ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA BIOMEDICÍNSKÉHO INŽENÝRSTVÍ

Katedra zdravotnických oborů a ochrany obyvatelstva

Analýzy příčin teroristických útoků na zdravotnická zařízení ve světě od roku 1985 dosud a připravenosti vybraných zdravotnických zařízení na kyberútok

Analysis of the Teroristic Attacks on Medical Facilities Causes in the World since 1985 until now and the Readiness of Selected Medical Facilities for Cyber Attack.

Diplomová práce

Studijní program:	Civilní nouzové plánování
Autor diplomové práce:	Bc. Jiří Fryjauf
Vedoucí diplomové práce:	prof. MUDr. Leoš Navrátil, CSc., MBA, dr.h.c.

Kladno 2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení:	**Fryjauf**	Jméno:	**Jiří**	Osobní číslo:	**503690**
Fakulta:	**Fakulta biomedicínského inženýrství**				
Garantující katedra:	**Katedra zdravotnických oborů a ochrany obyvatelstva**				
Studijní program:	**Civilní nouzové plánování**				

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Analýza příčin teroristických útoků na zdravotnická zařízení ve světě od roku 1985 dosud a připravenosti vybraných zdravotnických zařízení na kyberútok

Název diplomové práce anglicky:

Analysis of the Teroristic Attacks on Medical Facilities Causes in the World since 1985 until now and the Readiness of Selected Medical Facilities for Cyber Attack

Pokyny pro vypracování:

Předmětem diplomové práce je analýza příčin, průběhu a následků teroristických útoků a pokusů o útok na zdravotnická zařízení ve světě od roku 1985 do současnosti a jejich vývoj v čase s ohledem na specifičnost tohoto cíle pro teroristy. V práci bude analyzována korelace vybraných teroristických útoků s ozbrojenými konflikty a vývojem způsobu a formy útoku v průběhu času metodou deskripce a komparace. Součástí praktické části práce bude rozbor rizik nového fenoménu kyberteroristických útoků zaměřených na zdravotnická zařízení a připravenost vybraných zdravotnických zařízení na teroristický kyberútok. Tato část bude zkoumána metodou analýzy rizik, tedy zranitelností webových stránek zdravotnických zařízení za použití informací získaných z veřejně dostupných zdrojů. Výstupem práce bude ověření hypotéz týkajících se korelace útoků s ozbrojenými konflikty, jejich změnami v čase a dále ověření hypotézy ohledně úrovně zabezpečení vybraných nemocnic po masivních kybernetických útocích z jara 2020. Výstup z praktické části bude využitelný pro zdravotnická zařízení, jejichž webové stránky nejsou dobře zabezpečeny proti kyberútokům.

Seznam doporučené literatury:

[1] CARR, Caleb, Dějiny terorismu: dějiny války proti civilistům, Praha: Práh, 2002, ISBN 80-7252-063-6
[2] KARLOS, V., M. LARCHER a G. SOLOMOS, Review on Soft target/Public space protection guidance., ed. 2, Lucemburk: Publications Office of the European Union, 2018, ISBN 978-92-79- 79907-5
[3] AYALA, Luis, Cybersecurity for Hospitals and Healthcare Facilities. Fredericksburg, Virginia, USA: Apress, 2016, ISBN 978-1-4842- 2154-9

Jméno a příjmení vedoucí(ho) diplomové práce:

prof. MUDr. Leoš Navrátil, CSc., MBA, dr. h. c.

Jméno a příjmení konzultanta(ky) diplomové práce:

doc. RNDr. Josef Požár, CSc.

Datum zadání diplomové práce: **04.10.2021**
Platnost zadání diplomové práce: **22.09.2023**

doc. Mgr. Zdeněk Hon, Ph.D.
vedoucí katedry

prof. MUDr. Jozef Rosina, Ph.D., MBA
děkan

PROHLÁŠENÍ

Prohlašuji, že jsem diplomovou práci s názvem „Analýza příčin teroristických útoků na zdravotnická zařízení ve světě od roku 1985 dosud a připravenosti vybraných zdravotnických zařízení na kyberútok“ vypracoval samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

V Kladně dne 10.05.2022

…….

Bc. Jiří Fryjauf

PODĚKOVÁNÍ

Na tomto místě bych rád poděkoval prof. MUDr. Leoši Navrátilovi, CSc., MBA, dr.h.c. za odborné vedení, cenné připomínky a rady.

ABSTRAKT

Diplomová práce se věnuje příčinám, průběhu a následkům teroristických útoků na nemocnice a připravenosti vybraných zdravotnických zařízení na kybernetický útok.

Z práce vyplývá, že teroristické útoky na nemocnice jsou významně zvýšené v oblastech, kde probíhají ozbrojené konflikty a jsou prováděny většinou ve formě bombového útoku. Následkem toho dochází k medializaci, která zvyšuje riziko dalších teroristických útoků, zejména v zasažených oblastech. Celosvětově se zvyšuje počet teroristických útoků a souběžně s tím roste také počet útoků na zdravotnická zařízení. Tyto útoky rostou nadproporcionálně. Mezi lety 1985-2019 se jejich poměr na celkovém počtu teroristických útoků zdvojnásobil.

České zdravotnictví bylo s nástupem první vlny pandemie COVID-19 zasaženo masivními kybernetickými útoky, které se dosud nepodařilo objasnit. Bylo použito více forem útoků. Nemocnice jsou celosvětově lákavým cílem, protože kombinují možnost snadného útoku a vysokého ničivého efektu, který mimo jiné vede k možnosti vysoké medializace.

České nemocnice své zabezpečení v reakci na útoky z jara 2020 zvyšují, ale řada z nich je, stejně jako nemocnice na celém světě, zabezpečena nedostatečně a některé nechávají dveře k IT systému přímo otevřené. To dokazuje výzkum internetových stránek vybraných českých i světových nemocnic, z něhož vyplynulo, že velká část webových stránek zdravotnických zařízení může být hackery napadena a z některých z nich mohou přímo zaútočit i na IT systémy nemocnic.

Klíčová slova

Teroristické útoky; zdravotnická zařízení; kybernetické útoky; terorismus; nemocnice.

ABSTRACT

The diploma thesis deals with the causes, course and consequences of terrorist attacks on hospitals and the preparedness of selected medical facilities for cyber attacks.

The work shows that terrorist attacks on hospitals are significantly increased in areas where armed conflicts are taking place and are mostly carried out in the form of bomb attacks. As a result, there is media coverage, which increases the risk of further terrorist attacks, especially in the affected areas. The number of terrorist attacks is increasing worldwide, and so is the number of attacks on medical facilities. These attacks are growing disproportionately. Between 1985 and 2013, their proportion to the total number of terrorist attacks doubled.

With the onset of the first wave of the COVID-19 pandemic, the Czech healthcare system was hit by massive cyber attacks, which have not yet been clarified. Several forms of attacks have been used. Hospitals are an attractive destination worldwide because they combine the possibility of an easy attack and a high destoying effect, which, among other things, leads to the possibility of high media coverage.

Czech hospitals are increasing their security in response to the spring 2020 attacks, but many of them, like hospitals around the world, are insufficiently secured and some leave the door to the IT system directly open. This is proved by a research of the websites of selected Czech and world hospitals, which showed that a large part of the websites of medical facilities can be attacked by hackers and some of them can directly attack the IT systems of hospitals.

Keywords

Terrorist attacks; medical facilities, cyberattacks; terrorism; hospital.

Obsah

1 ÚVOD

Zdravotnická zařízení jsou s ohledem na jejich specifičnost a přítomnost velkého množství prakticky bezbranných lidí lákavým cílem pro teroristické útoky. Možnosti jejich aktivní ochrany jsou ve značné míře omezené, tedy se jedná o relativně snadný a dosažitelný cíl.

K zájmu o tuto problematiku mne přivedly kybernetické útoky, kterým byly vystaveny české nemocnice s nástupem koronavirové krize. Kybernetické útoky jsou rozšířením násilných útoků, jimž jsou nemocnice bez ohledu na Ženevské úmluvy a další humanitární konvence vystaveny.

Tím jsem se dostal k úvahám nad příčinami teroristických útoků na zdravotnická zařízení a jejich trendy, protože podle zpráv z médií se zdá, že útoky na zdravotnická probíhají se zvyšující se intenzitou.

Od své práce očekávám odpověď na otázku ohledně příčin násilných teroristických a kybernetických útoků na nemocnice, jejich průběhu a následků a také odpověď na to, zda se zdravotnická zařízení poučila z vlny útoků v letech 2020 a 2021 a kyberterorismu se samy nevystavují nedostatečným zabezpečením. Pro výzkum jsem zvolil eticky přijatelný výzkum zabezpečení internetových stránek nemocnic. Tato část bude využitelná pro řídící a IT pracovníky nemocnic k zamyšlení nad riziky a jejich efektivnějším zabezpečením.

2 CÍLE PRÁCE A HYPOTÉZY

2.1 Cíl 1 – analýza příčin, průběhu a následků teroristických útoků na zdravotnická zařízení

Hypotéza 1: Násilné útoky na zdravotnická zařízení korelují s místy ozbrojených konfliktů.

2.2 Cíl 2 – analýza kybernetických útoků na zdravotnická zařízení a připravenosti vybraných zdravotnických zařízení na kybernetický útok

Hypotéza 2: Část českých nemocnic stále není dostatečně chráněna proti kybernetickému útoku na webové stránky.

Hypotéza 3 společná pro oba cíle: Počet násilných teroristických útoků i kybernetických útoků na zdravotnická zařízení se zvyšuje.

3 PŘEHLED SOUČASNÉHO STAVU

Samotný pojem terorismus není v českém ani mezinárodním právu přesně definován, protože se hranice mezi různými druhy útoků stírají.

Podle oficiální definice Ministerstva vnitra České republiky lze za terorismus označit takové jednání, které je politicky, nábožensky či jinak ideologicky motivováno a užívá násilí či jeho hrozby zejména s cílem vyvolat strach. (Ministerstvo vnitra ČR 2016)

Z pohledu cílů terorismu se vžilo rozlišení na tzv. „měkké cíle“ a „tvrdé cíle“. Termíny nejsou nikde oficiálně definovány. Z praktického pohledu jsou jako „měkké cíle“ bezpečnostní komunitou označována místa s vysokou koncentrací osob a nízkou úrovní zabezpečení proti násilným útokům, jak uvádí MVČR. (Ministerstvo vnitra ČR 2021)

Tím se odlišují od tzv. tvrdých cílů, kterými jsou například objekty armádních, bezpečnostních složek a některých státních a soukromých objektů (sídlo prezidenta, jaderná elektrárna).

Nemocnice představují příklad takzvaných „měkkých cílů“:

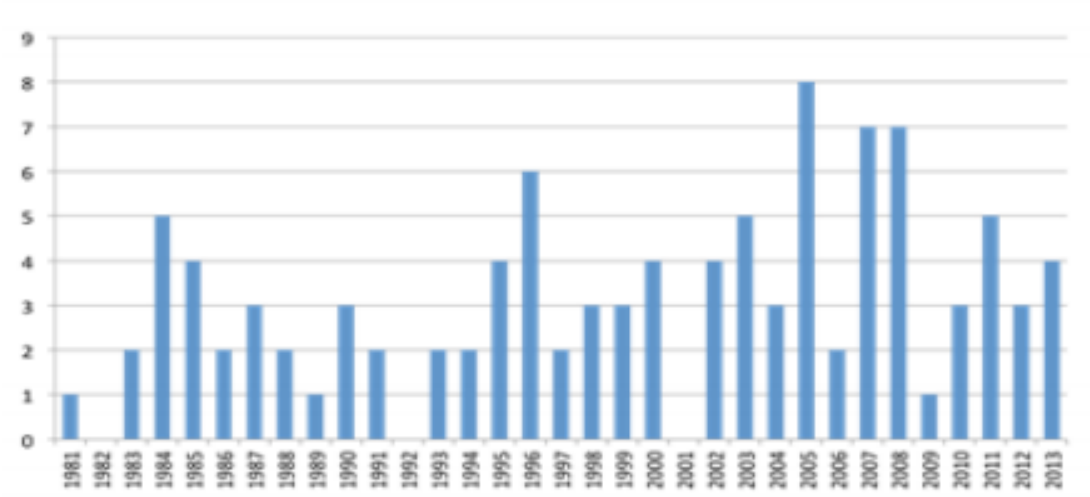
- nízký počet pracovníků ostrahy;
- volný průchod osob a průjezd vozidel;
- nedostatečný výcvik personálu k reakci na teroristický útok.

V posledních letech roste s rozvojem informačních technologií hrozba kyberterorismu.

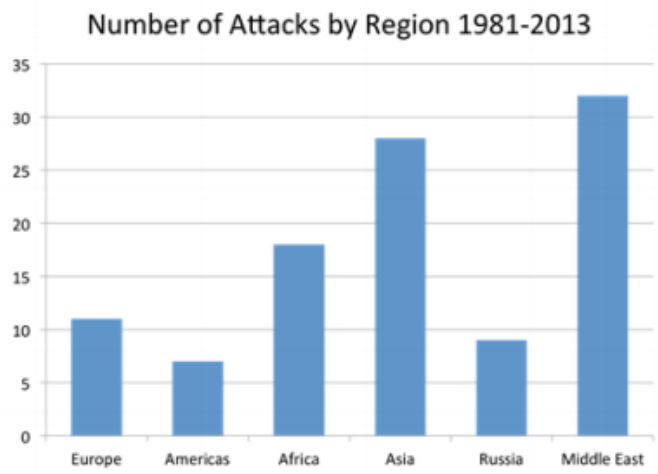
Výrazné problémy způsobily kybernetické útoky na nemocnice na jaře roku 2020, tedy v době, kdy se v Evropě šířil COVID-19. Největší problémy způsobil útok na Fakultní nemocnici Brno.

3.1 Útoky od roku 1985 s výjimkou kybernetických útoků

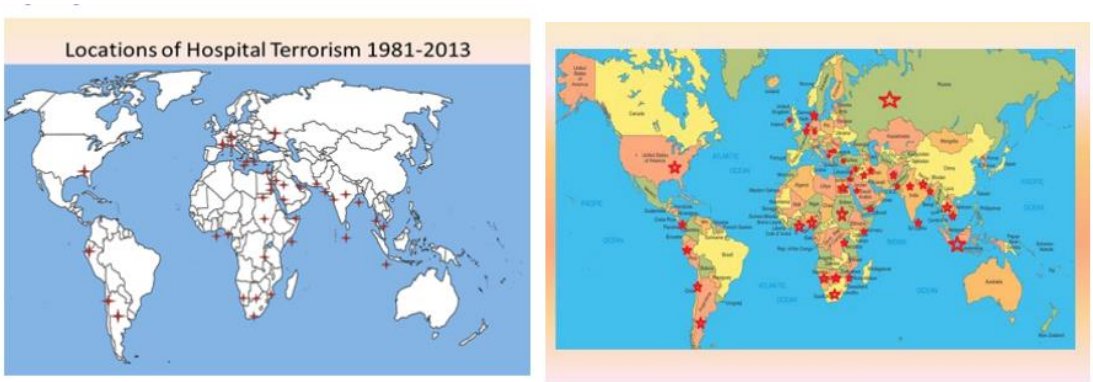
Sumární statistiku útoků na zdravotnická zařízení zveřejnila organizace International Institute for Counter-Terrorism (ICT). Z ní vyplývá, že od roku 1981 do roku 2013 bylo zaznamenáno přibližně 100 teroristických útoků na nemocnice ve 43 zemích světa, při nichž bylo zabito 775 osob a zraněno dalších 1217. (Ganor 2013)



Obrázek 1 - Teroristické útoky do roku 2013 (Ganor 2013)



Obrázek 2 – Počet útoků podle regionech v letech 1981 – 2013 (Ganor 2013)



Obrázek 3 a 4 – Místa útoků na nemocnice v letech 1981 – 2013 (Ganor 2013)

Nejvíce útoků se podle ICT odehrávalo v letech 1981 – 2013 na Blízkém Východě, následovala Asie (především jihovýchodní) a Afrika. (Ganor 2013)

3.2 Přehled největších útoků od roku 1985 do současnosti

Z útoků na nemocnice jsem do níže uvedené tabulky shrnul útoky s nejvyšším počtem obětí, nebo zraněných, které jsem nalezl v dostupné literatuře a také v Globální databázi terorismu a dále ty, které se něčím vymykaly, například se jednalo o cíl v Evropě, České republice, kombinovaný útok na více zařízení, nebo cíl v rámci pandemie koronaviru.

V útocích dominují místa ozbrojených konfliktů – Afghánistán, Irák, Rwanda, Sýrie, Sierra Leone. Objevuje se i několik útoků nebo pokusů o útok na evropské nemocnice. Jsou řazeny v chronologickém pořadí, ke každému případu je uvedeno místo, bližší popis a počet obětí.

Tabulka 1 – Přehled největších útoků na nemocnice (ČTK 2011; ČTK a Aktuálně.cz 2017; Ganor 2013; Global Terrorism Database 2009-2021; Kaclová, Lazáková, Karas a Šťáhlavský 2003; Kashirtseva 2013)

rok	Místo	bližší popis	Oběti
1991	Belfast	Musgrave Park Hospital – bombový útok (9,1 kg Semtexu). Útočila Irská republikánská armáda (IRA). Objekt byl do té doby považován za bezpečnou budovu, byl dobře střežen, protože v něm bylo umístěno vojenské křídlo pro zraněné vojáky. Útoku napomohl zaměstnanec sympatizující s IRA, který záměrně nezamkl dveře.	Nemocnice byla poničena, řada lidí, včetně dětí, byla zraněna, dva vojáci zemřeli.
1992	Filipíny, Lamitan	Skupina Abu Sayyaf převzala kontrolu nad nemocnicí a zajala jako rukojmí 200 lidí, především pacientů a personálu. Tito lidé byli zadržováni přibližně 370 dní.	16 obětí, 41 zraněných
1994	Kigali, Rwanda	V rámci kmenových a občanských válek mezi kmeny Hutu a Tutsi ve Rwandě zavraždili vojáci, kteří měli hlídat nemocnici, řadu pacientů kmene Tutsi.	Stovky obětí
1994	Kigali, Rwanda	Útok na zařízení pro mentálně hendikepované.	Přes 700 obětí
1995	Butare, Rwanda	Útoky na nemocnici ze strany Hutuů	Asi 150 obětí
1995	Buďonnovsk, Rusko	Skupina čečenských ozbrojenců vedená Basajeem obsadila nemocnici v ruském Buďonnovsku. Zadržela několik stovek rukojmích.	Celkem 129 civilních obětí, dále 18 policistů a 17 vojáků a 11 teroristů, dalších více než 400 bylo zraněno. Současně ozbrojenci ukradli rentgen, který jim později posloužil jako zdroj cesia-137 pro radiologický útok.
1996	Zaire, Kongo	Dva masakry – útok na misionářskou nemocnici a Lemera Hospital.	50 mrtvých, část pacientů byli vojáci, zbytek civilisté, také lékaři a sestry.
1996	Dagestán, Kizljar – polní nemocnice	Čečenští ozbrojenci zadrželi asi 2000 osob, žádali odchod ruských vojáků z Čečenska a Dagestánu.	Desítky příslušníků ruských sil a civilistů a přes 100 čečenských ozbrojenců.
1996	Bujumbura (Burundi)	Útok na nemocnici – spojitost s občanskou válkou ve Rwandě.	4 oběti ze strany kmene Tutsiů včetně šestiměsíčního kojence
1996	Sierra Leone, Masagna	Útok na pacienty.	36 obětí
2003	Hamburk, vojenská nemocnice	Pokus o pumový útok na vojenskou nemocnici – islámští radikálové.	Žádné oběti díky spolupráci německých a amerických zpravodajských služeb. Do přehledu byla zahrnuta z toho důvodu, že se jedná o jeden z mála incidentů přímo na evropské půdě.

Pokračování tabulky na straně 15

Pokračování tabulky ze strany 14

2003	Mozdok, Rusko	Ruská vojenská nemocnice – k výbuchu byl použit nákladní automobil s výbušninou – síla exploze byla minimálně tuna TNT.	Třípatrová budova byla zničena včetně oddělení JIP, kardiologie a chirurgie. 50 obětí a více než 80 zraněných
2005	Velká Británie	Plánovaný neuskutečněný útok v rámci teroristických útoků na více cílů ve Velké Británii, k útokům se přihlásila Al-Kajdá, útočníci tvrdili, že jejich cílem bylo šířit strach.	Útoky na nemocnice nebyly zrealizovány, ale při útocích na další cíle bylo identifikováno 52 obětí.
2005	Irák, Al-Mahmudiyah	Sebevražený bombový útok.	32 mrtvých, 27 zraněných, současně byly váženě poškozeno několik budov nemocnice. K odpovědnosti za útok se nikdo nepřihlásil.
2007	Somálsko, Mogadišu	Kombinovaný útok na etiopské vojenské velitelství a vojenskou nemocnici etiopských ozbrojených sil. K odpovědnosti se nikdo nepřihlásil.	Zabito 11 civilistů včetně dětí a 90 zraněno.
2008	Irák, Balad Ruz	Kombinovaný sebevražedný útok. Nejdříve se ve svatebním průvodu odpálila žena, která předstírala těhotenství, druhou nálož odpálil sebevražedný atentátník poté, co přijely sanitky a policie. Zabránil tedy tomu, aby prvním zraněným byla poskytnuta rychlá efektivní pomoc.	36 mrtvých, 66 zraněných. Nejednalo se sice přímo o útok na nemocnici, ale je třeba si povšimnout souběžnému útoku na civilní a zdravotnické cíle se záměrem způsobit co nejvyšší škodu.
2008	Pákistán, Dera Ismail Khan	Sebevražedný bombový útok. Za útok převzala odpovědnost odnož organizace Tálibán.	28 obětí, 30 zraněných
2010	Irák, Diyala	Kombinovaný útok. První útočník odpálil nálož u vládní budovy, druhá následovala o sto metrů dále na křižovatce. Třetí útok zaměřený na nemocnici byl odhalen a policisté bezpečně provedli řízenou detonaci nálože nalezené u nemocnice. K útoku se přihlásil Islámský stát.	36 obětí, 55 zraněných, pokud by se nepodařilo najít nálož u nemocnice, mohlo být obětí mnohem více jak na straně pacientů a personálu nemocnice, tak na straně účastníků předchozích atentátů.
2011	Tikrít, Irák	Sebevražedný bombový útok na University Public Hospital, k němuž se později přihlásila Al-Kájdá.	11 obětí, více než 30 zraněných
2011	Afghánistán, Kábul	Výbuch ve vojenské nemocnici v Kábulu.	Více než 50 zraněných
2011	Afghánistán, Azra	Sebevražedný atentátník se zabil v nemocnici, nikdo se k útoku nepřihlásil.	38 mrtvých, přes 100 zraněných, řada materiálních škod na vozidlech a nemocnici.
2013	Jemen, Sanaa	Opět kombinovaný útok na vojenskou nemocnici a ministerstvo obrany. K útoku se přihlásila Al-Kajdá.	28 mrtvých, 20 zraněných
2013	Nigérie, Damaturu	Několik kombinovaných útoků včetně policejní stanice a bezpečnostních složek. K útoku se přihlásila organizace Boko Haram.	30 obětí
2014	Sýrie, Alepo	Auto naložené výbušninami explodovalo před nemocnicí ve městě Atmeh. K útoku se nikdo nepřihlásil, předpokládaným útočníkem byl Islámský stát.	14 mrtvých, 65 zraněných

Pokračování tabulky na straně 16

Pokračování tabulky ze strany 15

2014	Sýrie, poblíž hranice s Tureckem	Auto naložené výbušninami explodovalo u nemocničního stanu.	12 mrtvých, 65 zraněných
2014	Irák, Hillah	Auto naložené výbušninami explodovalo před univerzitní nemocnicí. K útoku se přiznali čtyři zadržení členové Islámského státu.	8 mrtvých, 58 zraněných
2014	Jemen, Majzar	Auto naložené výbušninami explodovalo před polní nemocnicí. K útoku se přihlásila Al Kájdá.	15 mrtvých, 51 zraněných
2014	Nigérie, Damaturu	Kombinovaný útok na univerzitu, školy, policejní stanici a nemocnici.	Kromě ostatních obětí byli zabiti dva lékaři a tři byli uneseni. Opět snaha vyřadit pomoc zdravotníků a dalších bezpečnostních složek při teroristickém útoku.
2015	Libye, Syrta	Neznámí útočníci (pravděpodobně Islámský stát) založili požár v nemocnici.	22 mrtvých
2015	Sýrie, Damašek	Výbuch bomby u nemocnice, k útoku se nikdo nepřihlásil.	30 mrtvých, 20 zraněných
2016	Sýrie, Dei rez-Zor	Útok na nemocnici, ke kterému se přihlásil Islámský stát.	20 obětí, neznámý počet lidí byl unesen, jejich osud je neznámý.
2016	Sýrie, Jableh	Sebevražedný atentát u vstupu do nemocnice. Jednalo se o jeden ze šesti koordinovaných útoků v Tartusu a Jablehu, k odpovědnosti se přihlásil Islámský stát.	37 obětí u nemocnice, celkově při kombinovaných útocích zemřelo nejméně 108 lidí.
2016	Irák, Mosul	Útok na vojáky v nemocnici. K odpovědnosti se přihlásil Islámský stát.	13 mrtvých, 43 zraněných
2016	Pákistán	Pumový útok u nemocnice v Kvétě – jižní Pákistán, sebevražedný atentátník.	93 mrtvých, desítky zraněných
2017	Afghánistán, Kábul	Teroristé převlečení za zdravotníky napadli vojenskou nemocnici v Kábulu.	49 mrtvých, 90 zraněných
2018	Afghánistán, Kábul	Sebevražedný atentátník provedl kombinovaný bombový útok na nemocnici a policejní stanici (sanitkou naloženou výbušninami). K útoku se přihlásilo hnutí Tálibán.	103 mrtvých, 235 zraněných
2019	Afghánistán, Qalat, Zabul	Kombinovaný útok Tálibánu na ředitelství bezpečnostních složek a nemocnici.	40 mrtvých, 140 zraněných
2019	Afghánistán, v oblasti letadlové základny Bagram	Útok provedli dva sebevražední atentátníci v autech naložených výbušninou. K útoku se přihlásil Tálibán.	2 mrtví, 76 zraněných.
2019	Fakultní nemocnice Ostrava	Útok osamělého střelce.	7 mrtvých
2020	Afghánistán, Dašt-e Barči, Kábul	Islámský stát napadl porodnické oddělení nemocnice Lékařů bez hranic v Kábulu.	11 zavražděných pacientek porodnice, 2 děti, 1 porodní asistentka
2020	Kansas City, USA	Plánovaný bombový útok na nemocnici, která se starala o pacienty infikované koronavirem.	Žádné oběti, útočník, který chtěl ve zdravotnickém zařízení odpálit nálož v automobilu, byl zastřelen při domovní prohlídce

Z výše uvedeného seznamu je dále vybráno několik útoků, které jsou podrobněji rozebrány z níže popsaných důvodů (řazeno podle data). Každý z vybraných útoků má jinou charakteristiku a také reprezentuje nějakou formu změny, ke kterým v rámci vývoje teroristických útoků dochází:

- útok na Musgrave Park Hospital – jedná se o teroristický útok v Evropě a současně vojenskou nemocnici, charakterizuje ho rychlá a koordinovaná reakce záchranných složek a armády, na druhou stranu pokračuje v linii útoků před rokem 1985, které se většinou soustředily na vojenská zdravotnická zařízení;
- útok na Nemocnici Kigali, Univerzitní nemocnici Butare a Psychiatrické centrum Ndera ve Rwandě – útoky byly nástrojem genocidy;
- útok na Nemocnici Buďonnovsk – pro útočníky úspěšná operace, příčina obratu v první čečenské válce;
- Irák – kombinované útoky při nich útočníci napadli více cílů najednou, jedním z nich bylo zdravotnické zařízení Balad Ruz General Hospital a druhým Baquba General Hospital;
- útok v Ostravské fakultní nemocnici – útok na území České republiky;
- útok na Nemocnici Dašt-e-Barči – záměrné zabíjení matek a novorozenců v porodnici ve snaze vyvolat co největší šok.

3.3 Musgrave Park Hospital (Severní Irsko, Belfast - 1991)

2. listopadu 1991 se vojenské křídlo nemocnice v Belfastu stalo cílem bombového teroristického útoku. Bomba explodovala v požárním únikovém východu, který vedl ze společenské místnosti v přízemí. Útoku napomohl zaměstnanec, který záměrně nechal odemknuté dveře. V místnosti bylo v danou chvíli devět lidí, kteří sledovali televizi. Zřítila se dvě patra nad daným místem. Byla zničena pohotovost, ARO a operační sál. (HODGETTS 1993)

Základní zhodnocení situace provedli dva lékaři. Jeden z nich sám sebe jmenoval důstojníkem pro mimořádné události a informoval civilní záchranné služby. Hasičská záchranná služba převzala kontrolu nad záchrannou operací. Civilní záchranné sužbě pomáhala armáda a dobrovolníci. Oblast byla obklíčena armádou. Z obavy z dalších útoků byla evakuována dvě oddělení. (HODGETTS 1993)

Zranění byli prioritizováni do tří skupin:

P1 – respirační problémy, popáleniny 60 % povrchu těla, protržená tympanická membrána

P2 – fraktury lebky a poranění mozku, ostatní popáleniny

P3 – čtyři kategorie lehčích zranění

Vzhledem k úzkému průchodu ze zasypaného místa, nebylo nutné prioritizovat mezi nejhůře postiženými pacienty, ale klasifikace se ve větší míře uplatnila u lehčích zranění. Chyběly třídící štítky, z tohoto důvodu nebyla kvalita dokumentace pacientů dostatečná. (HODGETTS 1993)

Provizorní resuscitační zařízení bylo zřízeno vedle zřícené budovy, další ošetřovna byla zřízena na radiologii, po příchodu pomoci z civilního křídla nemocnice byli další pacienti ošetřováni na ulici. Helikoptéry nebyly použity, protože vzdálenost k nejbližší nemocnici lépe obsloužily sanitky. (HODGETTS 1993)

Z laboratoří ve městě byla uvolněna zásoba krve 0 negativní (univerzální dárce).

