POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra kriminální policie

Využití zpravodajství z otevřených zdrojů v oblasti národní bezpečnosti v kontextu vybraných aktuálních bezpečnostních hrozeb

Diplomová práce

The Use of Open Source Intelligence in the Field of National Security in the Context of Selected Current Security Threats

Master thesis

VEDOUCÍ PRÁCE

Ing. Bc. Luděk MICHÁLEK, Ph.D.

AUTOR PRÁCE

Bc. Tereza KOLEČKOVÁ

PRAHA

2023

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracovala samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpala, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 14. 03. 2023

……..

Bc. Kolečková Tereza

Poděkování

Tímto bych chtěla poděkovat vedoucímu mé diplomové práce, panu Ing. Bc. Luďku Michálkovi Ph.D., za jeho cenné rady, vstřícnost, trpělivost a ochotu, kterou mi v průběhu zpracování diplomové práce věnoval.

Dále bych ráda poděkovala i kolegům, rodině a přátelům za podporu, kterou mi věnovali v průběhu celého studia. Jmenovitě pak i Jiřímu Černému za motivaci a útěchu, kterou mi poskytoval v náročných studijních obdobích.

ANOTACE

Práce se zabývá využitím zpravodajství z otevřených zdrojů v obraně národní bezpečnosti z pohledu zpravodajských služeb ČR. V teoretické části jsou vymezeny základní pojmy, popsány výhody i nevýhody otevřených zdrojů a druhy zdrojů, z kterých tento zpravodajský obor čerpá. Na základě vybraných bezpečnostních dokumentů České republiky autorka vymezuje a charakterizuje aktuální hlavní bezpečnostní hrozby ohrožující národní bezpečnost. K vybraným hrozbám je zpracována rešerše zahraničních i tuzemských otevřených zdrojů, které podávají zpravodajsky relevantní informace o dané bezpečnostní problematice. Závěr práce představuje praktický příklad využití otevřených zdrojů a vymezuje jejich význam pro bezpečnostní prostředí v jaderné oblasti.

KLÍČOVÁ SLOVA

* zpravodajské služby ČR * zpravodajství z otevřených zdrojů * otevřené zdroje * zpravodajská informace * národní bezpečnost * aktuální bezpečnostní hrozby *

ANNOTATION

The thesis explores the use of the open source intelligence in the defense of national security from the perspective of the Czech republic intelligence services. The theoretical section defines the key terms, the advantages and disadvantages of open sources, and describes the different types of sources used within the intelligence field. Based on the selected Czech republic security documents, the author defines and characterizes the current main threats to the national security. The identified threats are accompanied by a list of foreign and domestic open sources that provide intelligence-relevant information on the given security issue. The final section of the thesis consists of a practical example of the use of open sources and further defines their importance for the nuclear security.

KEYWORDS

* Czech Republic intelligence services * open source intelligence * open source * intelligence * national security * current security threats *

Obsah

Úvod

Bezpečnostní prostředí prochází neustálým dramatickým vývojem. Národní bezpečnost již může být ohrožena i nestátním aktérem, hrozba použití jaderných zbraní ovlivňuje celosvětový mír, jednotlivci se mohou prostřednictvím internetu zradikalizovat, vytvořit si vlastní zbraň i bombu a zaútočit na státem chráněné zájmy. Teroristické útoky osamělých aktérů, útoky z kyberprostoru a agresivní extrémistické projevy v současnosti silněji, než kdy dříve ovlivňují mezinárodní rámec bezpečnosti.

Státy ohrožuje velké množství státních i nestátních subjektů a skupin s odlišnými zájmy. Jejich aktivita, obsah komunikací, plánované akce nebo propagační materiály jsou volně přístupné na osobních blozích, fórech, sociálních sítích nebo webových stránkách a poskytují pro zpravodajské důstojníky relevantní a aktuální informace z dané oblasti. Zpravodajský obor, který se zabývá shromažďováním, vyhodnocováním a analyzováním dat a informací dostupných z volně dostupných zdrojů se nazývá zpravodajstvím z otevřených zdrojů.

Od počátku 21. století je o tento druh zpravodajství zvýšený zájem. Monitorování rizikového obsahu je pro učinění preventivních bezpečnostních opatření v případě hrozící hrozby klíčové. Otevřené zdroje nabízí rychlý a včasný přísun důležitých informací. Státní instituce zajišťující bezpečnost České republiky musí aktivně reagovat na nově vznikající hrozby a vyvíjet nové techniky, které jsou při boji s hrozícím rizikem rychlé a účinné.

Diplomová práce pojednává o využití tohoto zpravodajského oboru v obraně národní bezpečnosti. Na základě analýzy strategických dokumentů a výročních zpráv zpravodajských služeb ČR si autorka práce klade za cíl stanovit vybrané hlavní aktuální hrozby, které ohrožují národní bezpečnost České republiky. U jednotlivě vytyčených bezpečnostních hrozeb autorka určí jejich vztah k národní bezpečnosti a dále vytvoří rešerši dostupných zahraničních i tuzemských zdrojů OSINT.

V poslední kapitole práce bude uveden praktický příklad možného využití OSINT v oblasti jaderné bezpečnosti. Autorka práce pouze s využitím otevřených zdrojů vyhledá a zhodnotí množství informací, které se dají získat o zabezpečení jaderné elektrárny Dukovany. K tomuto postupu budou využity obecné metody zpravodajského cyklu, tedy sběr dat, analýza a vyhodnocení informací. Výsledkem bude shrnutí všech relevantních informací a následně vytyčení rizikových veřejných informací, které mohou ulehčit teroristickým aktérům přípravu na útok.

1 Vymezení základních a souvisejících pojmů

Data lze definovat jako údaje, které je možné technicky zaznamenat, a to osobou nebo prostředkem. V procesu tvorby zpravodajských informací jsou data vstupní, základní jednotky, které se získávají v průběhu fáze shromažďování. Jedná se o soubor písmen, číslic a symbolů, které samy o sobě nemají vypovídací hodnotu. Až následovně jsou zpracovány a zařazeny do kontextu, získávají vlastní význam a stávají se z nich informace.

Informace jsou srozumitelné a do kontextu zasazené údaje. Soubor jednoduchých i komplexních informací, které pocházejí z rozmanité škály zdrojů slouží analytikům k vyhodnocení a následnému vytvoření dokumentu obsahujícímu zpravodajské informace.[1]

Dezinformace, je nepravdivá informace, která je šířena úmyslně. Zprávy, články i jiné příspěvky popisující okolní dění může prostřednictvím internetu šířit jakákoliv osoba a tuto skutečnost je potřeba vzít v potaz. Dezinformace jsou velmi závažným problémem, který může vyvolat řadu nepříjemných skutečností a představovat i hrozbu pro společnost jako celek.[2] Bezpečnostní informační služba pravidelně upozorňuje na dezinformační kampaně, zejména proruských aktivistů, kteří svou činností podrývají důvěru ve státní systém, ovlivňují názor veřejnosti a udržují společnost v pochybách a strachu.[3] Nebezpečnost dezinformací dokládá například fakt, že BIS v roce 2018 označila dezinformační aktivity za největší hrozbu ústavního systému ČR.[4]

---

[1] MICHÁLEK, Luděk. Základy zpravodajské činnosti. Praha: PAČR v Praze, 2011. ISBN 978-80-7251-360-4, str. 15-16.

[2] AKHBAR, Babak, BAYERL, Saskia, SAMPSON, Fraser (Eds.). *Open Source Intelligence Investigation. From Strategy to Implementation.* Canada: Springer International Publishing, 2016. ISBN 978-3-319-47671-1, str.88-89.

[3] Bezpečnostní informační služba. *Výroční zpráva Bezpečnostní informační služby za rok 2019.* [online]. Praha: Bezpečnostní informační služba, 2020. [cit. 22.10.2022]. Dostupné z: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf, str. 11.
Bezpečnostní informační služba. *Výroční zpráva Bezpečnostní informační služby za rok 2020.* [online]. Praha: Bezpečnostní informační služba, 2021. [cit. 22.10.2022]. Dostupné z: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf, str. 9.

[4] Bezpečnostní informační služba. *Výroční zpráva Bezpečnostní informační služby za rok 2018.* [online]. Praha: Bezpečnostní informační služba, 2019. [cit. 22.10.2022]. Dostupné z: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2018-vz-cz.pdf.pdf, str. 8-9.

Zpravodajská informace je specifický druh utajované skutečnosti, který svou podobu a hodnotu získává až prostřednictvím kvalifikovaného a utajovaného procesu. Výsledkem tohoto procesu je náležitě zpracovaný a analyticky vyhodnocený soubor dat i informací, který je následně předán oprávněnému subjektu v podobě zpravodajské informace.[5]

Zpravodajství, jakožto zpravodajská činnost je sofistikovaná práce důstojníků zpravodajských služeb, jejichž cílem je získávání informací ze specifické oblasti, specifickými prostředky a postupy. Takto získané informace musí být náležitě zpracovány, vyhodnoceny a předány příjemci nebo zadavateli. Pojem zpravodajství představuje zdlouhavý proces vyžadující kvalifikovaný přístup a kolektivní práci velkého počtu příslušníků zpravodajských služeb.[6]

Národní bezpečnost je na základě ústavního zákona zajišťována ozbrojenými bezpečnostními sbory, armádními silami, záchrannou a havarijní službou.[7] Již od pradávna mělo každé společenství osob zájem na zajištění a udržení své vlastní bezpečnosti, a to i nadále zůstalo jednou ze současných hlavních priorit a povinností států vůči svým občanům. Národní bezpečnost je zejména vymezena ústavním zákonem č. 110/1998 Sb., *o národní bezpečnosti České republiky.* Zde se pod bezpečnostní zájmy státu řadí ochrana demokracie, života, zdraví a majetku, dále pak udržení svrchovanosti a územní celistvosti.[8] Významné postavení při zajišťování národní bezpečnosti v rámci shromažďování, analyzování a vyhodnocování informací mají zpravodajské služby ČR.[9]

Zpravodajské služby jsou státem zřízené organizace, jejichž hlavním úkolem je utajovaný sběr informací, jejich vyhodnocování a předávání oprávněným adresátům.[10] Postavení, působnost a například kontrolu zpravodajských služeb

---

[5] MICHÁLEK, Luděk. *Základy zpravodajské činnosti*. Praha: PAČR v Praze, 2011. ISBN 978-80-7251-360-4, str. 13-17.
[6] ZRŮN, Michal a Lucie ŘEHOŘOVÁ. *Úvod do zpravodajství*. Praha: PAČR v Praze, 2007. ISBN 978-80-7251-252-2, str. 7-9.
[7] Ústavní zákon č. 110/1998 Sb., *o bezpečnosti České republiky,* v posledním znění, článek 3.
[8] Ústavní zákon č. 110/1998 Sb., *o bezpečnosti České republiky,* v posledním znění, článek 1.
[9] Vláda České republiky. *Bezpečnostní strategie České republiky 2015*. [online]. Praha: Vláda České republiky, 2015. [cit. 29.10.2022]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf, str. 21; bod. 99.
[10] ZRŮN, Michal a Lucie ŘEHOŘOVÁ. *Úvod do zpravodajství*. Praha: PAČR v Praze, 2007. ISBN 978-80-7251-252-2. str. 9.

