarem Ryuk. *Obrana a strategie (Defence and Strategy)*. 2021, č. 1, s. 32.

4 Např. KUDLÁČKOVÁ, I. – WALLACE, D. – HARAŠTA, J. *Cyber Weapons Review in Situations Below the Threshold of Armed Conflict*. Estonia, Tallinn: NATO CCDCOE Publications, 2020. Dostupné z: https://ieeexplore.ieee.org/document/9131728/.

5 Pro detailnější pojednání o daném útoku viz FILIPEC, O. – PLÁŠIL, D. *Poučení z případu benešovské nemocnice napadené ransomwarem Ryuk*.

6 Ibidem, s. 37; NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019*, s. 18.

a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti"). I tato nemocnice pak byla z pohledu kybernetické bezpečnosti sužována obdobnými problémy jako většina českého zdravotnictví, zejména tedy nedostatkem odborníků a podfinancováním.[7] Filipec a Plášil ovšem upozorňují, že ani tak nebylo zabezpečení nemocnice v katastrofálním stavu a navzdory některým mediálním reportům byla nemocnice v ohledu investic do IT bezpečnosti a IT infrastruktury na srovnatelné úrovni s dalšími českými nemocnicemi.[8]

Incident začal v říjnu 2019, kdy se nemocnice stala cílem phishingové kampaně, která provázela zvýšenou aktivitu botnetu *Emotet*.[9] Rozesílané e-maily byly obecně na vysoké úrovni[10] a obsahovaly infikované přílohy (pravděpodobně se jednalo o falešnou fakturu), po jejichž otevření a spuštění maker byl počítač infikován malwarem *Emotet*.[11] Ten byl původně vytvořen a používán jako bankovní trojský kůň, nyní však slouží primárně jako vstupní brána pro navazující infekci.[12] *Emotet* posléze překonal dva aktualizované antivirové systémy (Windows Defender a ESET) a firewall, pronikl do sítě a všechny systémy včetně zálohového serveru zmapoval.[13] Prostřednictvím cloudu pak navázal kontakt s útočníkem a stáhnul do sítě spyware *TrickBot*,[14] který mapoval citlivé (např. přihlašovací) údaje uživatelů, s preferencí přihlašovacích údajů správců sítě, které mohou útočníkovi poskytnout nejvyšší oprávnění.[15] Jak upozorňuje NÚKIB v již citované analýze, *„pro běžného uživatele je v případě nákazy Trickbotem obtížné vypozorovat nezvyklé chování počítače […]"*[16] a anomální chování bude zaznamenáno až správcem sítě v momentě, kdy virus kontaktuje C&C server při exfiltrování dat, k čemuž může dojít i několik měsíců po infekci.[17]

Poté, co *TrickBot* hesla objevil, zlomil a získal administrátorská oprávnění, inicioval poslední krok řetězce útoku – ransomware *Ryuk*.[18] Ten může často sloužit nejen jako prostředek pro získání peněz, ale logicky také pro zametení stop, které mohl útočník ponechat v síti. Dne 11. prosince 2019 ve 2:50 tento ransomware zašifroval data na *„serverech, nemocničních přístrojích a pracovních stanicích"*,[19] přičemž prolomení zašifrování nebylo reálné.[20]

---

7 NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019*, s. 18.

8 FILIPEC, O. – PLÁŠIL, D. *Poučení z případu benešovské nemocnice napadené ransomwarem Ryuk*, s. 37–39.

9 Mitre. Emotet. In: *Mitre Attack* [online]. 2023 [cit. 2023-04-25]. Dostupné z: https://attack.mitre.org/software/S0367/; NÚKIB. *Analýza hrozby: Vyděračské útoky ransomwarem jsou cílenější: Míří na velké firmy, státní a veřejné instituce*. 2020. Dostupné z: https://www.nukib.cz/download/publikace/analyzy/Analyza_hrozby_ransomware.pdf.

10 KUČÍNSKÝ, A. – SIKORA, V. Malware Emotet – Trickbot – Ryuk v benešovské nemocnici. *Data Security Management*. 2020, č. 1, s. 39–41.

11 NÚKIB. *Analýza hrozby: Vyděračské útoky ransomwarem jsou cílenější: Míří na velké firmy, státní a veřejné instituce*.

12 Ibidem.

13 FILIPEC, O. – PLÁŠIL, D. *Poučení z případu benešovské nemocnice napadené ransomwarem Ryuk*, s. 39.

14 Mitre. TrickBot. In: *Mitre Attack* [online]. 2023 [cit. 2023-04-25]. Dostupné z: https://attack.mitre.org/software/S0266/.

15 SHABU, M. Ukliknutí ‚stálo' nemocnici v Benešově 40 milionů. Kyberútok začal otevřením přílohy. In: *Lidovky.cz* [online]. 2020 [cit. 2023-04-25]. Dostupné z: https://www.lidovky.cz/domov/ukliknuti-stalo-nemocnici-v-benesove-40-milionu-kyberutok-zacal-kliknutim-na-prilohu.A200115_201359_ln_domov_vlh.

16 NÚKIB. *Analýza hrozby: Vyděračské útoky ransomwarem jsou cílenější: Míří na velké firmy, státní a veřejné instituce*.

17 Ibidem.

18 Mitre. Ryuk. In: *Mitre Attack* [online]. 2023 [cit. 2023-04-25]. Dostupné z: https://attack.mitre.org/software/S0446/; SHABU, M. *Ukliknutí ‚stálo' nemocnici v Benešově 40 milionů. Kyberútok začal otevřením přílohy*.