Útok byl proveden Irskou republikánskou armádou v období konfliktu v Severním Irsku (blíže viz kapitola 5). Dva lidé zemřeli, dalších jedenáct bylo zraněno. Při vyšetřování bylo zjištěno, že explodovalo devět kilogramů semtexu. (HODGETTS 1993)

3.4 Nemocnice Kigali, Univerzitní nemocnice Butare, Psychiatrické centrum Ndera v Kigali (Rwanda – 1994/1995)

V devadesátých letech probíhala občanská válka ve Rwandě mezi majoritním kmenem Hutuů a minoritním kmenem Tutsiů. V rámci této občanské války docházelo k rozsáhlé genocidě Tutsiů a to i přímo v nemocnicích. (BINET, BIQUET, BOUCHET-SAULNIER, HOFMAN, TERRY a VILASANJUAN 2013)

Podle Lékařů bez hranic, které v oblasti působili, byli ranění soustředěni do Nemocnice Kigali. Posléze v průběhu roku 1994 nalézali ošetřené pacienty druhého dne zabité. Raněné i své kolegy zabíjel také zdravotnický personál, který pocházel z kmene Hutu. (JANIŠOVÁ 2014)

Nemocnice byla přesunuta do polních podmínek na okraj Kigali. Nemocnice se poté změnila v uprchlický tábor. (JANIŠOVÁ 2014)

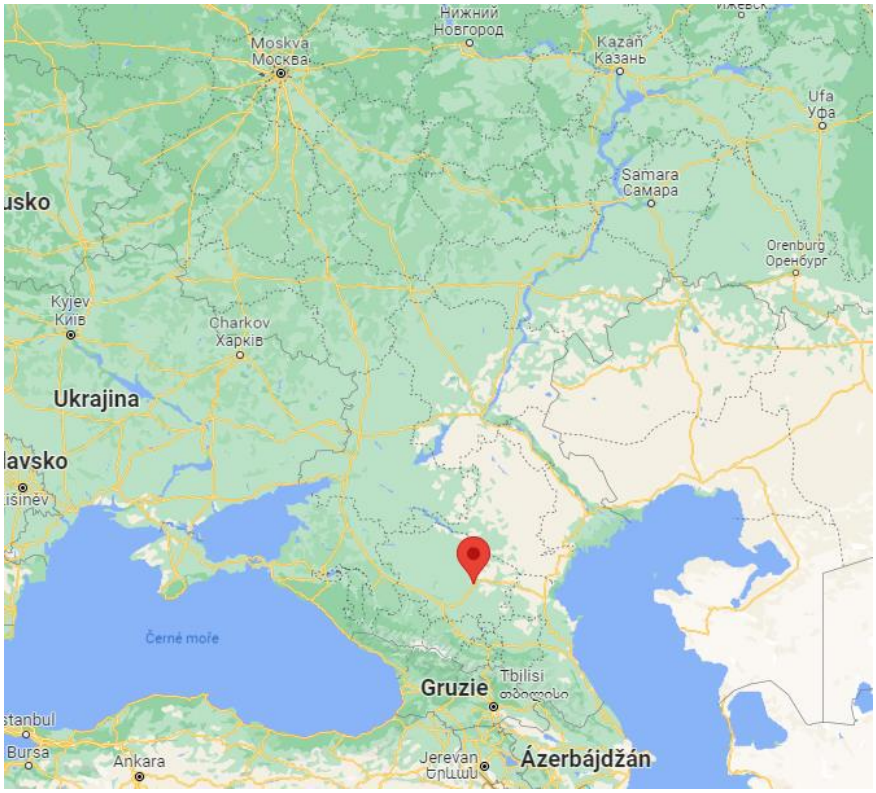
K zavraždění asi 750 mentálně hendikepovaných a přes tisíc uprchlíků došlo vojáky v Psychiatrickém centru Ndera, přibližně osm mil od Kigali. Nemocnice byla vedena belgickou charitativní organizací. Armáda obléhala nemocnici čtyři dny poté, co byl evakuován belgický zdravotnický personál. Kromě pacientů našlo v nemocnici útočiště asi 2000 dalších Tutsiů. Armáda pálila na nemocnici z automatických zbraní a házela granáty. Budova nemocnice byla značně poškozena, vybavení ukradeno nebo zničeno. (VIRET 2010)

K dalšímu masakru došlo 22. dubna 1995 v Butare, kde začaly síly rwandské vlastenecké armády (RPA) střílet do davu v nemocničním komplexu. Střelba trvala přes dvě hodiny, následkem bylo více než 150 mrtvých. (VIRET 2010; BIZIMANA 2020)

Kromě výše zmíněných probíhala útoků na nemocnice ještě celá řada. Vraždění Tutsiů bylo Organizací spojených národů prohlášeno za genocidu. (BIZIMANA 2020)

Bližší příčiny konfliktu ve Rwandě jsou popsány v kapitole 5.

3.5 Buďonnovská centrální oblastní nemocnice (Ruská federace – 1995)



Obrázek 5 – Poloha Buďonnovsku (maps.google.com 2021)

Buďonnovsk se nachází v Ruské federaci cca 100 km od hranic s Čečenskem. Útok na nemocnici se odehrál mezi 14. - 19. červnem 1995, tedy uprostřed tzv. první čečenské války mezi Ruskou federací a Čečenskem, která se odehrávala mezi lety 1994 a 1996. Útoku velel tehdy neznámý polní velitel Šamil Basajev. (Šamil Basajev byl původně příslušník sovětské armády, který se postavil na stranu čečenského hnutí za nezávislost, představoval radikální islamistický proud, jeho cílem bylo vytvořit z republiky islámský stát, podílel se na řadě teroristických útoků. Byl zabit při bombovém útoku ruských ozbrojených sil v roce 2006.) (BUKKVOLL 2007; POKALOVA 2015)

Prvotní příčinou útoku na nemocnici byl ozbrojený konflikt na daném území. Nejednalo se jen o útok na nemocnici, ale teroristé pronikli do města Buďonnovsk v několika vlnách. Část se vmísila do města v menších skupinkách, část v převlečení za ruské vojáky. Postupně se těmito a dalšími způsoby ocitlo ve městě 80-200 čečenských bojovníků. Po útoku na policejní stanici a administrativní budovy začali brát lidi na ulicích jako rukojmí a mířili s nimi k městské nemocnici. Tam shromáždili přes 1500

pacientů, zaměstnanců a civilistů, které dovedli z ulice. (BUKKVOLL 2007; POKALOVA 2015)

15. června předložili své požadavky. Večer nechal Basajev zabít prvního rukojmího, následně pět dalších. (ФИЛАТОВ 2020)

Speciální ruské vojenské síly se několikrát neúspěšně a s velkými ztrátami na životech civilistů pokusily o obsazení nemocnice. Podařilo se osvobodit 61 lidí. V mezičase teroristé propustili 150 dětí a těhotných žen.

18. června začal ruský předseda vlády vyjednávat se Šamilem Basajevem. Byly pozastaveny ruské ozbrojené akce v Čečensku. Teroristé vyměnili téměř většinu rukojmích za 123 dobrovolníků, které propustili 20. června po přesunu do Čečenska. (BUKKVOLL 2007)

Celkově si tento masivní útok vyžádal minimálně 129 obětí a 415 zraněných. Z pohledu teroristů byl útok úspěšný, pravděpodobně znamenal hlavní zvrat v první čečenské válce, protože došlo k pozastavení ruské ofenzivy, partyzáni v Čečensku se zmobilizovali, vysoký počet obětí posílil odpor ruské veřejnosti vůči čečenské válce, způsobil otřes na ruské politické scéně, z dosud neznámého Basajeva se stal vůdce radikálního křídla.

Celý útok byl ze strany teroristů záměrně silně medializován a ruskou i světovou sledován v přímém přenosu. Řada novinářů se nechala dobrovolně vyměnit za rukojmí.

Svůj vyzkoušený „modus operandi“ s útokem na měkké cíle později Basajev opakoval ve druhé čečenské válce, zejména při útoku na moskevské divadlo Dubrovka v roce 2002 a při beslanském školním masakru v roce 2004. Útok na nemocnici (tentokrát vojenskou) provedli čečenští bojovníci také v roce 2003 ve formě exploze v ruském Mozdogu za pomoci náklaďáku s výbušninou. (POKALOVA 2015)

Podrobnosti k první a druhé čečenské válce jsou uvedeny v kapitole 5.

3.6 Balad Ruz General Hospital, Baquba General Hospital (Irák, provincie Diyala - 2008, 2010)

Útoky na nemocnice po roce 2000 bývají často vedeny na více místech současně s tím, že jedním z cílů ve většině případů bývají složky policie, hasičů a zdravotnictví, nejčastěji

nemocnice. Cílem je způsobit vyšší ztráty na životech omezením přístupu zraněných k neodkladné péči.

V prvním případě byl sebevražedný bombový útok cílen na slavnostní průvod ve čtvrti Balad Ruz, která je známa svými restauracemi a obchody. Útok byl načasován na páteční pozdní odpoledne, kdy byly obchody plné lidí. Druhý bombový útok byl proveden na zdravotnický personál blízké nemocnice Balad Ruz General Hospital, která na místo vyslala sanitky a také na policisty, kteří rovněž přijeli pomáhat na místo útoku. (TOSINI 2010; UN High Commissioner for Refugees 2010)

Dalším příkladem je útok na Baquba General Hospital. Baquaba je hlavní město irácké provincie Diyala. První útok byl veden pomocí bomby nastražené v autě před vládní budovou a v blízkosti policejní stanice. O dvě minuty později došlo k dalšímu výbuchu další bomby poblíž stranického sídla bývalého premiéra Ibrahima al-Jaafariho v centrální části města. Zranění z těchto dvou explozí byli převáženi na centrální příjem do všeobecné nemocnice. Tam hodinu po prvních dvou útocích přijel sebevražedný atentátník, který vystupoval jako policista, v nastalém zmatku prošel na centrální příjem a odpálil nálož, kterou měl připevněnou na těle. Čtvrtou bombu se podařilo zneškodnit poblíž nemocnice. Útočníci nebyli vypátráni, z útoku je podezřelá organizace Al Kájdá, která dříve avizovala, že překazí volby. (TOSINI 2010; UN High Commissioner for Refugees 2010)

3.7 Fakultní nemocnice Ostrava – Útok osamělého střelce (2019)

Ráno 10. prosince 2019 došlo k tragické události na traumatologii ve Fakultní nemocnici v Ostravě. Muž s pistolí ČZ 75 v ruce začal procházet čekárny jednotlivých ambulancí a hledal, kde najde dostatečný počet pacientů. Na traumatologii byla v tu dobu plná čekárna lidí. Pachatel začal v 7:17 z nelegálně držené pistole střílet na čekající pacienty a jejich doprovod. Zbraň se mu několikrát zasekla, jelikož původně šlo o tak zvanou maketu v řezu, která byla dodatečně upravená ke střelbě. Během chvíle pachatel zastřelil šest osob. Na následky poranění zemřela později další osoba, dva zraněné se podařilo zachránit. (Jiroušková 2020; ČTK a Lesková 2019)

Mimořádná událost byla ohlášena 7:19 lékařem ambulance klinické úrazové chirurgie na linku 158. Na místo byly vyslány policejní hlídky, které se nacházely v blízkosti

nemocnice (dorazily cca 5 minut od přijetí oznámení), oddělení hlídkové služby, zásahové a speciální pořádkové jednotky, kynologové, kriminalisté, technici, krizoví interventi, policejní vyjednavač, psycholog a další složky IZS. Dále se zúčastnila letecká služba PČR a pyrotechnická služby. Díky rychlé práci a spolupráci s občany byla 8:55 známa totožnost pachatele (dvaačtyřicetiletého Ctirada Vitáska ze Zábřehu), později téhož dne byl vypátrán a spáchal sebevraždu. (Jiroušková 2020; ČTK a Lesková 2019)

Následně se zjistilo, že pachatel se na útok připravoval několik týdnů. Nebýt pistole, která se zasekávala, pravděpodobně by počet obětí byl vyšší.

Podle vyšetřovatelů bylo po vyhodnocení posudků, elektroniky, kamerových záznamů příčinou podezření pachatele, že má rakovinu a lékaři mu to záměrně zatajují a neléčí ho. Na základě toho se rozhodl spáchat rozšířenou sebevraždu. Bylo zjištěno, že dle posudků u něj nebyla rozvinuta žádná psychická porucha, jednalo se o úzkostný stav týkající se jeho zdravotního stavu. (Jiroušková 2020; ČTK a Lesková 2019)

3.8 Nemocnice Dašt-e Barči, (Afghánistán – 2020)

12. května 2020 vtrhli afghánští ozbrojenci do nemocnice Lékařů bez hranic Dašt-e Barči v Kábulu. Prvotní příčinou teroristického útoku je opět místo, kde probíhal ozbrojený konflikt. (Bonnot a MSF AFGANISTAN 2020)

Cílem byla od začátku porodnice. Tuto domněnku uvedli pracovníci z organizace Lékaři bez hranic při vyšetřování. Vycházeli z toho, že se v areálu nacházela řada dalších oddělení v různých budovách, ale ozbrojenci zamířili právě tam a začali vraždit ženy a děti. Porodnice v nemocnici Dašt-e Barči měla 55 lůžek a od roku 2014 se v ní narodilo 5401 dětí, patřila tedy mezi velká zařízení. (Bonnot a MSF AFGANISTAN 2020)

Daného dne bylo v porodnici 26 matek. Deseti z nich se spolu se zdravotníky podařilo ukrýt. Všechny zbylé byly zavražděny nebo postřeleny. Mezi jedenácti zastřelenými matkami byly tři na porodním sále. Zastřeleni byli také dva novorozenci a porodní asistentka. Pět dalších matek bylo zraněno, stejně jako dva novorozenci a tři pracovníci Lékařů bez hranic. Vedoucí programu Lékařů bez hranici Frederic Bonnot vypovídal, že zdi byly pokryté projektily, postup byl metodický. (Bonnot a MSF AFGANISTAN 2020)

Cílem útoku bylo šokovat veřejnost.

3.9 Kybernetické útoky na zdravotnická zařízení – nový fenomén

Předchozí kapitoly ukázaly vývoj násilných teroristických útoků na zdravotnická zařízení. Paralelně s posunem teroristických útoků do nových rovin se rozvinul další trend terorismu a tím jsou kybernetické útoky na zdravotnická zařízení. Ty se začaly objevovat v posledních pěti až deseti letech a představují odvrácenou stranu rozvoje komunikační a výpočetní techniky, na kterých se zdravotnická zařízení stala závislá. Ničivý dopad kybernetických útoků pociťují od roku 2019 ve větší míře také české nemocnice.

Definice kyberterorismu nejsou ujednocené. Za všechny vybírám tyto: „Jako kyberterorismus je označován promyšlený, politicky motivovaný útok organizovaných skupin, jednotlivců nebo tajných agentů namířený proti informačním sítím, počítačovým programům a datům.“ (Janczewski a Colarik 2005)

„Trestná činnost páchaná za primárního využití či cílení prostředků IT s cílem vyvolat strach či neadekvátní reakci. Používá se nejčastěji v kontextu extremisticky, nacionalisticky a politicky motivovaných útoků.“ (Jirásek, Novák a Požár 2015, s. 71)

Formy kyberterorismu mohou být psychologické (vyvolat strach a nejistotu) až skutečně destruktivní (narušení provozu, zničení systému).

Cílem může být snaha oslabit protivníka, zisk, dosažení politických cílů. O nebezpečí kyberterorismu se poprvé začalo mluvit na začátku 90. let, první útoky přišly ve druhé polovině 90. let, nejdříve ve formě tzv. „emailových bomb“, kterými se útočníci snažili zahltit systémy na tehdy málo výkonných serverech a sítích.

Hrozba kyberterorismu začala být brána skutečně vážně po útocích na Světové obchodní centrum v roce 2001 a postupně se dostalo procesu plánování obrany NATO. (Cyber defence, NATO 2021)

Existuje několik způsobů dělení útoků, jeden z přístupů rozlišuje lidský faktor (např. phishingové techniky, zejména sdělení přihlašovacích údajů nebo otevření podezřelých e-mailů, kliknutí na odkaz, který vede na škodlivý obsah) a technické chyby, případně nedostatky informačního systému.

V rámci kybernetických útoků je obtížné zjistit, zda se jedná skutečně o teroristický čin (=promyšlený, politicky motivovaný útok organizovaných skupin, jednotlivců nebo tajných služeb namířený proti informačním sítím), vyděračský útok pro peníze, nebo hru party hackerů, která si na nedostatečně zabezpečených institucích dokazuje a vylepšuje

své schopnosti. Například zdánlivý útok za cílem získání výkupného může být zástěrkou pro aktivity politických zájmových skupin.

Proto je v této kapitole abstrahováno od dělení kybernetických útoků na teroristické a jiné a tabulka 2 obsahuje útoky na zdravotnická zařízení, které byly nějakým způsobem významné nebo zajímavé, například tím, že způsobily vysokou škodu, upozornily na dosud neidentifikovaná rizika, nebo se dotýkaly České republiky.

Technik kybernetických útoků na zdravotnická zařízení je celá řada. Mezi nejčastější patří tyto:

- ransomware – vyděračský virus;
- malware – škodlivý virus;
- DDoS (Distributed Denial of Service) – přehlcení klíčových uzlů požadavky, na základě nichž se daný internetový bod a na něj napojené systémy (např. pošta) přehltí a přestanou pracovat;
- phishing – podvod postavený na lidské chybě – cílem je získat například přihlašovací údaje;
- využití chyb v softwaru.

Zejména phishigové techniky jsou jednoduché a účinné. Spočívají například v e-mailech, které imitují oficiální zprávu (například od IT administrátora), která vyzývá uživatele, aby nějakým způsobem poskytl citlivé údaje. Tím, že závisí na selhání lidského faktoru, jsou problematicky řiditelné. Mezi lidské chyby patří zejména sdělení přihlašovacích údajů nebo otevření podezřelých e-mailů, kliknutí na odkaz, který vede na škodlivý obsah.

Technické problémy souvisí se zastaralými počítačovým systémy, chybějícím antivirovým softwarem. Technickým problémům nahrává podfinancování zdravotnických zařízení.

Chyby v softwaru se nemusí omezit na klasické zdroje, jako jsou například webové stránky, ale také veřejně přístupné internetové sítě, kamery, chytré ledničky a televizory a bohužel také zdravotnické přístroje (například anestetické přístroje nebo inzulinové pumpy).

V tabulce 2 je přehled některých prvních velkých útoků. Byla zařazena také informace o zranitelnosti zdravotnického zařízení.

Ta bývají často opomíjena, ale ve skutečnosti mohou při nevhodném propojení posloužit jako vstup do systému (lednička na sesterně, kamera od bezpečnostního zařízení, „chytrý“ objednávkový panel u zasedací místnosti), případně jejich zneužití může ohrozit pacienta (anestetické přístroje, inzulinové pumpy).

Tabulka 2 – Přehled kyberteroristických útoků na zdravotnická zařízení/potenciálních útoků/zranitelností (Cimpanu 2019; ČTK a iDNES.cz 2020; ČTK a iROZHLAS 2020; Genovese 2021; Global Terrorism Database 2009-2021; Marsh 2017; Novotná 2021; Slouka 2020; Sweeney 2018)

Rok	***Místo***	***Bližší popis***	***Dopady***
2014	*USA, Boston*	*Útok na Bostonskou dětskou nemocnici – aktivista ze skupiny Anonymous.*	*Vyřazení systémů pečujících o děti a stránky pro dárce. Odhadované škody 600 tisíc dolarů.*
Květen 2017	*Velká Británie*	*Malware WannaCry nakazil Národní zdravotnickou službu ve Velké Británii.*	*Zásah minimálně 40 zařízení v Anglii a Skotsku. Zrušení všech naplánovaných operací a jiných výkonů (cca 20 000).*
2018	*Výzkumníci ze CyberMDX našli bezpečností hrozby u výrobků společnosti General Electric - GE Aestiva a GE Aespire (modely 7100 a 7900)*	*Objevení zranitelnosti některých medicinských zařízení GE, nedostatky v autorizaci vzdálených příkazů.*	*Hypotetické – výzkumníci zjistili, že příkaz může být využit k neautorizované změně na anestetických přístrojích (změna koncentrací kyslíku, oxidu uhličitého, oxidu dusného, případně jiných anestetických přísad, případně tlaku, ztlumení signalizačních údajů).*
Březen 2019	*Montpellier*	*Zaměstnanec otevřel e-mail s virem.*	*Infikování 600 počítačů (oddělené interní sítě zabránily přenosu na zbývajících 5400 počítačů).*
Prosinec 2019	*Nemocnice Rudolfa a Stefanie Benešov*	*Zašifrování dat na nemocničních serverech.*	*Rušení standardních ošetření i plánovaných operací, převod pacientů do okolních nemocnic, včetně pacientů z JIP. Náklady 40-60 milionů korun.*
Březen 2020	*Fakultní nemocnice Brno*	*Kryptovirus Defray*	*Rušení operací, převoz akutních pacientů do jiných nemocnic, ovlivnění provozu záchranné služby, ztráta administrativních a ekonomických dat, zničení objednávkového systému u dárců krve (pokles odběrů krve na polovinu). Ztráty v desítkách milionů.*
Březen 2020	*Psychiatrická nemocnice Kosmonosy*	*Kyberútok pomocí počítačového viru typu ransomware (ransom=výkupné) paralyzoval počítačový systém včetně kotelny, účtárny a kuchyně.*	*Počítače musely být odpojeny, péče o zaměstnance byla zajištěna.*
Duben 2020	*Fakulta nemocnice Ostrava* *Fakultní nemocnice Olomouc* *Další nemocnice*	*Malware (malware = škodlivý virus) CoVIPER*	*Útoky byly odraženy. K útokům vyjádřil americký ministr zahraničí Mike Pompeo, který před útoky na české nemocnice důrazně varoval.*

Pokračování tabulky na straně 28

Pokračování tabulky ze strany 27

Rok	***Místo***	***Bližší popis***	***Dopady***
Duben – červen 2020	*USA*	*Zaměstnanec Independence Blue Cross omylem na internetu zveřejnil informace cca 17000 pacientů.13*	*Únik informací.*
Listopad 2020 Düsseldorf	*Nemocnice v Düsseldorfu*	*Ransomware požadující výkupné*	*Z provozu byly vyřazeny systému společnosti, nemocnice nepřijímala ani pacienty ve vážném stavu. Jedna z převážených žen byla přesměrována na nemocnici do 30 kilometrů vzdáleného zařízení. Při převozu zemřela.*

V následujících kapitolách jsou podrobněji rozebrány kybernetické útoky na české nemocnice, protože jsou východiskem pro splnění druhého cíle a ověření hypotézy 2, která se týká připravenosti českých zdravotnických zařízení na kybernetický útok.

3.10 Útok na Nemocnici Rudolfa a Stefanie Benešov

Nemocnice Rudolfa a Stefanie Benešov je okresní nemocnice ve Středočeském kraji. Spádovost je přibližně 100 000 obyvatel, v létě se rozšiřuje ještě o desítky tisíc rekreantů, kteří do oblasti přijíždějí. Komplex zahrnuje 8 zdravotnických pavilonů a budovy správy a údržby. (Říha a Ballek 2018)

Útok na nemocnici Rudolfa a Stefanie v Benešově se odehrál 11. prosince 2019. Byl proveden pomocí takzvaného ransomwaru, který šifruje data. Pachatel zůstává neznámý. Jednalo se o součást organizovaného útoku na více institucí státní správy. (Novotná 2021)

Nemocnice dále přišla o objednávkový systém u dárců krve. Data o pacientech neunikla, došlo ale k jejich zašifrování, čímž byly ztraceny.

Nemocnice nebyla 20 dní v provozu, největší ztráta jí tak vznikla kvůli omezení lékařských výkonů, dále další prostředky vynaložila na zásah počítačových expertů. Celkově se ztráta nemocnice odhaduje na cca 60 milionů korun. (Novotná 2021)

Útok se obešel bez většího mediálního zájmu.

3.11 Útok na Fakultní nemocnici Brno

Fakultní nemocnice Brno sídlí ve čtvrti Bohunice. Její součástí je několik dalších pracovišť. Zajišťuje péči o občany města Brna a Jihomoravského kraje, dále pod ni spadá část pacientů ze zlínského a olomouckého kraje a také část kraje Vysočina. Jedná se o druhé největší zdravotnické zařízení v České republice. Zaměstnává přes tisíc lékařů, dva tisíce sester a dalších téměř šest tisíc zaměstnanců. Ročně je zde ošetřeno přes jeden milion obyvatel a hospitalizovány jsou desítky tisíc pacientů. (Fakultní nemocnice Brno 2017)

Hackerský útok začal 13. března ve dvě hodiny ráno, v době, kdy se české zdravotnictví snažilo vypořádat s první vlnou koronavirové krize.

Na základě vyšetřování bylo zjištěno, že se jednalo o více virů ze skupiny ransomware (vyděračský virus), které souběžně mapovaly síť, prolamovaly uživatelské účty, šifrovaly data. Následně byl zastaven celý standardní IT provoz, počítače byly odpojeny od sítě, lékaři nemohli operovat, pacienti byli převáženi do jiných nemocnic. V době útoku měla

nemocnice 2 500 koncových stanic, 1 000 terminálů, přes 250 serverů s desítkami informačních systémů a specializovaných aplikací, několik stovek laboratorních přístrojů, přes 6 500 uživatelů. IT podpora zahrnovala 50 specialistů. (Krajíčková 2021; Medical Tribune 2021)

Nemocnice využívá externí službu, která posloužila jako komunikační systém ke svolání krizového štábu. Byl povolán krizový IT manažer a zahájeny přípravy na nouzový chod nemocnice, tedy přípravu náhradních provozů IT bez použití datových sítí a zajištění urgentních výkonů.

Obnovení bazální podpory trvalo dva měsíce, základní provoz (většina specializovaných a doprovodných nástrojů) tři měsíce. Nemocnice přišla o kompletní vnitřní informační systém, data vědeckého významu, dokumenty a smlouvy, objednávkový systém dárců krve.

Řada dat se obnovovala ještě po roce. Celkové škody přesáhly 150 milionů korun, některá byla ztracena

Útok byl značně medializován, protože k útoku došlo v rámci první vlny koronavirové pandemie.

Případ dosud nebyl uzavřen. Je vedeno trestní řízení pro podezření z následujících deliktů:

- zločin vydírání;
- obecné ohrožení;
- neoprávněný přístup k počítačovému systému a nosiči informací.

Hackeři použili virus Defray, který je znám jako tak zvaný „vyděračský virus“, protože zašifruje data a útočníci za jejich dešifrování požadují výkupné. Útok pocházel ze zahraničí. Defray se zaměřuje právě na zdravotnická zařízení. (Krajíčková 2021)

3.12 Útok na Psychiatrickou nemocnici Kosmonosy

Psychiatrická nemocnice Kosmonosy je nejstarším psychiatrickým zařízením v České republice. Disponuje šesti sty lůžky a zaměstnává pět set pracovníků. Poskytuje ambulantní i hospitalizační péči. (Kotková 2019)

Čtrnáct dní po útoku na Fakultní nemocnici Brno, konkrétně v pátek 27. března byla napadena virem Psychiatrická nemocnice Kosmonosy. Jedná se o nemocnici pro dospělé pacienty, která ročně opatruje přes 2000 pacientů. (ČTK a iDNES 2020)

Na napadený počítačový systém byla napojena i kuchyně, kotelna, účetnictví. Bazální provoz byl převeden do papírové podoby, 70 % počítačů bylo zprovozněno po čtrnácti dnech. Příčinou byl pravděpodobně virus, který zašifroval data.

3.13 Útoky na nemocnice z dubna 2020

Pouhý měsíc po obrovském útoku na Fakultní nemocnici v Brně, se odehrála další série útoků na několik nemocnic v České republice. Nejčastěji byla v této souvislosti zmiňována Fakultní nemocnice Ostrava, Fakultní nemocnice Olomouc, Karlovarská krajská nemocnice a Nemocnice Pardubického kraje. (Magdoňová 2020; Magdoňová 2021)

Útočníci použili virus CoViper, který znemožňuje naběhnutí operačního systému. Nemocnice byly dopředu varovány Národním úřadem pro kybernetickou bezpečnost a Národní centrálou proti organizovanému zločinu a útoku se ubránily. (Magdoňová 2020; Magdoňová 2021)

Identita útočníků zůstala neznámá, společným prvkem byl virus typu malware (škodlivý virus). V tom je rozdíl mezi těmito útoky a předchozími útoky, při nichž byl použit vyděračský virus (ransomware). Útoky neunikly zahraničním pozorovatelům. Výrok ministra zahraničí Spojených států amerických naznačuje podezření z politického pozadí. Mike Pompeo prohlásil: „Vyzýváme toho, kdo je za to zodpovědný, aby se zdržel škodlivých kybernetických aktivit zaměřených proti českému zdravotnickému systému či podobné infrastruktuře na dalších místech.“ (ČTK a ČT24 2020)

3.14 Vývoj kybernetických útoků v České republice mezi lety 2019 – 2021

Národní úřad pro kybernetickou bezpečnost (NÚKIB) eviduje kybernetické incidenty. Podle informací, které zveřejnil NÚKIB, je zaznamenán zvyšující se tlak hackerů na české zdravotnictví. Konkrétně se jednalo:

- za rok 2019 o 6 útoků;

- za rok 2020 o 16 kybernetických útoků;
- ke konci října 2021 o celkem 24 kybernetických útoků. (NÚKIB 2021)

Za nárůstem podle NÚKIB stojí částečně skutečnost, že narostl počet nemocnic, které povinně tyto incidenty hlásí. (NÚKIB 2021)

To ale nevysvětluje celý nárůst. Podle společnosti Check Point, která se zabývá kybernetickou bezpečností, se v roce 2021 počet celosvětových kybernetických útoků zvýšil o 55 procent v porovnání s rokem 2020. V průměru jde celosvětově o 752 útoků týdně. (ČTK a iROZHLAS 2021; ČTK, NOVINKY a Miloslav FIŠER 2021)

4 METODIKA

V rámci práce hodnotím jak násilné teroristické útoky, tak nový fenomén kybernetických útoků, metodiky jsou proto níže rozděleny do dvou kapitol.

4.1 Metodika pro splnění prvního cíle

Pro splnění prvního cíle (analýza příčin, průběhu a následků teroristických útoků na zdravotnická zařízení) je použito metod deskripce a komparace. Jako zdroj pro zkoumání slouží materiály z veřejně dostupných zdrojů – knižní literatury a online zdrojů. Pro získání statistických dat používám Globální databázi terorismu (GTD). Globální databáze terorismu zahrnuje více než 200 000 teroristických útoků od roku 1970 do roku 2019. Je provozována Národním konsorciem pro studium terorismu a odezvu na terorismus – National Consortium for the Study of Terrorism and Responses of Terrorism (START) v USA.

Tato databáze nerozlišuje konkrétní instituce. Rozšířené vyhledávání najde na klíčové slovo všechny incidenty, při nichž je toto slovo použito, ale neumožňuje bližší specifikaci. Například klíčové slovo „hospital“ vrací nejen teroristické činy v nemocnicích a dalších zdravotnických zařízeních, ale všechny incidenty, při nichž bylo třeba někoho odvézt do nemocnice. Z tohoto důvodu je třeba vyfiltrované případy manuálně vytřídit a případy ze zdravotnických zařízení individuálně vybrat.

Klíčové slovo „hospital“ zobrazuje celkem 1 341 výsledků (celkovým teroristických útoků bylo od roku 1970 v databázi zaznamenáno 201 183).

Údaje jsou manuálně překopírovány do excelu kvůli možnosti filtrování. Výběr je omezen od roku 1985 do roku 2019 (novější údaje zatím v databázi nebyly uloženy) a všechny vrácené údaje jsou manuálně prověřeny, protože výběr dle klíčových slov zhruba ve 20 % případů odkazuje na jiné události, při nichž bylo nutné pacienty odvézt do nemocnic. Výsledkem je vytřídění útoků nemocnice.

Následně je očištěný soubor rozdělen na sedmileté intervaly, aby mohl být zkoumán vývoj v porovnatelných časových úsecích.

Dále je soubor rozdělen podle oblastí. Samostatné kategorie jsou přiděleny regionům, ve kterých se v období let 1985 - 2019 událo více než 20 incidentů. Zbytek světa je zařazen do kategorie Ostatní. Jednotlivé zkoumané oblasti:

- Blízký východ a severní Afrika;
- jižní Asie (Nepál, Srí Lanka, Indie, Pákistán, Afghánistán, Bangladéš);
- Jihovýchodní Asie (Filipíny, Thajsko, Indonésie);
- subsaharská Afrika;
- Jižní Amerika;
- východní Evropa (především Ukrajina a Rusko);
- ostatní.