upravuje zákon č. 153/1994 Sb. *o zpravodajských službách České republiky.* V třetím ustanovení tohoto zákona lze nalézt taxativní výčet zpravodajských služeb působících v České republice, kterými je Bezpečnostní informační služba (BIS), Úřad pro zahraniční styky a informace (ÚZSI) a Vojenské zpravodajství (VZ). Další ustanovení pak vymezují specifické oblasti, na které jsou jednotlivé služby zaměřeny, a tím rozděluje zpravodajské služby na civilní a vojenské, vnitřní a vnější. [11]

Bezpečnostní informační služba (BIS) je ozbrojená civilní zpravodajská služba ČR s vnitrostátní působností. Zabezpečuje informace o aktivitách zaměřených proti demokracii, svrchovanosti a suverenitě České republiky, dále zpracovává informace týkající se působení zpravodajských služeb cizí moci na tomto území, sbírá informace pro udržení ochrany ekonomických zájmů ČR a o činnostech týkajících se organizovaného zločinu, terorismu a extremismu. Monitoruje radikalizaci ve společnosti, násilné projevy a další aktivity zaměřené proti zájmům České republiky.[12] Na základě zákona č. 154/1994 Sb., *o Bezpečnostní informační službě* je BIS oprávněna získávat informace pomocí specifických prostředků. Mezi tyto prostředky patří získávání informací od osob, které jednají ve prospěch BIS a zpravodajské prostředky, kterými jsou zpravodajská technika, sledovací činnost a krycí prostředky a doklady.[13]

Útvar zahraničních styků a informací (ÚZSI) je ozbrojená civilní zpravodajská služba ČR s vnější působností. ÚZSI získává informace mající původ v zahraničí a jeho hlavním úkolem je se podílet na udržení vnitřní bezpečnosti státu. Pokud je to pro činnost ÚZSI nezbytné, je tento útvar oprávněn získávat informace i na území České republiky prostřednictvím specifických prostředků jmenovaných viz výše a dále pak prostřednictvím nástrahové a zabezpečovací techniky.[14]

---

[11] Zákon č. 153/1994 Sb., *o zpravodajských službách České republiky,* v posledním znění, §1-5.
[12] Zákon č. 153/1994 Sb., *o zpravodajských službách České republiky,* v posledním znění, §5. Bezpečnostní informační služba. *Výroční zpráva Bezpečnostní informační služby za rok 2020* [online]. Praha: Bezpečnostní informační služba, 2021. [cit. 22.10.2022]. Dostupné z: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf, str. 3-6.
[13] Zákon č. 154/1994 Sb., *o Bezpečnostní informační službě,* v posledním znění, §6-15.
[14] Zákon č. 153/1994 Sb., *o zpravodajských službách České republiky,* v posledním znění, §5, 17 - 19.

Vojenské zpravodajství (VZ) je ozbrojená vojenská zpravodajská služba ČR s vnitřní i vnější působností. Úlohou VZ je získávání, shromažďování a vyhodnocování informací namířených proti bezpečnostním zájmům ČR. VZ zajišťuje kybernetickou obranu ČR a v oblasti obrany dále získává informace o zpravodajských službách cizí moci, o utajovaných skutečnostech i jiných skutečnostech mající původ v zahraničí. Na základě zákona č. 289/2009 Sb., *o Vojenském zpravodajství* je Vojenské zpravodajství pro naplnění účelu své činnosti oprávněno používat specifické prostředky získávání informací, mezi které patří prostředky zpravodajské a využívání osob jednajících ve prospěch VZ.[15]

[15] Zákon č. 289/2009 Sb., *o Vojenském zpravodajství*, v posledním znění, §1, 6, 16a.
Zákon č. 153/1994 Sb., *o zpravodajských službách České republiky*, v posledním znění §2, 5.

2 Zpravodajství z otevřených zdrojů

V dřívějších dobách, kdy internet nepropojoval celý svět a kyberprostor v podstatě neexistoval, získávali zpravodajští příslušníci informace zejména prostřednictvím signálového zpravodajství – SIGINT (Signals Intelligence), zpravodajství lidských zdrojů – HUMINT (Human-Source Intelligence) a obrazového zpravodajství – IMINT (Imagery Intelligence). Se vznikem internetu, vznikl současně i nový prostor, prostor neomezených možností, informací, způsobů komunikace a šíření zpráv. Současně však vznikl i nový prostor pro páchání trestné činnosti, útoků na základní práva a svobody i na stát jakožto celek. Kyberprostor dal těmto hrozbám zcela novou, dosud neznámou podobu. Zpravodajské služby se už nemohly spoléhat pouze na informace získávané tradičními způsoby, ale byly nuceny vynalézt způsoby nové, přizpůsobit se informační době, a aktivně reagovat na dosud neznámé a sofistikované útoky nepřítele. Zpravodajství z otevřených zdrojů vzniklo jako reakce na rychle se rozvíjející možnosti informačních a komunikačních technologií a spektra dosažitelných a zveřejňovaných informací.[16]

Zpravodajství z otevřených zdrojů (dále jen OSINT) je zpravodajstvím, které využívá veřejně dostupných zdrojů pro tvorbu zpravodajských informací. To, co OSINT odlišuje od jiných zpravodajských disciplín je právě neutajovaný charakter získávaných informací, které jsou většinou přístupné volně a zdarma nebo za poplatek. Pod zdrojem OSINT si lze pak představit vše, co splňuje kritéria neutajovanosti a volného přístupu, tedy např. mediální vysílání, denní tisk, publikace, výroční zprávy státních institucí, webové portály, sociální sítě, videozáznamy atd. Množství zdrojů, z kterých OSINT čerpá, je dle obsahu rozsáhlé a z pohledu kvality a věrohodnosti informací velmi různorodé.[17]

[16] HORÁK, Oldřich a Ivo PIKNER. Zpravodajství z otevřených zdrojů. *Vojenské rozhledy.* [online]. 2007, č. 3. [cit. 08.10.2022]. ISSN 2336-2995. Dostupné z: https://www.vojenskerozhledy.cz/images/archiv_voj_rozhl/clanky/2007/3/4_zpravodajstvi_z_otevrenych_zdroju.pdf, str. 35-36.

[17] MICHÁLEK, L., POKORNÝ, L., STIERANKA, J., MARKO, M., VAŠKO, A., *Zpravodajské služby a zpravodajská činnost.* Praha: Wolters Kluwer ČR, 2021.ISBN 978-80-7598-725-9. str. 286

2.1 Zpravodajský cyklus

Vznik zpravodajské informace představuje celou řadu postupných, promyšlených a kvalitativních procesů, které vyžadují maximální píli a soustředěnost operativních i analytických zpravodajců. Tyto procesy se cyklicky opakují do té doby, než je dosaženo podoby cenných zpravodajských informací, které lze předat zadavateli požadavku.

Zpravodajský cyklus v sobě zahrnuje 4 základní fáze, dle kterých příslušníci zpravodajských služeb postupují. Prvním krokem je plánování zpravodajské činnosti, následuje sběr dat a informací, zpravodajská analýza a předání zpravodajských informací oprávněnému zadavateli.

Plánování zpravodajské činnosti – zadávání úkolů. V první fázi každého zpravodajské cyklu stojí požadavek na zjištění určitých informací.[18] Tento požadavek většinou zadává zadavatel, kterým může být dle zákona o zpravodajských službách pouze vláda nebo prezident republiky.[19] Kromě zákonem stanovených orgánů oprávněných k zadávání úkolů zpravodajským službám si může i služba sama stanovit požadavek pro zpracování a vyhodnocení zpravodajských informací v konkrétní oblasti. Tou může být pouze taková oblast, která spadá do působnosti zpravodajské služby a je službou dle jí dostupných informací považována za hrozbu pro ochranu bezpečnosti, ústavního a demokratického základu České republiky. Po obdržení zadaného úkolu provede příslušná zpravodajská organizace plán požadavků a určí cíl. Dle tohoto plánu budou dále jednotlivá oddělení v oboru své specializace postupovat.

Sběr dat a informací. Na základě zadaných úkolů a zpracovaných plánů zahájí zpravodajští příslušníci sběr informací, který představuje činnost zahrnující zapojení všech pro danou oblast použitelných zpravodajských odvětví. Shromážděná data a informace tvoří objemný a rozmanitý soubor, který má povahu poznatků z otevřených zdrojů, informací získaných specifickými prostředky, utajovaných informací, satelitních snímků apod. Celý tento soubor

[18] AKHBAR, Babak, BAYERL, Saskia, SAMPSON, Fraser (Eds.). *Open Source Intelligence Investigation. From Strategy to Implementation.* Canada: Springer International Publishing, 2016. ISBN 978-3-319-47671-1, str. 37-39.

[19] Zákon č. 153/1994 Sb., *o zpravodajských službách České republiky,* v posledním znění, §8.

musí před jeho postoupením k zpracování projít ještě třídícím a klasifikačním procesem.

Zpravodajská analýza. Po nashromáždění potřebného množství informací dochází k jejich zpracování analytickými pracovníky. Proces zpracování zahrnuje překlady textů z cizích jazyků, hodnocení věrohodnosti informací a spolehlivosti zdroje původu. Posuzují se dostupná data a informace ve vztahu k jejich kvalitě, všechny poznatky se hodnotí v komplexu a dochází k vytvoření zprávy obsahující zpravodajsky relevantní informace.

Předání zpravodajských informací oprávněnému zadavateli. Poslední fáze zpravodajského cyklu představuje nejen bezpečný proces předání utajovaných zpravodajských informací oprávněným adresátům, ale taktéž rozhodnutí o tom, jaké informace lze poskytnout, aby došlo k splnění úkolu, ale zároveň nedošlo k ohrožení utajovaných zdrojů. Riziko vyzrazení utajovaného zdroje s sebou přináší každá distribuce zpráv a povinností každé zpravodajské organizace je ochrana takového zdroje před vyzrazením.[20]

2.2 Výhody a nevýhody OSINT

Nastává zde zcela přirozená otázka, zdali zpravodajství, které čerpá převážně z veřejně dostupných zdrojů přináší pro svůj obor nepostradatelné informace, nebo se jedná pouze o doplňkové, ne tolik důležité zpravodajství. Dalo by se namítat, že jiné zpravodajské obory např. signálové, obrazové zpravodajství používají ke sběru dat utajované prostředky a postupy, a takto získané utajované informace mají již od počátku větší hodnotu a význam pro zpravodajskou analýzu. Charakter informací z otevřených zdrojů je vždy neutajovaný, což může na první pohled snižovat hodnotu těchto informací. Nicméně časem a dlouhodobou zkušeností analytických pracovníků se prokázalo, že i takto neklasifikované informace mohou být často jedinými dostupnými informacemi o náhlé situaci, které lze po zpracování předávat zadavateli na vysoké úrovni, např. vládě ČR. Zároveň je však nutno podotknout, že OSINT nemůže zcela nahradit jiné druhy zpravodajství.[21]

[20] MICHÁLEK, L., POKORNÝ, L., STIERANKA, J., MARKO, M., VAŠKO, A., *Zpravodajské služby a zpravodajská činnost.* Praha: Wolters Kluwer ČR, 2021.ISBN 978-80-7598-725-9. str. 269-275.
[21] HORÁK, Oldřich a Ivo PIKNER. Zpravodajství z otevřených zdrojů*. Vojenské rozhledy.* [online]. 2007, č. 3. [cit. 08.10.2022]. ISSN 2336-2995. Dostupné z:

Výhody OSINT

Obrovskou výhodu pro zpravodajství z otevřených zdrojů představuje jeho **okamžitý přístup k informacím**. Mnohdy ve světě dochází k náhlým situacím, jejichž lokalita nemá pokrytí jiných zpravodajských oborů a potřeba získání aktuálních informací o dané krizové situaci je akutní. V takovém případě je využití zpráv z hromadných sdělovacích prostředků klíčové pro pochopení a dostatečné informovanosti o nenadálé situaci.