19 NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019*, s. 18.

20 FILIPEC, O. – PLÁŠIL, D. *Poučení z případu benešovské nemocnice napadené ransomwarem Ryuk*, s. 41; NÚKIB. *Analýza hrozby: Vyděračské útoky ransomwarem jsou cílenější: Míří na velké firmy, státní a veřejné instituce*.

Fakticky tak ransomware vyřadil nemocnici z provozu, nebylo možné provádět ani standardní ošetření, nebylo možné přijímat nové pacienty a stávající museli být převezeni, a to navzdory tomu, že odpojení zařízení, přizvání analytiků i incident response týmů a další reakce přišly poměrně rychle.[21] Právě díky této rychlé a kompetentní reakci nedošlo ke ztrátám na životech a následky byly „toliko" majetkové povahy. I tak se ovšem vyčíslení škod vyšplhalo přes 59 milionů korun.[22]

Dle našich vědomostí byl kybernetický útok v Benešově jediným, který byl takto veřejně označen za použití kybernetické zbraně. V českém mediálním prostoru ovšem rezonovaly i kybernetické útoky uskutečněné vůči Fakultní nemocnici Brno, kde též došlo k zašifrování systémů ransomwarem, obdobně byla ochromena i psychiatrická nemocnice v Kosmonosech.[23] Tyto další útoky ovšem nebyly veřejně pojmenovány jako případy použití kybernetické zbraně. Přestože jeden takový incident nemůže být bez dalšího vnímán jako reprezentativní vzorek pro navazující právní analýzu, jedná se v tomto případě o odrazový můstek, který napomůže k rozklíčování pojmu kybernetická zbraň v českém právním řádu.

2. Základní normativní východiska použití zbraní

V tomto příspěvku přistupujeme k pojmu kybernetická zbraň jako k podmnožině obecného termínu zbraň, a to primárně z důvodu relativní novosti tohoto pojmu, kdy na tento pojem právo doposud ve všech relevantních odvětvích nereagovalo. V rozboru se zaměřujeme na takové možnosti výkladu pojmu zbraň, které by byly aplikovatelné na benešovský kybernetický incident.

Pokud nahlížíme na oblast zbraní a jejich případného použití či nasazení optikou právní regulace, je nezbytné oddělit právní úpravu národní (zde je tím myšlena specifická právní úprava jednotlivých států) a právní úpravu mezinárodní (zde se jedná především o právní normy mezinárodního práva veřejného). Oba tyto přístupy totiž sledují jiný účel.

V případě mezinárodního práva veřejného, respektive konkrétněji mezinárodního humanitárního práva, je použití zbraní zasazeno do kontextu vedení ozbrojeného konfliktu a dodržování jeho základních principů,[24] neboť se vždy musí jednat o použití zbraní legitimní a legální. Jedním z příkladů pravidel dopadajících na tuto problematiku je článek 36[25] Dodatkového protokolu I k Ženevským úmluvám z 12. srpna 1949 o ochraně

21 SHABU, M. *Ukliknutí ‚stálo' nemocnici v Benešově 40 milionů. Kyberútok začal otevřením přílohy*; FILIPEC, O. – PLÁŠIL, D. *Poučení z případu benešovské nemocnice napadené ransomwarem Ryuk*, s. 40–41.

22 Policie České republiky. Středočeští kriminalisté ukončili vyšetřování Ransomware útoku na benešovskou nemocnici. In: *Policie České republiky – KŘP Středočeského kraje* [online]. 18. 8. 2020 [cit. 2023-03-10]. Dostupné z: https://www.policie.cz/clanek/stredocesti-kriminaliste-ukoncili-vysetrovani-ransomware-utoku-na-benesovskou-nemocnici.aspx.

23 NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020*. 2021. Dostupné z: https://nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf.

24 SAUL, B. – AKANDE, D. (eds). *The Oxford Guide to International Humanitarian Law*. Oxford, United Kingdom: Oxford University Press, 2020, s. 261–276.

25 Článek 36 – Nové druhy zbraní.
„Při studiu, vývoji, získávání nebo zavádění nových druhů zbraní, prostředků nebo způsobů vedení války je Vysoká smluvní strana povinna určit, zda jejich použití není za některých nebo za všech okolností zakázáno tímto Protokolem nebo jinou normou mezinárodního práva aplikovatelnou na tuto Vysokou smluvní stranu."

obětí mezinárodních ozbrojených konfliktů a konfliktů nemajících mezinárodní charakter, přijatého v Ženevě dne 8. června 1977.[26] Tato mezinárodní úprava by dopadala i na kybernetické zbraně.[27]

Mezinárodní právo veřejné by zároveň hrálo nezastupitelnou roli v případě, kdy by došlo k použití zbraně vůči České republice v situaci, která by byla klasifikována jako ozbrojený konflikt mezinárodní povahy či jako konflikt takovou povahu nenaplňující. Břemeno závazku vyplývajícího z mezinárodního práva veřejného by v tomto případě bylo na všech stranách případného konfliktu. Česká republika by tak byla povinna při nasazení zbraní dbát dodržování odpovídajících pravidel, zároveň by mohla zcela legitimně požadovat dodržování téhož od ostatních stran zapojených do konfliktu.