Dále jsou přidána kritéria pro hodnocení průběhu:

- ozbrojený útok;
- atentát;
- bombový útok;
- útok na zařízení/infrastrukturu;
- únos;
- ostatní.

Důsledky v podobě ztrát na životech jsou kategorizovány v samostatné kategorii.

- počet obětí vyšší než 5;

Výsledky jsou sumarizovány do tabulek, ze kterých jsou vyvozovány trendy. Současně jsou výsledky porovnávány s ozbrojenými konflikty v dané oblasti v daném časovém intervalu vyhledaných dle literatury a je sledováno, zda mezi nimi existuje korelace, která by potvrdila hypotézu 1 „Násilné útoky na zdravotnická zařízení korelují s místy ozbrojených konfliktů.“

4.2 Metodika pro splnění druhého cíle

Druhý cíl (analýza kybernetických útoků na zdravotnická zařízení a připravenosti vybraných zdravotnických zařízení na kybernetický útok) je zkoumán metodou analýzy rizik. Jako eticky dostupný zdroj jsou zvoleny webové stránky, které jednak slouží jako vizitka daného zdravotnického zařízení, současně mohou v určitých případech sloužit

jako vstupní brána pro kybernetický útok a indikátor péče, jaké daná instituce věnuje IT záležitostem.

Nejdříve jsem vybral dle preference vyhledávače Google 69 českých zdravotnických zařízení, u kterých jsem zkoumal celkem 10 kritérií. Cílem bylo zjistit, zda některé z webových stránek těchto nemocnic obsahují chybu, která činí jejich internetové stránky zranitelnými a potenciálně mohou sloužit jako neoprávněný vstup do počítačového systému, případně mohou útočníkovi sloužit k jiné formě újmy. Dále jsem stejný test provedl také u 10 společností v soukromém nezdravotnickém sektoru a následně u největších světových nemocnic kvůli srovnání toho, jak si české nemocnice stojí v porovnání se soukromým nezdravotnickým sektorem a s největšími světovými nemocnicemi.

Základem zkoumání byla jednak analýza zabezpečení přenosu dat webových stránek a pak další kritéria, která byla zkoumána použitím nástroje Mozilla Observatory. Jedná se o online nástroj, který provádí analýzu zabezpečení webových stránek. Testuje nastavení šifer, přítomnost různých protokolů a zobrazuje také informace z dalších služeb. Mozilla Observatory zkoumá několik kritérií, které popisuji v následujících odstavcích. (The Mozilla Observatory 2016)

Kritéria pro lepší porozumění jejich závažnosti a možnosti ovlivnit bezpečnost webových stránek a potenciálně bezpečnosti nemocnice jako takové popisuji níže.

4.2.1 Zabezpečený přenos

Jako hlavní kritérium volím použití šifrované komunikace HTTPS místo nešifrované komunikace přes HTTP. HTTP, celým názvem Hypertext Transfer Protocol (hypertextový přenosový protokol), je internetový protokol, který slouží pro komunikaci se servery k přenosu různých souborů a informací. Samotný HTTP neumožňuje šifrování a zabezpečení dat. Pro zvýšení bezpečnosti se používá HTTPS, neboli Hypertext Transfer Protocol Secure (v překladu zabezpečený hypertextový přenosový protokol), který umožňuje mimo jiné ověření identity, důvěrnosti přenášených dat a jejich integrity. (Koďousková 2021)

Použití nešifrované komunikace HTTP místo šifrovaného protokolu HTTPS je vnímáno jako zásadní bezpečnostní chyba, která by se v dnešní době neměla vyskytovat. To může způsobovat příležitost k průniku do systému pomocí techniky, které se říká „man

in the middle“, což znamená česky „člověk uprostřed“ nebo „člověk mezi“. Podstatou je možnost sledovat nebo dokonce ovlivňovat komunikaci mezi účastníky.

Z tohoto důvodu se práce zaměřuje na identifikaci nemocnic, které stále používají pro webové stránky HTTP protokol a dále zkoumám další rizikové prvky v kombinaci s HTTP protokolem (například možnost zjištění hesla do systému, podstrčení falešných internetových stránek k vylákání dat).

4.2.2 Content Security Policy (zásady zabezpečení obsahu)

Content Security Policy (CSP), neboli zásady zabezpečení obsahu, umožňuje operátorům webových stránek obranu proti tzv. cross-site scriptingu (XSS), česky skriptování mezi weby. XSS útok je založen na tom, že je do dynamické stránky podstrčen kód, který bývá použit například k phishingu (podvodná technika k získávání citlivých údajů), poškození vzhledu stránek, nebo narušení bezpečnosti systému. CSP umožňuje kontrolu nad tím, odkud lze načíst prostředky na jejich webu a zabránit zranitelnostem vůči XSS útoku.

4.2.3 Cookies

Cookie je krátký textový soubor. Ten si v prohlížeči návštěvníka ukládá navštívená webová stránka a slouží k optimalizaci přístupu pro další návštěvu. Současně mohou cookies sloužit k útoku na webové stránky, opět například technikou XSS popsanou výše.

4.2.4 Cross-Origin Resource Sharing (sdílení zdrojů odjinud)

Cross-origin resource sharing (CORS), ve volném překladu sdílení zdrojů odjinud, slouží k nastavení přístupu cizích zdrojů k webovým stránkám. Správná implementace snižuje bezpečnostní riziko a čtení informací ze strany neoprávněných subjektů.

4.2.5 HTTP Public Key Pinning (připnutí veřejného klíče)

HTTP Public Key Pinning (HPKP), ve volném překladu připnutí veřejného klíče, je mechanismus zabezpečení, který umožňuje odolávat podvodným digitálním certifikátům.

4.2.6 HTTP Strict Transport Security (přísné zabezpečení přenosu HTTP)

Mechanismus umožňuje, aby webový server vynutil v prohlížeči komunikaci pomocí šifrovaného HTTPS připojení. Tím se eliminuje přenos dat nezabezpečeným HTTP protokolem. Pro použití je zásadním předpokladem vlastnictví SSL certifikátu, neboli Secure Socket Layer (česky uváděno jako SSL protokol). SSL protokol slouží k vytvoření bezpečného spojení, v rámci něhož je komunikace mezi serverem a klientem zabezpečena šifrováním.

4.2.7 Redirection (přesměrování)

Přesměrovávají zdroje z HTTP na stejnou verzi zabezpečeného HTTPS. Všechny stránky, které nejsou určeny pro veřejné využití, by měly http deaktivovat.

4.2.8 Referrer Policy (zásady odkazujícího serveru)

Pokud uživatel přejde na web pomocí hypertextového odkazu nebo je web načten z externího zdroje, prohlížeče informují cílový web o původu požadavků. To může sice být užitečné, na druhou stranu také nebezpečné. HTTP referrer policy umožňuje webům kontrolu nad tím, jak se do prohlížeče přenáší tyto informace.

4.2.9 Subresource Integrity (integrita podzrojů)

Tento nástroj chrání před útočníky, kteří upravují obsah knihoven JavaScript. Rizikem takových zásahů je změna obsahu stránek, který pochází z jiných zdrojů.

4.2.10 X-Content-Type Options

Nastavení X-Content_Type_Option zvyšuje bezpečnost uživatele před škodlivým obsahem před podstrčenými typy souboru. Příkladem může být například soubor, který se vydává za textový dokument, ale ve skutečnosti je to nějaký druh nebezpečného scriptu (část programu v podobě kódu).

4.2.11 X-Frame-Options

Nastavení X-Frame-Options chrání stránky před tzv. „clickjackingem“. „Clickjacking“ je technika, kdy si útočník založí podobnou stránku, na niž vloží obsah

napadené stránky a nad ni uloží další průhlednou vrstvu, která obsahuje škodlivé a nebezpečné odkazy.

4.2.12 X-XSS-Protection (ochrana proti skriptování mezi weby)

Hlavička X-XSS-Protection povoluje zabudovaný filtr proti cross-site scriptingu (skriptování mezi weby). Je vhodný pro uživatele starších prohlížečů, které ještě nepodporují CSP (content security policy – zásady zabezpečení obsahu).

Jako hlavní body výzkumu jsou použita následující kritéria:

- použití HTTP/HTTPS;
- použití HSTS;
- Content Security Policy;
- X-Content-Type Options;
- X-Frame-Options;
- X-XSS-Protections.

5 VÝSLEDKY

V rámci výsledků jsou v kapitole 5.1 sumarizovány výsledky související s násilnými teroristickými útoky a dále v kapitole 5.2 jsou shrnuty výsledky výzkumu zranitelnosti webových stránek vybraných nemocnic.

5.1 Cíl 1 - výsledky

V rámci prvního cíle byly zkoumány příčiny, průběh a následky teroristických útoků na zdravotnická zařízení pomocí Globální databáze terorismu. V tabulce 3 je sumarizován trend ověřující hypotézu příčiny teroristických útoků. Podle hypotézy 1 „Násilné útoky na zdravotnická zařízení korelují s místy ozbrojených konfliktů.“ Výsledky jsou porovnávány s místy válečných konfliktů

V tabulce 5 je zkoumán průběh teroristických útoků podle typu (například bombový útok, únos, atd.) a také důsledky z pohledu počtu více než pěti obětí.

5.1.1 Útoky na nemocnice podle oblastí

Podle sumarizace výzkumu je nejvyšší počet incidentů v oblasti Blízký východ a severní Afrika a současně se zvyšuje. Blízký východ je tradičně oblastí politického napětí, v daném období docházelo v oblasti k řadě konfliktů, které budou rozebrány v dalších kapitolách. Výrazný nárůst zaznamenala také oblast Jižní Asie zejména v souvislosti s válkou v Afghánistánu. Zvýšil se i počet útoků v subsaharské Africe.

Tabulka 3 – Útoky podle oblastí (vlastní)

	Incidentů	***Blízký východ a severní Afrika***	***Jižní Asie (Nepál, Srí Lanka, Indie, Pákistán, Afghánistán, Bangladéš)***	***Jihovýchodní Asie (Filipíny, Thajsko, Indonésie)***	***Subsaharská Afrika***	***Jižní Amerika***	***Východní Evropa (především Ukrajina a Rusko)***	***Ostatní***
1985 – 2019	***538***	***234***	***161***	***20***	***63***	***23***	***21***	***16***
Z toho:								
1985 – 1991	***46***	*8* *17 %*	*10* *22 %*	*2* *4 %*	*2* *4 %*	*15* *33 %*	*2* *4 %*	*7* *16 %*
1992 – 1998	***39***	*4* *10 %*	*9* *23 %*	*0* *0 %*	*13* *33 %*	*3* *8 %*	*3* *8 %*	*7* *18 %*
1999 – 2005	***31***	*9* *29 %*	*9* *29 %*	*5* *16 %*	*0* *0 %*	*2* *6 %*	*6* *20 %*	*0*
2006 - 2012	***117***	*37* *31 %*	*62* *53 %*	*1* *1 %*	*12* *10 %*	*3* *3 %*	*2* *2 %*	*0*
2013 - 2019	***305***	*176* *58 %*	*71* *23 %*	*12* *4 %*	*36* *11 %*	*0* *0 %*	*8* *3 %*	*2* *1 %*

5.1.2 Příčiny teroristických útoků na nemocnice - korelace válečných konfliktů s útoky na nemocnice

5.1.2.1 Období 1985 – 1991 (celkem 46 útoků)

Blízký východ a severní Afrika – 8 útoků

Blízký východ je častým místem teroristických útoků, protože se jedná o tradiční oblast napětí a konfliktů. V letech 1980 – 1988 probíhala irácko-íránská válka o území na ropu bohatému Chúzistánu, další příčinou byly náboženské spory mezi sunnity a šíity. (Durman 2009)

Jižní Asie – 10 útoků

Čtyři útoky v Jižní Asii (40 % útoků z daného období v Jižní Asii) se odehrály na Srí Lance, kde v letech 1983 – 2009 probíhala občanská válka. Válka začala v roce 1983 povstáním tzv. Tamilských tygrů, proti srílanské vládě. Jejich cílem bylo na severu a východě ostrova vytvořit samostatný stát. Občanská válka skončila v roce 2009 vítězstvím srílanských vládních vojsk.

Jižní Amerika – 15 útoků

Mezi lety 1985 a 1991 dosáhly vrcholů také útoky na nemocnice v Jižní Americe. Z nich sedm útoků (poměrem 47 %) bylo soustředěny v Peru, kde v té době působila maoistická organizace Světlá stezka, známá také pod názvem Komunistická strana Peru. Světlá stezka působila především mezi lety 1981 – 1990 s vrcholem aktivity právě v druhé polovině osmdesátých let. (Roku 1990, kdy organizace ovládala 19 departmentů z 24, se prezidentem Peru stal Alberto Fujimori, který proti Světlé stezce razantně zasáhl. V roce 1992 byl zadržen její vůdce, profesor filosofie Abimael Guzmán).

5.1.2.2 Období 1992 – 1998 (celkem 39 útoků)

Subsaharská Afrika – 13 útoků

Zvýšení počtu konfliktů v Subsaharské Africe ovlivnila občanská válka ve Rwandě, která se na počtu útoků ne nemocnice podílela 31 % (tři útoky ve Rwandě a jeden v Burundi). Občanská válka ve Rwandě byla vyvolána konfliktem mezi kmenem Hutu, který patřil ke vládnoucí vrstvě a příslušníky menšinového kmene Tutsiů (přibližně 10 % obyvatelstva).

Obrázek 6 – Poloha Rwandy (maps.google.com 2021)

Tento konflikt má své kořeny již v koloniální éře, kdy se po první světové válce stala Rwanda Belgickou kolonií. V této době se z řad Tutsiů začala rekrutovat místní elita, protože Tutsiové byli díky svým řídícím schopnostem dosazováni do řídících rolí, stali se tak řídícím etnikem. V roce 1931 byly zavedeny identifikační karty příslušnosti k jednotlivým etnikům a z Hutuů se stali občané druhé kategorie. Obrat přišel po druhé světové válce, kdy postupně docházelo k dekolonizaci. V roce 1959 došlo k tzv. Hutuské revoluci, po níž došlo k obratu a vylučování Tutsiů z politického i ekonomického života. Řada z nich odešla do exilu, zejména do sousední Ugandy, odkud v roce 1990 podnikala útoky na Rwandu a v roce 1992 tutsijská armáda získala převahu. V roce 1993 byla podepsána mírová dohoda, která znamenala ze strany Hutuů významné ústupky podmíněné zahraniční pomocí zemi, ale současně bývá považována na počátek občanské války, současně hutuský prezident Habyariman připravoval se svými vojenskými poradci genocidu Tutsiů. Byla spuštěna masivní propaganda, vedená extrémním duchu „buď zabiješ, nebo budeš zabit“ (Fujii 2004, s.103)

Přesto Hutuům chyběla vhodná příležitost ke spuštění genocidy. Tou se stalo sestřelení letounu prezidenta Habyarimana. Nikdy nebylo vyšetřeni jeho pachatelé, kterými mohla být i opozice Hutuů, která Habyarimanovi vyčítala jeho umírněnost. Tato událost vedla k vojenskému převratu, po kterém se do čela Rwandy dostalo radikální křídlo Hutuů, kteří spustili genocidu, které se účastnily všechny společenské vrstvy. Příčiny byly obdobné jako při nástupu fašismu v Německu: dehumanizace Tutsiů, chudoba, schopnost médií vytvářet kolektivní reakce, nenávist a paranoia i obava umírněných Hutuů z represí v případě, že se k zabíjení nepřipojí. Tutsiové se shromažďovali na místech, která tradičně ve válečných konfliktech požívají určité ochrany – kostely, školy, zdravotnická zařízení. I na ně se však soustředily teroristické útoky.

Právě útoky na nemocnice ve městě Butare a hlavní městě Kigali patřily mezi nejkrvavější (přes 100 obětí) – viz kapitola 3.

Obrázek 7 – Oblast Kigali a Butare (maps.google.com 2021)

Další dva útoky (15 % ze všech útoků v Subsaharské Africe ve sledovaném období) připadají na Sierru Leone, kde od roku 1991 do roku 2002 probíhala občanská válka, příčiny byly ekonomické (2/3 obyvatel pod hranicí chudoby), mocenské (povstalci z Jednotné revoluční fronty za pomoci pozdějšího liberijského prezidenta Taylora chtěli roku 1991 svrhnout vládu prezidenta Momoha), boj o suroviny (rebelové ovládli diamantové doly a domorodce donutili k otrockým pracem).

Ke dvěma útokům došlo také v Jihoafrické republice. Dané období lze v Jihoafrické republice označit jako končící etapu vlády apartheidu. (V roce 1994 vyhrál volby Africký národní kongres a bojovník proti apartheidu Nelson Mandela se stal prezidentem Jihoafrické republiky.)

Jižní Asie – 9 útoků

V oblasti Jižní Asie se opět jednalo o útoky na Srí Lance (33 %), kde stále probíhala občanská válka započatá povstáním tzv. Tamilských tygrů. Více útoků se odehrálo v Pákistánu (44 %), který je dlouhodobě politicky nestabilní a kde třetina obyvatel žije pod hranicí z chudoby. Období 1992-1998 bylo poznamenáno mimo jiné vládní krizí. V roce 1993 byla premiérkou opakovaně zvolena Bénázir Bhutová (poprvé zvolena v roce 1988), která byla v roce 1990 sesazena. V roce 1996 musela opět odstoupit kvůli podezření z korupce a v roce 1998 odešla do exilu do Dubaje.

Východní Evropa / Ostatní – 10 útoků

Od roku 1994 probíhala tzv. první čečenská válka. Její kořeny sahají k rozpadu Sovětského svazu, po němž Čečensko v roce 1991 vyhlásilo nezávislost, která nebyla mezinárodně uznána. V období 1992 – 1993 probíhala čečenská občanská válka, kdy se čečenská opozice vyzbrojená Ruskem pokusila svrhnout prezidenta Dudajeva. V prosinci 1994 zaútočila Ruská federace na Groznyj a do té doby rozdělená společnost se přiklonila k Dudajevovi, přes zničení čečenského letectva narazily ruské pozemní jednotky na tuhý odpor čečenských vojáků. (Moltaš 2014; Souleimanov 2011)

V rámci této války došlo v roce 1995 k útoku na ruské město Buďonnovsk, kde byla obsazena nemocnice, díky čemuž získali povstalci značné výhody, které jim umožnily zkonsolidovat síly. Následoval překvapivý útok Šamila Basajeva na Groznyj, který byl v té době ovládán ruskými vojáky. Poté čečenský premiér Machadov a ruský generál Lebeď Chasavjurtské dohody, které znamenaly demilitarizaci a stažení ruských jednotek z Čečenska. (Moltaš 2014; Souleimanov 2011)

5.1.2.3 Období 1999 – 2005 (31 útoků)

Východní Evropa/Ostatní (6 útoků)

V letech 1999-2009 probíhala druhá čečenská válka. Začala ofenzívou tehdejšího předsedy vlády Vladimíra Putina, kterému rychlý postup, během něhož obsadila ruská armáda hlavní město Groznyj, vynesl prezidentský úřad. (Moltaš 2014; Souleimanov 2011)

Po roce 2000 se čečenští ozbrojenci uchýlili ke guerillové válce, souběžně s tím koreloval počet teroristických ve východní Evropě, zejména v Ruské federaci. Jednalo se například o bombový útok čečenských separatistů v roce 2003, kdy sebevražedný atentátník v kamionu narazil na nemocnici v ruském městě Mozdok, v severní Osetii. Výbuch zcela zničil čtyřpatrovou budovu a zabil 50 lidí. (Moltaš 2014; Souleimanov 2011)

Obrázek 8 – (Vojenská nemocnice v Mozdogu 2003)

Útoků bylo více než v první čečenské válce, trendem je, že se útoky na nemocnice objevují s určitým zpožděním po zahájení konfliktu.

V daném období probíhala takzvaná Růžová revoluce v Gruzii (rok 2003), jejímž výsledkem bylo svržení prezidenta Eduarda Ševardnadzeho a jeho nahrazení novým prezidentem Michailem Saakašviliim po nových volbách v březnu 2004.

Další z revolucí se začala v roce 2004 na Ukrajině. Tak zvaná Oranžová revoluce (podle barvy opozičního bloku Naše Ukrajina) se rozběhla po druhém kole prezidentských kvůli sporům o jejich výsledky. Opozice vedená Viktorem Juščenkem dosáhla opakování voleb a její vůdce Viktor Juščenko se stal prezidentem. (Svetsova 2006)

V roce 2005 vypukla Tulipánová revoluce (někdy označována také jako Žlutá revoluce) v Kyrgyzstánu po vyhlášení druhého kola parlamentních voleb. Prezident Akajev vydal příkaz k rozehnání demonstrace, ale následně byl nucen ustoupit a rezignoval. Prezidentem byl jmenován vůdce opozice Bakijev, který byl ale po pěti letech také sesazen.

Jižní Asie – 9 útoků

V roce 2001 začala válka v Afghánistánu. Také u ní se projevilo zpoždění teroristických útoků na nemocnice oproti začátku konfliktu. Válka v Afghánistánu probíhala v letech 2001 – 2021 a začala v reakci na útoky z 11. září 2001. Paradoxně se v období do roku 2005 počet útoků na nemocnice v regionu výrazně nezvýšil oproti předchozímu období – byl zaznamenán jeden útok z roku 2003. Ke zvýšenému nárůstu útoků došlo až v období následujícím, přesto je vidět jasná korelace mezi válkou v Afghánistánu a pozdějšími útoky na nemocnice v tomto regionu.

Na číslech teroristických útoků na zdravotnická zařízení se například projevilo napětí v Nepálu, které panovalo po masakru královské rodiny v roce 2001.

Nejvíce byly teroristické útoky v daném období ovlivněny napětím mezi Indií a Pákistánem, například tzv. Kárgilskou válkou, která probíhala mezi květnem a července roku 1999 v kašmírském Kárgilu. Válku vyprovokoval přechod pákistánských vojáků a kašmírských bojovníků za hranici mezi oběma zeměmi. Na to zareagovala indická armáda v kombinaci pozemních sil a letectva. Do války se také vložily mezinárodní diplomatické síly. Nakonec se pákistánské jednotky stáhly za tzv. linii kontroly.

Blízký východ - 9 útoků

Tradiční oblastí napětí, která se projevuje na teroristických útocích na nemocnice, je Blízký východ, což nebylo výjimkou ani pro nemocnice v relativně klidném období let 1999-2005. Již se začínaly projevovat první dopady války v Iráku (Druhá válka v Zálivu), která začala v roce 2003 a skončila v roce 2011.

5.1.2.4 Období 2006 – 2012 (117 útoků)

Dané období je ve znamení výrazného nárůstu útoků na nemocnice. Z toho se naprostá většina odehrávala na Blízkém východě v Jihovýchodní Asii.

Jižní Asie – 62 útoků

Ve zkoumaném období se jednalo o teroristické útoky v Afghánistánu ve spojitosti s válkou v Afghánistánu, která začala jako odveta za útoky 11. září 2001. Tyto útoky se projevily se zpožděním od začátku konfliktu, jak bylo popsáno v předchozí kapitole.

Neustávající napětí mezi Indií a Pákistánem se také negativně projevilo na neklidu a teroristických útocích v oblasti Jihovýchodní Asie. Několik útoků zaznamenala také Srí

Lanka, kde do roku 2009 stále probíhala občanská válka popsaná v předchozích obdobích.

Východní Evropa/Ostatní – 2 útoky

Situaci ve východní Evropě stále ovlivňovala doznívající druhá čečenská válka.

Blízký východ – 37 útoků

Blízký východ se nacházel v atmosféře probíhající války v Iráku. 29 útoků z tohoto období, tedy 78 % teroristických útoků na nemocnice, se odehrálo právě v Iráku.

Dále Blízký východ a severní Afriku ke konci daného období ovlivnilo tzv. Arabské jaro, tedy vlna protestů a revolucí, které probíhaly ve většině arabských států (Tunisko, Alžírsko, Egypt, Jemen, Jordánsko, Libye, Maroko, Omán, Saúdská Arábie, Sýrie, Bahrajn) mezi lety 2010 – 2012. Jejich odraz můžeme vidět na teroristických útocích v Sýrii, kde se situace přelila v občanskou válku (4 útoky), Alžíru (1 útok), Jemenu (2 útoky), ostatní se projevily se zpožděním od začátku konfliktu, jejich dopady budou popsány v dalším období. Důvody zpoždění teroristických na zdravotnická zařízení proti začátku konfliktu budou analyzovány v kapitole 6.

5.1.2.5 Období 2013 – 2019

Východní Evropa – 8 útoků

Teroristické útoky na nemocnice ve východní Evropě se z 90 % odehrávaly na Ukrajině, kde byly ovlivněny válkou na východní Ukrajině a anexí Krymu Ruskou federací.

Jižní Asie – 71 útoků

Ostatní oblasti byly setrvale ovlivněny konflikty z předchozích období. Pro oblasti Jižní Asie se stále jednalo o válku v Afghánistánu a nekončící napětí mezi Indií a Pákistánem.

Subsaharská Afrika – 36 útoků

Nárůst v subsaharské Africe se týkal především Nigérie a Somálska. V Nigérii došlo k sérii masových vražd spáchaných skupinou Boko Haram v nigerijském městě Baga (označováno také jako masakr v Baze). Bylo zničeno nejméně 16 měst, 35 tisíc lidí muselo opustit své domovy, hnutí Boko Haram získalo kontrolu nad většinou nigerijského státu

Borno. Boko Haram byla původně umírněná organizace, která vznikla v roce 2002. Po roce 2009 se radikalizovala, jejím cílem se stalo vytvořit z Nigérie muslimský stát založený na striktním výkladu práva šaria. Do roku 2014 ovládla většinu území severovýchodní Nigérie, armády Nigérie, Kamerunu, Čadu a Nigeru ji donutily ke stažení do základen na neprostupných územích, odkud podniká teroristické útoky. (Adebayo 2014)

K dramatickému zvýšení teroristických útoků došlo na Blízkém východě a severní Africe, více v přiložené tabulce:

Tabulka 4 - Počet útoků na nemocnice na Blízkém východě a v severní Africe v letech 2013 – 2019 (vlastní)

Stát	***Počet útoků***
Egypt	*8*
Irák	*41*
Libanon	*1*
Libye	*36*
Saudská Arábie	*3*
Sýrie	*34*
Turecko	*5*
Jemen	*48*
Celkem	**176**

Tento výčet je spojen s dozvuky tzv. Arabského jara, současně potvrzuje trend zpožděných reakcí teroristických útoků na nemocnice na válečné napětí. Mezi konkrétní ozbrojené konflikty patřila občanská válka v Sýrii (20 % všech útoků), protesty v Turecku (2013), občanská válka v Lybii (začátek 2014, celkem 20 % útoků, vojenská intervence v Jemenu (od 2015). Vojenskou intervenci v Jemenu zahájila Saúdská Arábie v čele mezinárodní vojenské intervence. Jedná se o pokračování boje mezi sunnity (zejména Saúdská Arábie) a šíity (Írán). Svou daň si vybrala i probíhající válka v Iráku (23 % všech útoků tohoto období).

5.1.3 Průběh teroristických útoků na zdravotnická zařízení - korelace válečných konfliktů s útoky na nemocnice

Proporce průběhu útoku se v čase mění. Většina kategorií osciluje kolem jednotek a nižších desítek procent. Od přelomu tisíciletí se zvýšil počet bombových útoků a explozí.

Tabulka 5 – Útoky na nemocnice podle průběhu útoku (vlastní)

	Incidentů	***Minimálně 5 obětí***	***Ozbrojený útok***	***Atentát***	***Bombový útok / exploze***	***Útok na zařízení / infrastrukturu***	***Únos / rukojmí***	***Neozbrojený a neznámý***
1985 – 2019	***538***	***76*** ***14 %***	***89*** ***17 %***	***18*** ***3 %***	***337*** ***63 %***	***14*** ***3 %***	***61*** ***11 %***	***19*** ***3 %***
Z toho:								
1985 – 1991	***46***	*3* *7 %*	*8* *17 %*	*10* *22 %*	*20* *43 %*	*4* *9 %*	*3* *7 %*	*1* *2 %*
1992 – 1998	***39***	*8* *21 %*	*12* *31 %*	*7* *18 %*	*11* *28 %*	*2* *5 %*	*3* *8 %*	*4* *10 %*
1999 – 2005	***31***	*11* *35 %*	*9* *29 %*	*0* *0 %*	*21* ***68 %***	*0* *0 %*	*0* *0 %*	*1* *3 %*
2006 - 2012	***117***	*16* *15 %*	*14* *12 %*	*0* *0 %*	*92* ***79 %***	*1* *1 %*	*8* *7 %*	*2* *1 %*
2013 – 2019	***305***	*38* *12 %*	*46* *15 %*	*1* *0 %*	*193* ***64 %***	*7* *2 %*	*47* *15 %*	*11* *4 %*

Za povšimnutí stojí hlavní trend, tedy zvyšující se počet teroristických útoků.

Tabulka 6 – Podíl útoků na nemocnice na celkových teroristických útocích (vlastní)

	Teroristických incidentů celkem	***Incidentů v nemocnicích***	***% v nemocnicích***
1985 – 2019	***177 114***	***538***	***0,3 %***
Z toho:			
1985 – 1991	*25 570*	*46*	***0,18 %***
1992 – 1998	*18 798*	*39*	***0,21 %***
1999 – 2005	*10 920*	*31*	***0,28 %***
2006 – 2012	*33 950*	*117*	***0,34 %***
2013 – 2019	*87 876*	*305*	***0,35 %***

Z výše uvedené tabulky vyplývá, že se počet útoků na nemocnice zvyšuje. Zvyšuje se počet teroristických útoků obecně, což by samo o sobě při stejné proporci vedlo ke zvýšení počtu útoků na nemocnice.

Současně kontinuálně roste podíl útoků na zdravotnická zařízení na celkovém počtu teroristických útoků. Mezi lety 1985 a 2019 se podíl zdvojnásobil.

5.2 Cíl 2 - výsledky

V rámci 2. cíle byla prováděna analýza kybernetických útoků na zdravotnická zařízení a připravenosti vybraných zdravotnických zařízení na kybernetický útok, jako zdroj byly zvoleny webové stránky nemocnic, které slouží jako první indikátor péče, jakou jednotlivé instituce věnují IT systému. Byl zvolen nástroj Mozilla Observatory, který zkoumá kritéria, která jsou blíže popsána v kapitole 4 věnované metodám.

Zkoumání bylo provedeno ve třech oblastech. V první je zkoumána zranitelnost českých nemocnic v období květen – srpen 2021. U nejzávažnějšího kritéria, které se týká šifrované komunikace, byl výzkum znovu zopakován v září 2021 – listopadu 2021, aby bylo zjištěno, zda došlo ke zlepšení.

V další části této kapitoly je stejné zkoumání provedeno na největších světových nemocnicích, aby bylo docíleno srovnání s tím, jak si v porovnání bezpečnosti internetových stránek stojí České nemocnice v porovnání se zahraničím. V poslední části je stejné porovnání provedeno u významných zástupců českých soukromých nezdravotnických subjektů pro porovnání sektoru zdravotnictví se soukromým nezdravotnickým sektorem.