OSINT čerpá z nepřeberného **množství veřejně dostupných zdrojů**. Zpravodajský důstojník má k dispozici velký počet druhově rozmanitých zdrojů, které jsou přístupné v různých jazycích a formách.

Informace lze kdykoliv ověřit. Zdroje jsou veřejně dostupné a zpětná kontrola a ověření zpravodajsky získaných informací je podstatně jednodušší než u informací získávaných utajovaným způsobem, které mnohdy vychází pouze z jediného zdroje.

Původ a kvalita informací z otevřeného zdroje je zpravodajským analytikům ve většině případů známa. Míru věrohodnosti informace lze lépe dohledat a určit, což ulehčuje analytickou fází zpracování.[22]

Nepochybným pozitivem otevřených zdrojů je **nízká finanční** náročnost, která je způsobena postupem získávání informací, tedy z volně dostupných zdrojů, které jsou buď přístupné zcela zdarma, nebo za drobný poplatek.[23]

Mezi další výhody otevřených zdrojů patří jejich relativní **neomezená časová a místní dostupnost**. Přístup k online informacím je možný v jakoukoliv denní dobu a na jakémkoliv místě.

---

https://www.vojenskerozhledy.cz/images/archiv_voj_rozhl/clanky/2007/3/4_zpravodajstvi_z_otevrenych_zdroju.pdf, str. 35-36.

[22] MICHÁLEK, L., POKORNÝ, L., STIERANKA, J., MARKO, M., VAŠKO, A., *Zpravodajské služby a zpravodajská činnost.* Praha: Wolters Kluwer ČR, 2021.ISBN 978-80-7598-725-9. str. 287-288.

[23] HORÁK, Oldřich a Ivo PIKNER. Zpravodajství z otevřených zdrojů*. Vojenské rozhledy.* [online]. 2007, č. 3. [cit. 08.10.2022]. ISSN 2336-2995. Dostupné z: https://www.vojenskerozhledy.cz/images/archiv_voj_rozhl/clanky/2007/3/4_zpravodajstvi_z_otevrenych_zdroju.pdf, str. 42.

Informace získávané z otevřených zdrojů **nejsou omezeny jen na určitá témata**, jako jiné zpravodajské obory mohou být. K porozumění celosvětové bezpečnostní situace je zapotřebí pochopit souvislosti jevů, událostí, hrozeb a postojů. Všechna tato témata OSINT nabízí.[24]

Nevýhody OSINT

Jak již bylo zmíněno výše, OSINT nabízí mnoho různorodých zdrojů, které zahrnují velký objem dat a informací. Velké množství informací znesnadňuje hledání té správné a potřebné informace v celé řadě jiných informací, dále je pak zapotřebí **vynaložit větší úsilí na správnou selekci získaných poznatků** a vyřadit informace chybné, popř. odhalit záměrné šíření dezinformací.[25]

Snadný přístup k informacím prostřednictvím otevřených zdrojů mohou využít pro svůj prospěch i nepřátelské subjekty. Mimo šíření nepravdivých a smyšlených zpráv, **mohou nepřátelé monitorovat svůj cíl** a shromažďovat informace o jeho slabinách.[26] Příkladem by mohli být teroristé, kteří mohou prostřednictvím otevřených zdrojů získat mnoho informací o způsobu zabezpečení státních institucí, a tyto informace zneužít k zdařilému útoku. Více k této problematice bude pojednáno v praktické části diplomové práce.

2.3 Zdroje OSINT

Otevřené zdroje jsou zdroje, které jsou volně dostupné veřejnosti, a to buď v elektronické podobě nebo formou některé publikace dostupné pouze fyzicky. OSINT tedy není odkázán pouze na online platformu, ačkoliv se zde nachází největší počet informací, s kterými pracuje. Určité otevřené zdroje jsou přístupné všem a bez rozdílu, jiné jsou pak určené omezenému okruhu osob. Mezi tento vybraný okruh osob patří předplatitelé periodik nebo jiných služeb. Otevřeným zdrojem nikdy nebude informace, která podléhá nějakému stupni utajení, ať už dle

[24] CHRISS, Pallaris. Center For Security Studies. *Open Source Intelligence: A strategic enabler of national security.* [online]. 2008, roč. 3, č. 32 [cit. 08.10.2022]. ISSN 2296-0244. Dostupné z: https://www.files.ethz.ch/isn/50169/css_analysen_nr%2032-0408_E.pdf, str. 1-3

[25] HORÁK, Oldřich a Ivo PIKNER. Zpravodajství z otevřených zdrojů*. Vojenské rozhledy.* [online]. 2007, č. 3. [cit. 08.10.2022]. ISSN 2336-2995. Dostupné z: https://www.vojenskerozhledy.cz/images/archiv_voj_rozhl/clanky/2007/3/4_zpravodajstvi_z_otevrenych_zdroju.pdf, str. 42.

[26] Recorded Future. *What Is Open Source Intelligence and How Is IT Used?* [online]. [cit. 25.02.2023]. Dostupné z: https://www.recordedfuture.com/open-source-intelligence-definition

státního nebo mezinárodního členění. Nebude se ani jednat o informace získané zpravodajskými důstojníky z kontaktů osob a za použití zpravodajské techniky či zpravodajských prostředků.[27]

Tradiční mediální zdroje

Mezi tradiční mediální zdroje patří zahraniční tisk, televizní, rozhlasové i rádiové vysílání. Velmi významný poskytovatel zahraničních zpráv je např. BBC (British Broadcasting Corporation) News, který několikrát denně zveřejňuje zprávy a událostí z celého světa v téměř aktuálním čase.[28] Zprávy s aktuálním děním jsou vysílány na národní i mezinárodní úrovni v mnoha jazycích. Televizní zpravodajství může poskytnout osobní údaje určitých osob, popř. jejich identifikační rysy prostřednictvím zveřejněných obrázků nebo prezentovaných videí. Mediální zprávy mohou také dopomoci při orientaci v nastalé situaci a vytváření si představy o pravděpodobném chronologickém sledu jednotlivých událostí.

Při čerpání informací ze zpráv hromadných sdělovacích prostředků je zapotřebí brát v úvahu případy záměrné úpravy reality ze strany mediálních společností, které můžou zjištěné informace o události úmyslně upravit na více znepokojující nebo senzacechtivé.[29]

Šedá literatura

Pod označením šedá literatura se rozumí taková literatura, ke které existuje legální, avšak omezený přístup. Přístup k této literatuře je možný pouze prostřednictvím speciální kanálů, nebo osobně, fyzicky, a to na určitém místě. Tento druh informací nelze získat prostřednictvím předplatného nebo poplatku zaplaceného agentuře, ani si tuto literaturu nelze koupit v knihkupectví nebo jiných obchodech. Šedá literatura není vydávána komerčním vydavatelstvím, není nijak komerčně distribuována ani jinak zveřejňována. Většinou se jedná o neziskové

[27] HORÁK, Oldřich a Ivo PIKNER. Zpravodajství z otevřených zdrojů. *Vojenské rozhledy.* [online]. 2007, č. 3. [cit. 08.10.2022]. ISSN 2336-2995. Dostupné z: https://www.vojenskerozhledy.cz/images/archiv_voj_rozhl/clanky/2007/3/4_zpravodajstvi_z_otevrenych_zdroju.pdf, str. 35-36.

[28] KERNAR, F. William. *NATO Open Source Intelligence Handbook*. [online]. USA, 2001. [cit. 01. 10. 2022]. Dostupné z: https://archive.org/details/NATOOSINTHandbookV1.2/page/n5/mode/2up, str. 5

[29] Blackdot solutions. *OSINT Sources: What Are The Different Types of Open Source Data*? [online]. [cit. 25.02.2023]. Dostupné z: https://blackdotsolutions.com/blog/osint-sources/

organizace, vzdělávací instituce nebo jiné soukromé subjekty, které tento druh literatury vydávají pro své členy nebo pro interní užití. Šedou literaturu publikují i státní a vládní instituce, které svou činnost pro vnitřní potřebu zaznamenávají a vydávají. V neposlední řadě se mezi vydavatele šedé literatury řadí i široké spektrum neformálních sdružení, uskupení, klubů a spolků.[30]

Surface Web

Od roku 1994 lze zaznamenat masivní rozmach internetu. Standardními vyhledavači dostupný Surface Web obsahuje nepřeberné množství zpráv, videí, dokumentů a dalších stránek obsahující mnoho informací. Pouze část z těchto informací však mají potenciální zpravodajskou hodnotu. Lehká a rychlá dostupnost informací nevyžadující téměř žádnou speciální techniku, znalost nebo přístup není však zcela bezchybná. Informace mohou být zkreslené, záměrně upravené nebo špatně podané. Ne všechny zdroje informací jsou spolehlivé, jakýkoliv krok a aktivita na internetu vytvoří trvalou stopu v kyberprostoru a při úniku informací může dojít k jejich nekontrolovatelnému šíření.[31]

Deep web, Dark web

Miliardy uživatelů po celém světě používají internet k prohledávání tzv. Surface webu. Celý tento prostor je nicméně jen pouhá část toho, co se ve skutečnosti skrývá v Deep webu a co není standardními vyhledávači jako je Google, Yahoo a Bing dohledatelné. Deep Web v sobě ukrývá malou anonymní část s názvem Dark web, který pro své anonymní vystupování může sloužit pro mnohé nezákonné trestné činnosti. Anonymita je přesně to, co přitahuje subjekty, které se snaží zůstat v bezpečném prostředí při šíření nelegálních informací, nabízení nezákonných služeb a prodeji či koupi zakázaného zboží. Dark web je tedy ideálním prostředím pro nájemné vrahy, pedofily, teroristy šířící svou propagandu, obchod se zbraněmi, drogami i lidským masem. Dark web je v tomto směru významným místem pro