Při přesunu do národní právní úpravy, které se v tomto článku věnujeme, jsme na základě analýzy výskytu pojmů kybernetická zbraň a zbraň v právním řádu ČR museli uzavřít, že první zmíněný pojem je pro národní regulaci pojmem neznámým. Oproti tomu problematika dotýkající se pojmu zbraň je, poněkud překvapivě, mnohem širší než v kontextu mezinárodního práva veřejného. Zbraň zde totiž není tolik limitována kontextem, kdy dojde k jejímu použití, ale východiskem je spíše hodnota, jež je použitím zbraně ohrožena. Pojem zbraně se pak dotýká zejména oblastí trestního či správního práva, kde cílem této regulace je zpravidla zvýšení bezpečnosti společnosti. Toho je dosaženo prostřednictvím široké hmotněprávní a procesněprávní úpravy regulující použití a nakládání se zbraněmi, střelivem, municí a bezpečnostním materiálem a do její realizace je zapojeno několik institucí – Ministerstvo vnitra, Český úřad pro zkoušení zbraní a střeliva, Licenční správa Ministerstva průmyslu a obchodu nebo Český báňský úřad.[28]

Navzdory právě zmíněné šíři právní úpravy zbraní se ovšem značná část na námi zkoumanou materii vztahovat vůbec nebude, například zákon o zbraních[29] ani zákony s ním související, neboť s pojmem kybernetická zbraň, respektive se specifiky s tímto spojenými, jednoduše nepočítají a jejich ustanovení není možné na danou situaci vztáhnout ani extenzivním výkladem. Klíčovým právním předpisem, který daný pojem obsahuje a zároveň umožňuje dostatečně extenzivní výklad, abychom pod něj mohli podřadit i pojem kybernetická zbraň v kontextu benešovského kybernetického incidentu, je pak pouze zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (dále jen „trestní zákoník“).

Sdělení č. 168/1991 Sb., sdělení federálního ministerstva zahraničních věcí o vázanosti České a Slovenské Federativní Republiky Dodatkovými protokoly I a II k Ženevským úmluvám z 12. srpna 1949 o ochraně obětí mezinárodních ozbrojených konfliktů a konfliktů nemajících mezinárodní charakter, přijatých v Ženevě dne 8. června 1977. In: *Zákony pro lidi* [online]. 2023. Dostupné z: https://www.zakonyprolidi.cz/cs/1991-168.

26 International Committee of the Red Cross. A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977. *International Review of the Red Cross*. 2006, č. 864.

27 KUDLÁČKOVÁ, I. – WALLACE, D. – HARAŠTA, J. *Cyber Weapons Review in Situations Below the Threshold of Armed Conflict*.

28 Ministerstvo vnitra České republiky. Právní úprava na úseku zbraní, střeliva, munice, nakládání s bezpečnostním materiálem a další související právní předpisy. In: *Ministerstvo vnitra České republiky* [online]. 2023 [cit. 2023-05-23]. Dostupné z: https://www.mvcr.cz/clanek/pravni-uprava-na-useku-zbrani-a-streliva.aspx.

29 Zákon č. 119/2002 Sb., o střelných zbraních a střelivu a o změně zákona č. 156/2000 Sb., o ověřování střelných zbraní, střeliva a pyrotechnických předmětů a o změně zákona č. 288/1995 Sb., o střelných zbraních a střelivu (zákon o střelných zbraních), ve znění zákona č. 13/1998 Sb., a zákona č. 368/1992 Sb., o správních poplatcích, ve znění pozdějších předpisů, a zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů.

3. Kybernetická zbraň pohledem trestního práva

3.1 Právní kvalifikace benešovského kybernetického incidentu

Na první pohled by se mohlo zdát, že na hledání normativního významu pojmu kybernetické zbraně je zájem čiře akademický a tradiční přístup ke kybernetickým trestným činům nabízí v případě benešovského kybernetického incidentu dostatečné záruky ochrany dotčených zájmů. Jak již bylo zmíněno v první kapitole, během kybernetického útoku na benešovskou nemocnici došlo k zašifrování dat ransomwarem na *„serverech, nemocničních přístrojích a pracovních stanicích"*.[30] Ransomware zde chápeme jako jeden z možných druhů malwaru, což je *„nejobecnější označení pro počítačové programy, které byly vytvořeny za účelem poškodit, narušit, omezit, zneužít či získat kontrolu nad počítačovým systémem nebo jeho součástí."*[31]

Jednání útočníků v případu benešovské nemocnice naplňuje skutkovou podstatu trestného činu neoprávněného přístupu k počítačovému systému a neoprávněného zásahu do počítačového systému nebo nosiče informací dle § 230 trestního zákoníku. Kromě prvního odstavce, který dopadne primárně na fázi infekce, je rozhodující znění odst. 2 písm. b), které stanoví, že

> *„2) Kdo zasáhne do počítačového systému nebo nosiče informací tím, že […]*
> *b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými, bude potrestán odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci."*

V případě benešovské nemocnice útočník zasáhnul do počítačového systému tak, že zmíněná data potlačil, tedy *„zamezil přístupu oprávněné osobě k datům"*.[32] Vzhledem k tomu, že spáchané škody byly vyčísleny na částku přes 59 milionů korun, uplatní se v tomto případě kvalifikovaná skutková podstata dle § 230 odst. 5, která stanoví, že

> *„5) Odnětím svobody na tři léta až osm let bude pachatel potrestán,*
> *a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu"*.[33]

Kybernetický útok na nemocnici v Benešově by tedy bylo možné kvalifikovat jako trestný čin proti majetku, kdy byla naplněna kvalifikovaná skutková podstata trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230, odst. 5, písm. a) trestního zákoníku.