5.2.1 Zkoumání zabezpečení webových stránek českých nemocnic pomocí nástroje Mozzila Observatory

Tabulka 7 – Zkoumání zabezpečení webových stránek českých nemocnic nástrojem Mozzila Observatory (vlastní, pojmy vysvětleny v kapitole 4.2)

Název nemocnice	*Cookies*	*Cross-origin resource sharing*	*HSTS*	*Redirection*	*Referrer Policy*	*Subresouce Integrity*	*X-Content-Type Options*	*X-Frame-Options*	*X-XSS-Protection*	*HTTPS*
Nemocnice AGEL Šternberk	*x*	*ok*	*x*	*Ok*	*-*	*X*	*X*	*X*	*x*	*ok*
Poliklinika Bílovec, s.r.o.	*-*	*ok*	*x*	*X*	*-*	*-*	*X*	*X*	*x*	*x*
Nemocnice Blansko	*x*	*ok*	*x*	*Ok*	*-*	*X*	*X*	*X*	*x*	*ok*
Psychiatrická nemocnice Bohnice	*Ok*	*ok*	*x*	*Ok*	*-*	*-*	*X*	*X*	*x*	*ok*
Bohumínská městská nemocnice, a.s.	*X*	*ok*	*x*	*X*	*-*	*x*	*x*	*X*	*x*	*x*
Fakultní nemocnice Brno	*Ok*	*ok*	*x*	*Ok*	*-*	*-*	*ok*	*ok*	*ok*	*ok*
Městská nemocnice Čáslav	*-*	*ok*	*x*	*X*	*-*	*-*	*x*	*ok*	*x*	*x*
Městská nemocnice Duchcov	*-*	*ok*	*x*	*X*	*-*	*-*	*x*	*x*	*x*	*x*
Nemocnice Dvůr Králové nad Labem	*-*	*ok*	*x*	*Ok*	*-*	*-*	*x*	*ok*	*x*	*ok*
Fakultní nemocnice Ostrava	*Ok*	*ok*	*x*	*X*	*ok*	*x*	*ok*	*ok*	*ok*	*ok*
Nemocnice ve Frýdku-Místku	*X*	*ok*	*x*	*x*	*-*	*-*	*x*	*x*	*x*	*x*
Nemocnice Havířov, p.o.	*-*	*ok*	*x*	*x*	*-*	*-*	*x*	*x*	*x*	*x*
Nemocnice Havlíčkův Brod	*X*	*ok*	*x*	*x*	*-*	*x*	*x*	*x*	*x*	*x*
Bílovecká nemocnice, a.s.	*X*	*ok*	*x*	*x*	*-*	*x*	*x*	*x*	*x*	*x*
Nemocnice TGM Hodonín	*X*	*ok*	*ok*	*ok*	*-*	*x*	*ok*	*ok*	*ok*	*ok*
Nemocnice Hranice a.s.	*X*	*ok*	*x*	*ok*	*-*	*x*	*x*	*x*	*x*	*ok*
Vysočinské nemocnice, s.r.o.	*X*	*ok*	*x*	*ok*	*-*	*x*	*x*	*x*	*x*	*ok*
Nemocnice Ivančice, p.o.	*X*	*ok*	*x*	*x*	*-*	*x*	*x*	*x*	*x*	*x*
Nemonice Jihlava, p.o.	*-*	*ok*	*x*	*ok*	*ok*	*-*	*ok*	*ok*	*x*	*ok*
MMN, a.s. Jilemnice	*X*	*ok*	*x*	*ok*	*-*	*-*	*x*	*ok*	*x*	*ok*

Pokračování tabulky na straně 53

Pokračování tabulky ze strany 52

Nemocnice Kadaň s.r.o.	*Ok*	*ok*	*x*	*ok*	*-*	*x*	*x*	*ok*	*x*	*ok*
Oblastní nemocnice Kladno, a.s.	*-*	*ok*	*x*	*x*	*-*	*-*	*x*	*x*	*x*	*x*
Oblastní nemocnice Mladá Boleslav, a.s.	*x*	*ok*	*x*	*x*	*-*	*x*	*ok*	*x*	*x*	*x*
Kroměřížská nemocnice a.s.	*x*	*ok*	*x*	*ok*	*-*	*x*	*x*	*x*	*x*	*ok*
Nemocnice Kyjov, p.o.	*x*	*ok*	*ok*	*ok*	*-*	*x*	*ok*	*ok*	*ok*	*ok*
Nemocnice Litoměřice, o.z.	*ok*	*ok*	*x*	*ok*	*-*	*-*	*ok*	*x*	*ok*	*ok*
Masarykova nemocnice Rakovník	*x*	*ok*	*x*	*ok*	*-*	*-*	*x*	*x*	*x*	*ok*
Nemocnice s poliklinikou Mělník	*-*	*ok*	*ok*	*ok*	*-*	*x*	*x*	*x*	*x*	*ok*
Městská nemocnice Ostrava, p.o.	*x*	*ok*	*x*	*ok*	*-*	*x*	*x*	*x*	*x*	*ok*
Nemocnice Milosrdných bratří, p.o. Brno	*x*	*ok*	*x*	*ok*	*-*	*-*	*x*	*x*	*x*	*ok*
Nemocnice Milosrdných sester sv. Vincence de Paul Kroměříž	*-*	*ok*	*x*	*x*	*-*	*-*	*x*	*x*	*x*	*x*
Nemocnice následné péče Moravská Třebová	*x*	*ok*	*x*	*ok*	*-*	*-*	*x*	*x*	*x*	*ok*
Fakultní nemocnice v Motole	*x*	*ok*	*x*	*ok*	*-*	*x*	*x*	*x*	*x*	*ok*
Mulačova nemocnice, s.r.o. Plzeň	*-*	*ok*	*x*	*x*	*-*	*-*	*x*	*x*	*x*	*x*
Nemocnice Na Františku	*-*	*ok*	*x*	*x*	*-*	*x*	*x*	*x*	*x*	*x*
Nemocnice Na Homolce	*x*	*ok*	*ok*	*ok*	*ok*	*x*	*ok*	*ok*	*ok*	*ok*
Levitovo centrum následné péče Hořice	*x*	*ok*	*x*	*x*	*-*	*x*	*x*	*ok*	*x*	*x*
Nemocnice následné péče Praha	*-*	*ok*	*x*	*ok*	*-*	*x*	*x*	*x*	*x*	*ok*
Nemocnice Nové Město na Moravě	*x*	*ok*	*x*	*ok*	*ok*	*-*	*ok*	*x*	*x*	*ok*
Nemocnice Nymburk, s.r.o.	*-*	*ok*	*x*	*x*	*-*	*-*	*x*	*x*	*x*	*x*
Fakultní nemocnice Olomouc	*x*	*ok*	*x*	*ok*	*-*	*x*	*x*	*ok*	*x*	*ok*
Pardubická nemocnice	*x*	*ok*	*x*	*x*	*-*	*x*	*ok*	*ok*	*ok*	*ok*

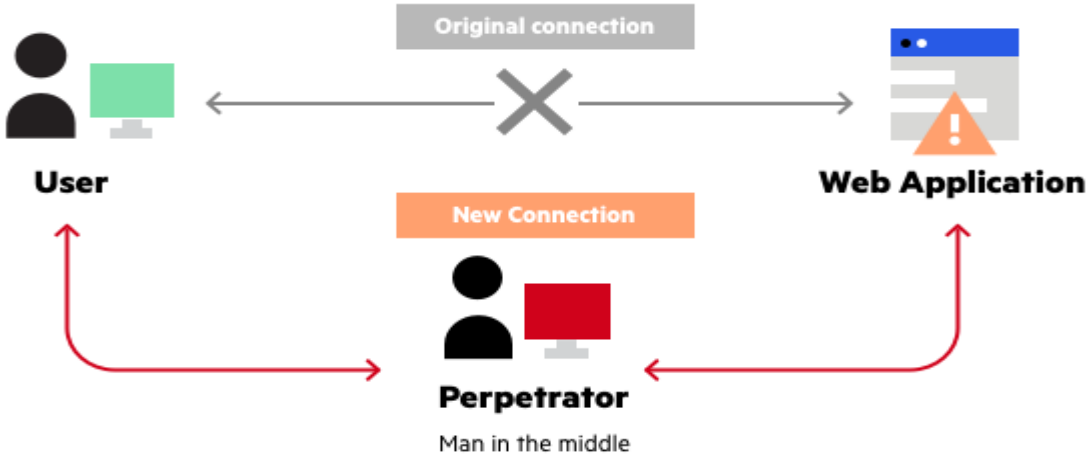
Pokračování tabulky na straně 54

Pokračování tabulky ze strany 53

Nemocnice Pelhřimov, p.o.	-	*ok*	*x*	*x*	-	-	*x*	*x*	*x*	*x*
Nemocnice Roudnice nad Labem	-	*ok*	*x*	*ok*	-	*x*	*x*	*x*	*x*	*ok*
Nemocnice Prachatice, a.s.	*x*	*ok*	*x*	*x*	-	*x*	*x*	*x*	*x*	*ok*
Oblastní nemocnice Příbram, a.s.	*x*	*ok*	*x*	*x*	-	-	*x*	*x*	*x*	*ok*
Psychiatrická nemocnice Havlíčkův Brod	*x*	*ok*	*x*	*ok*	-	*x*	*x*	*x*	*x*	*ok*
Psychiatrická nemocnice v Kroměříži	-	*ok*	*x*	*x*	-	-	*x*	*x*	*x*	*x*
Psychiatrická nemocnice v Opavě	-	*ok*	*x*	*x*	-	-	*x*	*ok*	*x*	*x*
Rehabilitační nemocnice Beroun	*x*	*ok*	*ok*	*ok*	-	*x*	*x*	*x*	*x*	*ok*
Nemocnice Slaný	*x*	*ok*	*x*	*ok*	-	*x*	*x*	*x*	*x*	*ok*
Městská nemocnice Slavičín	-	*ok*	*ok*	*ok*	-	*x*	*ok*	*x*	*x*	*ok*
Nemocnice Strakonice, a.s.	*x*	*ok*	*x*	*x*	-	*x*	*x*	*x*	*x*	*x*
Nemocnice Šumperk, a.s.	*x*	*ok*	*x*	*ok*	-	*x*	*ok*	*ok*	*ok*	*ok*
Nemocnice Tábor, a.s.	-	*ok*	*x*	*ok*	-	*x*	*x*	*x*	*x*	*ok*
Fakultní Thomayerova nemocnice	*ok*	*ok*	*x*	*ok*	-	*x*	*x*	*x*	*x*	*ok*
Nemocnice Tišňov	*x*	*ok*	*x*	*x*	-	-	*ok*	*ok*	*ok*	*ok*
Krajská nemocnice Tomáše Bati, a.s.	*x*	*ok*	*ok*	*ok*	-	*x*	*ok*	*ok*	*x*	*ok*
Nemocnice Třebíč, p.o.	*x*	*ok*	*x*	*ok*	-	*x*	*x*	*x*	*x*	*ok*
Nemocnice Třinec, p.o.	*x*	*ok*	*x*	*ok*	-	*x*	*x*	*x*	*x*	*ok*
Oblastní nemocnice Trutnov, a.s.	-	*ok*	*x*	*ok*	-	-	*x*	*ok*	*x*	*ok*
Orlickoústecká nemocnice	*x*	*ok*	*x*	*x*	-	*x*	*ok*	*ok*	*ok*	*ok*
Nemocnice Varnsdorf, p.o.	-	*ok*	*x*	*x*	-	-	*x*	*x*	*x*	*x*
Nemocnice Vimperk, a.s.	*x*	*ok*	*x*	*x*	-	*x*	*x*	*x*	*x*	*x*
Nemocnice Milosrdných bratří Vizovice	*ok*	*ok*	*x*	*ok*	-	-	*x*	*x*	*x*	*ok*
Vojenská nemocnice Brno	-	*ok*	*x*	*x*	-	*x*	*x*	*x*	*x*	*x*
Nemocnice Vyškov, p.o.	*x*	*ok*	*ok*	*ok*	-	*x*	*ok*	*ok*	*ok*	*ok*
Nemocnice Žatec	*x*	*ok*	*x*	*x*	-	*x*	*x*	*x*	*x*	*x*
Nemocnice Znojmo, p.o.	*x*	*ok*	*x*	*x*	-	-	*x*	*x*	*x*	*ok*

5.2.1.1 Výsledek zkoumání použití zabezpečeného přenosu (zkoumání prováděno mezi květnem 2021 – srpnem 2021)

Důvod zranitelnosti HTTP protokolu je ve způsobu jeho architektury. Funguje na principu otázka/odpověď. Pokud je klientem webový prohlížeč a webová stránka na internetu funguje jako server, je pro provozovatele internetových služeb nebo případného administrátora jednoduché spustit nějaký druh analyzátoru a sledovat datový provoz mezi klientem a serverem. (Kingatua 2021)



Obrázek 9 – Útok man in the midle – člověk uprostřed, user – uživatel, original connection – původní připojení, new connection – nové připojení, perpetrator – pachatel, web application – webová aplikace (Kingatua 2021)

Tabulka 8 – podíl použití zabezpečeného přenosu HTTP/HTTPS květen až srpen 2021 (vlastní)

Protokol	***Počet nemocnic***	***%***
HTTPS	*44*	*64%*
HTTP	*25*	*36%*
Celkem	***69***	***100%***

Protokol HTTP používalo v době výzkumu alarmujících 25 českých nemocnic z celkového počtu 69. Použití HTTP ještě nemusí nutně znamenat zranitelnost nemocnice

jako takové, pokud přes stránky nemocnice neexistuje propojení do dalších částí IT systému.

Pokud je tedy přes danou webovou stránku umožněno přihlašování do systému, nebo jiný druh komunikace, útočník může pohodlně vypozorovat přístupová data.

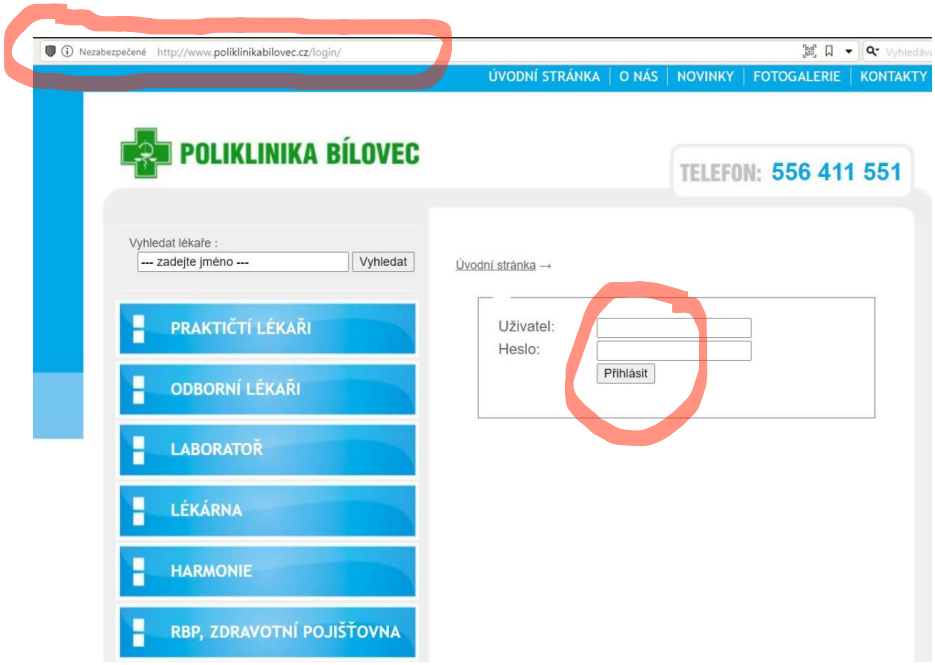
Poliklinika Bílovec

První příkladem pochybení jsem nalezl na internetových stránky polikliniky Bílovec k 30. červnu 2021.

Poliklinika Bílovec v současnosti zajišťuje provoz a správu budovy, veškeré prostory pronajímá soukromým praxím, celkem se jedná o 2 praktické a 2 dětské lékaře, 14 odborných ambulancí a laboratoř. (Poliklinika Bílovec 2010)

Útok na zjištěnou bezpečnostní chybu by primárně znamenal lokální problém pro několik lékařů, potenciálně ztrátu/zneužití dat několika tisíc pacientů.

U Polikliniky Bílovec je použita kombinace nezabezpečeného protokolu HTTP a přihlašovacího stránky, přes kterou by se útočník mohl dostat do systému.



Obrázek 10 – ukázka nezabezpečeného přihlášení (vlastní výstřižek)

Hacker by mohl přes techniku „man in the middle“ zachytit nešifrovaný síťový provoz, získat uživatelské údaje osob hlásících se do systému a pak pomocí získaných dat dál pokračovat v nabourávání se do nemocničního informačního systému.

Snažil jsem se tedy mezi zkoumanými nemocnicemi vysledovat ty, které měly na webové stránky napojené své přihlašovací údaje, stejně jako poliklinika Bílovec.

Městská nemocnice Čáslav

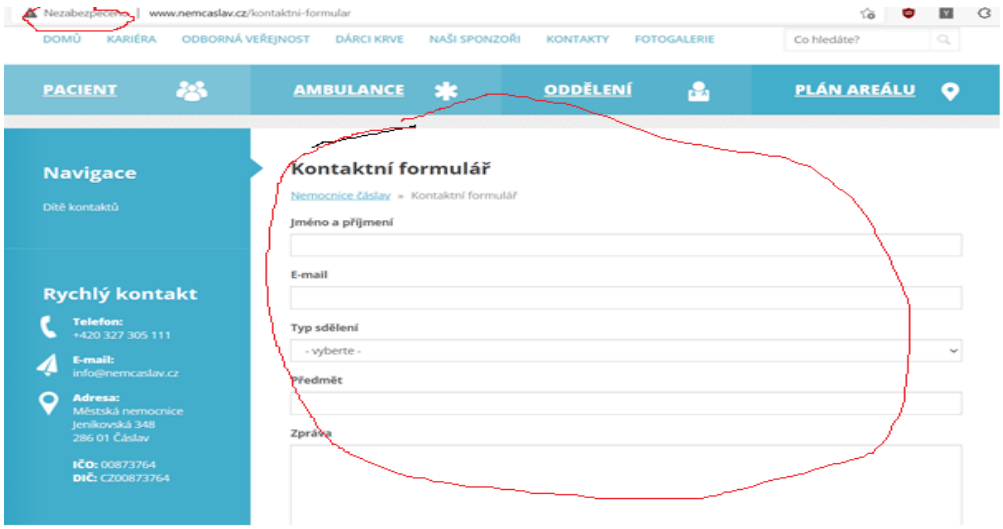
Městská nemocnice Čáslav má svou hlavní webovou stránku také nezabezpečenou.

Jedná se o nemocnici ve Středočeském kraji v okrese Kutná Hora.

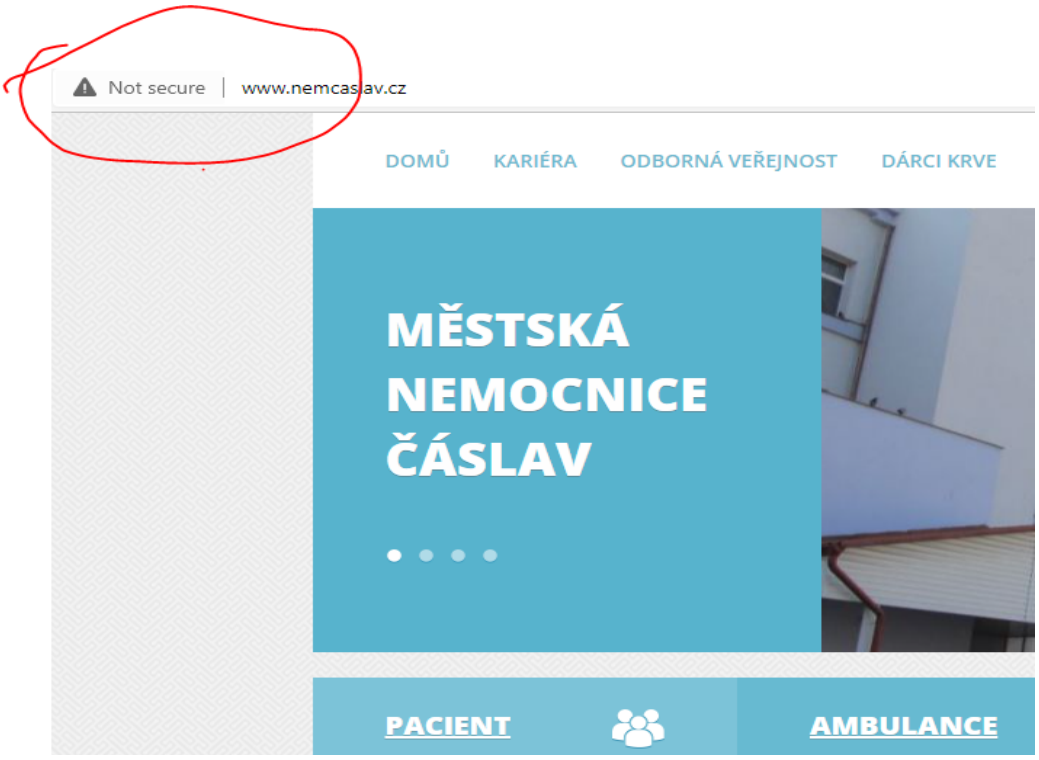
V roce 2021 zaměstnávala nemocnice 275 pracovníků. (Ceginformacio 2021)

Zneužití dat by znamenalo ohrožení citlivých údajů občanů daného města, kteří posílají přes formulář dotazy, mohlo by se jednat o několik desítek, maximálně stovek případů. Na druhou stranu nezabezpečené webové stránky indikují útočníkům, že systém nemocnice není dobře chráněn a může se stát terčem pokusů o útok.

Z webových stránek je možné se dostat do kontaktního formuláře, pomocí něhož je možné s nemocnicí komunikovat. Pokud pacient zadá do formuláře citlivé údaje, mohou být zaznamenány útočníkem a následně zneužity, například kombinace jména, e-mailu a symptomy nemoci.

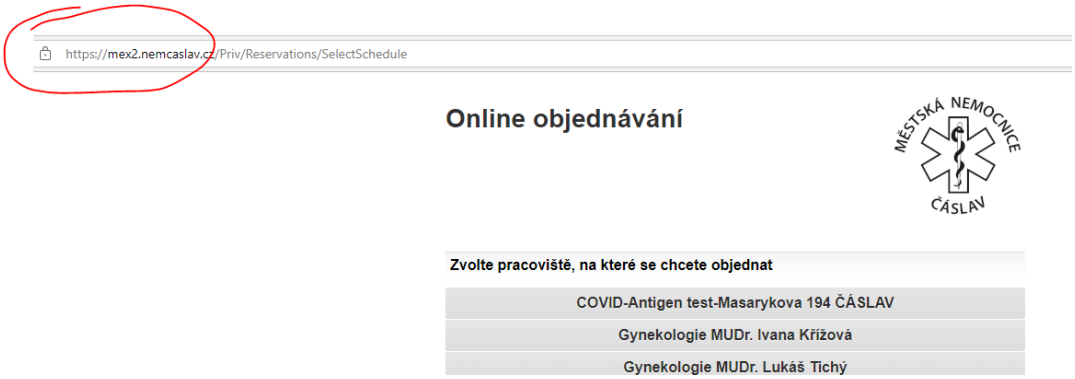


Obrázek 11 – ukázka nezabezpečeného formuláře (vlastní výstřižek)



Obrázek 12 – ukázka nezabezpečeného webu (vlastní výstřižek)

Z této části vede odkaz na objednávkový systém, který ale již je na stránce https v šifrované podobě.



Obrázek 13 – ukázka zabezpečené části webu (vlastní výstřižek)

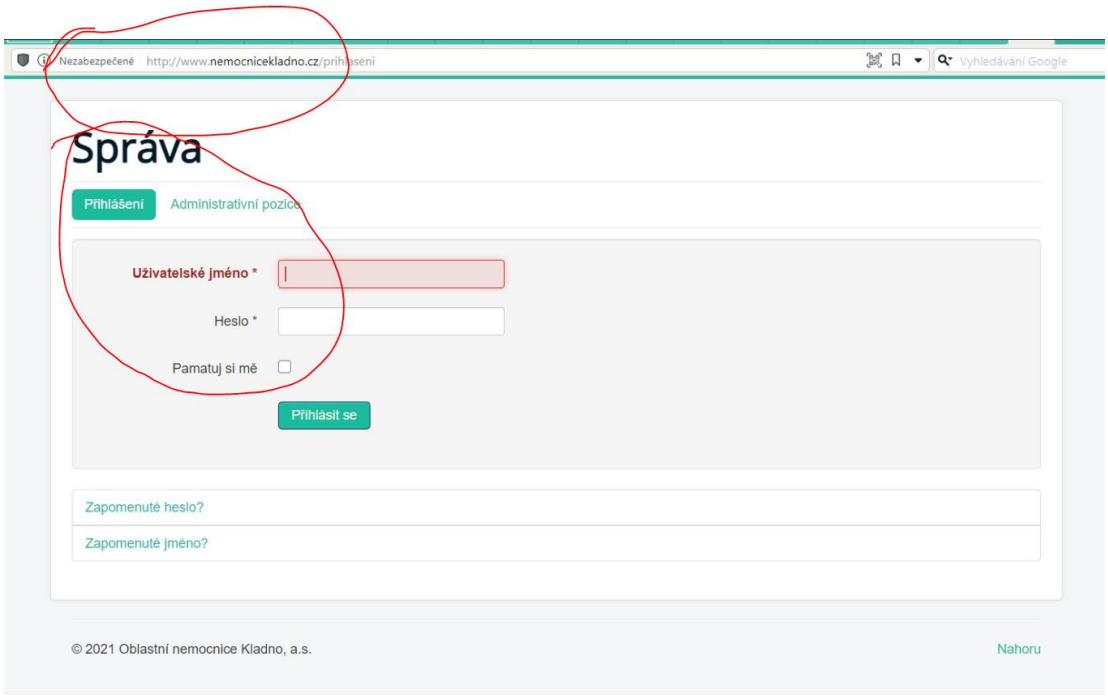
Základní bezpečnostní pravidlo bylo zavedeno, přesto zde Mozzila Observer zjistil řadu nedostatků. Jedná se zejména o chybějící „HTTP Strict Transport Security“, „X-Content-Type-Options“, „X-Frame-Options“, „X-XSS-Protection“.

Oblastní nemocnice Kladno

Také u Oblastní nemocnice Kladno jsem našel k 30. červnu 2021 významné bezpečnostní opomenutí, které spočívalo v tom, že nezabezpečený přístup na stránky přes „http“ je propojen přihlašovacím menu do správy webových stránek nemocnice.

Oblastní nemocnice Kladno je akciová společnost ve Středočeském kraji a v roce 2020 zaměstnávala 1 341 zaměstnanců. (Oblastní nemocnice Kladno 2020)

V případě zneužití bezpečnostní chyby by se v tomto případě jednalo o záležitost krajského významu, která by významně ovlivnila zdravotní péči v regionu.

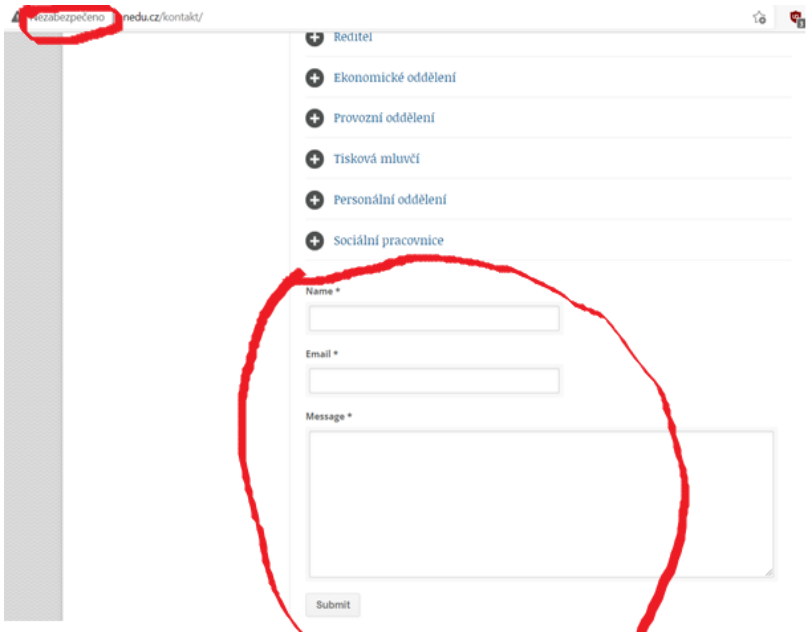


Obrázek 14 – ukázka nezabezpečeného přihlášení (vlastní výstřižek)

Nemocnice Duchcov

Nezabezpečené stránky sice neodkazují přímo na přihlašovací údaje, jako tomu bylo v případě polikliniky Bílovec nebo kladenské nemocnice, ale odkazuje na stránky jednotlivých oddělení, kde jsou k dispozici e-mailové údaje, případně kontaktní formuláře. Nezabezpečený přístup může otevřít dveře ke sběru citlivých údajů o pacientech.

Městská nemocnice Duchcov nezveřejňuje rozpočet ani počet zaměstnanců. Podle evropské databanky je jejich počet mezi 100-500. Dopad by tedy byl spíše lokálního významu. (Evropská databanka 2021)



Obrázek 15 – ukázka nezabezpečeného formuláře (vlastní výstřižek)

Klaudiánova nemocnice Mladá Boleslav

U Klaudiánovy nemocnice v Mladé Boleslavi se opět jedná o závažné pochybení, protože umožňuje přes nezabezpečenou stránku přímé odezírání přístupových práv jednotlivých zaměstnanců, kteří se přes tyto stránky hlásí do systému.

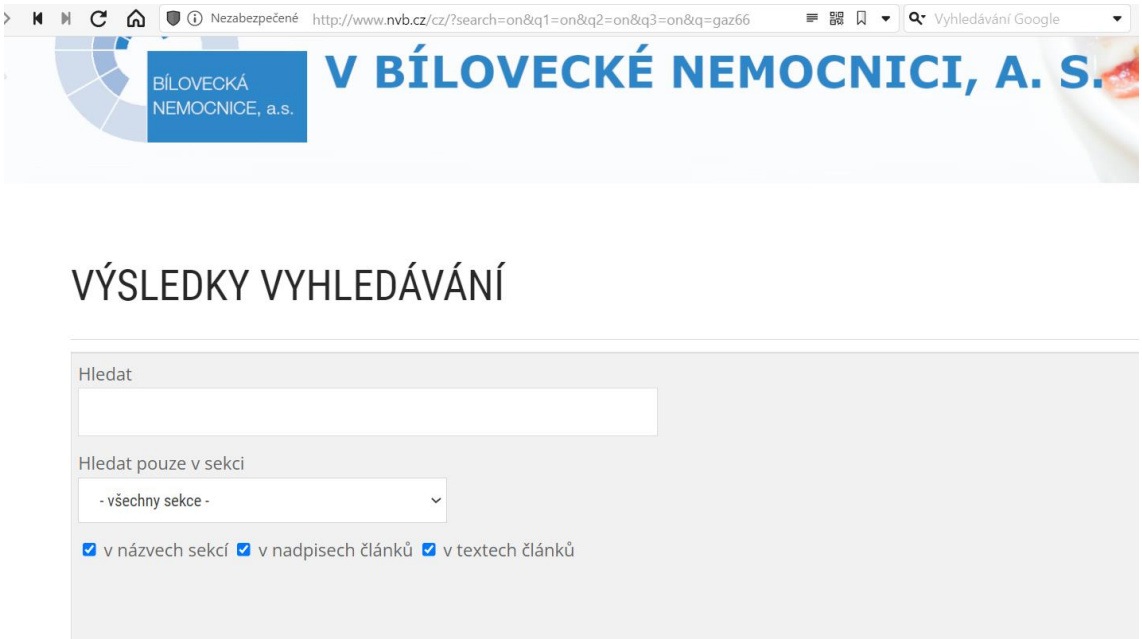
Klaudiánova nemocnice Mladá Boleslav, a.s. je nemocnice Středočeského kraje, která v roce 2020 zaměstnávala přes 1500 pracovníků, tedy přibližně velikost podobná jako u Oblastní nemocnice Kladno. V případě útoku na tuto nemocnici by se jednalo o událost krajského významu. (Rozpočet Oblastní nemocnice Mladá Boleslav, a.s. 2022)

Obrázek 16 – ukázka nezabezpečeného uživatelského přihlášení (vlastní výstřižek)

Bílovecká nemocnice, a.s.