[30] KERNAR, F. William. *NATO Open Source Intelligence Handbook*. [online]. USA, 2001. [cit. 01. 10. 2022]. Dostupné z: https://archive.org/details/NATOOSINTHandbookV1.2/page/n5/mode/2up, str. 8–9

[31] KERNAR, F. William. *NATO Open Source Intelligence Handbook*. [online]. USA, 2001. [cit. 01. 10. 2022]. Dostupné z: https://archive.org/details/NATOOSINTHandbookV1.2/page/n5/mode/2up, str. 5–6

zpravodajství z otevřených zdrojů, jelikož zde lze dohledat mnoho klíčových informací o závažných bezpečnostních tématech.[32]

Sociální sítě

Sociální sítě jsou platformy, na kterých jsou aktivní stovky až tisíce milionů uživatelů. Prostřednictvím těchto sítí sdílí uživatelé svůj vlastní obsah, názory, fotografie, vytváří soukromé skupiny, a to pro OSINT zpravodajce představuje přístup k mnohým zajímavým informacím týkajících se např. krizových a mimořádných událostí, složení různých radikálních skupin a jejich názorů.[33] Společnost *Statista* pravidelně zveřejňuje statistické údaje o počtu uživatelů na jednotlivých sítích. Mezi ty nejčastěji používané, kde počet uživatelů za měsíc pravidelně překračuje 2 biliony, se řadí Facebook, YouTube, WhatsApp a Instagram.[34]

Osobní blogy

Osobní blogy jsou platformy nezávislé na sociálních sítích a komunitě. Osoba vlastnící blog zde zveřejňuje příspěvky a vytváří vlastní obsah. Pro OSINT mohou představovat blogy významný zdroj z hlediska bezpečnostních expertů zveřejňující své názory nebo např. zradikalizovaných uskupení, které na blozích upevňují svou komunitu.[35]

---

[32] AKHBAR, Babak, BAYERL, Saskia, SAMPSON, Fraser (Eds.). *Open Source Intelligence Investigation. From Strategy to Implementation.* Canada: Springer International Publishing, 2016. ISBN 978-3-319-47671-1, str. 114-123.

[33] ÜNVER, H. Akın. *Digital Open Source Intelligence and International Security*: *A Primer.* [online]. Oxford: Centre for Economics and Foreign Policy Studies, 2018. [cit. 06.02.2023]. Dostupné z: http://www.jstor.org/stable/resrep21048, str. 1

[34] Statista. *Most popular social networks worldwide as of January 2023, ranked by number of monthly active users.* [online]. [cit. 25.02.2023]. Dostupné z: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[35] AKHBAR, Babak, BAYERL, Saskia, SAMPSON, Fraser (Eds.). *Open Source Intelligence Investigation. From Strategy to Implementation.* Canada: Springer International Publishing, 2016. ISBN 978-3-319-47671-1, str. 136-137.

Blogging guide. *Best Open Source Blogging platforms*. [online]. [cit. 25.02.2023]. Dostupné z: https://bloggingguide.com/best-open-source-blogging-platforms/

Online prémiové zdroje

Do otevřených zdrojů řadíme i zdroje, které jsou veřejnosti přístupné, avšak ne zcela zdarma. Tyto zdroje poskytují přístup k informacím za poplatek při registraci, nebo poplatek ve formě pravidelného předplatného.[36]

Odborníci, specialisté

Většina zpráv a informací, které se k lidem dostávají prostřednictvím médií nejsou samotnými žurnalisty nebo televizními či rádiovými moderátory získávány přímo, ale zprostředkovaně, a to od jiného subjektu, který tyto informace mohl taktéž získat od jiné osoby a takhle by se mohlo pokračovat dále. Velmi významný zdroj, od kterého lze v rámci OSINT analýzy čerpat informace je odborník s dlouholetou zkušeností, specializující se na pozorování určitých jevů, popřípadě vyskytující se na určitém, pro zadavatele významném místě. Napříč světem existuje mnoho míst, ze kterých nelze získat konkrétní informace o tamních poměrech, podmínkách a událostech jinak, než prostřednictvím těchto osob. Na specialistu se však není vhodné obrátit jen za výše zmíněných podmínek. O některých zájmových oblastech existuje mnoho informací, které lze získat dostupnými prostředky, avšak i tyto informace nemusí být natolik přesné a realitě odpovídající, pak i v těchto případech je vhodné využít znalostí a zkušeností dostatečně důvěryhodné osoby, která dostává a vnímá informace přímo, na základě svých zkušeností a znalostí je hodnotí a následně posoudí a vyhodnotí. Tento expert je mnohdy velmi levná a efektivní varianta pro OSINT analýzu.[37]

[36] KERNAR, F. William. *NATO Open Source Intelligence Handbook*. [online]. USA, 2001. [cit. 01. 10. 2022]. Dostupné z: https://archive.org/details/NATOOSINTHandbookV1.2/page/n5/mode/2up, str. 6–7

[37] KERNAR, F. William. *NATO Open Source Intelligence Handbook*. [online]. USA, 2001. [cit. 01. 10. 2022]. Dostupné z: https://archive.org/details/NATOOSINTHandbookV1.2/page/n5/mode/2up, str. 9

3 Vybrané aktuální bezpečnostní hrozby a využití OSINT

Bezpečnostní prostředí se stále vyvíjí, dochází k řadám změn, vznikají nová bezpečnostní rizika, útočníci přicházejí na nové sofistikované způsoby vedení útoků. Pro zachování bezpečnosti je nezbytné, aby byl každý nový způsob ohrožení rychle zaregistrován a efektivně vyřešen. V současné době mohou pro Českou republiku, jakožto členský stát mezinárodních organizací, představovat hrozbu konflikty nadnárodního charakteru. Konflikty, které jsou od území České republiky vzdálené, avšak přímo ohrožují spojenecké státy představují hrozbu pro bezpečnostní situaci všech členských zemí, včetně České republiky.[38]

Hrozbu pro národní bezpečnost může představovat velké množství různorodých rizik z oblasti ekonomické, sociální, environmentální, vojenské, politické i technické. Další ohrožující hrozby mohou vyplývat např. z terorismu, trestné činnosti, radikalizace i z mezinárodního prostředí.[39] Všechna tato odvětví lze více či méně monitorovat prostřednictvím zpravodajství z otevřených zdrojů. Uvádí se, že informace získané prostřednictvím otevřených zdrojů tvoří 80 % až 95 % zpravodajsky využívaných informací.[40]

V následujícím textu budou uvedeny hlavní zdroje rizik v oblasti národní bezpečnosti České republiky, kterými se zabývají zpravodajské služby ČR, jakožto útvary zřízené pro ochranu ústavních, demokratických, právních i bezpečnostních základů této země.

3.1 Destabilizace státního systému

Hrozbami pro základní atributy demokratického zřízení jsou činnosti některých státních i nestátních aktérů, které mají hybridní charakter. Hybridní válčení je způsob, kterým útočník vede konflikt. Jeho cílem je vyhledat slabá místa státního systému a pomocí nátlaku poškodit, zkomplikovat nebo zcela zastavit jeho chod.

[38] Vláda České republiky. *Bezpečnostní strategie České republiky 2015* [online]. Praha: Vláda České republiky, 2015 [cit. 29.10.2022]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf, str. 8; bod. 16.
[39] *Bezpečnostní výzvy současného světa: Security challenges of the world of today.* Praha: Policejní akademie České republiky v Praze, 2020. ISBN 978-80-7251-498-4, str. 34-40.
[40] CHRISS, Pallaris. Center For Security Studies.*Open Source Intelligence: A strategic enabler of national security* [online]. 2008, roč. 3, č. 32 [cit. 01.03.2023]. ISSN 2296-0244. Dostupné z: https://www.files.ethz.ch/isn/50169/css_analysen_nr%2032-0408_E.pdf, str. 1.

Hybridní hrozby představují rozmanité a vzájemně propojené modely útoku. Mohou mít různou povahu, skrytou či otevřenou, vojenskou či nevojenskou a mohou být vedeny v oblasti ekonomické, energetické, průmyslové, finanční či např. zpravodajské. Pomocí těchto hybridních útoků dochází k vyvolání konfliktu a poškození cílového subjektu.[41] Hybridní strategie se mezi občany snaží vyvolat nedůvěru ve funkční chod systému. Hrozbu pak dále představuje skutečnost, že ze strany útočníků může dojít k získání částečného nebo úplného vlivu v důležitých složkách státu, což může mít za následek oslabení státního mechanismu v rovině politické, ekonomické, mezinárodněprávní i bezpečnostní.[42]

V roce 2020 BIS ve své výroční zprávě uvedla, že stále intenzivněji budou hlavní bezpečnostní hrozbu pro národní bezpečnost představovat zejména útoky namířené proti základním demokratickým principům země.[43] V Auditu národní bezpečnosti se pak toto tvrzení potvrzuje s dodatkem, že rozsah a způsob jednotlivých nástrojů nabývá v poslední době na intenzitě a jejich sofistikovaný způsob použití ztěžuje možnost včasného odhalení.[44]

V roce 2021 představovalo nejvýznamnější hrozbu pro stabilitu státního systému šíření dezinformací prostřednictvím sociální sítě Facebook, dezinformačních platforem a šířením nevyžádaných hromadných emailů. Rozsah šíření dezinformací se rozšiřoval i kvůli podpoře některých politických subjektů, kteří je ve velké míře používali v rámci své populistické rétoriky.[45]

---

[41] Ministerstvo vnitra České republiky. *Audit národní bezpečnosti.* [online]. Praha: Ministerstvo vnitra České republiky, 2016 [cit. 06.11.2022]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf, str. 127-128.

[42] Vláda České republiky. *Bezpečnostní strategie České republiky 2015.* [online]. Praha: Vláda České republiky, 2015 [cit. 29.10.2022]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf, str. 11.

[43] Bezpečnostní informační služba. *Výroční zpráva Bezpečnostní informační služby za rok 2020.* [online]. Praha: Bezpečnostní informační služba, 2021 [cit. 05.11.2022]. Dostupné z: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf, str. 9.

[44] Ministerstvo vnitra České republiky. *Audit národní bezpečnosti.* [online]. Praha: Ministerstvo vnitra České republiky, 2016 [cit. 06.11.2022]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf, str. 128.

[45] Bezpečnostní informační služba. *Výroční zpráva Bezpečnostní informační služby za rok 2021.* [online]. Praha: Bezpečnostní informační služba, 2022 [cit. 03.02.2023]. Dostupné z: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2021-vz-cz-2.pdf, str. 15.