V případě většiny kybernetických útoků může být ochrana majetkových hodnot či soukromí dostačující, v benešovské nemocnici ovšem došlo z povahy věci k ohrožení i jiné hodnoty, která je chráněna trestním zákoníkem, a tou je život obyvatel. Ustanovení § 230 s touto možností ovšem cíleně nepracuje a soustředí se toliko na ochranu majetku, z čehož je evidentní, že společnost stále obtížně chápe možný vliv kybernetických útoků na podobu každodenního fungování fyzického světa.[34] Považujeme tak ochranu poskytovanou

30 NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019*.

31 DRAŠTÍK, A. et al. *Trestní zákoník: komentář*. Praha: Wolters Kluwer, 2015, komentář k § 230, odst. 11.

32 Ibidem, komentář k § 230, odst. 10.

33 Ve spojení s § 138, odst. 1, písm. e) trestního zákoníku, který za škodu velkého rozsahu označuje škodu dosahující částky nejméně 10 milionů korun.

34 To potvrzuje i dosavadní absence aplikace trestných činů proti životu a zdraví na podobné kybernetické útoky. Více viz níže v kontextu killware.

§ 230 trestního zákoníku za nedostatečnou, na základě čehož může být v daném kontextu nutné uvažovat o přístupu rozšiřujícím a mj. zvážit aplikaci i jiných ustanovení trestního zákoníku, např. § 272 Obecné ohrožení, či § 276 Poškození a ohrožení provozu obecně prospěšného zařízení.[35] Vzhledem k úzkému kauzálnímu propojení podobných útoků a hodnot zdraví a života obyvatel je pak možné uvažovat i o aplikaci trestných činů proti životu a zdraví, a to přinejmenším ve stádiu pokusu.

3.2 Konstituční znaky kybernetické zbraně v kontextu § 118 trestního zákoníku

Pokud kybernetický útok zasahuje nejen ochranu majetku a soukromí, ale také života a zdraví, může již být relevantní zvážit použitelnost pojmu kybernetická zbraň (viz první konstituční znak níže). Jak jsme ale již dříve zmiňovali, v trestním zákoníku se tento pojem nevyskytuje, důvodová zpráva k trestnímu zákoníku zde není nikterak nápomocná[36] a taktéž soudy se této otázce v českém právním systému doposud nevěnovaly. Je proto nutné pracovat s obecnějším pojmem zbraň, který se v trestním zákoníku nejčastěji objevuje v situaci, kdy byl trestný čin spáchán se zbraní. Do popředí se tak dostává možnost kvalifikované skutkové podstaty, kdy dojde ke stanovení přísnějšího trestu,[37] přičemž přímo k této možnosti se samostatně vyjadřujeme níže v textu.

Hovoříme-li o obecné situaci, kdy byl trestný čin spáchán se zbraní, odkazujeme se na § 118 trestního zákoníku:

> *„trestný čin je spáchán se zbraní, jestliže pachatel nebo s jeho vědomím některý ze spolupachatelů užije zbraně k útoku, k překonání nebo zamezení odporu anebo jestliže ji k tomu účelu má u sebe; zbraní se tu rozumí, pokud z jednotlivého ustanovení trestního zákona nevyplývá něco jiného, cokoli, čím je možno učinit útok proti tělu důraznějším“.*

Komentář k trestnímu zákoníku pak toto chápání upřesňuje s tím, že zbraní se nerozumí pouze střelná zbraň, ale i *„zbraň v technickém pojetí, tj. v užším pojetí významu tohoto pojmu“*.[38]

Určující tak není podoba zbraně, ale hodnota, která je tímto chráněna, a tou je zde tělesná integrita člověka. Přestože nelze bez dalšího usuzovat, že autor komentáře k trestnímu zákoníku měl na mysli i zbraň, která by získala přívlastek kybernetická, je nezbytné se

---

35 Dle § 132 trestního zákoníku lze pod obecně prospěšné zařízení zařadit i zařízení a sítě elektronických komunikací a koncová telekomunikační rádiová zařízení.

36 Parlament České republiky. *Sněmovní tisk 410/0, část č. 1/9 Vl.n.z. trestní zákoník – EU*. 2008. Dostupné z: https://www.psp.cz/sqw/text/orig2.sqw?idd=26247&pdf=1.

37 Jedná se o širokou paletu 25 trestných činů, dle ustanovení § 175 Vydírání, § 176 Omezování svobody vyznání, § 178 Porušování domovní svobody, § 185 Znásilnění, § 186 Sexuální nátlak, § 312f Vyhrožování teroristickým trestným činem, § 323 Násilí proti orgánu veřejné moci, § 324 Vyhrožování s cílem působit na orgán veřejné moci, § 325 Násilí proti úřední osobě, § 326 Vyhrožování s cílem působit na úřední osobu, § 338 Osvobození vězně, § 339 Násilné překročení státní hranice, § 340 Organizování a umožnění nedovoleného překročení státní hranice, § 344 Vzpoura vězňů, § 353 Nebezpečné vyhrožování, § 354 Nebezpečné pronásledování, § 375 Neuposlechnutí rozkazu, § 377 Zprotivení a donucení k porušení vojenské povinnosti, § 379 Urážka mezi vojáky násilím nebo pohrůžkou násilí, § 380 Urážka vojáka stejné hodnosti násilím nebo pohrůžkou násilí, § 381 Násilí vůči nadřízenému, § 382 Porušování práv a chráněných zájmů vojáků stejné hodnosti, § 383 Porušování práv a chráněných zájmů vojáků podřízených nebo s nižší hodností, § 386 Zběhnutí, § 395 Nesplnění bojového úkolu.