Na stránkách Bílovecké nemocnice můžeme vidět další příklad nezabezpečeného vyhledávacího formuláře, kde může dojít k narušení soukromí.

Bílovecká nemocnice je akciová společnost, která poskytuje ambulantní i lůžkovou péči. K dispozici má 130 lůžek a okolo 200 zaměstnanců. Útok na nemocnici by měl lokální dopad. (Výroční zpráva 2020)

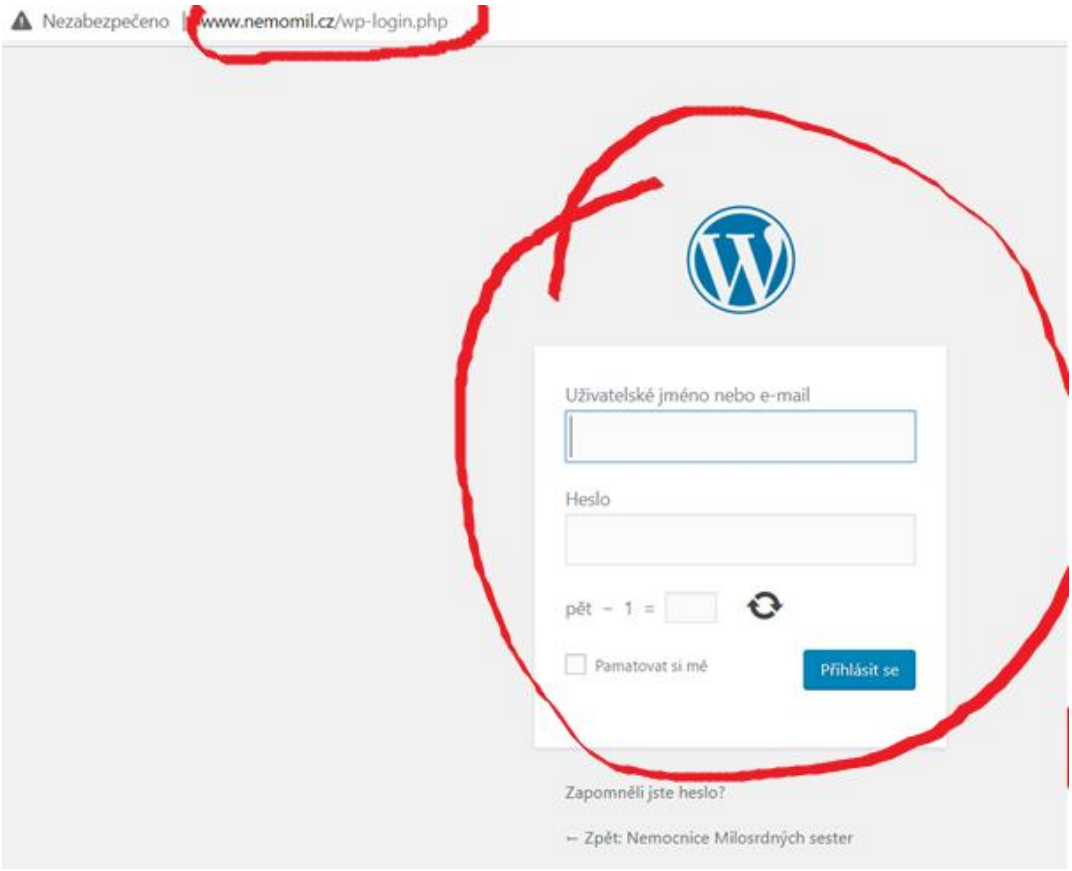


Obrázek 17 – ukázka nezabezpečeného vyhledávání (vlastní výstřižek)

Nemocnice milosrdných sester sv. Vincence de Paul Kroměříž

U Nemocnice milosrdných sester v Kroměříži jsem opět našel závažné pochybení v podobě kombinace nezabezpečené „http stránky“ a uživatelského jména a hesla určených k administraci a editaci webu v prostředí Wordpressu.

Nemocnice Milosrdných sester sv. Vincence de Paul Kroměříž je soukromé zdravotnické zařízení se 105 lůžky, které se stará především o geriatrické a dlouhodobě nemocné pacienty. Útok na nemocnici by měl lokální dopad. (Historie 2021)

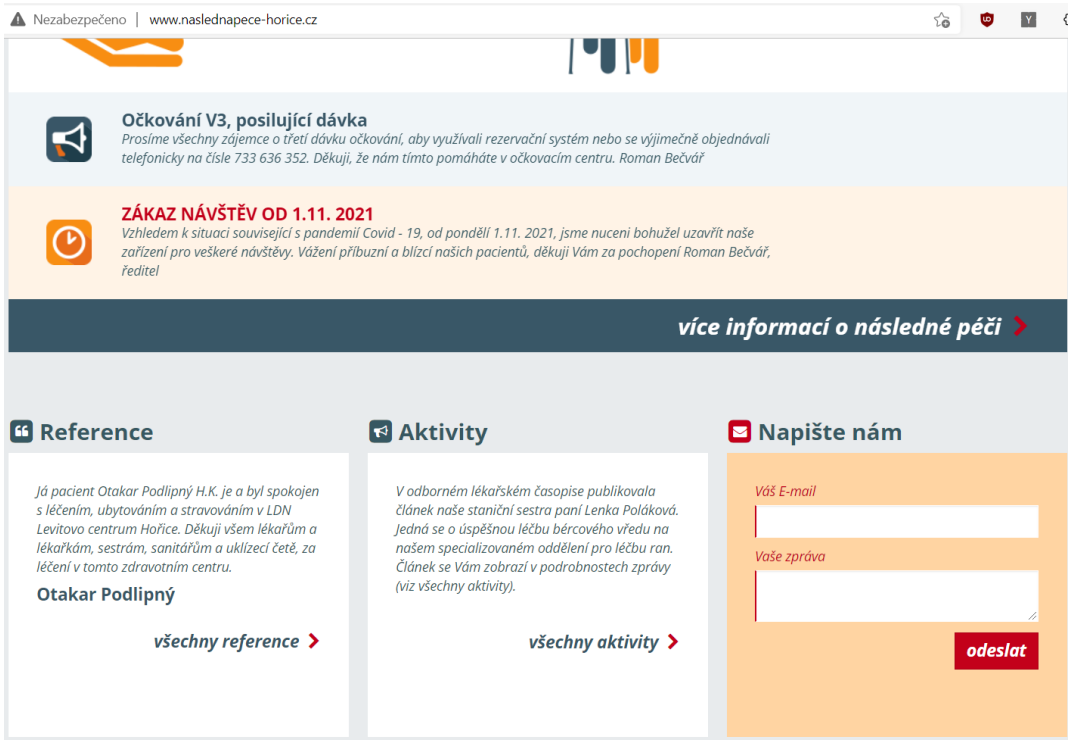


Obrázek 18 – ukázka nezabezpečeného přihlášení k redakčnímu systému (vlastní výstřižek)

Levitovo centrum následné péče Hořice

Propojení nezabezpečené stránky s komunikačním kanálem pro veřejnost umožňuje získat citlivé údaje kontaktujících osob, zejména pacientů.

Levitovo centrum následné péče Hořice je příspěvková organizace v Královéhradeckém kraji, specializuje se na léčbu bércových vředů a jiných nehojících se ran, například po operacích. Má celkem 120 lůžek, 24 hodinovou chirurgickou ambulanci, laboratoř a interní ambulanci. V roce 2019 zaměstnávala 127 pracovníků. Dopad proniknutí do systému by byl opět lokální. (Výroční zpráva 2019)

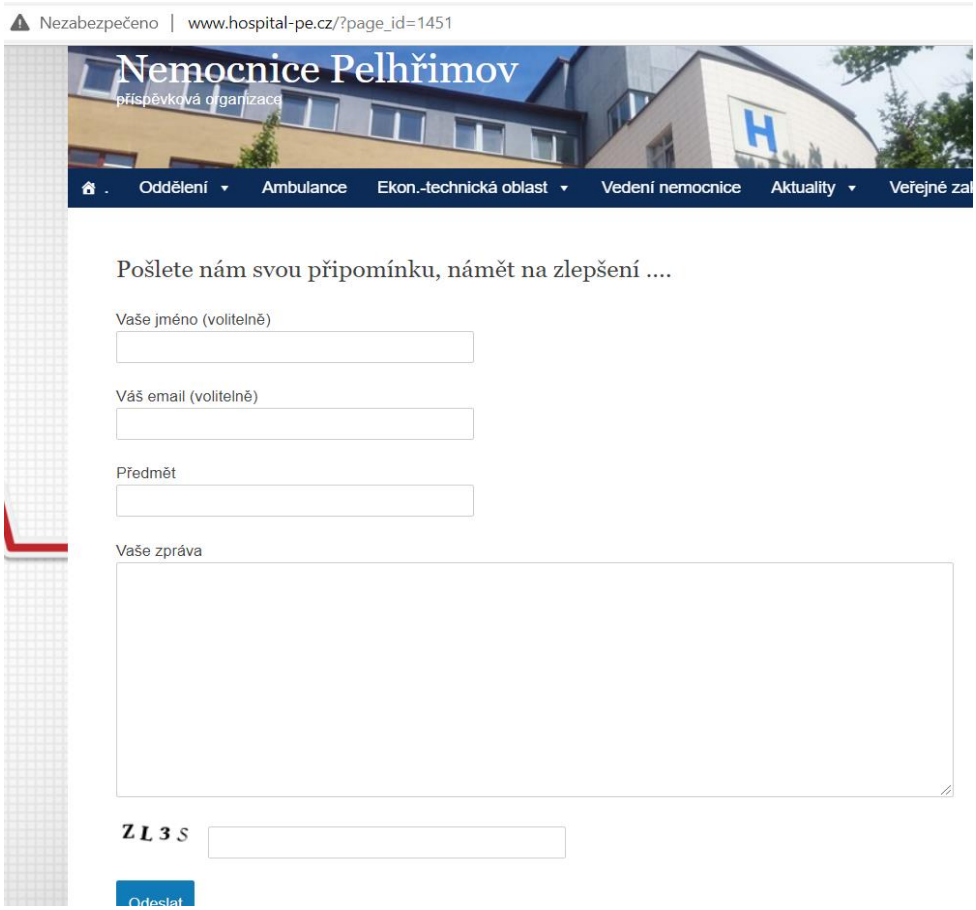


Obrázek 19 – ukázka nezabezpečeného formuláře k odeslání emailu Hořice (vlastní výstřižek)

Nemocnice Pelhřimov

Pelhřimov je další ukázkou potenciálního ohrožení třetí strany přes nezabezpečený komunikační kanál.

Nemocnice Pelhřimov je příspěvková organizace v kraji Vysočina, kde je zaměstnáno 684 pracovníků. Na 10 odděleních je umístěno 340 lůžek. (Nemocnice Pelhřimov 2020)

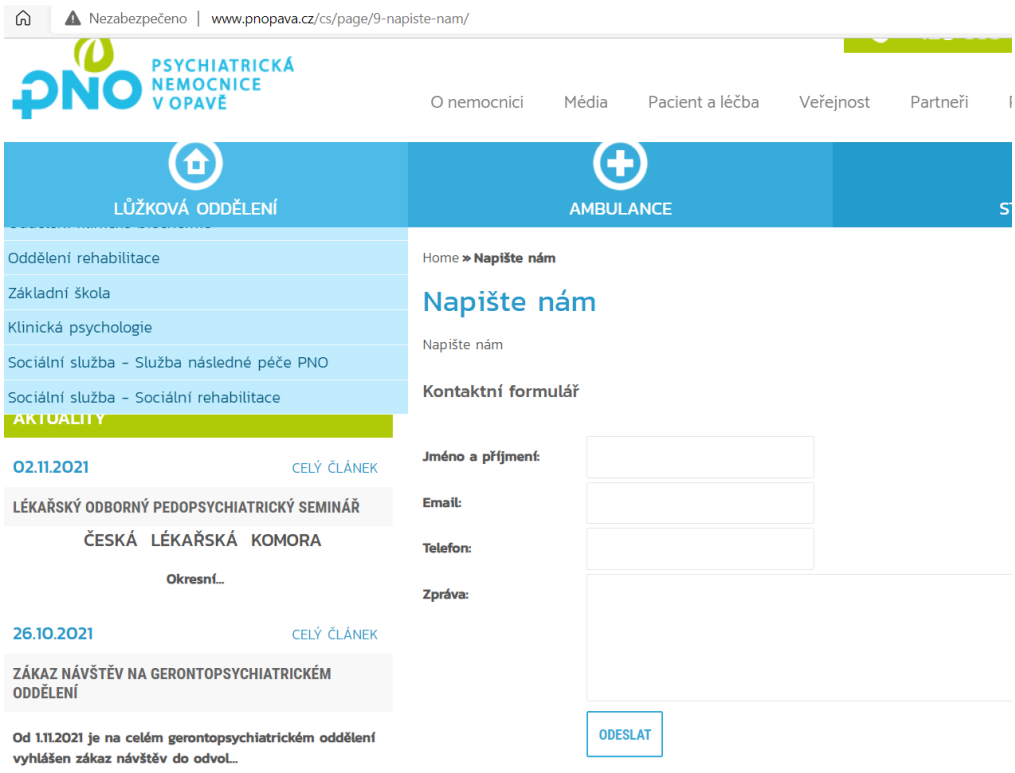


Obrázek 20 – ukázka nezabezpečeného formuláře k odeslání emailu Pelhřimov (vlastní výstřižek)

Psychiatrická nemocnice v Opavě

Psychiatrická nemocnice v Opavě je vzhledem ke specializaci v oblasti duševního zdraví závažnějším případem ohrožení citlivých dat, protože tomuto nebezpečí jsou vystaveni pacienti s psychickými problémy, tedy pravděpodobně citlivější a snáze manipulovatelní, než průměrná populace. Navíc je vedle e-mailu možné získat i jejich telefonní číslo.

Psychiatrická nemocnice v Opavě je zdravotnické zařízení, jehož zřizovatelem je ministerstvo zdravotnictví ČR. Nemocnice má 863 lůžek, ročně se zde léčí 6 500 pacientů. Představuje spádové území pro 1,3 mil. obyvatel Moravskoslezského kraje. (Psychiatrická nemocnice v Opavě 2021)



Obrázek 21 – ukázka nezabezpečeného formuláře s citlivými údaji Opava (vlastní výstřižek)

Nemocnice Vimperk

Nemocnice ve Vimperku je posledním závažným případem, který se mi podařilo najít. Opět se zde objevuje možnost odpozorovat uživatelské jméno a heslo a přihlásit se do systému.

Nemocnice Vimperk je nestátní zdravotnické zařízení poskytující zdravotní a sociální následnou péči. Pracuje zde více než 170 zaměstnanců.

Obrázek 22 – ukázka nezabezpečeného přihlášení do systému (vlastní výstřižek)

Ostatní nemocnice

U ostatních 25 z 69 nemocnic s nezabezpečeným protokolem HTTP jsem propojení na interní systémy/případně citlivé informace nenašel, je tedy otázka, jestli přes ně existuje nějaké napojení do systému, které by se hackerům podařilo využít. V každém případě je třeba přechod na HTTPS doporučit.

5.2.1.2 Výsledek zkoumání HTTP Strict Transport Security (přísné zabezpečení přenosu HTTP)

Mechanismus HTTP Strict Transport Security (dále zkráceně HSTS) umožňuje, aby webový server vynutil v prohlížeči komunikaci pomocí šifrovaného HTTPS připojení. Tím se eliminuje přenos dat nezabezpečeným HTTP protokolem. Pro použití je zásadním předpokladem mít SSL certifikát.

Tabulka 9 – podíl použití HSTS (vlastní)

Protokol	***Počet nemocnic***	***%***
HSTS	*8*	*12 %*
Nemá HSTS	*61*	*88 %*
Celkem	*69*	*100 %*

Tento výsledek je překvapivý v tom ohledu, že zatímco 64% společností zainvestovalo do bezpečnější platformy HTTPS, a používá tedy SSL certifikát, jen 12% z nich šlo dále směrem k HSTS zabezpečení šifrované komunikace.

5.2.1.3 Výsledek zkoumání Content Security Policy

Umožňuje operátorům webu kontrolu nad tím, odkud lze načíst prostředky na jejich webu a zabránit zranitelnostem skriptování mezi weby XSS (cross-site scripting). Je to v podstatě hlavička, která prohlížeči říká, jaké soubory lze do stránek nahrát a jakým způsobem. Hlavní výhoda CSP spočívá v obraně proti XSS útokům, které vkládají zákeřný kódu útočícího na stránky napadené strany. CSP umožňují deaktivaci používání vloženého Java Scriptu. Nevýhodou je, že u komplexnějších webů je potřebná podrobná analýza obsahu a precizní nastavení pravidel, tedy se jedná o pracnou, specializovanou činnost.

Snad proto ji naprostá většina nemocnic neměla implementovanou vůbec a pouze jedna z nemocnic ji měla zavedenou (Fakultní nemocnice Ostrava), ale software v ní vyhodnotil chyby. K vyváženosti faktů je třeba dodat, že kvůli složitosti obvykle tuto politiku nemají naimplementovány ani stránky soukromých nezdravotnických subjektů, nebo ji podle analýzy mají zavedenou nedostatečně.

5.2.1.4 Výsledek zkoumání X-Content-Type Options

Hlavička sděluje prohlížeči, aby ověřoval, zda zdroj má v hlavičce správně nastavený MIME typ a tím chrání web před tzv. „content-sniffingem“, kdy prohlížeč spustí například podvržený java script v textovém souboru nebo obrázku.

Tabulka 10 – nasazení X-Content-Type Options (vlastní)

X-Content-Type Options	***Počet nemocnic***	***%***
Implementováno	*16*	*23%*
Ne	*53*	*77%*
Celkem	*69*	*100%*

5.2.1.5 Výsledek zkoumání X-Frame-Option

Hlavička X-Frame-Options říká, zda lze webovou stránku či její část zobrazit v rámu při použití HTML značek <frame>, <iframe> nebo <object> a ochraňuje uživatele od zneužití pomocí tzv. „clickjackingu“, podvržením podvodné průhledné vrstvy přes originální.

Tabulka 11 – nasazení X-Frame-Options (vlastní)

X-Frame-Option	***Počet nemocnic***	***%***
Implementováno	*20*	*29%*
Ne	*49*	*71%*
Celkem	*69*	*100%*

5.2.1.6 Výsledek zkoumání X-XSS-Protection

Hlavička X-XSS-Protection povoluje zabudovaný filtr proti cross-site scriptingu. Moderní prohlížeče tuto hlavičku ignorují. Hlavička je podporována už jen prohlížeči Internet Explorer a Safari, nebo starými verzemi ostatních. V moderních prohlížečích je již ignorována.

Tabulka 12 – nasazení X-XSS-Protection (vlastní)

X-XSS	***Počet nemocnic***	***%***
Implementováno	*11*	*16%*
Ne	*58*	*84%*
Celkem	*69*	*100%*

5.2.1.7 Zaznamenaná zlepšení v období září 2021 – listopad 2021

Skenování nemocnic poprvé probíhalo v období květen 2021 – srpen 2021. K polovině listopadu jsem znovu analyzoval nejzávažnější oblast týkající se nezabezpečeného HTTP protokolu a u několika nemocnic zlepšení.

Konkrétně jsem zaznamenal zlepšení u těchto nemocnic:

- Nemocnice Havířov;

- Nemocnice Milosrdných bratří Brno;
- Mulačova nemocnice Plzeň;
- Nemocnice Nymburk.

K 15. listopadu došlo k následujícímu zlepšení:

Tabulka 13 – podíl použití HTTP/HTTPS listopad 2021 (vlastní)

Protokol	***Počet nemocnic***	***%***
HTTPS	*48*	*70 %*
http	*21*	*30 %*
Celkem	*69*	*100 %*

Tabulka 14 – nedostatky zabezpečení nemocnic listopad 2021 (vlastní)

Protokol HTTP	***Počet nemocnic***	***%***
HTTP, z toho:	**21**	**30 % z celkového počtu 69 zkoumaných nemocnic**
- *Závažný nález v podobě odkazu na uživatelské jméno a heslo na nezabezpečené stránce*	*5*	*7 % z celkového počtu 69 nemocnic*
- *Možnost odezírat citlivé údaje kromě výše uvedených odkazů na e-mail a heslo*	*6*	*9 % z celkového počtu 69 nemocnic*

5.2.2 Porovnání zabezpečení webových stránek zdravotnických zařízení v České republice proti kybernetickým útokům se zabezpečením stránek zdravotnických zařízení v zahraničí

Výsledky českých nemocnic nejsou příliš dobré, proto byl stejný test proveden u vybraných zahraničních nemocnic, konkrétně největších světových a evropských nemocnic napříč kontinenty.

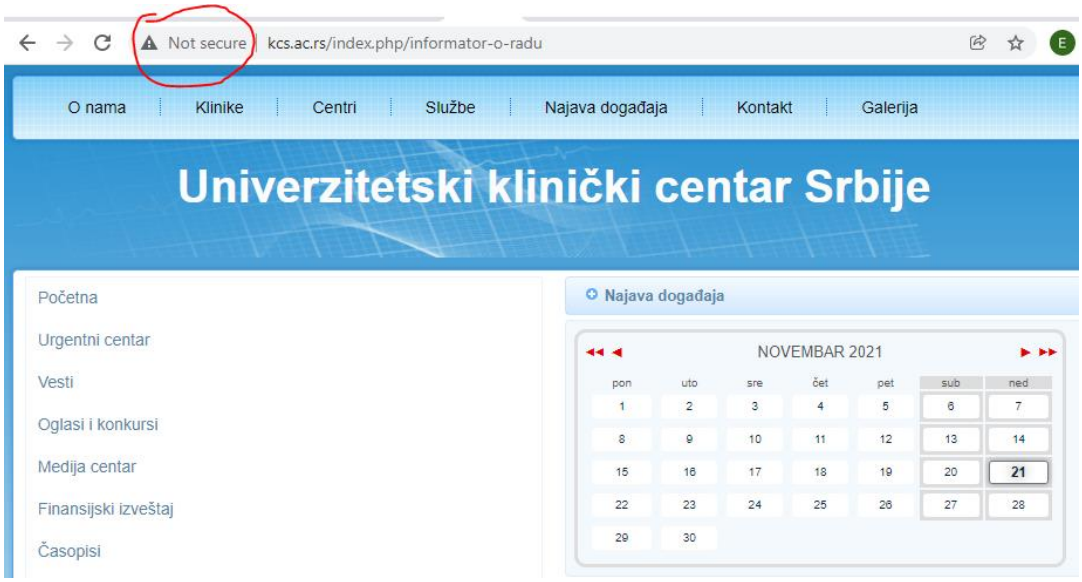
Tabulka 15 – Zkoumání zabezpečení webových stránek zahraničních nemocnic nástrojem Mozzila Observatory (vlastní, pojmy viz kapitola 4.2)

Název nemocnice	***Cookies***	***Cross-origin resource sharing***	***HSTS***	***Redirection***	***Referrer Policy***	***Subresouce Integrity***	***X-Content-Type Options***	***X-Frame-Options***	***X-XSS-Protection***	***HTTPS***
Chris Hani Baragwanath Hospital, JAR	*ok*	*ok*	*ok*	*ok*	*ok*	*-*	*ok*	*ok*	*ok*	*ok*
Univerzitní klinické centrum Srbska	*x*	*ok*	*x*	*x*	*-*	*x*	*x*	*x*	*x*	*x*
Jackson Memorial Hospital, Miami, Florida	*-*	*ok*	*x*	*ok*	*x*	*x*	*x*	*x*	*x*	*ok*
The Royal Melbourne Hospital	*-*	*ok*	*x*	*ok*	*-*	*-*	*x*	*ok*	*x*	*ok*
West China Hospital of Sichuan University	*x*	*ok*	*x*	*x*	*-*	*-*	*x*	*ok*	*ok*	*ok*
Chang Gung Memorial Hospital, Taoyuan, Taiwan	*-*	*ok*	*x*	*x*	*-*	*x*	*x*	*x*	*x*	*x*
Hospital das clinicas da faculdade, Sao Paulo, Brazílie	*-*	*ok*	*x*	*ok*	*-*	*x*	*x*	*X*	*x*	*ok*
Charité Universitätsmedizin Berlin	*x*	*ok*	*ok*	*ok*	*-*	*-*	*ok*	*x*	*x*	*ok*
Allgemaines Krankenhaus der Stadt Wien	*ok*	*ok*	*ok*	*ok*	*ok*	*-*	*ok*	*ok*	*ok*	*ok*
Hôpital Universitaire Pitié Salpêtrière	*-*	*ok*	*x*	*x*	*-*	*x*	*x*	*x*	*x*	*x*

Přestože se jedná o nejvýznamnější instituce, jejich stránky také nejsou příliš dobře zabezpečené. Mezi výjimky patří nemocnice v Jihoafrické republice, v Melbourne a ve Vídni. Oproti tomu velké nemocnice v Srbsku, na Taiwanu a ve Francii neměly ani zabezpečený HTTPS protokol.

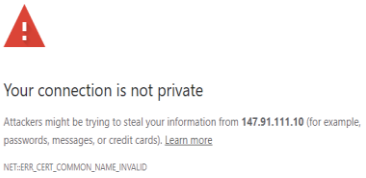
Univerzitní klinické centrum Srbska

Univerzitní klinické centrum Srbska patří k největším zdravotnickým zařízením v Evropě. Přesto nemá základní zabezpečení přes HTTPS protokol.



Obrázek 23 – ukázka nezabezpečeného webu Srbsko (vlastní výstřižek)

Při rozklepnutí možnosti napsat do nemocnice e-mail přes webové rozhraní, varuje prohlížeč uživatele, že jeho data by mohla být zneužita.



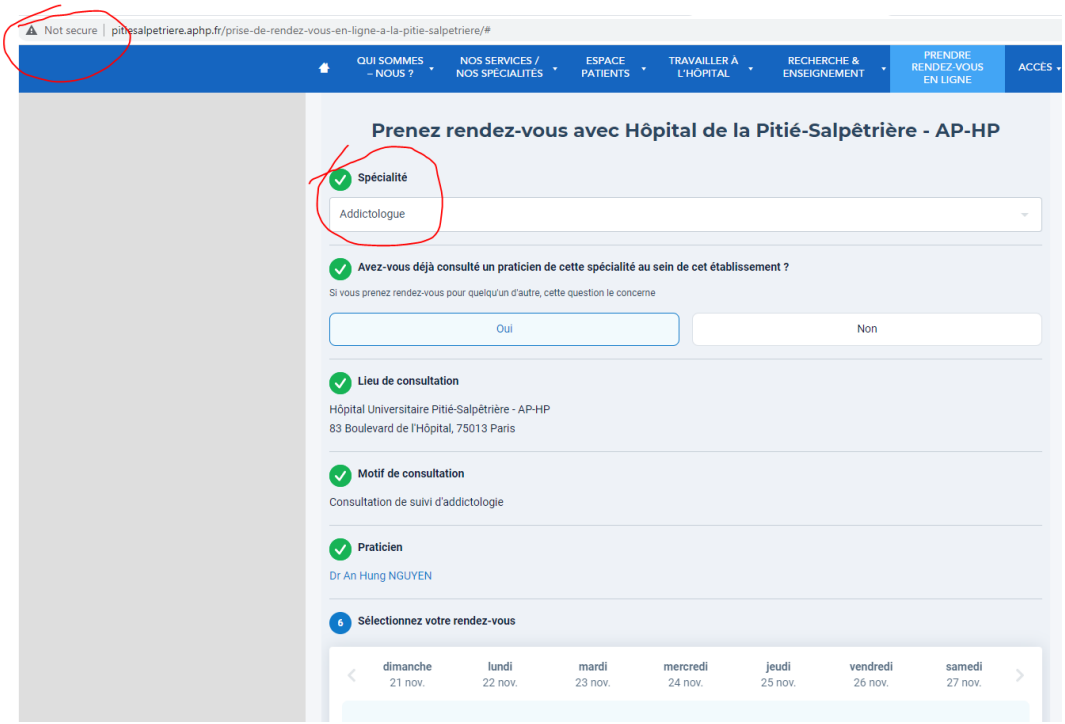
Obrázek 24 a 25 – varování při pokusu o klepnutí na e-mail (vlastní výstřižek)

Stejně tak odkazy na jednotlivé kliniky jsou vedeny na nezabezpečené stránky.

Hôpital Universitaire Pitié Salpêtrière

Příklad vyhlášené francouzské nemocnice Hôpital Universitaire Pitié Salpêtrière potvrzuje, že velikost ani věhlas nemocnice stále nezaručuje, že jsou její stránky dobře chráněny.

Kromě nezabezpečeného HTTP protokolu je prohřeškem propojení nezabezpečených stránek na objednávkový systém, kde pacient zadává citlivé informace.



Obrázek 26 – ukázka nezabezpečeného webu Francie (vlastní výstřižek)

Menší nemocnice

Menší nemocnice byly vybrány namátkově a výsledky potvrzují, že velikost nemocnice není určujícím kritériem pro její zabezpečení. Například menší nemocnice v padesátitisícovém Hollabrunu v Rakousku vychází z porovnání dobře, zato nemocnice v Gmündu v testu Mozilla Observatory propadla. Vždy tedy záleží na aktuálním managementu, IT řízení nemocnice a prioritách, situace je tedy podobná jako v českých nemocnicích.

Výsledky porovnání v jednotlivých oblastech

Z níže uvedeného srovnání je patrné, že kvalita zabezpečení vybraných českých nemocnic se nevymyká celosvětovému průměru, zvlášť vezmeme-li v úvahu, že jsou srovnávány s největšími světovými nemocnicemi, které patří k hlavním ve svém státě a největším na daném kontinentu.

Na druhou stranu asi žádné zdravotnictví nebylo v přepočtu na počet obyvatel pod takovým hackerským náporem jako české nemocnice od jara 2020. Analýze příčin se budu věnovat v kapitole věnované diskuzi.