3.1.1 Využití OSINT při útocích na stabilitu státního systému

Strategickým cílem v oblasti čelení hybridnímu působení je zejména včasná identifikace hrozícího rizika hybridního útoku, identifikace útočníka a učinění vládních opatření proti zjištěnému útoku. Hybridní útok cílí na poměrně široké spektrum oblastí, proto se i zpravodajská činnost musí v rámci získávání informací zaměřit na mnohé úseky státního systému, kam by mohly hybridní aktivity směřovat. Shromažďování zpravodajsky relevantních informací a monitorování situace na jednotlivých úsecích pak představuje dlouhodobou a soustavnou činnost.[46]

Z kontextu výročních zpráv BIS vyplývá, že se mezi nejčastější aktéry útočící na státní systém prostřednictvím hybridních hrozeb řadí Ruská federace a Čínská lidová republika. Toto tvrzení mimo jiné konstatuje i Národní strategie pro čelení hybridnímu působení, která uvádí, že Česká republika musí snížit svou strategickou závislost na státech, jejichž hodnoty a ideje se výrazně liší od orientace demokratické republiky.[47]

Proruské síly se rozpínají v sociálních mediích a v rámci politických institucí, jejich cílem je snaha o oslabení a destabilizaci systému. Čínské síly pak cílí spíše na ekonomické odvětví, akademické instituce a prostřednictvím médií se snaží šířit čínskou propagandu.

Využití OSINT hraje významnou roli v monitorování podezřelých aktivit na sociálních médiích a dezinformačních webech. Zpravodajství z otevřených zdrojů monitoruje weby zaměřené proti politické scéně ČR, členství v EU a NATO, dalším z témat je pak polarizace společnosti, podpora zájmů cizí moc, protizápadní postoje, protiimigrační a proruské názory.

[46] Ministerstvo obrany České republiky – VHÚ Praha. *Národní strategie pro čelení hybridnímu působení: National strategy for countering hybrid interference*. Praha: Ministerstvo obrany České republiky – VHÚ Praha, 2021. ISBN 978-80-7278-827-9. str. 7-8

[47] Ministerstvo obrany České republiky – VHÚ Praha. *Národní strategie pro čelení hybridnímu působení: National strategy for countering hybrid interference*. Praha: Ministerstvo obrany České republiky – VHÚ Praha, 2021. ISBN 978-80-7278-827-9. str. 6-7

V této oblasti jsou významné například **dezinformační weby či pseudo-zpravodajské servery** šířící ruskou propagandu:

- AC 24,[48]
- Aeronet,[49]
- Důležité 24,[50]
- Nová republika,[51]
- Protiproud,[52]
- Parlamentní listy,[53]
- CZ24 NEWS,[54]
- Národní noviny,[55]

dále konspirační weby zaměřené proti politické sféře:

- Czechfreepress.[56]

Webový portál *Education in Russia* je určený pro potenciální zájemce z ČR o edukační programy v Rusku. Osoba zde pro odeslání přihlášky ke studiu zasílá naskenované informace o cestovních dokladech, vlastní fotografii, vyplňuje informační dotazník a dokládá kopie o ukončených studijních programech v ČR. Tyto informace následně končí v rukou Ruských bezpečnostních složek.[57]

Významné **případové studie** a výzkumné zprávy, které se zabývají nebezpečným charakterem dezinformačních kampaní jsou *The Lisa Case STRATCOM Lessons*

[48] *AC24.* [online]. [cit. 05.02.2023]. Dostupné z: https://www.ac24.cz/
[49] *Aeronet*. [online]. [cit. 05.02.2023]. Dostupné z: https://aeronet.news/
[50] *Důležité 24.* [online]. [cit. 05.02.2023]. Dostupné z: https://zpravy.dt24.cz/
[51] *Nová republika*. [online]. [cit. 05.02.2023]. Dostupné z: https://www.novarepublika.online/
[52] *Protiproud.* [online]. [cit. 05.02.2023]. Dostupné z: https://protiproud.info/
[53] *Parlamentní listy.* [online]. [cit. 05.02.2023]. Dostupné z: https://www.parlamentnilisty.cz/
[54] *CZ24 News.* [online]. [cit. 05.02.2023]. Dostupné z: https://cz24.news/
[55] *Národní noviny.* [online]. [cit. 05.02.2023]. Dostupné z: https://www.narodni-noviny.cz/
[56] *Czech free press.* [online]. [cit. 05.02.2023]. Dostupné z: https://www.czechfreepress.cz/
[57] BŘEŠŤAN, Robert. Hlídací pes. *Pojďte k nám na vysokou, vábí Rusko Čechy. BIS i Černínský palác to „silně nedoporučují“.* [online]. [cit. 01.02.2023]. Dostupné z: https://hlidacipes.org/pojdte-k-nam-na-vysokou-vabi-rusko-cechy-bis-i-cerninsky-palac-to-silne-nedoporucuji/

for European states[58] a *Analýza manipulativních technik na vybraných českých serverech*.[59]

3.2 Mezinárodní konflikty

Spory vedené se státy, jež jsou členové nadnárodních organizací mohou v nejkrajnějších případech vést až k násilnému, ozbrojenému konfliktu a dalším souvisejícím problémům a tím může být přímo či nepřímo ohrožena národní bezpečnost.[60]

Vojenské zpravodajství ve své výroční zprávě z roku 2021 upozornilo na postupný vývoj autonomních zbraňových systémů, které ke své činnosti využívají tzv. všestrannou umělou inteligenci, jež je schopná plně nahradit lidský mozek. Tyto systémy již k plnění úkolů nepotřebují lidský faktor, jednotlivé operace jsou schopny plnit samy, jsou schopny se samy učit z vlastních chyb. Ačkoliv zatím nejsou součástí výzbroje žádné armádní síly státu, jejich zdokonalování stále pokračuje a v případě vzniku konfliktu by jejich použití mohlo mít za následek nepředstavitelné škody. V současné době nejistých a napjatých mezinárodních vztahů je docela nepravděpodobné, že by vznikla úmluva mezi státy o zákazu používání plně autonomních zbraňových systémů, které by v případě použití umožnily jedné ze stran technologickou výhodu nad nepřítelem. Proto lze předpokládat, že v budoucnu se budou tyto systémy stávat součástí vojenské výzbroje.[61]

Bezpečnostní strategie ČR již v roce 2015 konstatovala, že hrozba přímého ozbrojeného konfliktu je vůči České republice nízká, nicméně upozornila na aspirace mocenských států, které odmítají respektovat atributy mezinárodního práva a tím ohrožují demokratické základy států, i deklarovaná základní lidská

[58] JANDA, Jakub. *The Lisa Case STRATCOM Lessons for European states.* Security Policy Working Paper. [online]. 2016, č. 11. [cit. 02.02.2023]. Dostupné z: https://www.baks.bund.de/sites/baks010/files/working_paper_2016_11.pdf

[59] VEJVODOVÁ, Petra a Miloš GREGOR. *Analýza manipulativních technik na vybraných českých serverech. Výzkumná zpráva.* [online]. 2016. [cit. 02.02.2023]. Dostupné z: https://www.academia.edu/26046763

[60] Vláda České republiky. *Bezpečnostní strategie České republiky 2015.* [online]. Praha: Vláda České republiky, 2015. [cit. 29.10.2022]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf, str. 11.

[61] Vojenské zpravodajství. *Výroční zpráva Vojenského zpravodajství za rok 2021.* [online]. Praha: Vojenské zpravodajství, Ministerstvo obrany, 2022 [cit. 10.11.2022]. Dostupné z: https://www.vzcr.cz/uploads/41-Vyrocni-zprava-2021.pdf, str. 6-9.

práva a svobody.[62] Počátkem roku 2022 se svět stal svědkem vojenské konfrontace a napadení suverénního státu Ukrajiny Ruskou federací. Dlouho trvající celosvětový mír se tak otřásl v základech a hrozba použití jaderných zbraní se stala způsobem komunikace mezi mocenskými státy. Globální konfliktní prostředí, ačkoliv vojensky přímo neohrožuje Českou republiku, zcela bezpochyby představuje hrozbu pro bezpečnostní stabilitu EU, jako i pro národní bezpečnost ČR. Zpravodajské služby ČR získávají a shromažďují informace z mezinárodního prostředí. Na základě těchto informací se stanovují hrozby a činí se kroky, díky kterým lze krizovým situacím předcházet.

3.2.1 Využití OSINT v mezinárodních konfliktech

Vojenského zpravodajství, zabezpečuje informace důležité pro obranu a bezpečnost České republiky, Útvar pro zahraniční styky a informace zabezpečuje zpravodajsky relevantní informace důležité pro bezpečnost a ochranu státních zájmů mající původ v zahraničí.[63] Obě tyto zpravodajské služby se podílí na udržení národní bezpečnosti a v problematice mezinárodních konfliktů a získávají informace z otevřených zdrojů. Dostatečné množství těchto informací je pro bezpečnostní systém České republiky významný, z hlediska přijetí včasných obranných opatření.

International Crisis Group je nezisková organizace, která poskytuje **analýzy z konfliktních prostředí** ve světe a podává návody, jak řešit krizové situace. Nástroj *CrisisWatch* je pak určen k monitorování všech konfliktních situací po celém světě. Tento nástroj se aktualizuje na začátku každého měsíce a poskytuje popis bezpečnostní a politické situace v jednotlivých zemí konfliktu, identifikuje hrozby, upozorňuje na rizika eskalace a pomáhá porozumět a identifikovat budoucí vývoj konfliktních situací. V tomto roce zahrnuje pravidelná měsíční zpráva *CrisisWatch* zhruba 70 popisů z problémového prostředí.[64]

PRIO – The Peace Research Institute Oslo je instituce, která se zabývá konfliktními projevy, obecnými trendy a mírovými studiemi. Na stránkách instituce lze nalézt

[62] Vláda České republiky. *Bezpečnostní strategie České republiky 2015.* [online]. Praha: Vláda České republiky, 2015. [cit. 29.10.2022]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf, str. 8
[63] Zákon č. 153/1994 Sb., *o zpravodajských službách České republiky,* v posledním znění, §5
[64] *International Crisis Group.* [online]. [cit. 06.02.2023]. Dostupné z: https://www.crisisgroup.org/

výzkumné výstupy z široké škály témat, jako např.: civilní válka, trendy v konfliktních situacích, extremismus, migrace, mír, terorismus, válka na Ukrajině a mnohé další.[65]

Institute for the Study of War je nezisková organizace, která od roku 2007 shromažďuje **informace o vojenských záležitostech** z Afghánistánu, Iráku, Sýrie, Íránu, Pákistánu a dalších zemí. Od roku 2022 se aktivně věnuje informování o Ruské invazi na Ukrajině.[66]

Obrázek 1 Interaktivní mapa Ruské invaze na Ukrajinu (zdroj: ISW)

Na této webové stránce lze najít i aktuální interaktivní mapu, která se aktualizuje každých pár hodin a zaznamenává **posun Ruských vojsk na Ukrajinském území**.[67]

[65] *PRIO – The Peace Research Institute Oslo.* [online]. [cit. 06.02.2023]. Dostupné z: https://www.prio.org/

[66] *ISW – Institue for the Study of War* [online]. [cit. 06.02.2023]. Dostupné z: https://www.understandingwar.org/

[67] *Interactive map: Russia's Invasion of Ukraine*. Institue for the Study of War, 2023 [online]. [cit. 06.02.2023]. Dostupné z: https://storymaps.arcgis.com/stories/36a7f6a6f5a9448496de641cf64bd375