38 DRAŠTÍK, A. et al. *Trestní zákoník: komentář*, komentář k § 118.

dívat i na § 118 trestního zákoníku optikou technologického vývoje a obecně proměny bezpečnostního prostředí.[39] Níže tak představujeme konstituční znaky pro možnost rozšíření výkladu § 118 trestního zákoníku tak, aby umožňoval aplikaci pojmu kybernetická zbraň jako podmnožiny pojmu zbraň, a to v kontextu kybernetického útoku proti nemocnici.

Jako první konstituční znak vnímáme schopnost zasáhnout do hodnoty, kvůli které je pojem zbraň v trestním zákoníku v obecné podobě zakotven, tedy do fyzické integrity člověka. Jedná se o kauzální propojení kybernetického útoku a ohrožení života a zdraví, které bývá v posledních letech, kdy počet kybernetických útoků na nemocnice výrazně vzrostl,[40] skloňováno zvláště v kontextu právního posouzení tzv. killware, tedy malwaru, který vede ke smrti pacientů.[41] Tato otázka se řeší zvláště v USA,[42] nevyhnula se však ani nám geograficky bližšímu Německu. Zde se jednalo o příběh nemocnice v Düsseldorfu, která kvůli ransomwarovému útoku nemohla přijmout pacientku v kritickém stavu.[43] Tuto pacientku tak převáželi do 32 km vzdáleného města Wuppertal, což zpozdilo poskytnutí péče téměř o hodinu a pacientka krátce po příjezdu zemřela.[44] Daný ransomwarový útok nakonec nebyl shledán přímou příčinou smrti, německý soud zde ovšem (patrně z opatrnosti) aplikoval extrémně přísný příčinný test,[45] který ignoruje širší bezpečnostní situaci a není dlouhodobě udržitelný.

S přihlédnutím k technologickému vývoji, změnám v bezpečnostní situaci (častějším útokům na nemocnice) a ochraně člověka tak může být nutné tento opatrný přístup změnit. Vhodnějším se tak může jevit hodnocení dopadů kybernetického útoku v úzké souvislosti s povahou sektoru, vůči kterému byl kybernetický útok spáchán.[46] Konkrétně, že napadení a znepřístupnění nástrojů a zařízení, na nichž je již současná medicína naprosto závislá, a tím znemožnění poskytnutí péče v plném rozsahu tak, jak by zdravotnické zařízení bylo schopno poskytnout za běžného provozu před kybernetickým útokem, je v příčinné souvislosti s potenciální újmou na tělesné integritě.[47] A přestože útočník ve většině případů pravděpodobně nechce nikoho zabít ani mu přivodit újmu na zdraví, jedná při zacílení takto destruktivního útoku na nemocniční zařízení v nepřímém úmyslu (či přinejlepším ve vědomé nedbalosti v případě nezamýšlené infekce nemocnice). V úvahu by

39 Např. NATO. Emerging and disruptive technologies. In: *NATO* [online]. 22. 6. 2023 [cit. 2023-06-27]. Dostupné z: https://www.nato.int/cps/en/natohq/topics_184303.htm.

40 ENISA. *Health Threat Landscape*. 2023 [cit. 2023-06-27]. Dostupné z: https://www.enisa.europa.eu/publications/health-threat-landscape.

41 BRYAN, K. L. – LAMOUREUX, C. – HELPLING, E. P. Killware: The New Cyber Threat and What It May Mean for Data Breach and Cybersecurity Litigations. *The National Law Review*. 2021, č. 307 [cit. 2023-06-27]. Dostupné z: https://www.natlawreview.com/article/killware-new-cyber-threat-and-what-it-may-mean-data-breach-and-cybersecurity.

42 Ibidem.

43 RALSTON, W. The untold story of a cyberattack, a hospital and a dying woman. In: *Wired UK* [online]. 2020 [cit. 2023-06-27]. Dostupné z: https://www.wired.co.uk/article/ransomware-hospital-death-germany.

44 Ibidem.

45 Ibidem.

46 Obdobně kritický z pohledu zranitelnosti i rizikovosti může být např. i petrochemický průmysl a jeho SCADA a ICS systémy, více viz malware Triton v JOHNSON, B. et al. Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure. In: *Mandiant* [online]. 2022 [cit. 2023-06-27]. Dostupné z: https://www.mandiant.com/resources/blog/attackers-deploy-new-ics-attack-framework-triton.

47 Představitelnější alternativou může být situace, kdy útočník zamkne lékaře mimo operační sál, či případ, kdy by útočník vtrhnul na operační sál při probíhající operaci, vypnul všechny přístroje, rozsypal skalpely a sebral operujícímu lékaři brýle. Útočník tak poskytování péče nebrání nutně úplně, ale podstatně zvyšuje obtížnost poskytování péče a snižuje její úroveň.

pak mohla přijít i aplikace § 140 Vražda, § 142 Usmrcení z nedbalosti, či § 145–148 zaměřených na ublížení na zdraví.

Prvním konstitučním znakem (a nutným předpokladem) by tak bylo zacílení kybernetického útoku na systémy, které mají přímý vliv na poskytování péče pacientům jakožto naplnění schopnosti zasáhnout do tělesné integrity člověka.

Zbraň ve smyslu § 118 pak zahrnuje ještě další dva konstituční znaky, které musí být v kontextu kybernetických zbraní naplněny – rozlišitelnost mezi zbraní a útočníkem a míra efektu.