Tabulka 16 – podíl použití protokolu HTTP/HTTPS u stránek českých a zahraničních nemocnic (vlastní)

Protokol	***Počet českých nemocnic***	***%***	***Počet velkých zahraničních nemocnic***	***%***
HTTPS	*48*	*70 %*	*7*	*70 %*
http	*21*	*30 %*	*3*	*30 %*
Celkem	***69***	***100 %***	***10***	***100 %***

Tabulka 17 – podíl použití protokolu HSTS u stránek českých a zahraničních nemocnic (vlastní)

Protokol	***Počet českých nemocnic***	***%***	***Počet velkých zahraničních nemocnic***	***%***
HSTS	*8*	*12 %*	*3*	*30 %*
Nemá HSTS	*61*	*88 %*	*7*	*70 %*
Celkem	***69***	***100 %***	***10***	***100 %***

Tabulka 18 – srovnání nasazení X-Content-Type Options u českých a zahraničních nemocnic (vlastní)

X-Content-Type Options	***Počet českých nemocnic***	***%***	***Počet velkých zahraničních nemocnic***	***%***
Implementováno	*16*	*23 %*	*3*	*30 %*
Ne	*53*	*77 %*	*7*	*70 %*
Celkem	***69***	***100 %***	***10***	***100 %***

Tabulka 19 – srovnání nasazení X-Frame-Options u českých a zahraničních nemocnic (vlastní)

X-Frame-Option	***Počet českých nemocnic***	***%***	***Počet velkých zahraničních nemocnic***	***%***
Implementováno	*20*	*29 %*	*4*	*40 %*
Ne	*49*	*71 %*	*6*	*60 %*
Celkem	***69***	***100 %***	***10***	***100 %***

Tabulka 20 – srovnání nasazení X-XXS u českých a zahraničních nemocnic (vlastní)

X-XSS	***Počet českých nemocnic***	***%***	***Počet velkých zahraničních nemocnic***	***%***
Implementováno	*11*	*16 %*	*3*	*30 %*
Ne	*58*	*84 %*	*7*	*70 %*
Celkem	*69*	*100 %*	*10*	*100 %*

5.2.3 Porovnání zabezpečení internetových stránek nemocnic v České republice proti kybernetickým útokům se zabezpečením internetových stránek významných soukromých nezdravotnických subjektů v České republice

Ve druhé srovnávací studii byl vybrán náhodný vzorek největších soukromých nezdravotnických společností na českém trhu z různých sektorů. Na první pohled je zřejmé, že největší soukromé nezdravotnické společnosti mají své stránky chráněné lépe než české a světové nemocnice.

Tabulka 21 – Zkoumání zabezpečení webových stránek významných společností nástrojem Mozzila Observatory (vlastní, pojmy viz kapitola 4.2)

Název nemocnice	*Cookies*	*Cross-origin resource sharing*	*HSTS*	*Redirection*	*Referrer Policy*	*Subresouce Integrity*	*X-Content-Type Options*	*X-Frame-Options*	*X-XSS-Protection*	*HTTPS*
Česká spořitelna	-	ok	ok	ok	-	x	ok	ok	ok	ok
ČEZ	x	ok	ok	ok	ok	-	ok	ok	ok	ok
Google - česká verze stránek	ok	ok	ok	ok	-	-	ok	x	ok	ok
Škoda Mladá Boleslav	-	ok	ok	ok	-	x	ok	ok	ok	ok
T-mobile	x	ok	ok	ok	-	x	ok	ok	ok	ok
Lidl	-	ok	ok	ok	ok	x	ok	ok	ok	ok
Foxconn	x	ok	ok	ok	-	x	ok	ok	ok	ok
Sazka	x	ok	ok	x	-	x	x	ok	x	ok
Metrostav	ok	ok	ok	ok	-	-	Ok	ok	ok	ok
MOL	-	ok	x	x	-	-	x	x	x	ok

Společnosti, které svým stránkám věnovaly menší pozornost, jsou MOL, Sazka a také Foxconn, u kterého to z výše uvedené tabulky není patrné, ale celkové hodnocení testu i vzhledem k dalším kritériím pro něj nedopadlo dobře. Nejvyšší záporné body nasbíral MOL za nezabezpečené nastavení Cookies a také za natahování externích skriptů přes nezabezpečený HSTS protokol.

Podrobné výsledky porovnání českých nemocnic a soukromých nezdravotnických společností v jednotlivých oblastech

Také porovnání jednotlivých oblastí ukazuje, že největší soukromé nezdravotnické společnosti mají své stránky chráněny lépe než vybrané české a světové nemocnice.

Tabulka 22 – podíl použití protokolu HTTP/HTTPS u stránek českých nemocnic a soukromých nezdravotnických společností (vlastní)

Protokol	***Počet českých nemocnic***	***%***	***Počet velkých českých společností***	***%***
HTTPS	*48*	*70%*	*10*	*100%*
HTTP	*21*	*30%*	*0*	*0%*
Celkem	*69*	*100%*	*10*	*100%*

Tabulka 23 – podíl použití protokolu HSTS u stránek českých nemocnic a soukromých nezdravotnických společností (vlastní)

Protokol	***Počet českých nemocnic***	***%***	***Počet velkých českých společností***	***%***
HSTS	*8*	*12%*	*9*	*90%*
Nemá HSTS	*61*	*88%*	*1*	*10%*
Celkem	*69*	*100%*	*10*	*100%*

Tabulka 24 – srovnání nasazení X-Content-Type Options u českých nemocnic a soukromých nezdravotnických společností (vlastní)

X-Content-Type Options	***Počet českých nemocnic***	***%***	***Počet velkých českých společností***	***%***
Implementováno	*16*	*23%*	*8*	*80%*
Ne	*53*	*77%*	*2*	*20%*
Celkem	*69*	*100%*	*10*	*100%*

Tabulka 25 – srovnání nasazení X-Frame-Options u českých nemocnic a soukromých nezdravotnických společností (vlastní)

X-Frame-Option	***Počet českých nemocnic***	***%***	***Počet velkých českých společností***	***%***
Implementováno	*20*	*29%*	*8*	*80%*
Ne	*49*	*71%*	*2*	*20%*
Celkem	*69*	*100%*	*10*	*100%*

Tabulka 26 – srovnání nasazení X-XSS u českých nemocnic a soukromých nezdravotnických společností (vlastní)

X-XSS	***Počet českých nemocnic***	***%***	***Počet velkých českých společností***	***%***
Implementováno	*11*	*16%*	*8*	*80%*
Ne	*58*	*84%*	*2*	*20%*
Celkem	*69*	*100%*	*10*	*100%*

Diskuzi nad výsledky bude věnována následující kapitola.

5.2.4 Shrnutí výsledků

Z pozorování je patrné, že i přes neustálé hackerské útoky a jejich medializace, bylo v období května – srpna 2021 nalezeno 36 % zkoumaných nemocnic, které používají na internetových stránkách nezabezpečený HTTP protokol, přes který lze relativně snadno odezírat komunikaci. Z nich v době psaní této diplomové práce 4 nemocnice přešly na zabezpečený HTTPS protokol, počet nezabezpečených stránek tedy poklesl na 30 %.

V rámci nezabezpečených nemocnic jsem našel 6 případů, kdy případný útočník mohl získat citlivá data účastníků komunikace s nemocnicí, zejména pacientů. V jednom z případů se jednalo o psychiatrickou kliniku, kdy by citlivá data v kombinaci s e-mailem a telefonním číslem mohla mít závažné dopady.

V pěti případech se mi podařilo odhalit závažné bezpečnostní pochybení, které by mohlo vést přímo k nabourání do systému nemocnice.

Přes zlepšování trendu, v tomto případě v období necelých šesti měsíců, má ještě řada nemocnic své webové stránky zabezpečené nedostatečně.

6 DISKUZE

V této části diplomové práce jsou zhodnoceny výsledky výzkumu rozdělené do dvou částí – jedna zhodnocuje příčiny, průběh a následky násilných teroristických útoků na zdravotnická zařízení, druhá zhodnocuje příčiny, průběh a následky **kybernetických** útoků na zdravotnická zařízení a testování webových stránek vybraných nemocnic proti případnému kybernetickému útoku.

6.1 Diskuze k analýze příčin, průběhu a následků teroristických útoků na zdravotnická zařízení

Pro posouzení analýzy příčin, průběhu a následků byla použita Globální databáze terorismu a z ní byly kombinací vyhledávání a manuálního třídění vybrány informace o nemocnicích. Získané informace byly porovnávány s odbornou literaturou a tiskovými zprávami a byl hledán trend porovnávající teroristické útoky s ozbrojenými konflikty.

6.1.1 Příčiny násilných teroristických útoků na zdravotnická zařízení

Z výzkumu v kapitole 5.1 vyplývá, že místa útoku na zdravotnická zařízení korelují s místy aktivních válečných konfliktů. V daných případech se v naprosté většině jedná o teroristické útoky na místě, kde ozbrojený střet probíhá.

Nastolil jsem otázku, zda probíhají teroristické útoky také na zařízení válčících stran, které leží mimo oblast konfliktu (např. nemocnice členů NATO při válce v Afgánistánu), například jako odvetné akce. Jak vyplývá z kapitoly 3 a 5, zdravotnických zařízení stran, které jsou do válečného konfliktu zapojeny, se útok většinou netýká, pokud nejsou umístěny na válečném území, nebo v jeho těsné blízkosti. Výjimkou byl plánovaný útok islámských radikálů na vojenskou nemocnici v Hamburku v roce 2003 (Kaclová, Lazáková, Karas a Šťáhlavský 2003), který byl překažen díky spolupráci tajných služeb. Dále se nemocnice měly stát součástí velkých teroristických útoků v Londýně provedených Al-Kajdou v roce 2005 (Global Terrorism Database 2009-2021). Tyto útoky ale byly na rozdíl od dalších cílů v Londýně odvráceny.

Teroristické útoky se tedy obvykle neodehrávají v místech původu válčících stran, ale zejména v místech, kde ozbrojený střet aktivně probíhá. „Odvetné“ teroristické útoky se

soustředí na jiné cíle, případně se je dosud dařilo v počátku odhalit. Pro nemocnice v mírových oblastech tedy dosud zůstává největším nebezpečím útok tzv. osamělých střelců (viz případ ve Fakultní nemocnici Ostrava v roce 2019 (Jiroušková 2020; ČTK a Lesková 2019)) a dále kybernetické útoky, které jsou popsány v další části.

Primární příčinou násilných teroristických útoků na zdravotnická zařízení je tedy déletrvající ozbrojený konflikt v dané lokalitě.

Byla potvrzena Hypotéza 1: Násilné útoky na zdravotnická zařízení korelují s místy ozbrojených konfliktů.

Sekundární příčiny bývají různé, mezi nejčastější patří tyto:

- jedná se o vojenskou nemocnici, tedy ji nepřítel chápe jako vojenský cíl, byť je to proti humanitárním konvencím (např. vojenské křídlo nemocnice Musgrave Park Hospital (HODGETTS 1993));
- nástroj cílené likvidace civilního obyvatelstva (útok na Nemocnici Kigali, Univerzitní nemocnici Butare a Psychiatrické centrum Ndera ve Rwandě (VIRET 2010; BIZIMANA 2020));
- vydírání válečné protistrany a úspěch útočníků (útok na Nemocnici Buďonnovsk), který podnítí další podobné akce (BUKKVOLL 2007; POKALOVA 2015; ФИЛАТОВ 2020);
- zdravotnické zařízení je vedlejším cílem kombinovaného útoku, kdy primárním cílem byly jiné objekty a útok na zdravotnické zařízení má zvýšit chaos a ztráty na životech (Balad Ruz General Hospital, Baquba General Hospital, Irák (TOSINI 2010; UN High Commissioner for Refugees 2010));
- medializace a snaha šokovat (útok na Nemocnici Dašt-e-Barči (Bonnot a MSF AFGANISTAN 2020)).

Teroristické útoky často přicházejí s určitým zpožděním po započetí ozbrojených střetů (válka v Iráku, válka v Afghánistánu, Arabské jaro), tedy v době, kdy jsou již válčící strany konfliktem značně vyčerpány a ztrácí zábrany.

Je otázkou, jakou roli v teroristických útocích na nemocnice hraje otupělost účastníků konfliktu vůči násilí a jakou hraje medializace útoků.

Ve prospěch medializace jako sekundární příčiny hovoří to, že teroristické útoky na nemocnice (a teroristické útoky obecně) přicházejí se zpožděním a stabilně rostou. Na jedné straně tento trend koreluje s celosvětově narůstajícím počtem teroristických útoků, na straně druhé se ve zkoumaném období zdvojnásobil počet útoků na zdravotnická zařízení jako taková. Pokud by do počtu teroristických útoků byly zahrnuty také kybernetické útoky, nárůst by byl ještě výraznější.

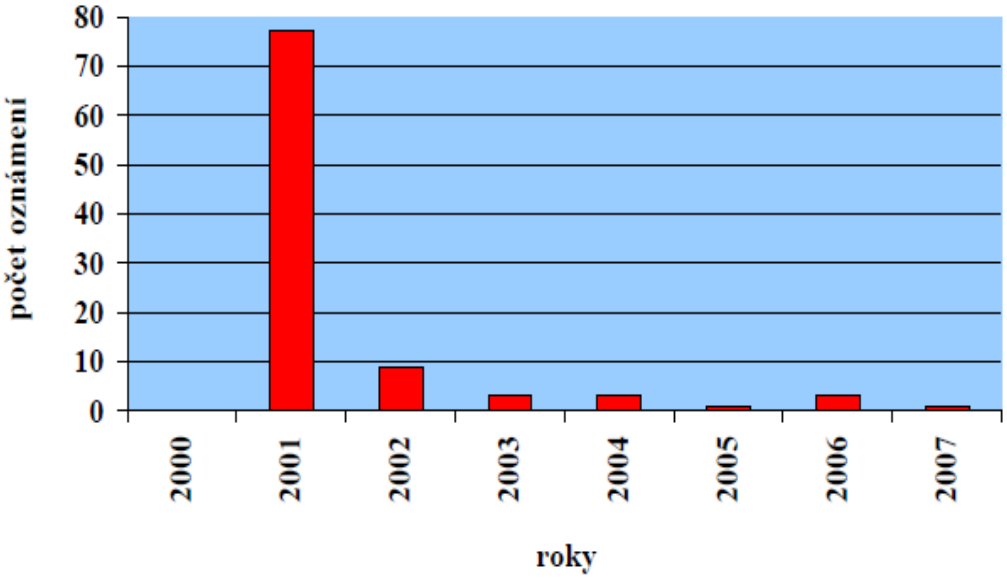
Myšlenka medializace negativních událostí, které vyvolávají následování, je postavena na psychologickém efektu, který je znám z podobných oblastí. Např. tzv. Wertherův efekt, kdy po publikování Goethova románu Utrpení mladého Werthera páchali mladí muži ve zvýšené míře sebevraždu. Následně došlo k potvrzení na základě sociologických výzkumů, že po medializaci sebevraždy může v následujících týdnech dojít ke zvýšenému počtu sebevražd. (LUTTER, ROEX a TISCH 2020; KASÍK 2016)

Opačný efekt způsobila v osmdesátých letech dohoda rakouských médií, která snížila medializovanou atraktivitu sebevražd, následkem čehož došlo k poklesu sebevražd o 75 %. (SONNECK, ETZERSDORFER a NAGEL-KUESS 1994)

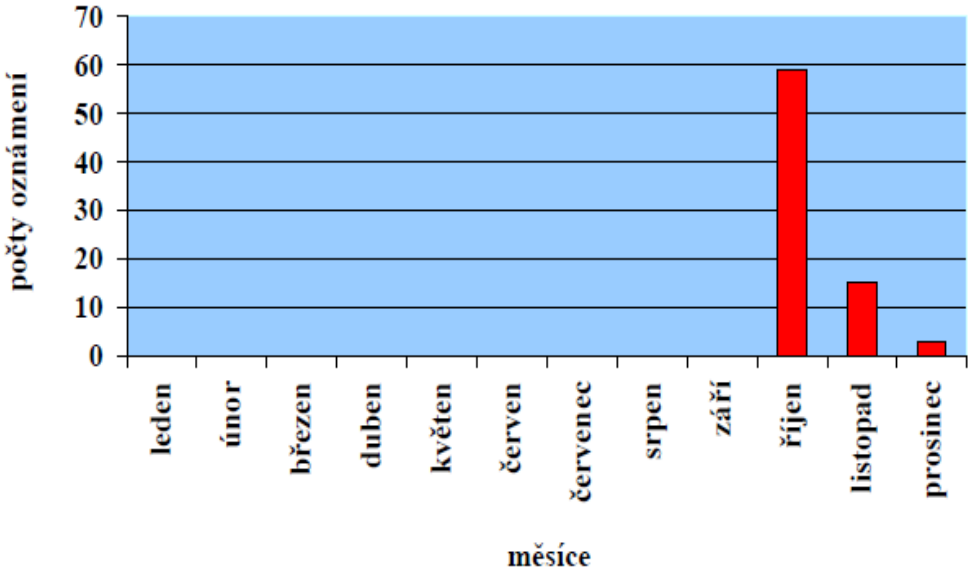
Obdobně se studie soustředí na příčinnou souvislost mezi medializací teroristického činu a jeho následným opakováním.

Například Michale Jetter analyzoval světové teroristické útoky mezi lety 1970 – 2012. Odhalil, že zvýšená medializace teroristického činu zvyšuje šanci na teroristický útok v dalších dnech o 11 až 15 procent. (Jetter 2015)

Rovněž v bakalářské práci „Vliv medializace terorismu po roce 2001 ve vztahu na nárůst zneužití tohoto jevu ve společnosti“ (Hnilička 2010) sledoval Petr Hnilička počty oznámení na hrozby teroristického útoku za jednotlivé roky v souvislosti s útoky z jedenáctého září v Jihočeském kraji, ke kterému vyjížděl Hasičský záchranný sbor Jihočeského kraje, kde je vidět příčinná souvislost mezi útoky jedenáctého září a počtem oznámení.



Obrázek 27 – Počty oznámení teroristických útoků 2000 – 2007 (Hnilička 2010)



Obrázek 28 – Počty oznámení teroristických útoků v roce 2001 (Hnilička 2010)

Podobná souvislost je také patrná z rozborů v kapitole 5. V případě větších ozbrojených konfliktů obvykle útoky probíhají ve vlnách:

- ozbrojený konflikt na určitém místě;
- prodleva;

- teroristický útok na zdravotnické zařízení a jeho medializace;
- několik následujících útoků na zdravotnické zařízení případně jiné měkké cíle (viz dále popsaná souvislost útoku na Buďonnovskou oblastní centrální nemocnici v první čečenské nemocnice a útok na několik dalších měkkých cílů v druhé čečenské válce), přičemž brutalita útoků se zvyšuje;
- po konci ozbrojeného konfliktu v oblasti eliminace teroristických útoků v oblasti.

Například z následující tabulky ukazující časovou souvislost mezi útoky v Afgánistánu, vyplývá, že 17 útoků z 30 bylo v následujících 90 dnech následováno minimálně jedním útokem, přičemž rovnoměrný rozestup mezi incidenty by byl 140 dnů a rozestup mezi zbývajícími incidenty je v průměru 280 dnů. Z toho 14 bylo realizováno v následujících 60 dnech.

Tabulka 27 – časové souvislosti – Afghánistán (vlastní)

Datum	Méně než 90 dnů posledního útoku	Méně než 60 dnů posledního útoku
21.05.2011	1064	1064
25.06.2011	35	35
15.04.2012	295	295
17.04.2012	2	2
11.06.2012	55	55
21.06.2012	10	10
14.08.2012	54	54
22.05.2013	281	281
17.08.2013	87	87
14.10.2013	58	58
24.04.2014	192	192
11.05.2014	17	17
09.06.2014	29	29
13.10.2014	126	126
18.02.2015	128	128
10.03.2015	20	20
14.07.2015	126	126
13.08.2015	30	30
12.09.2016	396	396
26.10.2016	44	44
08.03.2017	133	133
13.07.2017	127	127
22.07.2017	9	9

Pokračování tabulky na straně 84

Pokračování tabulky ze strany 83

27.01.2018	*189*	*189*
14.06.2018	*138*	*138*
23.07.2018	*39*	*39*
03.08.2018	*11*	*11*
09.07.2019	*340*	*340*
19.09.2019	*72*	*72*
11.12.2019	*83*	*83*

Lze samozřejmě namítat, že 60-90 dní zpoždění od posledního útoku může být náhoda, protože například sebevraždy po medializaci probíhají v rámci dnů až týdnů. V této souvislosti je třeba vzít v potaz, že například realizace bombového útoku obvykle nemůže být provedena ze dne na den. Od doby prvotního impulzu je třeba získat dobrovolníka, vycvičit ho, sehnat munici a naplánovat vhodný okamžik. Z tohoto důvodu odvozuji, že daný časový úsek je zvolen vhodně a kauzalitu potvrzuje.

Dřívější teroristické útoky (před rokem 2000) navíc obecně nebyly medializovány tolik jako v dnešní době.

Změnil se výrazně typ zpravodajství. Z konce 90. let se datuje internetové zpravodajství. 17. ledna 1991 začala operace Pouštní bouře, která bývá označována za první válku v přímém přenosu.

Jedním z prvních medializovaných útoků na nemocnice byl dříve popisovaný útok na nemocnici v Buďonnovsku. Současně útok skončil dosažením cílů útočníků a měl další významné důsledky:

- umožnil obrat v první čečenské válce;
- otřásl ruskou vládou a ozbrojenými složkami;
- zvedl odpor veřejného mínění proti válce s Čečenskem;
- z neznámého polního velitele učinil známého vůdce radikálního křídla čečenských bojovníků.

Tyto výsledky byly podle mého názoru pro ostatní teroristy lákavou výzvou. Jinými slovy, čím více se teroristické útoky na nemocnice medializují a čím více otřásají politickými scénami a veřejným míněním a umožňují teroristům dosahovat jejich cílů, tím se stávají pravděpodobnějšími.

Například Basaajev podobný scénář později zopakoval na dalších měkkých cílech, tedy při útoku na moskevské divadlo Dubrovka v roce 2002, při bombovém útoku na nemocnici v Mozdoku v roce 2003 a při beslanském školním masakru v roce 2004. I tyto události byly silně medializovány.

V případě rwandské genocidy popsané v kapitole 3 a 5 se rozběhla mediální propaganda, která přímo vyzývala ke genocidě Tutsiů. Objevila se řada extremisticky zaměřených deníků, negramotným byl obsah předčítán. Zlomovým projevem byla řeč jednoho z Habyarimanových přívrženců Léona Mugusera z listopadu 1992 o potřebě „vyhlazení a likvidaci tutsijské havěti a špíny." (Fujii 2004, s.103) Rádio RTLM vysílalo celý den protitutsijské projevy, písně a anekdoty s texty zaměřenými proti Tutsiům.

Po roce 2000 se rozšířily sociální sítě. Internet přinesl méně formální formu žurnalistiky a také možnost prezentovat teroristické činy online velkému množství příjemců. Sociální sítě začaly být využívány k sebeprezentaci teroristů i plánování útoků.

Evropská Unie prosadila provozovatelům sociální sítí povinnost mazání teroristického obsahu nařízením Evropského parlamentu ze dne 29. dubna 2021 o potírání šíření teroristického obsahu online (EVROPSKÝ PARLAMENT 2021). Odstavec 17 tohoto nařízení stanoví, že: *„S ohledem na rychlost šíření teroristického obsahu napříč online službami by měla být poskytovatelům hostingových služeb uložena povinnost zajistit, aby byl teroristický obsah určený v příkazu k odstranění odstraněn nebo přístup k němu znemožněn ve všech členských státech do jedné hodiny od přijetí příkazu k odstranění."* Toto nařízení vyvolalo v době jeho schvalování řadu kontroverzí. Jeho odpůrci namítali, že se jedná o krok k omezení svobody projevu a že bude zneužíván při posilování autoritářsky laděných vlád v Evropě. Dále argumentovali vymahatelností, protože teroristický obsah bývá nahráván ve velkém množství kopií, které není možné rychle zlikvidovat.

Příznivci nařízení naopak oponovali tím, že cílem je omezit koordinace teroristických útoků, sdílení návodů na výrobu výbušnin a omezit reklamu terorismu, která může nalákat nové členy.

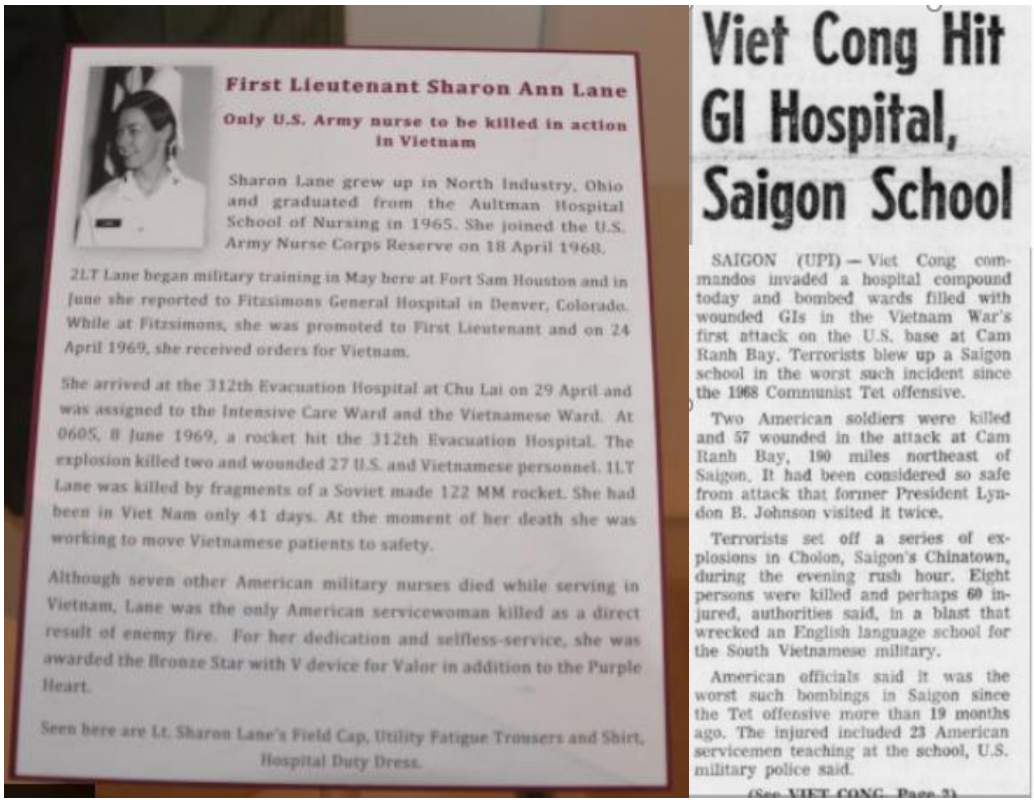
Otázkou „reklamy" terorismu se po roce 1990 zabývá řada studií například (Zubair Iqbal 2015; Archetti 2013). Řada autorů zejména z 90 let upozorňuje na to, že jak mediální články, tak studie se často opírají více o pocity než vědecká fakta (Archetti 2013), což se týká studií o vlivu médií na terorismus. Články po roce 2010 (Jetter 2015, Hnilička 2010)

se již k této kauzalitě stále častěji přiklánějí a dokládají ji studiemi nad hladinou statistické významnosti.

Pokud se na tento vztah podíváme metodou komparace, tak je zřejmé, že jak v literatuře, tak v ojedinělých článcích se v dřívější době objevovala spíše suchá fakta o útočnících, způsobu útoků, počtu obětí a materiálních škod, zatímco dnešní zpravodajství o terorismu často v případě větších incidentů probíhá online, se zaměřením na atmosféru s podrobnými záběry na místa včetně krvavých stop a emotivních rozhovorů s příbuznými obětí.

Na následujících stránkách je srovnání líčení o teroristických útocích v dobovém tisku.

Novinová zpráva o útoku z roku 1969



First Lieutenant Sharon Ann Lane

Only U.S. Army nurse to be killed in action in Vietnam

Sharon Lane grew up in North Industry, Ohio and graduated from the Aultman Hospital School of Nursing in 1965. She joined the U.S. Army Nurse Corps Reserve on 18 April 1968.

2LT Lane began military training in May here at Fort Sam Houston and in June she reported to Fitzsimons General Hospital in Denver, Colorado. While at Fitzsimons, she was promoted to First Lieutenant and on 24 April 1969, she received orders for Vietnam.

She arrived at the 312th Evacuation Hospital at Chu Lai on 29 April and was assigned to the Intensive Care Ward and the Vietnamese Ward. At 0605, 8 June 1969, a rocket hit the 312th Evacuation Hospital. The explosion killed two and wounded 27 U.S. and Vietnamese personnel. 1LT Lane was killed by fragments of a Soviet made 122 MM rocket. She had been in Viet Nam only 41 days. At the moment of her death she was working to move Vietnamese patients to safety.

Although seven other American military nurses died while serving in Vietnam, Lane was the only American servicewoman killed as a direct result of enemy fire. For her dedication and selfless-service, she was awarded the Bronze Star with V device for Valor in addition to the Purple Heart.

Seen here are Lt. Sharon Lane's Field Cap, Utility Fatigue Trousers and Shirt, Hospital Duty Dress.

Viet Cong Hit GI Hospital, Saigon School

SAIGON (UPI) — Viet Cong commandos invaded a hospital compound today and bombed wards filled with wounded GIs in the Vietnam War's first attack on the U.S. base at Cam Ranh Bay. Terrorists blew up a Saigon school in the worst such incident since the 1968 Communist Tet offensive.

Two American soldiers were killed and 57 wounded in the attack at Cam Ranh Bay, 190 miles northeast of Saigon. It had been considered so safe from attack that former President Lyndon B. Johnson visited it twice.

Terrorists set off a series of explosions in Cholon, Saigon's Chinatown, during the evening rush hour. Eight persons were killed and perhaps 60 injured, authorities said, in a blast that wrecked an English language school for the South Vietnamese military.

American officials said it was the worst such bombings in Saigon since the Tet offensive more than 19 months ago. The injured included 23 American servicemen teaching at the school, U.S. military police said.

(See VIET CONG, Page 2)

Obrázek 29 – Zpráva o útoku z roku 1969 (DeKunder 1969); Novinová zpráva o útoku z roku 1969 (Desert Sun 1969)

V novinové zprávě je stručně shrnuto, co se stalo, kde, kolik bylo mrtvých, zraněných, stručný životopis zabité zdravotní sestry.

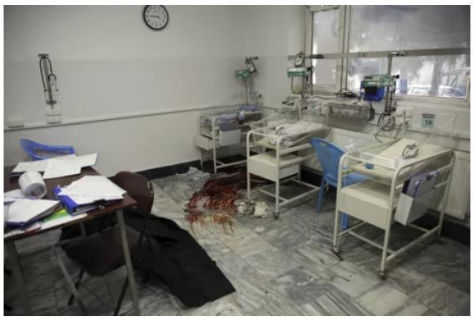
Zpráva z útoku v roce 2020

Teroristické útoky neutichají ani v době světové pandemie koronaviru, tento týden neznámí ozbrojenci zaútočili na porodnici v afghánské metropoli Kábulu, jejich řádění si vyžádalo 24 mrtvých. Mezi oběťmi jsou dva novorozenci, jejich matky i zdravotní sestry a jeden policista, informovala agentura AP. K násilnému činu se zatím nikdo nepřihlásil a ani není jasné, proč se terčem radikálů stala právě nemocnice na západě hlavního města Afghánistánu.