UCDP – Upsala Conflict Data Program je program, který ve své databázi od roku 1975 historicky zaznamenává konflikty ve světě.[68]

Liveuamap je interaktivní mapa, která na základě informací z médií zpracovává **aktuální polohu ozbrojených konfliktů ve světě**. Ohledně aktuální války mezi Ukrajinou a Ruskem zveřejňuje místa, kde v poslední době docházelo k odstřelování, bombardování, braní rukojmích, výbuchům. Na území USA ukazuje lokality nejnovějších případů střelby, pobodání, požárů, fatálních nehod. Podobné informace interaktivní mapa spravuje i pro území Sýrie, Palestiny, Íránu, Iráku, Afghánistánu a dalších.[69]

Freedom House je webový portál, který monitoruje **dodržování základních lidských práv a svobod** a udržování demokracie ve světě. Každý ze států je pak hodnocen na bodové stupnici. Organizace vydává každoročně zprávy *Freedom in the World* a hodnotí jednotlivé státy podle stavu a míry dodržování lidských práv.[70]

Eurobarometr zpracoval **přehled veřejného mínění** členských států a jejich občanů **o válce na Ukrajině**.[71]

K českým otevřeným zdrojům by se dal řadit portál Ústavu mezinárodních vztahů Praha, kde lze zakoupit předplatné časopisů *Mezinárodní vztahy* a *New Perspectives*, pro širokou veřejnost vydává Ústav i časopis *Mezinárodní politika.*[72]

3.3 Terorismus

Terorismus je nástroj, který pod hrozbou násilí vede k agresivnímu prosazení politických cílů a zastrašení obyvatelstva. Jeho riziko neustále narůstá na své

[68] *UCDP – Upsala Conflict Data Program.* [online]. [cit. 06.02.2023]. Dostupné z: https://ucdp.uu.se/encyclopedia
[69] *Liveuamap*. [online]. [cit. 06.02.2023]. Dostupné z: https://liveuamap.com/
[70] Freedom House. *Freedom in the World 2022, The Global Expansion of Authoritarian Rule.* [online]. [cit. 06.02.2023]. Dostupné z: https://freedomhouse.org/report/freedom-world/2022/global-expansion-authoritarian-rule
[71] Eurobarometr. *Public opinion on the war in Ukraine.* [online]. [cit. 20.02.2023]. Dostupné z: https://www.europarl.europa.eu/at-your-service/cs/be-heard/eurobarometer/public-opinion-on-the-war-in-ukraine
[72] *Ústav mezinárodních vztahů Praha.* [online]. [cit. 06.02.2023]. Dostupné z: https://www.iir.cz/

intenzitě i nebezpečnosti, a to v celosvětovém měřítku.[73] BIS již řadu let informuje české občany o skutečnosti, že hrozba islamistického terorismu na území České republiky je dlouhodobě nízká. Bezpečnostní situace v ČR z hlediska terorismu je však významně ovlivněna situací v Evropě (např. migrace, finanční i psychické problémy obyvatel spojené s ekonomickou situací, radikalizace společnosti atd.).[74]

V roce 2021 BIS informovala o teroristické aktivitě známých teroristických organizací Al-Qáida a Islámský stát, kdy tito aktéři mají stálý zájem na plánování teroristických útoků v západních zemích, avšak uskutečnění zamýšlených plánů je pro ně obtížné a mnohdy nereálné. Jejich propagandistické působení nicméně ovlivňuje slabší jednotlivce, mnohdy trpící duševní nemocí, kteří pod vlivem jejich ideologií, ale bez přímého napojení na jejich organizaci, páchají teroristické útoky.[75]

Terorismus pro Českou republiku představuje hrozbu spíše z pozice osamělého aktéra ovlivněného teroristickou propagandou než z pozice hlavních teroristických organizací, jejichž cílem jsou země Západu. I přes tuto skutečnost jsou však sekundární dopady na vnitřní bezpečnost České republiky veliké. Teroristická propaganda vzbuzuje strach, způsobuje nárust agresivity a násilí, radikalizuje společnost, podporuje vznik nenávistných uskupení. Ve snaze o potírání všech forem terorismu je zapotřebí sdílet zpravodajské informace mezi spojeneckými státy.[76]

Fenomén osamělého aktéra může být pro národní bezpečnost komplikovaný ze způsobu radikalizace jedince. Jedinec může prostřednictvím internetu získat

[73] Vláda České republiky. *Bezpečnostní strategie České republiky 2015*. [online]. Praha: Vláda České republiky, 2015 [cit. 29.10.2022]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf, str. 11.
[74] Bezpečnostní informační služba. *Výroční zpráva Bezpečnostní informační služby za rok 2020* [online]. Praha: Bezpečnostní informační služba, 2021 [cit. 05.11.2022]. Dostupné z: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf, str. 11,22.
Bezpečnostní informační služba. *Výroční zpráva Bezpečnostní informační služby za rok 2021* [online]. Praha: Bezpečnostní informační služba, 2022 [cit. 05.11.2022]. Dostupné z: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2021-vz-cz-2.pdf, str. 9.
[75] Bezpečnostní informační služba. *Výroční zpráva Bezpečnostní informační služby za rok 2021* [online]. Praha: Bezpečnostní informační služba, 2022 [cit. 03.02.2023]. Dostupné z: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2021-vz-cz-2.pdf, str. 18-19.
[76] Ministerstvo vnitra České republiky. *Audit národní bezpečnosti* [online]. Praha: Ministerstvo vnitra České republiky, 2016 [cit. 03.02.2023]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf, str. 11-14.

mnohé informace o formách páchání teroristických činů a k jeho radikalizaci může dojít bez toho, aniž by se s teroristickou organizací fyzicky spojil. Osamělý aktér nemusí zrovna sympatizovat s islámským terorismem. Separatistická hnutí i pravicoví extrémisté mohou být touto strategií do omezené míry ovlivněni také. Určení motivace osamělého aktéra je mnohdy nelehký úkol. Dle literatury ji lze rozdělit do třech základních kategorií: ideologická, psychopatologická a kategorie jiných osobních důvodů, popř. jejich vzájemná kombinace. Do ideologických důvodů se řadí náboženské, komunistické, anarchistické, separatistické, fašistické vyznávání ideologií. Psychopatologičtí aktéři pak konají pod vlivem duševní poruchy, popř. touhou spáchat sebevraždu. Jiné osobní důvody motivují pachatele z důvodů tíživé ekonomické situace, vztahových problémů nebo špatného sociálního postavení.[77]

3.3.1 Využití OSINT v boji proti terorismu

K velkému množství svých aktivit využívají teroristické organizace sociální sítě, diskuzní fóra, osobní blogy, online časopisy. Pomocí Dark Webu šíří propagandu, nabírají a radikalizují své členy, šíří návody a manuály k výrobě zbraní i k různým taktickým postupům při samotném útoku.[78] Platformy, kde jsou tyto informace uveřejněny představují pro OSINT cenné místo zpravodajsky relevantních informací. Shromažďování a analytické zpracování těchto dat může podat významné informace o struktuře a postavení organizace, ideologii, radikálním postoji, cíli útoku i budoucích plánech. K sociálním sítím, které teroristé často používají patří Twitter, YouTube a Facebook. Účinné monitorování těchto stránek může vést k včasnému zmaření teroristického činu, jako tomu bylo v roce 2013, kdy byl terorista Mambo Wahab zadržen, ještě před samotným spácháním bombového útoku na Indonéskou ambasádu. Právě změna jeho statusu na Facebooku odhalila a včas dopomohla k jeho dopadení. Monitorování a analýza

[77] GANOR, Boaz. Understanding the Motivations of 'Lone Wolf' Terrorists: The 'Bathtub' Model. *Perspectives on Terrorism.* [online] 2021, roč. 15, č. 2. [cit. 05.02.2023]. ISSN 2334-3745. Dostupné z: https://www.jstor.org/stable/27007294. str. 23-29.

[78] AKHBAR, Babak, BAYERL, Saskia, SAMPSON, Fraser (Eds.). *Open Source Intelligence Investigation. From Strategy to Implementation.* Canada: Springer International Publishing, 2016. ISBN 978-3-319-47671-1, str. 114-120.

džihádistických chatovacích skupin vede k určení hrozeb a přijetí účinných protiteroristických opatření.[79]

Na Úředním věstníku Evropské unie jsou zveřejněny významné dokumenty, které podávají důležité informace z teroristické problematiky:

Seznamy teroristických aktivistů vedené Evropskou Unií

Prováděcí nařízení Rady (EU) 2022/1230, o zvláštních omezujících opatřeních namířených proti některým osobám a subjektům s cílem bojovat proti terorismu. Přílohou tohoto nařízení je seznam osob. Osoby na tomto seznamu jsou označeny za teroristy, nebo za osoby, které se podílely na teroristických útocích a je proti nim zapotřebí přijmout zvláštní omezující opatření ve formě zmrazení finančních prostředků. V tomto seznamu se nachází dostatečně přesné identifikační údaje osoby, její jméno a příjmení, popř. přezdívka, datum a místo narození, státní příslušnost, číslo cestovního pasu. Dále jsou zde zahrnuty jiné subjekty a skupiny, na které platí stejná omezující opatření.[80]

Rozhodnutí Rady (SZBP) 2020/1132, kterým se aktualizuje seznam osob, skupin a subjektů, na něž se vztahují články 2, 3 a 4 společného postoje 2001/931/SZBP o uplatnění zvláštních opatření k boji proti terorismu. Přílohou tohoto rozhodnutí je seznam osob, skupin a subjektů, jejichž činnost je spojena s teroristickou aktivitou a vztahují se na ně posílená opatření v rámci policejní a justiční spolupráce. Seznam obsahuje shodné identifikační prvky, jako seznam prováděcího nařízení Rady EU viz výše.[81]

Europol vydává **výroční zprávy o vývoji a trendech v oblasti terorism**u. Zpráva zahrnuje např. údaje o ideologické motivaci teroristů, počtu zadržených teroristů,

[79] YOUNAS, Muhammad Ahsan. Digital Jihad' and Its Significance to Counterterrorism. *Counter Terrorist Trends and Analyses.* [online]. 2014, roč. 6, č. 2. [cit. 03.02.2023]. ISSN 2382-6444. Dostupné z: https://www.jstor.org/stable/26351231. str. 10-17.