V případě prvního zmíněného se jedná o skutečnost, že zbraň v tradičním chápání je ve svém jádru nástroj odlišitelný od osoby útočníka samotného, nejedná se o využití útočníkových specifických schopností (pro lepší ilustraci si lze představit např. bojové sporty osvojené útočníkem). Kybernetická zbraň musí naplnit stejné měřítko. V kontextu benešovského kybernetického incidentu je tak nutné se vrátit k povaze útoku a fungování současné kybernetické kriminální scény. V současnosti již neplatí, že by si každý útočník tvořil daný útočný nástroj sám, ani že by tyto nástroje zrcadlily jeho schopnosti.[48] Zvláště pak pokročilé nástroje, jako je např. *Emotet, Trickbot* a *Ryuk* použité v případě Benešova, je možné si pronajmout jako *Ransomware as a Service – RaaS*,[49] čímž je ostatně tato trojice známá.[50] To, že i aktéři, kteří by na provedení podobného útoku původně neměli schopnosti (např. *script kiddies*), jsou díky RaaS schopni útok provést, je důkazem, že tyto nástroje jsou již na svém autorovi nezávislým destruktivním nástrojem, a nikoliv toliko projevem jeho speciálních schopností.

Posledním konstitučním znakem je míra efektu, tedy schopnost použitých nástrojů učinit útok proti chráněné hodnotě důraznější. Tento znak úzce souvisí s předešlým, neboť porovnává efekt útoku provedeného prostřednictvím schopností útočníka samotného s efektem útoku za použití kybernetických zbraní. Je pak nasnadě, že zvláště v případě RaaS a dalších pokročilých malwarů (v porovnání s např. relativně jednoduchým, ale základním *Denial of Service* útokem), které si může útočník pronajmout (a proto vůbec nemít dostatečně schopnosti na samostatné provedení takového útoku), se jedná o nástroje, které intenzitu útoku významně posilují (sofistikovanost a míra efektu tria užitého v případu Benešova je evidentní v první kapitole). Je navíc nutné zdůraznit, že efekt zbraně se může na poškozených promítnout nejen fyzicky, ale také psychicky, neboť jak Draštík et al. poukazují, *„užití zbraně může mít podobu jak přímého fyzického násilí vůči poškozenému […], tak podobu psychického násilí, jako prostředek působení na vůli poškozeného"*.[51] A je pochopitelné, že vyřazení provozuschopnosti nemocnice má na pacienty značný psychický dopad.

V kontextu kybernetického útoku na benešovskou nemocnici tedy můžeme shrnout, že mezi znaky, které musí určitý nástroj splňovat, abychom jej mohli označit za kybernetickou zbraň, lze zařadit zacílení efektů zbraně na systémy přímo spjaté s péčí o pacienty, oddělitelnost nástroje od pouhého projevu schopností útočníka a míru účinku vyvolanou pokročilostí daného nástroje.

---

48 BAKER, K. What is Ransomware as a Service (RaaS). In: *CrowdStrike* [online]. 2023 [cit. 2023-06-27]. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/.

49 Ibidem.

50 Intel 471. Understanding the relationship between Emotet, Ryuk and TrickBot. In: *Intel 471* [online]. 2020 [cit. 2023-03-27]. Dostupné z: https://intel471.com/blog/understanding-the-relationship-between-emotet-ryuk-and-trickbot.

51 DRAŠTÍK, A. et al. *Trestní zákoník: komentář*, komentář k § 118, odst. 5.

3.3 Možnosti právního dopadu pojmu kybernetická zbraň

Nasazování pokročilých malwarů proti nemocnicím je bez debat jevem nechtěným, jehož výskyt může být posilován i nedostatečně přísnou právní úpravou. Výše zmíněné rozšíření pojmu zbraň může s tímto pomoci několika způsoby.

Jak jsme již zmínili, pojem zbraň se v trestním zákoníku objevuje v různých kontextech. V prvé řadě se jedná o střelnou zbraň (§ 32 Oprávněné použití zbraně a § 279 Nedovolené ozbrojování), dále se pak použití pojmu zbraň specificky váže na situaci ozbrojeného konfliktu (§ 321a Účast na nestátní ozbrojené skupině zaměřené na působení v ozbrojeném konfliktu, § 412 Válečná krutost a § 413 Perzekuce obyvatelstva), nebo je přesně vymezeno, jak je třeba zbraň v daném ustanovení interpretovat (§ 280 Vývoj, výroba a držení zakázaných bojových prostředků, kdy jsou zbraněmi rozuměny takové zbraně, které jsou zakázány zákonem nebo mezinárodní smlouvou; dále § 281a Vysoce nebezpečná látka, kde se zbraní rozumí chemická zbraň). V následující části ale budeme věnovat pozornost pouze dvěma institutům, které jsou pro naše potřeby nejrelevantnější, a to kvalifikované skutkové podstatě a přitěžujícím okolnostem.