Ozbrojenci přepadli zdravotnické zařízení, které spolupracuje s mezinárodní organizací Lékaři bez hranic (MSF), v úterý 12. května ráno a **několik hodin bojovali s příslušníky afghánských bezpečnostních sil. Těm se podařilo evakuovat z objektu asi stovku lidí**. Prvotní bilance hovořila o 16 mrtvých, nový počet obětí na tiskové konferenci oznámil náměstek ministra zdravotnictví Wahid Madžrúh. **Šestnáct lidí bylo podle něj zraněno.**

Zázrak ve chvíli masakru

„Jsem stále v šoku, víte, bohužel už jsme si zvykli vídat mrtvá těla po útocích. Ale tohle? Prostřílené matky a čerstvě narozené děti? To byl horor," řekl Madžrúh. Zmínil se také o tom, že během masakru porodila jedna z nastávajících matek. **„Dítě a matka jsou v pořádku. Je to zázrak,"** oznámil Madžrúh, jeho slova potvrdili i MSF.



Teroristický útok v nemocnici v Kábulu si vyžádal 24 obětí, včetně dvou novorozenců, (14.05.2020). | ČTK/AP/Rahmat Gul

„Začali střílet, jen co vešli do dveří," popsal pro stanici Tolo jeden z kábulských lékařů. **„Čtyři matky byly zabity přímo na svém pokoji**, dvě se schovaly a přežily. **Jedna rodička zalehla inkubátor, aby zachránila své dítě. Byla to devastující scéna**, lidé křičeli a pobíhali v naprosté panice," vypověděl.

Reportéři, kterým se záhy po útoku podařilo dostat do porodnice, doplnili, že útočníci střídali v každém pokoji. **„V poporodním pokoji se po zemi válela těla,"** řekli o hrůze v nemocnici.

„Máma se domů nikdy nevrátí."

Zoufalí manželé, otcové, bratři a rodiny rodiček čekali před porodnicí a prosili vojáky o nějakou zprávu. „Bylo zmasakrováno přes dvacet žen a dětí, dalších 16 civilistů bylo zraněno. **Tohle byl barbarský a zbabělý teroristický útok,"** prohlásil ředitel státních médií Faroz Bašíří. **„18 čerstvě narozených dětí zůstalo bez matky,"** dodal.

Utekly před ISIS a živoří v uprchlických táborech. Tisícovkám žen zabrali domy i pozemky

„Moje žena Hadžár měla porodit naše druhé dítě, teroristi ji zastihli na porodním sále, nevím, co dělat, nevím, jak mám naší šestileté holčičce říct, že máma ani malý bráška se z nemocnice už nikdy nevrátí," svěřil se tisku truchlící Mohammad Hussajn.

Tchýně pláče pro mrtvého vnoučka

Zainab porodila těsně před útokem, svého vymodleného syna pojmenovala Omid, což v jejím jazyce znamená naděje. Roky měli s manželem problémy počít, když začala střelba, byla Zainab v koupelně. **Vystrašená běžela zpátky do pokoje, kde našla svého 4 hodiny starého synka zastřeleného,** její příběh s reportéry Reuters sdílela její tchýně.

„Byl to můj nápad vzít Zainab do nemocnice, chtěla jsem zajistit, aby porod proběhl v naprostém pořádku. Teď domů povezu zlomenou snachu a mrtvého vnoučka, na miminko čekali sedm let," vypověděla Zahra Muhammadíová. Útok silně poznamenal i vojáky, kteří vynášeli novorozence v zakrvácených dekách do přistavených sanitek, kde lékaři bojovali o jejich život.

„První zvuk, první hlasy, které tihle novorozenci na světě slyšeli, byl zvuk střel a nářek umírajících. Tohle je jejich první životní zkušenost, stali se cílem ve válce, za kterou oni ani jejich matky nenesou žádnou vinu nebo odpovědnost," uvedla Šahárzád Akbárová, ředitelka nezávislé afghánské komise pro lidská práva. **„Budou jejich životy, stejně jako ty naše, formované válkou?"** dodala na svém twitteru.

V ukázce článku z roku 2020 je před stručnými skutečnostmi upřednostněn naturalistický popis tragédie a emoce. Článek je působivý. Podporuje atmosféru strachu, nejistoty, napětí a znechucení, která teroristům vyhovuje:

- „zázrak ve chvíli masakru";
- „máma se domů nikdy nevrátí";
- „tchýně pláče pro mrtvého vnoučka";
- „první zvuk, první hlasy, které tihle novorozenci na světě slyšeli, byl zvuk střel a nářek umírajících".

Obrázek 30 – Novinový výstřižek z roku 2020 (ČTK a Jichová 2020)

Na základě výše uvedeného si jako další sekundární příčinu útoků zdůvodňuji jejich vysokou medializací a snadnou dosažitelností cíle. Teroristické organizace si začaly uvědomovat vysoký mediální a nátlakový potenciál, který útok na nemocnice skýtá.

Důvodem může být rostoucí publicita a prostor, který je takovým zprávám poskytován, šíření děsivých záběrů na sociálních sítích a další aspekty související s rozvojem médií a internetového propojení, které umocňuje dopad akce na psychiku.

Obdobně je tomu v případě kybernetických útoků na české nemocnice. První velký kybernetický útok v Benešově nebyl výrazně medializován a nebyl následován žádným významným útokem. Oproti tomu, kybernetický útok na Fakultní nemocnici v Brně probíhal na vlně strachu, která Evropu i Českou republiku zachvátila s nástupem první vlny nemoci COVID-19. Noviny a internetová média se mu obšírně věnovaly. Tento útok byl v rychlém sledu následován dalšími útoky v horizontu jednoho měsíce. Útoky spolu pravděpodobně nesouvisely (jiný typ útoku i použitý virus). Útoky následující byly tedy nejspíš inspirovány útokem prvním a to v takové míře, že to neuniklo zahraničním novinářům a politikům. To pravděpodobně povzbudilo další hackery k útoku na další nemocnice.

Podporou pro argument medializace je to, že zabezpečení českých nemocnic se v průměru neliší od velkých světových nemocnic (viz výsledky 5. kapitoly), přesto se české nemocnice ocitly v nadprůměrném zájmu hackerů. Žádný jiný evropský stát v daném období nehlásil takový masivní kybernetický útok. Jedním z nabízejících se vysvětlení je, že kybernetický útok na jednu z klíčových českých nemocnic v době pandemie, byl natolik lákavým mediálním cílem, že přitáhl další útočníky, ať již jejich cílem byl vyděračský nebo teroristický útok.

Další možnou variantou příčiny útoku je soustředěný nepřímý politický tlak některé ze zemí nebo skupin, které se snaží Českou republiku destabilizovat, o němž by svědčil již dříve zmiňovaný výrok amerického ministra zahraničí (ČTK a ČT24 2020).

Poslední analogii představuje případ ostravského střelce. Nemoc si začal sugerovat v létě roku 2019, hledal články na internetu, zadával klíčová slova o sebevraždách a vraždách, současně došlo mezi létem a prosincem k řadě útoků zbraněmi, jeden z článků v říjnu 2019 dokonce popisoval vlastní výrobu zbraní střelce z jiného útoku v Německu. Začátkem prosince došlo ke střelbě. Souvislosti mohou být náhodně, přesto, pokud střelec opravdu klíčová slova vyhledával, musel na články narazit a mohly ho tedy ovlivnit.

Útok na porodnici v Afghánistánu měl dle chování teroristů jasný cíl a tím bylo šokovat. Jiný cíl není pravděpodobný – nejednalo se o zisk či strategický objekt. Jednalo se čistě o to, napadnout ty nejzranitelnější a přilákat tak pozornost. To se i kvůli medializaci útočníkům podařilo.

Pokud shrnu výsledky svého zkoumání, vychází mi jako hlavní příčiny teroristických útoků na zdravotnická zařízení dlouhodobý ozbrojený konflikt v dané lokalitě a stále silnější medializace teroristických útoků.

6.1.2 Průběh násilných teroristických útoků na zdravotnická zařízení

Co se týká průběhu násilných teroristických útoků, z výsledků vyplývá, že stabilně nejčastějším způsobem útoku je bombový útok s výjimkou let 1992 – 1998, kdy byl tento typ útoků početně vyrovnán ozbrojenými útoky. Počet bombových útoků procentuálně narůstá. Bombový typ útoku teroristé volí pravděpodobně z toho důvodu, že nevyžaduje velké plánování, ani velký počet útočníků. Je třeba, aby byl k dispozici jeden nebo několik sebevražedných atentátníků a trhavina.

To by se v našich podmínkách mohlo zdát jako náročný cíl, ale je třeba si uvědomit, že v místech dlouho sužovaných ozbrojenými konflikty je řada lidí, kteří nemají co ztratit a jsou snadno ovlivnitelní vyššími cíli, ať se jedná o politickou propagandu, nebo náboženský fanatismus. Stejně snadné je získat v oblastech ozbrojených konfliktů dostatek výbušnin k provedení útoku.

Průběh útoků se v čase mění – přibývá kombinovaných útoků, kdy jsou nemocnice sekundárním cílem. Jako primární cíl je zvolen jiný měkký cíl a nemocnice je paralyzována výbuchem v době, kdy jsou do ní sváženi ranění. Roste i brutalita útoků.

Co se týká odpovědi na útok, záleží na konkrétní situaci. Pokud je konflikt izolovaný a na místě s dobře vybudovanou strukturou záchranného systému, je odpověď rychlá a profesionální (např. Musgrave Park Hospital v severním Irsku a útok střelce ve Fakultní nemocnici Ostrava) a v takovém případě se podaří řadu raněných zachránit a zamezit dalším ztrátám na životech.

Pokud se jedná o hybridní útok při zasažení více cílů záchranného systému, schopnost reakce klesá. V místě cílené likvidace civilního obyvatelstva (Rwanda v průběhu

občanské války v 90. letech), se reakce na útoky omezuje na přestěhování nemocnice do provizorních podmínek méně exponované lokality. Místo léčby se z nemocnice stává provizorní azylové místo.

6.1.3 Důsledky násilných teroristických útoků na zdravotnická zařízení

Vzhledem k tomu, že se ve většině případů jedná o bombové útoky, dochází při nich k poškození budov a zařízení nemocnic v dnešních cenách v řádech desítek až stovek milionů, v největších případech škody dosahují až miliardových částek. Současně dochází k omezení nebo zastavení provozu pro spádovou lokalitu.

Neméně významným důsledkem jsou ztráty na životech. Podle výzkumu se útoky s minimálně pěti oběťmi podílely na celkových útocích na zdravotnická zařízení v průměrně 15 % případů zkoumaného období v letech 1985 – 2019, přičemž oscilovaly mezi 7 % v letech 1985-1991 a 35 % v letech 1999-2005.

Dalším důsledkem násilných teroristických útoků je jejich medializace, která se sama o sobě stává sekundární příčinou dalších teroristických útoků, jak bylo diskutováno v kapitole 6.1.1.

Je otázkou, co by pomohlo snížit počet teroristických útoků na zdravotnická zařízení, nebo alespoň jejich dopadu. Legislativa je v tomto ohledu dostatečná, protože nemocnice jsou chráněny podle humanitárního práva. Snížení počtu ozbrojených konfliktů je otázkou geopolitickou a mimo možná opatření.

Jako určitá cesta se jeví regulace medializace útoků. Inspirací by mohla být již zmiňovaná dohoda rakouských médií v osmdesátých letech, která snížila medializovanou atraktivitu sebevražd, následkem čehož došlo k poklesu sebevražd o 75 %. (Sonneck, Etzersdorfer a Nagel-Kuess 1994) a dále Nařízení Evropského parlamentu ze dne 29. dubna 2021 o potírání šíření teroristického obsahu online. (EVROPSKÝ PARLAMENT 2021)

V současnosti nejsou standardní média, jako jsou televize, rádia a noviny jedinými aktéry mediálního prostoru. Na sociálních sítích se objevují soukromé zprávy a videa, média jako je YouTube mají algoritmus, který nabízí divákům stále extrémnější obsah, aby udržely jejich pozornost. Přesto je i tady viditelná snaha o změnu. Například

Ministerstvo vnitra připravilo návrhu zákona proti šíření teroristického obsahu on-line, kdy policisté budou moci přikázat českým i evropským poskytovatelům hostingových služeb, aby znepřístupnily teroristický obsah (teroristický útok, záznam zabíjení) hodinu po zaslaném příkazu. Tento zákaz vychází z nařízení Evropské unie o potírání šíření teroristickéo obsahu on-line. (ČTK 2022)

Shrnu-li obsah této kapitoly, tak hlavními příčinami násilných útoků na zdravotnická zařízení jsou ozbrojené konflikty v dané oblasti, probíhají nejčastěji formou bombového útoku a důsledkem je v průměrně 14 % případů více než 5 obětí na životech a dále poškození budov a zařízení. Dalším důsledkem je medializace, která se stává sekundární příčinou dalších útoků.

6.2 Diskuze k analýze kybernetických útoků na zdravotnická zařízení a připravenosti vybraných zdravotnických zařízení na kybernetický útok

6.2.1 Příčiny kybernetických útoků na zdravotnická zařízení

Z výzkumu je patrné, že kybernetické útoky probíhají již několik let, ale právě kombinace vyhrocené situace v souvislosti s první vlnou COVID-19 ve spojitosti s velkými škodami, které tento útok napáchal ve Fakultní nemocnici Brno (více než 150 milionů korun a část nenávratně ztracených dat), byla důvodem k masivní celosvětové medializaci. Dosud nebylo vyšetřeno, kdo stál za těmito útoky. Stopy útoku ve Fakultní nemocnici Brno míří k finančním vyděračům. Naznačuje to směr vyšetřování i použitý virus. Kryptovirus Defray se specializuje právě na požadování výkupného. (Krajíčková 2021)

Další útoky, které v rychlém sledu následovaly, se útoky pravděpodobně inspirovaly, protože proběhly v rychlém sledu, přestože se jejich charakter liší.

Z pohledu útočníka jsou zdravotnická zařízení výhodným cílem:

- škoda v rámci desítek až stovek milionů korun je z hmotného pohledu srovnatelná s bombovým útokem;
- šíří obavy;
- obvykle nižší úroveň zabezpečení než u soukromých nezdravotnických subjektů;

- lze útočit na dálku;
- možnost matení a dezinformací;
- možnost kombinovaného útoku s ozbrojeným útokem nebo přírodní katastrofou;
- nízké riziko dopadení útočníků.

To indikuje, že jednou z příčin je nedostatečné zabezpečení nemocnic, které v kombinaci s vysokými škodami útočníky přitahuje.

Tento předpoklad byl zkoumán hypotézou 2: „Část českých nemocnic stále není dostatečně chráněna proti kybernetickému útoku.“ Použito bylo eticky přípustné zkoumání zabezpečení internetových stránek pomocí nástroje Mozilla observatory, jak bylo popsáno v kapitolách 4 a 5.

Výzkumná část ukázala, že část českých zdravotnických zařízení stále nemá dobře zabezpečeny internetové stránky, ale jsou na tom obdobně jako přední světové nemocnice. Současně jsou zabezpečeny hůře než soukromé nezdravotnické subjekty. Je samozřejmě možné podat dvě námitky:

1. že nedostatečné zabezpečení internetových stránek ještě nemusí znamenat pochybení systému IT systému jako takového;
2. že ochranu nemocnic a soukromých nezdravotnických subjektů nelze srovnávat.

Námitka 1 je relevantní, přesto ale v řadě případů tato kauzalita funguje. Navíc, ve výzkumné části bylo v několika případech ukázáno zřejmé pochybení, které by případným hackerům cestu do systému významně usnadnilo, protože by internetové stránky sloužily jako vstupní brána pro útoky.

Odpověď na námitku 2 je, že ochrana nemocnic by měla být na stejné nebo vyšší úrovni než úroveň ochrany soukromých nezdravotnických zařízení, protože se jedná o lidské životy a zdraví a v případě vyřazení nemocnice z provozu se ztráty mohou vyšplhat až do stovek milionů korun.

Jako hlavní příčinu kybernetických útoků na nemocnice dle výzkumu vidím kombinaci nedostatečné ochrany nemocnic a vysokého ničivému dopadu na jejich fungování. To má pro útočníky velký mediální potenciál a vede je to k dalšímu zvyšování aktivity.

Byla potvrzena hypotéza 2, podle níž část českých nemocnic stále není dostatečně chráněna proti kybernetickému útoku na webové stránky.

Připravenost má ale zlepšující se trend, jak je patrné z kapitoly 5.

Současně se charakter kybernetických útoků na zdravotnická zařízení nekoncentruje na území státu, kde probíhá ozbrojený konflikt, právě útoky na české nemocnice jsou toho důkazem. Kromě potenciálních ekonomických vyděračů mohou útoky na nemocnice odrážet zvyšující se napětí v regionu, případně odrážet hru různých mocenských stran. Státní autority i zdravotnická zařízení si na tuto realitu začínají zvykat a připravovat se. Například Americká asociace nemocnic (Americal Hospital Association = AHA) v den útoku Ruské federace na Ukrajinu vydala varování, ve kterém nabádala nemocnice, aby zvýšily své zabezpečení proti ruskému kybernetickému útoku. (AHA 2022)

Obecně se kybernetických útoků začíná využívat k ochromení cíle těsně před útokem. Například ukrajinské státní i soukromé organizace se staly masivním cílem kybernetických útoků těsně před započetím ruské invaze.

Kybernetické útoky bývají také využívány při odvetě. Například hackeři celého světa začali po invazi na Ukrajinu využívat nejjednodušší a nejstarší techniku k ochromení ruských institucí. Touto technikou je Distributed Denial of Service (DDoS), které spočívá v přehlcení serverů masivními požadavky. Jeho dopad můžeme omezit instalací nejnovějších bezpečnostních záplat, filtrováním protokolu UDP požadavků z internetu ve firewallu, vypnutím všech nepoužívaných služeb a rozložením zátěže na záložní zdroje dat. (UDP = User Datagram Protocol, nemá záruku doručení a regulaci zahlcení sítě.)

Aktivně se útokům na Ruskou federaci věnuje skupina Anonymous, odborníci ale v tomto případě varují před bezhlavým zasažením civilních cílů včetně zdravotnických zařízení. V této souvislosti je třeba také připomenou dřívější incident skupiny Anonymous, která v roce 2014 na dva týdny vyřadila z provozu Bostonskou dětskou nemocnici. Cílem bylo zasáhnout do soudu, který se týkal opatrovnictví Justiny Pelletierové, kdy došlo ke sporu mezi rodiči a nemocnicí, v níž byla umístěna na uzavřené psychiatrické oddělení.

Na jedné straně etický vnímaný záměr hackerů pomoci rodině v boji proti instituci vyústil v ohrožení zdraví mnoha dětských pacientů. Hlavní pachatel byl odsouzen k deseti letům vězení (Nate 2019)

Jak je patrné z předchozí diskuze, příčin kybernetických útoků na zdravotnická zařízení je více, než u klasických teroristických útoků:

- ozbrojený konflikt na daném území;
- účast na ozbrojeném konfliktu mimo přímou oblast, kde konflikt probíhá fyzicky
- zvyšující se napětí v oblasti;
- ekonomické vydírání;
- snaha upozornit na konkrétní problém formou vydírání;
- součást hybridního útoku na začátku války nebo synchornizace s jinými ozbrojenými útoky.

6.2.2 Průběh kybernetických útoků na zdravotnická zařízení

Průběh kybernetických útoků se liší. U Fakultní nemocnice Brno se jednalo o tzv. vyděračský virus, který zašifruje data a požaduje po nemocnicích výkupné za jejich navrácení. U dalších nemocnic pachatelé útočí pomocí malwaru, jehož cílem je primárně škodit, má tedy charakter teroristického činu. Ani u prvního typu útoku není teroristické pozadí zcela vyloučeno, protože pachatele nebyli dopadeni a kyberteroristický útok může být jako vyděračský útok maskován. Například Jevgenij Kasperskij, zakladatel ruské antivirové firmy Kaspersky Lab, však zastává názor, že útoky na nemocnice v době pandemie jsou specifickým druhem terorismu, protože míří na kritickou infrastrukturu a lidské životy.

Sama firma Kaspersky Lab a její zakladatel Jevgenij Valentinovič Kasperkij vyvolává v posledních letech a zejména posledních měsících obavy a rozdílné názory. Na jednu stranu je Kasperskij jedním z největších odborníků na kybernetickou bezpečnost na světě, na druhou stranu je jeho firma jako ruský podnikatelský subjekt podřízena legislativě Ruské federace, která umožňuje zpravodajským službám a silovým složkám narušit důvěrnost, dostupnost či integritu uchovávaných nebo zpracovávaných dat společností v její jurisdikci (NÚKIB 2022).

Americké státní úřady nepoužívají produkty firmy Kaspersky Lab od roku 2017, v roce 2018 vyzval Evropský parlament unijní státy k ukončení používání tohoto softwaru. V té době se ale jednalo o nepřímé důkazy, unijní státy tedy nepostupovaly jednotně. Do nové dimenze přenesla spory o firmu Kaspersky Lab válka na Ukrajině. Dne 15. března 2022 přidala americká FCC (Federální komise pro komunikaci) firmu Kaspersky Lab na

sankční list kvůli obavám o národní bezpečnost, obdobným způsobem varoval 15. března 2022 německý BSI (Spolkový úřad pro bezpečnost informačních technologií). (BSI 2022)

Národní úřad pro kybernetickou a informační bezpečnost zatím reagoval neutrálně a vydal krátké vyjádření ve smyslu, že nemá dostatečnou informační jistotu k tomu, aby vydal zákonné opatření, přesto upozorňuje na výše zmíněnou ruskou legislativu a možnou zhoršenou dostupnost služeb způsobenou izolací Ruska. (NÚKIB 2022). Aktuálně stále antivirus Kaspersky používá řada nemocnic, krajů. Podle zpráv, které proběhly tiskem před odevzdáním této diplomové práce, se Všeobecná zdravotní pojišťovna rozhodla ukončit používání tohoto antiviru, vzhledem k nedostatku času se mi nepodařilo tuto informaci ověřit u zdroje (poslal jsem na VZP dotaz, ale nedostal jsem dosud odpověď).

Sama firma Kaspersky Lab se nařčením od roku 2016 brání, přesunula část svých aktivit do Švýcarska, ale obecně nelze tuto hrozbu podceňovat. Nemusí se jednat o přímé napadení systému nemocnice nebo jiné organizace, ale například přístup k datům – třeba o nemocech či závislostech důležitých osob, nebo členů jejich rodiny a využití těchto informací k vydírání nebo zpravodajským akcím.

Je ale nutné mít na paměti, že válka o data se vede po celém světě, na sankčních listech jsou například čínské firmy a americká FBI vede dlouhodobě spor o utajení dat například s firmami FBI a Google.

Útoky na data přes softwary poskytovatelů služeb se všeobecně stávají stále vyšším rizikem.

Dalšími typy útoků jsou:

- DDoS (Distributed Denial of Service) – přehlcení klíčových uzlů požadavky, na základě nichž systémy přestanou pracovat;
- phishing – podvod postavený na lidské chybě;
- využití chyb v softwaru (internetové stránky, ale i přístroje).

Vzhledem k tomu, že kybernetické útoky na nemocnice jsou novinkou několika posledních let, dá se očekávat jejich další vývoj a zdokonalování útočníků. Dá se očekávat také hybridní trend kombinace násilných teroristických útoků a kyberútoků, ostatně

hybridní útok zažily české nemocnice oslabené první vlnou koronavirové pandemie na jaře 2020.

Dá se také očekávat, že se teroristé zaměří i na zdánlivě nečekané cíle, které jim mohou přinést cestu do systému či poškození zdraví pacientů. Bezpečnostní chybu může obsahovat lednička na sesterně napojená na síť, systém automatického zamlouvání místností, inzulinová pumpa nebo kardiostimulátor.

6.2.3 Důsledky kybernetických útoků na zdravotnická zařízení

Důsledky kybernetických útok na zdravotnická zařízení jsou zatím primárně materiální (desítky až stovky milionů korun). Přímé úmrtí v souvislosti s kybernetickým útokem nebylo dosud na rozdíl od zahraničí v českém zdravotnickém zařízení zaznamenáno, dopady na zdraví jsou ale diskutabilní. Odkládané operace nebo návštěvy lékaře mohou vést ke snížené kvalitě lidského života v důsledku neléčených zdravotních omezení či bolesti a v případě pozdní diagnostiky také sekundárně k úmrtí pacienta.

Pozitivním důsledkem je zvyšování zabezpečení nemocnic, jejichž zřizovatelé do IT bezpečnosti začali ve větší míře investovat (např. 350 milionů u Fakultní nemocnice Plzeň).

6.2.4 Možnosti ochrany proti kybernetickým útokům

Cílem je, aby se nemocnice samy zřejmými chybami nestavěly do role terče. Ve výzkumné části byla nalezena bezpečnostní rizika u celé řady subjektů, jak v České republice, tak v zahraničí. Vyplývá z toho, že v případě zájmu mohou i průměrní útočníci najít stále hodně snadných cílů k útoku.

Je otázkou, jak by se nemocnice mohly ochránit. Obvyklou argumentací nad špatným zabezpečením jsou chybějící finanční prostředky. To je pravda, protože hackeři a tvůrci počítačových virů mají vždy náskok před společnostmi i v soukromém nezdravotnickém sektoru. Je třeba investovat do kvalitního softwarového, technického vybavení a lidských zdrojů.

Například Fakultní nemocnice Plzeň v roce 2021 investovala do kybernetické ochrany svého systému 351 milionů korun. (ČTK a Novinky 2021)

Na druhou stranu se tyto prostředky vrátí v „úsporách“ na způsobených škodách. I když částka 351 milionů vypadá hrozivě, a jen větší nemocnice si takovou investici mohou dovolit, jediný útok dosahuje škod v desítkách a nižších stovkách milionů a může se opakovat. Z tohoto pohledu je návratnost investice poměrně rychlá, na druhou stranu útočníci vyvíjejí stále nové techniky, je tedy třeba systém pravidelně vylepšovat.

V nejhorších případech, lze ale určité zvýšení provést i s minimem nákladů. Jedním z nich je přechod z HTTP protokolu na HTTPS protokol. Ten se dá zrealizovat relativně levně. Pro přechod na HTTPS je nutné nastavit SSL certifikát. Jeho získání a udržování se obvykle pohybuje v řádu stovek až tisíců korun za rok. Dále je třeba získat hosting, který s těmito certifikáty pracuje.

Následně je také třeba upravit další objekty na stránkách, které se načítají z HTTP protokolu. Nakonec je třeba přesměrovat HTTP na HTTPS.

Zvláště u stránek s uživatelským heslem tento zásah výrazně zvýší obtížnost vstupu do systému.

Dalším možným prvkem zabezpečení při nedostatku zdrojů je omezení systémů napojených na veřejnou internetovou síť.

Nejslabším článkem zabezpečení jako u většiny rizik je lidský faktor. Pracovníci by měli podstupovat pravidelná školení a praxi je propojit do rutiny (neodpovídat bezmyšlenkovitě na e-maily, neotvírat podezřelé přílohy, v případě podezření na útok okamžitě odpojit počítač od sítě).

Doporučení týkající se zvýšení bezpečnosti lez shrnout následovně:

- Zlepšení technického vybavení, které je možno čerpat mimo jiné z fondů Evropské Unie;
- zvýšení kapacit a ohodnocení zaměstnanců IT oddělení nemocnic;
- financování umožňující zapojení externích specializovaných konzultantů k preventivnímu odhalení bezpečnostních rizik a doporučení;
- školení zaměstnanců v oblasti bezpečnosti a jeho pravidelné opakování;
- omezení zaměstnanců přístupu k informacím, které nejsou nezbytně nutné;
- zamyšlení o tom, která zařízení jsou datově propojena a zda je jejich propojení nutné a žádoucí, případné zabezpečit citlivá data izolováním na intranetu.

7 ZÁVĚR

V diplomové práci byly sledovány dva cíle. Prvním z nich byla analýza příčin, průběhu a následků teroristických útoků na zdravotnická zařízení. Druhým cílem, byla analýza kybernetických útoků na zdravotnická zařízení a připravenosti vybraných zdravotnických zařízení na kybernetický útok, která byla ověřována eticky přijatelným výzkumem zranitelností internetových stránek.

Jako hlavní příčiny násilných útoků na nemocnice byly shledány oblasti násilných ozbrojených konfliktů, nejčastějším průběhem byl bombový útok. Důsledkem bývá často poškození budov a zařízení v průměrně 14 % útoků je více než 5 obětí na životech. Dalším důsledkem bývá medializace útoků, která se stává sekundární příčinou. Ideální by bylo omezit medializaci teroristických útoků, k čemuž spějí evropské legislativní iniciativy.

V rámci druhého cíle bylo zjištěno, že příčinami kybernetických útoků na nemocnice je kombinace jejich nedostatečného zabezpečení a výrazného efektu (ztráty v řádech desítek až stovek milionů korun a medializace). Největší české útoky byly provedeny pomocí ransomware (vyděračský virus), malware (škodlivý virus), DDoS (přehlcení systému požadavky) a phishing postavený na lidské důvěřivosti.

Důsledky kybernetických útoků se počítají v řádech desítek a stovek milionů korun, přesto mají i pozitivní důsledky v podobě zvyšujícího se zabezpečení nemocnic.

Ve výzkumu byla potvrzena hypotéza 1, že „Násilné útoky na zdravotnická zařízení korelují s místy ozbrojených konfliktů.“ a hypotéza 2, „Část českých nemocnic stále není dostatečně chráněna proti kybernetickému útoku.“

Byla také splněna hypotéza 3, že „Počet násilných teroristických útoků i kybernetických útoků na zdravotnická zařízení se zvyšuje.“

To jednoznačně podporuje myšlenku, že do připravenosti zdravotnických zařízení na kybernetický útok je potřeba investovat, protože trend má rostoucí tendenci a škody, které dosahují desítek, až stovek milionů se mohou opakovat.