[80] Prováděcí nařízení Rady EU č. 2022/1230 ze dne 18. července 2022, kterým se provádí čl. 2 odst. 3 nařízení (ES) č. 2580/2001 o zvláštních omezujících opatřeních namířených proti některým osobám a subjektům s cílem bojovat proti terorismu a kterým se zrušuje prováděcí nařízení (EU) č. 2022/147

[81] Rozhodnutí Rady (SZBP) č. 2020/1132 ze dne 30. července 2020, kterým se aktualizuje seznam osob, skupin a subjektů, na něž se vztahují články 2, 3 a 4 společného postoje 2001/931/SZBP o uplatnění zvláštních opatření k boji proti terorismu, a kterým se zrušuje rozhodnutí (SZBP) č. 2020/20

počet teroristických útoků v jednotlivých státech, informace popisující druhy použitých zbraní a exploziv.[82]

Mezi další organizace zabývající se analýzou terorismu patří také *African Centre for the Study and Research on Terrorism.*[83]

Pro zpravodajské účely mohou dále posloužit některé webové portály určené k shromažďování nejnovějších analytických zpráv a jiných informací o terorismu z celého světa, jako např.:

START National Consortium for the Study of Terrorism and Responses to Terrorism – organizace, jejímž cílem je vzdělávat a informovat o terorismu. Přínosem jejich webových stránek je nespočetné množství aktuálních dat, výzkumů a teroristických analýz.[84]

Databáze teroristických útoků z celého světa. GTD – *Global Terrorism Database* je databází společnosti START, která od roku 1970 eviduje přes více než 200 000 teroristických útoků zemí z celého světa. Databáze shromažďuje informace týkající se útoku, cíle, způsobu spáchání, pachatelů a teroristických organizací odpovědných za útok, počtů obětí a výše škody.[85]

Databáze teroristů a extremistů zveřejňuje všechny známé osobní údaje a další informace o známých teroristických lídrech, rekrutech, propagandistů apod.[86]

Databáze teroristických skupin vede evidenci známých teroristických uskupení, jejich hlavních vůdčích osobnostech a o dosud známých aktivitách.[87]

---

[82] Europol. *European Union Terrorism Situation and Trend report 2022. (TE-SAT).* [online]. [cit. 20.02.2023]. Dostupné z: https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2022-te-sat

[83] *ACSRT/CAERT.* [online]. [cit. 04.02.2023]. Dostupné z: https://caert.org.dz/

[84] *START – Study of Terrorism and Responses to Terrorism.* [online]. [cit. 04.02.2023]. Dostupné z: https://www.start.umd.edu/

[85] *GTD – Global Terrorism Database.* [online]. [cit. 04.02.2023]. Dostupné z: https://www.start.umd.edu/gtd/

[86] *Counter Extremism Project. Terrorists and Extremists Database.* [online]. [cit. 18.02.2023]. Dostupné z: https://www.counterextremism.com/extremists

[87] *Counter Extremism Project. Extremist Groups.* [online]. [cit. 18.02.2023]. Dostupné z: https://www.counterextremism.com/global-extremist-groups

Almanach islamismu popisuje aktuální aktivity radikálního islamismu ve vybraných 60 státech světa.[88]

Na oficiálních stránkách vlády USA *Rewards for Justice. Intelligence-Driven Law Enforcement* jsou zveřejněny **seznamy hledaných osob usvědčených nebo podezřelých z teroristických útoků**, za jejichž nalezení nebo podání informací o jejich pobytu náleží osobě odměna.[89]

European Eye on Radicalization je organizace, která ve spolupráci s analytiky z celého světa zveřejňuje zprávy zachycující aktuální dění, které souvisí s radikalizací, extremismem nebo terorismem v Evropě. V oddílu *„Analysis“* **popisuje a předvídá i budoucí vývoj jednotlivých situací**.[90]

TRAC je webový portál sdružují informace o teroristických skupinách i útocích. Přístup k aktuálním zprávám, analytickým zprávám a průzkumným zprávám je možný pouze za placené členství.[91]

Zpravodajsky významné informace se také dají dohledat přímo od tvůrců teroristické propagandy, jako např. kompletní výcvikový **manuál teroristické organizace Al-Qádia**, který vzdělává a motivuje k páchání teroristických útoků.[92]

Teroristické časopisy *Inspire* a *Dabiq* povzbuzují a inspirují čtenáře k útokům, nabízí řadu rad, návodů a doporučení, jak se stát teroristou a jak si opatřit prostředky. Tzv. šéfkuchař Al-Qádia radí např.:

- jak vytvořit bombu v kuchyni své matky
- jak provést atentát
- jak uschovat bombu v letadle
- jak instalovat bomby do aut

---

[88] American Foreign Policy Council. *World Almanac od Islamism* [online]. [cit. 15.02.2023]. Dostupné z: https://almanac.afpc.org/almanac

[89] Rewards for Justice. Intelligence-Driven Law Enforcement. *Terrorism Reward Offers.* [online]. [cit. 04.02.2023]. Dostupné z: https://rewardsforjustice.net/index/?jsf=jet-engine:rewards-grid&tax=crime-category:1070%2C1071%2C1073%2C1072%2C1074

[90] *European Eye on Radicalization.* [online]. [cit. 18.02.2023]. Dostupné z: https://eeradicalization.com/

[91] *TRACK. Tracking Terrorism.* [online]. [cit. 18.02.2023]. Dostupné z: https://trackingterrorism.org/

[92] POST Jerrold, *Military Studies in the Jihad Against the Tyrants: The Al-Qaeda Training Manual.* Maxwell Air Force Base, Alabama: USAF Counterproliferation Center, 2004. ISBN 9781907521249.

- jak použít nákladní automobil jako žací stroj na nepřátele
- jak uschovat bombu do balíku
- jak umístit bombu jako past na dveře.[93]

V roce 2021 byla vydána publikace *„Perspective of Terrorism“,* která obsahuje **nejnovější online zdroje pro analýzu teroristických aktivit**. Publikace rozděluje zdroje do 12 kategorií s teroristickou tématikou, např. náboženský a nenáboženský terorismus, teroristické strategie, boj proti terorismu, prevence, represe, analytické prognózy budoucího vývoje, kybernetické útoky apod.[94]

Teroristé používají ke komunikaci šifrovací aplikaci *Telegram*. Prostřednictvím této aplikace šíří teroristickou propagandu, hledají finance na podporu svých aktivit, šíří manuály a doporučení a koordinují své aktivity.[95]

3.4 Proliferace zbraní hromadného ničení

Distribuce jaderných, chemických, biologických zbraní a jiného vojenského materiálu je souhrnně označována jako proliferace zbraní hromadného ničení (ZHN). Tyto zbraně mají mimořádně ničivou sílu a mohou způsobit destrukci velké oblasti, způsobit smrt velkému počtu osob a další škody na majetku vyskytujícímu se v okolí cíle. Kontrola a monitorování výroby, vývoje i šíření těchto zbraní je pro udržení celosvětové bezpečnosti klíčová. Hrozbu představují zejména státní aktéři, kteří usilují o jejich získání a dále teroristické organizace, které mají zájem na jejich velkém destruktivním potenciálu. Při zneužití zbraní hromadného ničení teroristickými organizacemi se tyto zbraně mohou stát prostředkem zkázy pro lidstvo.

Nebezpečné je dále i šíření technologického know-how. Výroba jaderné hlavice a opatření potřebného materiálu je velmi náročná, její výroba nestátním aktérem je tak téměř nemožná. Biologické a chemické zbraně jsou ale z hlediska domácí

[93] WISKID, Claire. *Lone Wolf Terrorism and Open Source Jihad: An Explanation and Assessment.* [online]. International Institute for Counter-Terrorism, 2016. [cit. 05.02.2023]. Dostupné z: https://www.ict.org.il/UserFiles/ict-lone-wolf-osint-jihad-wiskind.pdf, str. 7-37.
[94] JONGMAN, Berto. Recent Online Resources for the Analysis of Terrorism and Related Subjects. *Perspectives on Terrorism*. [online]. 2021, roč. 15, č. 3. [cit. 03.03.2023]. ISSN 2334-3745. Dostupné z: https://www.jstor.org/stable/27030911
[95] *Counter Extremism Project. Terrorists On Telegram.* [online]. [cit. 18.02.2023]. Dostupné z: https://www.counterextremism.com/terrorists-on-telegram

výroby a získání přístupu ke komponentům podstatně jednodušší. Nedostatečně účinná mezinárodní kontrola těchto zbraní pak celý proces podstatně zjednodušuje.[96]

Devět zemí na světě disponuje dle agentury *SIPRI* **jadernými zbraněmi**. Jedná se o Ruskou federaci, Spojené státy americké, Spojené království, Francii, Čínskou lidovou republiku, Indii, Pákistán, Izrael a Severní Koreu. Jednotlivé země v průběhu posledních let informovaly o plánech navyšovat kapacity jaderných zbraní, popř. modernizovat stávající vybavení. V průběhu následujícího desetiletí tak lze očekávat navyšování kapacity jaderného arzenálu.[97]

3.4.1 Využití OSINT při proliferaci zbraní hromadného ničení

Riziko při vývozu ZHN představují státy se špatnými kontrolními i celními mechanismy, s vysokou mírou korupce a nedostatečnou legislativou. Tyto země se mohou stát cílem pro nelegální překupníky zbraní, mafii nebo teroristické organizace.[98] Volně přístupné databáze, které spravují data o exportu a importu ZHN, o počtech vyrobených kusů ZHN nebo o kapacitách arzenálu ZHN jednotlivých států jsou významným otevřeným zdrojem pro OSINT.

Zamezení vývozu zbraní do zemí, na která se vztahují zbrojní embarga nebo do jiných rizikových států je dalším ze způsobů boje proti proliferaci zbraní hromadného ničení. Dostatek informací o uvalených sankcích, rizikových osobách, podezřelých aktivitách autoritativních států představují pro zpravodajské služby cenný zdroj informací. Na základě těchto informací dochází k přijetí opatření pro zákaz obchodu s vojenským materiálem, nebo k vydání stanoviska o povolení k obchodu a vývozu ZHN.[99]

---

[96] DURDIAK, Jaroslav et al. *Zbrane hromadného ničenia – aktuálna bezpečnostná hrozba.* [online]. Bratislava: Ministerstvo obrany Slovenskej republiky, Inštitút bezpečnostních a obranných štúdií, 2005. [cit. 05.02.2023]. ISBN 978–80–88842–76–X Dostupné z: https://inis.iaea.org/collection/NCLCollectionStore/_Public/40/100/40100341.pdf, str. 10

[97] *SIPRI Year Book, World Nuclear Forces.* [online]. Stockholm International Peace Research Institute, 2022. [cit. 15.02.2023]. Dostupné z: https://sipri.org/sites/default/files/YB22%2010%20World%20Nuclear%20Forces.pdf

[98] United Nations Office on Drugs and Crime. *The illicit market in firearms.* [online]. Vienna: United Nations Office on Drugs and Crime, 2019. [cit. 19.02.2023]. Dostupné z: https://www.unodc.org/documents/e4j/Module_04_-_The_Illicit_Market_in_Firearms_FINAL.pdf, str. 14-15

[99] ZRŮN, Michal a Lucie ŘEHOŘOVÁ. *Úvod do zpravodajství*. Praha: PAČR v Praze, 2007. ISBN 978-80-7251-252-2, str. 31.

Webový portál *Royal United Services Institute (RUSI)* se v jedné ze svých mnoha průzkumných oblastí s názvem *„Sanctions“* zabývá **sankcemi uvalenými na určité státy** a jejich globálním dopadem. V souvislosti s Ruskou invazí pak zveřejňuje jména státních aktérů, které spolupracují s Ruskem a dováží na jejich území zbraně. Rozebírá tak přímý dopad na evropskou bezpečnost.[100] Články z počátku roku 2023 pak upozorňují na nebezpečí ZHN pocházejících z Íránu, jejich technologiemi a vývojem útočných dronů.[101]

Stockholm International Peace Research Institute (SIPRI) je švédský institut **zabývající se kontrolou zbrojní výbavy států**. Přínos pro OSINT představují jeho výroční zprávy a databáze.