První možností, ve které může mít pojem kybernetická zbraň kýžený dopad, je již zmíněná kvalifikovaná skutková podstata, kdy se nabízí termín kybernetická zbraň zakomponovat legislativně, například do § 230 trestního zákoníku. V rámci úvah *de lege ferenda* se tak nabízí rozšířit nejen § 230 o následky zásahu do fyzické integrity člověka, ale také přistoupit na skutečnost, že kybernetický útok může zasáhnout do zájmů chráněných v hlavě první zvláštní části trestního zákoníku, čímž by bylo možné chápat využití pokročilých malwarů jako kybernetických zbraní a tvrději stíhat jejich nasazení, zejména při zacílení na zvláště zranitelné sektory jako je zdravotnictví.[52]

Pokračováním této argumentace pak můžeme dojít i k modifikaci významu pojmu zbraň v hlavě deváté zvláštní části trestního zákoníku, kde jsou zakomponovány trestné činy proti České republice, cizímu státu a mezinárodní organizaci. Konkrétně ve skutkových podstatách trestných činů dle § 311 Teroristický útok [odst. 2, písm. f)] a § 312e Podpora a propagace terorismu [odst. 2, písm. b) a c)] se objevuje (a nikoli v kvalifikované skutkové podstatě) pojem zbraň. Lze si tak představit scénář, kdy např. výrobou zbraně či poskytnutím informací o její výrobě nebo používání by bylo rozuměno taktéž mj. poskytnutí návodu na použití malwaru. Pojetí zbraně v § 312e je pak dostatečně flexibilní a teoreticky by umožňovalo aplikaci i na kybernetickou zbraň jakožto pokročilý malware.

Druhou možností je aplikace pojmu kybernetická zbraň v kontextu přitěžující okolnosti dle § 42 trestního zákoníku, kde se v zásadě nabízí tři varianty.

První z nich je posouzení spáchání trestného činu se zbraní jako v zákoně výslovně neuvedené obecné přitěžující okolnosti podle § 42 trestního zákoníku.[53]

Druhou variantou je přitěžující okolnost dle § 42, písm. g) trestního zákoníku,[54] která by odpovídala povaze cíle kybernetického útoku, kterým byla nemocnice v Benešově.

---

52 Přestože je náš článek zaměřen na sektor zdravotnictví, není nutné tyto myšlenky limitovat toliko tímto okruhem. Jak jsme zmínili výše, obdobné znaky vykazuje i mj. petrochemický průmysl, v čemž znovu odkazujeme na kybernetický bezpečnostní incident s malwarem Triton. Viz JOHNSON, B. et al. *Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure*.

53 DRAŠTÍK, A. et al. *Trestní zákoník: komentář*, komentář k § 118, odst. 3.

54 *„Soud jako k přitěžující okolnosti přihlédne zejména k tomu, že pachatel g) spáchal trestný čin vůči osobě podílející se na záchraně života a zdraví nebo na ochraně majetku […].“*

Dle komentáře není explicitně stanoveno, že se musí jednat o fyzický útok, kybernetická povaha by zde mohla býti dostatečnou.[55]

Třetí možností je přitěžující okolnost uvedená v § 42, písm. h) trestního zákoníku,[56] která opět reflektuje povahu nemocničního zařízení. Stát zde tak vyjadřuje *„zájem na zvýšené ochraně určitých skupin lidí cestou přísnějšího postihu trestných činů spáchaných k jejich újmě“*.[57] Obdobně jako v předchozím případě se nemusí jednat o fyzický útok, rozhodující je, že se jedná o útok na integritu člověka.[58]

Lze tak shrnout, že ve spojení s kybernetickým útokem na nemocnici v Benešově by se mohlo jednat o trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací, kde by jeho spáchání se zbraní mohlo být využito jako v zákoně výslovně neuvedená obecná přitěžující okolnost či přitěžující okolnost dle § 42 písm. g) nebo h) trestního zákoníku.

4. Vyhodnocení a budoucí vývoj

Dle analýzy provedené výše je zřejmé, že v české trestněprávní úpravě lze přistoupit k výkladu a aplikaci pojmu kybernetická zbraň dvěma základními směry. První z nich obnáší rozšíření dosavadní kvalifikace kybernetických útoků na nemocnice o další trestné činy mj. z hlavy první a sedmé zvláštní části trestního zákoníku a tím i rozšíření stávajícího výkladu pojmu zbraň o pokročilé malwary, čímž by došlo k faktickému zahrnutí kybernetických zbraní do právní kvalifikace. To se pojí i s navazující úvahou *de lege ferenda* o rozšíření skutkové podstaty § 230 o kvalifikovanou podstatu spáchání činu se zbraní (v tomto kontextu s kybernetickou zbraní) a způsobení újmy na hodnotách chráněných hlavou první zvláštní části trestního zákoníku.

Druhou možností je kvalifikovat situaci označovanou za použití kybernetické zbraně jako trestný čin dle § 230 trestního zákoníku, charakter samotného kybernetického útoku by pak mohl být kvalifikován jako výslovně neuvedená obecná přitěžující okolnost podle § 42 trestního zákoníku či přitěžující okolnost dle § 42 písm. g) a h) trestního zákoníku. Je ovšem zřejmé, že v tomto kontextu by bylo nezbytné se vypořádat s faktem, že pod definici zbraně by bylo možné subsumovat i malware, jakožto nemateriální věc.

Na základě vyhodnocení daných variant a v kontextu probíhajících debat k tématu killware a kybernetických útoků proti nemocnicím soudíme, že je nezbytné zohlednit technologický vývoj i z pohledu právního výkladu již existujících právních norem, nevidíme ovšem smysl v zavádění samostatného pojmu kybernetická zbraň a místo toho podporujeme otevření širších debat o koncepčním přístupu s ohledem na technologický i geopolitický vývoj.