8 SEZNAM POUŽITÝCH ZKRATEK

ICT	International Institute for Counter-Terrorism
GTD	Global Terrorism Database (Globální databáze terorismu)
START	National Consortium for the Study of Terrorism and Responses of Terrorism (Náročí konsorcium pro studium terorismu a odezvu na terorismus)
CSP	Content Security Policy (zásady zabezpečení obsahu)
XSS	Cross-site scripting (skriptování mezi weby)
CORS	Cross-Origin Resource Sharing (sdílení zdrojů odjinud)
HPKP	HTTP Public Key Pinning (připnutí veřejného klíče)
HTTP	Hypertext Transfer Protokol (hypertextový přenosový protokol)
HTTPS	Hypertext Transfer Protocol Secure (hypertextový přenosový zabezpečený protokol)
NÚKIB	Národní úřad pro kybernetickou bezpečnost
AHA	American Hospital Association
BSI	Bundesamt für Sicherheit in der Informationstechnik
DDoS	Distributed Denial of Service (přehlcení klíčových uzlů požadavky)
UDP	User Datagram Protocol (internetový protokol, který postrádá záruku doručení a regulaci zahlcení sítě)

9 SEZNAM POUŽITÉ LITERATURY

1. ADEBAYO, Anthony Abayomi. Implications of 'Boko Haram' Terrorism on National Development in Nigeria: A Critical Review. Mediterranean Journal of Social Sciences [online]. 2014, 2014, 5(16), 480-489 [cit. 2022-02-19]. ISSN 2039-2117. Dostupné z: doi:10.36941/mjss
2. AHA advises hospitals to protect against increased Russian cyberthreat. American Hospital Association [online]. 2022, Feb 24, 2022 [cit. 2022-04-23]. Dostupné z: (https://www.aha.org/news/headline/2022-02-24-aha-advises-hospitals-protect-against-increased-russian-cyberthreat
3. Akční plán k národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025 [online]. Národní úřad pro kybernetickou a informační bezpečnost, 2021, 26.7.2021, 22 [cit. 2021-11-21]. Dostupné z: https://www.nukib.cz/download/publikace/strategie_akcni_plany/akcni_plan_2021-2025.pdf
4. Annex: Reports of Attacks and Security Incidents in Iraq since April 2010 [online]. UN High Commissioner for Refugees, 2010 [cit. 2022-02-19]. Dostupné z: https://www.refworld.org/pdfid/517521334.pdf
5. ARCHETTI, Cristina. Terrorism, Communication, and the Media. In: Understanding Terrorism in the Age of Global Media: A Communication Approach. London: Palgrave Macmillan UK, 2013, s. 32--59. ISBN 978-1-349-34780-3. Dostupné z: doi:https://doi.org/10.1057/9781137291387_3
6. Bezpečnější zdravotnictví i řešení rizikových dodavatelů - Vláda schválila Akční plán ke strategii kybernetické bezpečnosti. NÚKIB [online]. Národní úřad pro kybernetickou a informační bezpečnost, 2021, 26. červenec 2021 [cit. 2021-11-21]. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/1735-bezpecnejsi-zdravotnictvi-i-reseni-rizikovych-dodavatelu-vlada-schvalila-akcni-plan-ke-strategii-kyberneticke-bezpecnosti/
7. BINET, Laurence, Jean-Marc BIQUET, Françoise BOUCHET-SAULNIER, Michiel HOFMAN, Fiona TERRY a Rafa VILASANJUAN. The violence of the new rwandan regime 1994-1995 [online]. 78 Rue de Lausanne CP 1016 1211 Geneva Switzerland: Médecins Sans Frontières International Movement, 2013 [cit. 2022-02-19]. Dostupné z: https://www.msf.org/sites/msf.org/files/2019-

04/MSF%20Speaking%20Out%20Violence%20of%20the%20new%20Rwandan%20regime%201994-1995.pdf

8. BIZIMANA, Jean Damascène. DOCTORS, NURSES AND MEDICAL STAFF COMMITTING GENOCIDE CRIME WHILE PRACTICING WITHIN HEALTH STRUCTURES IN THE SOUTHERN PROVINCE WITHOUT HUYE DISTRICT [online]. Republic of Rwanda - Kigali: National Commission for the Fight against Genocide, 2020, 15.5.2020 [cit. 2022-02-19]. Dostupné z: https://cnlg.gov.rw/fileadmin/user_upload/Doctors__Nurses_and_Medical_staff_committing_Genocide_crime_while_practicing_within_health_structures_in_the_southern_province_without_Huye_District.PDF
9. BONNOT, Frederic a MSF AFGANISTAN. Afghanistan: Pregnant women and babies attacked in Kabul hospital. Doctors Without Borders [online]. 2020, 13.5.2020, 2020 [cit. 2022-02-19]. Dostupné z: https://www.doctorswithoutborders.org/what-we-do/news-stories/news/afghanistan-pregnant-women-and-babies-attacked-kabul-hospital
10. BUKKVOLL, Tor. Waiting for the next Beslan: Russia's handling of major hostage-takings [online]. Norwegian Defence Research Establishment, 2007, 8.8.2007 [cit. 2022-02-19]. ISBN 978-82-464-1254-2. Dostupné z: http://18.195.19.6/bitstream/handle/20.500.12242/2041/07-01888.pdf
11. BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten. Bundesamt für Sicherheit in der Informationstechnik [online]. Bonn, 2022, 15.03.2022 [cit. 2022-04-23]. Dostupné z: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html
12. Ceginformacio. Ceginformacio.hu [online]. 2021 [cit. 2022-02-20]. Dostupné z: https://www.ceginformacio.hu/cr9210293133_CZ
13. CIMPANU, Catalin. Vulnerabilities found in GE anesthesia machines. ZDNet [online]. ZDNET, A RED VENTURES COMPANY, 2019, July 9, 2019 [cit. 2021-11-28]. Dostupné z: https://www.zdnet.com/article/vulnerabilities-found-in-ge-anesthesia-machines/
14. COLLIER, Kevin. Major hospital system hit with cyberattack, potentially largest in U.S. history: Computer systems for Universal Health Services, which has more than 400 locations, primarily in the U.S., began to fail over the weekend. NBC News [online]. NBC Universal, 28.9.2020 [cit. 2022-02-01]. Dostupné z:

https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254

15. Cyber defence, NATO [online]. NORTH ATLANTIC TREATY ORGANIZATION, 2021, 02 Jul. 2021 [cit. 2021-11-21]. Dostupné z: https://www.nato.int/cps/en/natohq/topics_78170.htm
16. ČTK a Darina JÍCHOVÁ. Teroristé zaútočili na porodnici, při masakru s 24 mrtvými se narodilo i zdravé dítě. Blesk.cz [online]. CZECH NEWS CENTER, 14. května 2020 [cit. 2022-01-30]. Dostupné z: https://www.blesk.cz/clanek/zpravy-svet/643688/teroriste-zautocili-na-porodnici-pri-masakru-s-24-mrtvymi-se-narodilo-i-zdrave-dite.html
17. ČTK a IDNES.CZ. Kybernetický útok stál nemocnici v Brně desítky milionů, klesly odběry krve: 17. dubna 2020. IDNES.cz [online]. MAFRA, 2020 [cit. 2021-11-28]. Dostupné z: https://www.idnes.cz/brno/zpravy/fakultni-nemocnice-brno-kyberneticky-utok-skody-odber-krve.A200417_093436_brno-zpravy_krut
18. ČTK. Vnitro připravilo návrh zákona proti šíření teroristického obsahu on-line [online]. © Copyright 2022 ČTK, 2022, 17.02.2022 [cit. 2022-02-19]. ISSN 1213-5003. Dostupné z: https://www.ceskenoviny.cz/zpravy/vnitro-pripravilo-navrh-zakona-proti-sireni-teroristickeho-obsahu-on-line/2162881
19. ČTK. Výbuch v nemocnici: 3 mrtví, mnoho zraněných. Deník.cz [online]. VLTAVA LABE MEDIA, 2011, 21. 5. 2011 [cit. 2021-11-28]. Dostupné z: https://www.denik.cz/ze_sveta/vybuch-v-nemocnici--mrtvi-mnoho-zranenych20110521.html
20. ČTK a Aktuálně.cz. Útok na vojenskou nemocnici v Kábulu má už 49 obětí. Islamisté se převlékli za lékaře. Aktuálně.cz [online]. Economia, 2017, 9. 3. 2017 [cit. 2021-11-21]. Dostupné z: https://zpravy.aktualne.cz/zahranici/utok-na-vojenskou-nemocnici-v-kabulu-ma-uz-49-obeti-islamist/r~51e898dc04a411e78ad70025900fea04/
21. ČTK a ČT24. Kyberútoky na české nemocnice už zneklidňují i Američany. Ten nejnovější hlásí Karlovy Vary. ČT24 [online]. 2020, 18. dubna 2020 [cit. 2022-01-24]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3079028-usa-jsou-znepokojene-kyberutoky-na-ceske-nemocnice-rekl-pompeo
22. ČTK a Ivana LESKOVÁ. Střelec v ostravské nemocnici zabil šest lidí. Policie ho našla, je po smrti. IDNES.cz [online]. MAFRA, 2019, 10.12.2019 [cit. 2022-01-23].

Dostupné z: https://www.idnes.cz/ostrava/zpravy/strelba-ostrava-nemocnice-policie-zasah.A191210_081440_ostrava-zpravy_klu

23. ČTK a iDNES.cz. Psychiatrickou nemocnici v Kosmonosech ochromil kyberútok, péči neomezil [online]. MAFRA, 2020 [cit. 2022-01-24]. Dostupné z: https://www.idnes.cz/praha/zpravy/mlada-boleslav-kyberutok-psychiatricka-nemocnice-kosmonosy.A200330_172510_praha-zpravy_rsr
24. ČTK a iROZHLAS. Počítače v Psychiatrické nemocnici Kosmonosy ochromil kyberútok. Péče o pacienty není ohrožena [online]. 2020. 2020, 30.3.2020 [cit. 2022-01-24]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/pocitace-nemocnice-psychiatrie-kosmonosy-kyberutok-nukib_2003301855_aur
25. ČTK a iROZHLAS. Úřady evidují za říjen 14 kybernetických incidentů. Zvýšenému tlaku hackerů stále čelí nemocnice. iROZHLAS [online]. 2021, 10. listopadu 2021 [cit. 2022-01-24]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/nukib-kyberutok-kyberneticke-incidenty-rijen-nemocnice-zdravotnictvi_2111101425_svi
26. ČTK a NOVINKY. Nemocnice se připravují na nájezdy hackerů. FN Plzeň investovala 351 milionů korun [online]. Borgis, a.s. a Seznam.cz, 29. 9. 2021 [cit. 2022-01-30]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/nemocnice-se-pripravuji-na-najezdy-hackeru-fn-plzen-investovala-351-milionu-korun-40373333
27. ČTK, NOVINKY a Miloslav FIŠER. NÚKIB: České nemocnice stále čelí hackerským útokům. Novinky.cz [online]. 2021, 10. listopadu 2021 [cit. 2022-01-24]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/nukib-ceske-nemocnice-stale-celi-hackerskym-utokum-40377614
28. Definice terorismu. Ministerstvo vnitra České republiky [online]. [cit. 2021-11-21]. Dostupné z: https://www.mvcr.cz/cthh/clanek/definice-terorismu.aspx
29. DEKUNDER, David. JBSA Photo Gallery. Joint Base San Antonio: 190111-F-JV236-1004.JPG [online]. 1969, USA.gov [cit. 2022-01-30]. Dostupné z: https://www.jbsa.mil/News/Photos/igphoto/2002082996/
30. Desert Sun, Volume 43, Number 3, 7 August 1969. California Digital Newspaper Collection [online]. DL Consulting, 7.8.1969 [cit. 2022-01-30]. Dostupné z: https://cdnc.ucr.edu/?a=d&d=DS19690807.2.6&e=-------en--20--1--txt-txIN--------1
31. DURMAN, Karel. Popely ještě žhavé: velká politika 1938-1991. [Díl II., Konce dobrodružství 1964-1991]. Praha: Karolinum, 2009. ISBN 978-80-246-1536-3.

32. Evropská databanka. MĚSTSKÁ NEMOCNICE DUCHCOV VITA, S.R.O. [online]. 2021 [cit. 2022-02-20]. Dostupné z: https://www.edb.cz/firma-257037-vita-duchcov/kontakt
33. EVROPSKÝ PARLAMENT. NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2021/784 ze dne 29. dubna 2021 o potírání šíření teroristického obsahu online. Úřední věstník Evropské unie [online]. Brusel, 2021, 29. dubna 2021 [cit. 2022-04-23]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32021R0784&from=EN
34. Fakultní nemocnice Brno [online]. 2017 [cit. 2022-02-17]. Dostupné z: https://www.fnbrno.cz/prezentacni-publikace-o-fn-brno/f3642
35. ФИЛАТОВ, Алексей. Будённовский рубеж: Расследование участника событий. 1. ЛитРес: Самиздат, 2020. ISBN 978-5-532-05217-8.
36. FOLTIN, Pavel a David ŘEHÁK. HISTORICKÝ VÝVOJ TERORISMU. Obrana a strategie [online]. Kounicova 65, 662 10 Brno: Univerzita obrany, 2006, 2006(1), 45-60 [cit. 2021-11-28]. ISSN 1802-7199. Dostupné z: https://www.obranaastrategie.cz/filemanager/files/6263.pdf
37. FUJII, Lee Ann. Transforming the moral landscape: the diffusion of a genocidal norm in Rwanda. Journal of Genocide research [online]. 2004, 2004(6), 99-114 [cit. 2022-02-19]. Dostupné z: https://doi.org/10.1080/1462352042000194737
38. GANOR, Boaz. Terrorist Attacks against Hospitals Case Studies. The ICT Working Paper Series [online]. International Institute for Counter-Terrorism, 2013, 2013(25), 1-34 [cit. 2021-11-28]. Dostupné z: https://www.ict.org.il/UserFiles/ICTWPS%20-%20Ganor%20&%20Halperin%20Wernli%20-%2025.pdf
39. GAWRON, Tomáš. Zbraně z hobbymarketu: Útočník v Halle si vyrobil samopal, pistoli, brokovnice, výbušniny – a také střelivo. ZBROJNICE.COM [online]. Copyright © Tomáš Gawron / zbrojnice.com, 2020, 10.10.2019 [cit. 2022-02-02]. Dostupné z: https://zbrojnice.com/2019/10/10/zbrane-z-hobbymarketu-utocnik-v-halle-si-vyrobil-samopal-pistoli-brokovnice-vybusniny-a-take-strelivo/
40. GENOVESE, Marco. Top 5 cyberattacks against the health care industry. STORMSHIELD [online]. Stormshield, 2021, 18. 11. 2021 [cit. 2021-11-28]. Dostupné z: https://www.stormshield.com/news/top-5-cyberattacks-against-the-health-care-industry/

41. Global Terrorism Database [online]. University of Maryland: National Consortium for the Study of Terrorism and Responses to Terrorism An Emeritus Center of Excellence of the U.S. Department of Homeland Security, c2009-2021 [cit. 2021-11-28]. Dostupné z: https://www.start.umd.edu/gtd/
42. Historie. Nemocnice Milosrdných sester sv. Vincence de Paul Kroměříž [online]. 2021 [cit. 2022-02-20]. Dostupné z: https://www.nemomil.cz/historie/
43. HNILIČKA, Petr. Vliv medializace terorismu po roce 2001 ve vztahu na nárůst zneužití tohoto jevu ve společnosti. Č. Budějovice, 2010. bakalářská práce (Bc.). JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH. Zdravotně sociální fakulta
44. HODGETTS, T.J. Lessons from the Musgrave Park Hospital bombing. Injury [online]. 1993, 1.4.1993, 1993(24), 219-221 [cit. 2022-02-19]. ISSN 0020-1383. Dostupné z: https://www.sciencedirect.com/science/article/pii/0020138393901712
45. Maps.google.com [online]. 2021: Google, 2021 [cit. 2021-11-21]. Dostupné z: maps.google.com
46. JANCZEWSKI, Lech a Andrew M. COLARIK. Managerial Guide for Handling Cyber-terrorism and Information Warfare [online]. Idea Group Publishing, 2005 [cit. 2021-11-21]. ISBN 1-59140-550-5. Dostupné z: https://books.google.cz/books?id=9C8qX6Ul2bIC&printsec=frontcover&hl=cs#v=onepage&q&f=false
47. JANIŠOVÁ, Míla. Genocida ve Rwandě v roce 1994 očima Lékařů bez hranic [online]. ÚSTAV MEZINÁRODNÍCH VZTAHŮ PRAHA, 2014, 18.6.2014 [cit. 2022-02-19]. Dostupné z: https://www.iir.cz/genocida-ve-rwande-v-roce-1994-ocima-lekaru-bez-hranic
48. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
49. JIROUŠKOVÁ, Pavla. Odložení případu. Policie České republiky – KŘP Moravskoslezského kraje [online]. 2020, 13.5.2020, 2020 [cit. 2022-02-19]. Dostupné z: https://www.policie.cz/clanek/krajske-reditelstvi-severomoravskeho-kraje-zpravodajstvi-odlozeni-pripadu.aspx

50. JETTER, Michael. Blowing Things Up: The Effect of Media Attention on Terrorism [online]. Crawley, Australia: The University of Western Australia, 4.12.2015 [cit. 2022-02-02]. Dostupné z: https://ecompapers.biz.uwa.edu.au/paper/PDF%20of%20Discussion%20Papers/2015/DP%2015.28_Jetter1.pdf
51. KACLOVÁ, Markéta, Petra LAZÁKOVÁ, Miroslav KARAS a David ŠŤÁHLAVSKÝ. Teroristé měli zaútočit na Hamburk. IRozhlas [online]. Český rozhlas, 2003, 31. prosince 2003 [cit. 2021-11-28]. Dostupné z: https://www.irozhlas.cz/zpravy-svet/teroriste-meli-zautocit-na-hamburk_200312311042_mkaclova
52. KASHIRTSEVA, Yuliya. Protiteroristická politika Ruské Federace, Ukrajiny a Běloruska. Ochrana & Bezpečnost [online]. Lamačova 825/11, 152 00 Praha 5: Ochrana a bezpečnost o. s., 2013, 2013(2), 1-40 [cit. 2021-11-28]. ISSN 1805-5656. Dostupné z: http://ochab.ezin.cz/O-a-B_2013_B/2013_B_05_kashirtseva.pdf
53. KASÍK, Pavel. Teroristé a novináři jsou v „symbióze“. Jde to zvrátit jako u sebevražd?. IDNES.cz [online]. MAFRA, 2016, 4.8.2016 [cit. 2022-02-02]. Dostupné z: https://www.idnes.cz/technet/veda/terorismus-media-sebevrazdy-vyzkum.A160803_154621_veda_pka
54. KINGATUA, Amos. 6 HTTP MITM Attack Tools for Security Researchers. GEEKFLARE [online]. Geekflare, 2021, July 7, 2021 [cit. 2021-11-21]. Dostupné z: https://geekflare.com/mitm-attack-tools/
55. KLEIN, Christopher. When a US Hospital Ship Was Attacked by a Kamikaze Pilot During WWII. HISTORY [online]. A&E Television Networks, 2020, MAY 1, 2020 [cit. 2021-11-21]. Dostupné z: https://www.history.com/news/hospital-ship-uss-comfort-world-war-ii-kamikaze-attack
56. KOĎOUSKOVÁ, Barbora. HTTPS V KOSTCE: CO TO JE, JAK FUNGUJE A JAK NA NĚJ PŘEJÍT [online]. Praha: Rascasone, 17.11. 2021 [cit. 2022-01-30]. Dostupné z: https://www.rascasone.com/cs/blog/co-je-https-http-ssl-tls
57. KOPECKÝ, Kamil. Za kybernetické útoky často nemohou “hackeři”, ale obyčejné lidské chyby. Prevenci kybernetické bezpečnosti v kritické infrastruktuře nesmíme podceňovat!. E-Bezpečí, roč. 5, č. 1, s. 74-79. Olomouc: Univerzita Palackého, 2020. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=1840

58. KOTKOVÁ, Veronika. 150 let Psychiatrické nemocnice Kosmonosy [online]. 2019 [cit. 2022-02-17]. Dostupné z: https://www.pnkosmonosy.cz/grafika/150_let.pdf
59. KRUPKA, Jaroslav. Nejhorší útoky v nemocnicích: teror v Rusku byl popravou, v USA stříleli lékaři. Deník.cz [online]. VLTAVA LABE MEDIA, 2019, 11. 12. 2019 [cit. 2021-11-21]. Dostupné z: https://www.denik.cz/ze_sveta/terorismus-strelba-utok-rukojmi-nemocnice-samil-basajev-rusko-francie-policie.html
60. KUBÁTOVÁ, Zuzana. Útok na nemocnice je terorismus, říká antivirový miliardář Kasperskij. Seznam Zprávy [online]. Seznam.cz, 2020, 4. 8. 2020 [cit. 2021-11-21]. Dostupné z: https://www.seznamzpravy.cz/clanek/utok-na-nemocnice-je-terorismus-rika-antivirovy-miliardar-kasperskij-113592
61. LUTTER, Mark, Karlijn L.A. ROEX a Daria TISCH. Anomie or imitation? The Werther effect of celebrity suicides on suicide rates in 34 OECD countries, 1960–2014 [online]. 246. Social Science & Medicine, 2020, 10 s. [cit. 2022-02-02]. ISSN 0277-9536. Dostupné z: https://reader.elsevier.com/reader/sd/pii/S0277953619307506?token=A7B0C96DE72D66D85E6DA71E01F20D743357644B7C81FFAE9964474C1E624EB958990CD9E80CA7673B1261B7796C400E&originRegion=eu-west-1&originCreation=20220202113822
62. Medical Tribune. Kybernetický útok na FN Brno – rok poté. Medical Tribune [online]. MEDICAL TRIBUNE, 2021, 29. 3. 2021 [cit. 2021-11-28]. Dostupné z: https://www.tribune.cz/komentare/kyberneticky-utok-na-fn-brno-rok-pote/
63. MAGDOŇOVÁ, Jana. Českou nemocnici opět napadli hackeři. Úřady tají, o jaké zařízení se jedná. iRozhlas [online]. Český rozhlas, 2021, 12. ledna 2021 [cit. 2021-11-28]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/koronavirus-v-cesku-aktualne-kyberneticky-utok-na-nemocnice_2101120758_oro
64. MAGDOŇOVÁ, Jana. Experti z Avastu a Esetu identifikovali virus, který ohrožuje nemocnice. Lze ho obejít stiskem tří kláves. iRozhlas [online]. 2020, 18. dubna 2020 [cit. 2022-01-24]. Dostupné z: https://www.irozhlas.cz/veda-technologie/koronavirus-coviper-narodni-urad-pro-kybernetickou-a-informacni-bezpecnost_2004181017_pj
65. MAGDOŇOVÁ, Jana. Nemocnice odolaly hackerským útokům. Varování padlo na úrodnou půdu, říká ředitel kyberúřadu. iRozhlas [online]. Český rozhlas, 2020, 29. dubna 2020 [cit. 2021-11-28]. Dostupné z: https://www.irozhlas.cz/zpravy-

domov/narodni-urad-pro-kybernetickou-a-informacni-bezpecnost-kyberneticke-utoky_2004291747_tef

66. MARSH, Sarah. The NHS trusts hit by malware – full list. The Guardian [online]. Guardian News & Media Limited, 2017, 12 May 2017 [cit. 2021-11-21]. ISSN 0261-3077. Dostupné z: https://www.theguardian.com/society/2017/may/12/global-cyber-attack-nhs-trusts-malware
67. Měkké cíle. Ministerstvo vnitra České republiky [online]. [cit. 2021-11-21]. Dostupné z: https://www.mvcr.cz/cthh/clanek/mekke-cile.aspx
68. Městská nemocnice Čáslav. Městská nemocnice Čáslav [online]. 2022 [cit. 2022-02-20]. Dostupné z: http://www.nemcaslav.cz/dokumenty
69. MOLTAŠ, Zbyněk. Vzbouřenectví na severovýchodním Kavkaze. Masarykova univerzita, 2014. Diplomová práce. Masarykova univerzita, Fakulta sociálních studií. Vedoucí práce Tomáš Šmíd, Ph.D. Dostupné z: https://is.muni.cz/th/zrtvt/Diplomova_prace.pdf
70. MORGAN, Steve. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. CYBERCRIME MAGAZIN [online]. Sausalito: Cybersecurity Ventures, 11.11.2020 [cit. 2022-02-01]. Dostupné z: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
71. NATE, Raymond. Massachusetts man gets 10 years in prison for hospital cyberattack. Reuters [online]. 2019, JANUARY 10, 2019 [cit. 2022-04-23]. Dostupné z: https://www.reuters.com/article/us-massachusetts-cyber-idUSKCN1P42J8
72. Nemocnice Pelhřimov. Výroční zprávy [online]. 2020 [cit. 2022-02-20]. Dostupné z: https://www.hospital-pe.cz/file.php?nid=19023&oid=8572452
73. NOVOTNÁ, Karolína. Nemocnice jsou pro hackery stále snadným cílem. Útoků přitom přibývá. IDNES.cz [online]. MAFRA, 2021, 20. února 2021 [cit. 2021-11-21]. Dostupné z: https://www.idnes.cz/zpravy/domaci/kyberneticky-utok-hacker-nemocnice-zabezpeceni.A210203_141638_domaci_knn
74. NÚKIB. Ruské firmy a dopady na ICT. NÚKIB [online]. Národní úřad pro kybernetickou a informační bezpečnost, 2022, 4. březen 2022 [cit. 2022-04-23]. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/1820-ruske-firmy-a-dopady-na-ict/

75. Oblastní nemocnice Kladno. Výroční zpráva 2020 [online]. 2020 [cit. 2022-02-20]. Dostupné z: http://www.nemocnicekladno.cz/images/dokumenty/vyrocni-zpravy/v%C3%BDro%C4%8Dn%C3%AD_zpr%C3%A1va_2020.pdf
76. PERDOCH, Jaroslav. Rok po tragédii: Proč zabíjel ostravský vrah? Rekonstrukce Deníku krok po kroku. Deník.cz [online]. VLTAVA LABE MEDIA, 2020, 7.12.2020 [cit. 2022-02-02]. Dostupné z: https://www.denik.cz/z_domova/smutne-vyroci-strelba-fno-nemocnice-ostrava-rok-pote-casova-osa202012.html
77. POKALOVA, Elena. Chechnya's Terrorist Network: The Evolution of Terrorism in Russia's North Caucasus. 1. 147 Castilian Drive, Santa Barbara, CA 93117: Praeger ABC-CLIO, LLC., 2015, 259 s. ISBN 978-1-4408-3154-6.
78. Poliklinika Bílovec. Poliklinika Bílovec [online]. 2010 [cit. 2022-02-20]. Dostupné z: http://www.poliklinikabilovec.cz/o-nas/
79. Psychiatrická nemocnice v Opavě. O společnosti [online]. 2021 [cit. 2022-02-20]. Dostupné z: https://www.pnopava.cz/cs/page/1-o-spolecnosti/
80. ROKOS, Milan. SEZNAM ZPRÁVY. Izrael zažil nejhorší hackerský útok na nemocnici ve své historii [online]. Seznam.cz, 16. 10. 2021 [cit. 2022-01-30]. Dostupné z: https://www.seznamzpravy.cz/clanek/izrael-zazil-nejhorsi-hackersky-utok-na-nemocnici-ve-sve-historii-178005
81. Rozpočet Oblastní nemocnice Mladá Boleslav, a.s. Http://www.klaudianovanemocnice.cz [online]. 2022 [cit. 2022-02-20]. Dostupné z: http://www.klaudianovanemocnice.cz/assets/File.ashx?id_org=427004&id_dokumenty=2223
82. ŘÍHA, Jiří a Petr BALLEK. Sborník odborných článků: 1898-2018 [online]. 2018 [cit. 2022-02-17]. ISBN 978-80-270-3678-3. Dostupné z: https://www.hospital-bn.cz/wp-content/uploads/2019/01/sbornik-odbornych-clanku.pdf
83. SEDLÁK, Jan. Jak probíhá kybernetický útok v české nemocnici? Podívejte se na přednášky. Lupa.cz [online]. Internet Info, 2020, 18. 9. 2020 [cit. 2021-11-28]. Dostupné z: https://www.lupa.cz/aktuality/jak-probiha-kyberneticky-utok-v-ceske-nemocnici-podivejte-se-na-prednasky/
84. Seoul National University Hospital massacre. Wikipedia [online]. [cit. 2021-11-21]. Dostupné z: https://en.m.wikipedia.org/wiki/Seoul_National_University_Hospital_massacre

85. SLOUKA, David. První přímá oběť kybernetického útoku na nemocnici? Žena v Německu zemřela při převozu do vzdálenější nemocnice. InSmart [online]. RightWords Solution, 2020, 18. 9. 2020 [cit. 2021-11-28]. Dostupné z: https://insmart.cz/prvni-obet-kybernetickeho-utoku-na-nemocnici/
86. SONNECK, G, E ETZERSDORFER a S NAGEL-KUESS. Imitative suicide on the Viennese subway [online]. Printed in Great Britain: Pergamon Press, 1994, 5 s. [cit. 2022-02-02]. Dostupné z: doi:10.1016/0277-9536(94)90447
87. SOULEIMANOV, Emil. Konflikt v Čečensku: minulost, současnost, perspektivy. Praha: Sociologické nakladatelství (SLON), 2011. Knižnice Sociologické aktuality, sv. 25. ISBN 978-80-7419-066-7.
88. SPURNÝ, Jaroslav. V NEJHORŠÍM PŘÍPADĚ MOHLI PŘI KYBERÚTOKU NA NEMOCNICE UMÍRAT LIDÉ. RESPEKT [online]. Economia, 2020, 6. 5. 2020 [cit. 2021-11-21]. Dostupné z: https://www.respekt.cz/rozhovor/v-nejhorsim-pripade-mohli-pri-kyberutoku-na-nemocnice-umirat-lide
89. SVETSOVA, Iryna. Oranžová revoluce. Masarykova univerzita, 2006. Bakalářská práce. Masarykova univerzita, Fakulta sociálních studií. Vedoucí práce PhDr. Lubomír Kopeček, Ph.D.
90. SWEENEY, Evan. Payer Independence Blue Cross reports data breach affecting 17,000 members. FIERCE Healthcare [online]. Questex, 2018, Sep 20, 2018 [cit. 2021-11-28]. Dostupné z: https://www.fiercehealthcare.com/payer/independence-blue-cross-data-breach-cybersecurity-privacy
91. ŠUSTR, Ladislav. Snadný cíl a lehký byznys. Kybernetický útok může nemocnici paralyzovat na měsíce. Echo24.cz [online]. ECHO MEDIA, 2019, 13. prosince 2019 [cit. 2021-11-28]. Dostupné z: https://echo24.cz/a/S9DCD/snadny-cil-a-lehky-byznys-kyberneticky-utok-muze-nemocnici-paralyzovat-na-mesice
92. The Mozilla Observatory [online]. Mozilla.org [cit. 2022-01-30]. Dostupné z: https://observatory.mozilla.org
93. TOSINI, Domenico. Al-Qaeda's Strategic Gamble: The Sociology of Suicide Bombings in Iraq. The Canadian Journal of Sociology [online]. 2010, 2010(2), 271-308 [cit. 2022-02-19]. Dostupné z: https://www.jstor.org/stable/canajsocicahican.35.2.271
94. VIRET, EMMANUEL. RWANDA - A CHRONOLOGY (1867-1994): Mass Violence & Résistance. SciencesPo [online]. 2010, 1.3.2010 [cit. 2022-02-19]. ISSN 1961-9898.

Dostupné z: https://www.sciencespo.fr/mass-violence-war-massacre-resistance/en/document/rwanda-chronology-1867-1994.html

95. Vojenská nemocnice v Mozdogu. DW [online]. 2003, 2003 [cit. 2022-02-21]. Dostupné z: https://www.dw.com/en/search-for-survivors-goes-on-after-russian-blast/a-939387
96. Výroční zpráva: Levitovo centrum následné péče. Levitovo centrum následné péče [online]. 2019 [cit. 2022-02-20]. Dostupné z: https://horice.org/assets/File.ashx?id_org=4516&id_dokumenty=17668
97. Výroční zpráva 2020. Bílovecká nemocnice, a.s. [online]. 2020 [cit. 2022-02-20]. Dostupné z: https://or.justice.cz/ias/content/download?id=a2c7b142edfe4bc3adc765398b5b66c6
98. ZUBAIR IQBAL, Muhammad. The media–terrorism symbiosis: a case study of Mumbai attacks, 2008. In: Asian Journal of Communication. Routledge, 2015, s. 197-212. Dostupné z: doi:https://doi.org/10.1080/01292986.2014.944924

10 SEZNAM POUŽITÝCH OBRÁZKŮ

11 SEZNAM POUŽITÝCH TABULEK