Nepopíráme však, že by možnost přistoupit k právní úpravě kybernetických zbraní obdobně, jak to známe např. již na poli regulace střelných zbraní, nebyla otevřena i nad rámec právní úpravy týkající se hodnot chráněných trestním zákoníkem. K tomuto kroku

---

55 DRAŠTÍK, A. et al. *Trestní zákoník: komentář*, komentář k § 42.

56 *„Soud jako k přitěžující okolnosti přihlédne zejména k tomu, že pachatel*
h) spáchal trestný čin vůči dítěti, osobě blízké, těhotné, nemocné, zdravotně postižené, vysokého věku nebo nemohoucí a ohrozil tím jejich život nebo zdraví, způsobil jim škodu, újmu na zdraví nebo jinou újmu anebo se na jejich úkor bezdůvodně obohatil […].“

57 DRAŠTÍK, A. et al. *Trestní zákoník: komentář*, komentář k § 42.

58 Ibidem.

je ovšem zapotřebí zdárné synergie vícero faktorů, tedy nejenom právních. Prvním faktorem je obecná společenská poptávka, která by vytvářela dostatečný tlak na to, aby vůbec započaly diskuze k danému tématu (např. uspořádání kulatého stolu v rámci konference[59]). Následně by došlo k vygenerování samotného zadání, kde by klíčovou otázkou byla právě regulace kybernetických zbraní. Jako vhodný gestor by se nabízelo Ministerstvo vnitra, které na poli regulace zbraní hraje nezastupitelnou roli s ohledem na to, že je *„ústředním orgánem státní správy pro vnitřní věci, zejména pro […] zbraně a střelivo“*.[60] Po zhodnocení všech dopadů by teprve nastala fáze případných legislativních prací a vypracování návrhu odpovídajících právních norem. Česká republika tedy již v této chvíli disponuje procesy a nástroji k případné cílené právní regulaci kybernetických zbraní v případě, že bude tato možnost shledána jako účelná a sloužící k efektivnější ochraně nejenom života a majetku obyvatel, ale i dalších chráněných zájmů.

Závěr

V článku jsme se zabývali možným normativním významem pojmu kybernetická zbraň a jeho potenciální pozicí v českém právním systému, a to po jeho použití bývalým premiérem Andrejem Babišem ve veřejném prostoru v roce 2020. Po analýze relevantní právní úpravy shledáváme, že se daný pojem používá primárně jako tzv. *buzzword* (z anglického „populární/módní slovo“), který sice vyvolává silné emoce, ale český právní řád jej nezná a je v současnosti bez právní definice, kvůli čemuž je jen obtížně uchopitelný.

Pokusili jsme se ovšem přistoupit na narativ bývalého premiéra a analyzovali jsme situaci benešovského kybernetického incidentu za účelem bližšího vyjasnění, co může použití kybernetických zbraní představovat.

Analyzovali jsme tak relevantní právní prameny, které umožňují rozšíření pojmu zbraň o faktické znaky nástrojů použitých při útoku na benešovskou nemocnici a které by tedy měly naplňovat pojem kybernetická zbraň. Jediné relevantní odvětví, které nabízelo dostatečně rozšiřitelný institut zbraně, bylo trestní právo.

V něm jsme představili několik myšlenkových směrů. První z nich je opřený o základní kvalifikaci benešovského kybernetického incidentu jakožto činu naplňujícího znaky skutkové podstaty dle § 230 trestního zákoníku. Tuto možnost jsme dále rozšířili o úvahu *de lege ferenda* spočívající ve vytvoření nové kvalifikované skutkové podstaty § 230 trestního zákoníku a vymezení souvisejících možných konstitučních znaků kybernetické zbraně. V druhé řadě jsme popsali charakter kybernetického útoku jakožto přitěžující okolnosti ve smyslu § 42 trestního zákoníku. Na základě provedené analýzy jsme nedošli k názoru, že by bylo potřeba legislativně ukotvit samostatný pojem kybernetické zbraně, je ovšem v tomto kontextu naprosto nezbytné zohlednit technologický vývoj a změny v bezpečnostní situaci.

---

59 Zde se nabízí např. konference CyberCon pořádaná každoročně Národním úřadem pro kybernetickou a informační bezpečnost.

60 § 12, odst. 1, písm. f) zákona č. 2/1969 Sb., *o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky (kompetenční zákon)*, ve znění pozdějších předpisů. Zákon č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky (kompetenční zákon). In: *Zákony pro lidi* [online]. 2023. Dostupné z: https://www.zakonyprolidi.cz/cs/1969-2.

Cyber Weapon and the Law: Cyber Attacks Against Hospitals

Jakub Vostoupal (https://orcid.org/0000-0002-1669-9931) – Ivana Kudláčková

Abstract: In this article, the authors discuss the potential meaning and normative grasp of the term cyber weapon, which has been used in the public space in the context of the cyber-attack against the Rudolf and Stefanie Hospital in Benesov. In this respect, authors analyze details of the cyber incident to identify constitutive elements of a cyber weapon and a possibility of subsequent subsumption and application of the term cyber weapon in the Czech legal environment. As a part of the legal analysis, the authors try to deal with the situation that the Czech legal system not only does not know the concept but also does not envisage it and, in a large number of areas, does not allow for its application even through extensive legal interpretation, and therefore they focus on the criminal law as the most relevant branch for the given issue. The authors assess whether the criminal law consideration of advanced malware is desirable and offer several directions in which the subsumption and application can be considered, focusing primarily on the issue of the qualifying extension and regulatory completion of the qualified offence of unauthorized access to a computer system and the possibilities offered by the aggravating circumstances legislation. They conclude the article by an evaluation and recommendations for a future development.

Keywords: cyber weapon, weapon, Benešov cyber incident, criminal law, cyber crime