SIPRI na svých stránkách poskytuje hned několik **databází**.

- ***Databáze vojenských nákladů*** shromažďuje informace o tom, kolik jednotlivé státy vkládají do svých armád.
- ***Databáze zbrojního průmyslu*** představuje souhrnné informace o společnostech vyrábějících zbraně a o prodeji těchto zbraní.
- ***Databáze o vývozu zbraní*** podává komplexní informace o mezinárodních dovozech a vývozech zbraní.
- ***Databáze zbrojních embarg*** poskytuje informace o udělených mezinárodních embargách a době trvání těchto sankcí.
- Dále pak SIPRI nabízí i ***databázi výročních zpráv jednotlivých států o exportech zbraní a vojenského materiálu***.[102]

Výroční zpráva SIPRI je volně dostupná pouze ve zkrácené verzi, po zakoupení předplatného[103] však podává souhrn detailních informací týkajících se mezinárodní bezpečnosti, vývoje v oblasti ozbrojených konfliktů a mírových jednání po celém

[100] Royal United Services Institute. *Sanctions*. [online]. [cit. 18.02.2023]. Dostupné z: https://rusi.org/explore-our-research/topics/sanctions#latest-publications
[101] ALSULAMI, Mohammed. *Europe and the Challenge of Dual-Use Technology Transfer to Iran.* [online]. [cit. 18.02.2023]. Dostupné z: https://rusi.org/explore-our-research/publications/commentary/europe-and-challenge-dual-use-technology-transfer-iran
[102] Stockholm International Peace Research Institute. *SIPRI Databases* [online]. [cit. 15.02.2023]. Dostupné z: https://sipri.org/databases
[103] Stockholm International Peace Research Institute. *SIPRI Year Book Online.* [online]. [cit. 15.02.2023]. Dostupné z: https://www.sipriyearbook.org/

světě, vývozů a dovozů zbraní, jaderných mocností a jejich jaderného arzenálu, konvenčních zbraní a nových zbraňových systémů.[104]

United Nations Register of Conventional Arms (UNROCA) je **registr obchodu se zbraněmi napříč státy**. Přehledně zpracovaná interaktivní mapa, popř. i tabulka nabízí údaje o tom, kolik jednotlivý stát vyvezl vojenského materiálu do kterých zemí a kolik materiálu zase objednal. Data zahrnují informace o počtu kusů jednotlivých exportovaných a importovaných zbraní pro konkrétní zemi. První kategorií jsou hlavní konvenční zbraně, do kterých patří válečné tanky, obrněná vozidla, dělostřelectvo, bojová letadla, vrtulníky a lodě, rakety. Druhou kategorií jsou pak ruční zbraně, pod které jsou zařazeny exporty revolverů, pistolí, pušek, samopalů, kulometů, granátometů, protitankových zbraní. Konkrétně pro Českou republiku zde lze dohledat záznamy o obchodu se zbraněmi od roku 1992 až po současnost. Podobně transparentních je pak zhruba dalších 40 států.[105]

Army Recognition je webový portál poskytující **informace o armádní výzbroji a výstroji jednotlivých států** a dále zveřejňující analytické zprávy z oblasti mezinárodních konfliktů, obrany, bezpečnosti a armády.[106]

Jane's Information Group je společností, pracující s otevřenými zdroji a podávající **informace z oblasti národní bezpečnosti, armády a letectví**. Za předplatné zde lze např. dohledat novinky z oblasti zbraňových systémů, analytické zprávy a satelitní snímky armádní výzbroje států.[107]

Přes webový portál společnosti *NTI* lze stáhnout excelovou tabulku upravující **databázi všech incidentů s radioaktivním materiálem**, které nastaly do roku

[104] Stockholm International Peace Research Institute. *SIPRI Yearbook 2022. Armaments, Disarmament and International Security* [online]. Oxford University Press, 2022. [cit. 15.02.2023]. ISBN 978-0-19-197961-3. Dostupné z: https://sipri.org/sites/default/files/2022-06/yb22_summary_en_v2_0.pdf, str.1

[105] *United Nations Register of Conventional Arms. Transparency in the global reported arms trade.* [online]. [cit. 16.02.2023]. Dostupné z: https://www.unroca.org/

[106] *Army Recognition.* [online]. [cit. 18.02.2023]. Dostupné z: https://armyrecognition.com/

[107] *Janes.* [online]. [cit. 18.02.2023]. Dostupné z: https://www.janes.com/

2019. Incidenty zahrnují krádež, ztrátu jaderného materiálu, popř. i materiál, který byl měl podléhat regulační kontrole, ale nepodléhá.[108]

3.5 Mezinárodní migrace

Jak již bylo zmíněno v úvodu 3. kapitoly, na bezpečnostním prostředí České republiky mají vliv konfliktní situace ve světě, ty totiž mohou být jedním z hlavních důvodů neřízených migračních vln. Neřízená masová migrace s sebou přináší bezpečnostní hrozby v podobě terorismu, organizovaného zločinu, šíření závažných nemocí i radikalizace. Odlišná kultura imigrantů může vést k obtížné integraci do majoritní společnosti. Nedostatečná integrace cizinců může představovat problémové soužití se společností, pocit sociálního vyloučení, vytváření uzavřených cizineckých komunit. Konfliktní situace a vztahy neintegrovaných cizinců s občany státu pak vedou ke vzniku sociálního napětí, xenofobního chování, extremismu, násilných aktivit a radikálních postojů vůči minoritní skupině obyvatelů.[109]

Česká republika má jako jeden ze států schengenského prostoru v důsledku zrušených hraničních kontrol ztíženou možnost kontroly nelegálních migrantů. V současnosti se však připravuje nový evropský kontrolní systém ETIAS *(The Europian Travel Information and Authorisation System)*, který bude sloužit pro státy, které v důsledku osvobozené vízové povinnosti ztrácí přehled o všech cestujících překračující hranice schengenského prostoru. Udělené povolení ETIAS o vycestování do zemí schengenského prostoru se stane obligatorní náležitostí pro možnost vycestovat do země. Tento systém zamítne osobě, která by mohla představovat bezpečnostní hrozbu, vstup do země. Cílem ETIAS je snaha o zajištění vyšší vnitřní bezpečnosti v zemích schengenského prostoru. Dle dostupných informací bude systém zprovozněn na počátku roku 2024.[110]

---

[108] NSI. *CNS Global Incidents and Trafficking Database Archived Reports and Graphics.* [online]. [cit. 03.03.2023]. Dostupné z https://www.nti.org/analysis/articles/cns-global-incidents-and-trafficking-database-archived-reports-and-graphics/

[109] Ministerstvo vnitra České republiky. *Audit národní bezpečnosti.* [online]. Praha: Ministerstvo vnitra České republiky, 2016 [cit. 06.11.2022]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf, str. 62-69

[110] European Union. *New requirements to travel to Europe.* [online]. [cit. 24.02.2023]. Dostupné z: https://travel-europe.europa.eu/etias/what-etias_en

3.5.1 Využití OSINT při mezinárodních migracích

Zpravodajství z otevřených zdrojů má v oblasti nelegální migrace silný potenciál, jelikož tradiční zpravodajské obory nemají v určitých lokalitách takovou možnost využití svých zpravodajských prostředků.

Otevřené zdroje mohou nabídnout informace podávající důležité charakteristiky země původu migrantů, zejména kulturní a společenskou tradici země, konfliktní nebo ekonomickou situaci, která mohla být důvodem pro migrační vlnu. Významnou roli představují informace o migračních trasách, způsobech dopravy, způsobech překročení hranic a další informace popisující přeshraniční pohyb. Mezi významné zdroje OSINT se řadí oficiální stránky státních a nadnárodních organizací, zabývající se problematikou mezinárodní migrace.

Informace o nelegální migraci lze získat i v tradičních mediálních zdrojích – denní tisk, rozhlas, televizní vysílání. Obecný problém tohoto zdroje je však ten, že média se mohou často zaměřovat na senzace a jejich zpravodajství tak nemusí být vždy a zcela objektivní. Poslední dobou se lze v mediálním prostoru setkat s negativním pojetí migrace, a to má za následek xenofobii, sociální opovrhování, což má silný a negativní dopad na veřejné mínění. Sociální sítě pak představují prostor, kde může mezi nelegálními migranty docházet ke konverzacím a radám týkajících se např. způsobů překročení hranic. Mediální zdroje i sociální média musí být brány s rezervou a věrohodnost a pravdivost z nich získaných informací musí být vždy náležitě prověřena.[111]

Organizace *The UN Refugee Agency (UNHCR)* se zabývá globálními uprchlickými krizemi.

- Každý rok vydává souhrnnou zprávu *Global Trends*, kde uvádí **statistické údaje** z předchozího roku **o uprchlících**, žadatelích o azyl i o osobách, které se vrátily do země původu.[112]

[111] MUNTEANU, Nicoleta Annemarie. Illegal migration approach from the perspective of open source intelligence. *Research and Science Today.* [online]. 2019, roč. 18, č. 2 [cit. 21.02.2023]. ISSN 2285-9632. Dostupné z: https://www.rstjournal.com/?mdocs-file=3826, str. 105-112.
[112] The UN Refugee Agency. *Global Trends.* [online]. [cit. 18.02.2023]. Dostupné z: https://www.unhcr.org/globaltrends

- *Mid-Year Trends* poskytuje statistické údaje za 6 měsíců předcházejícího roku o uprchlících, žadatelích o azyl, o zemí původu a příjmu.[113]
- **Statistická databáze uprchlické populace** podává souhrnný přehled počtu osob a dětí, hostitelských zemí i zemí původu, za 70letou historii.[114]
- **Portál uprchlických situací** nabízí interaktivní mapu s aktuálními uprchlickými situacemi z celého světa.[115]

Mezinárodní organizace pro migraci – *International Organization for Migration (IOM)* je společností zabývající se mezinárodní migrací.

- Každoročně vydává *World Migration Report*, kde uvádí aspekty, které utváří a modifikují migraci, a podává globální přehled o ní.[116]
- **Databáze publikací s imigrační tématikou** zahrnuje téměř 3000 studií a zpráv. Dle filtrů lze jednotlivé publikace rozdělit podle data vydání, tématu a zemí, kterých se týká.[117]
- Nejnovější aktuality, zprávy a výstupy z aktivit IOM lze dohledat v oddílu *Latest Research Updates*.[118]
- IOM spravuje i **českou verzi stránek**. Zde se nacházejí základní informace o počtu migrantů na území České republiky a aktuální zprávy z činnosti IOM na území ČR.[119]

[113] The UN Refugee Agency. *Mid-Year Trends*. [online]. [cit. 18.02.2023]. Dostupné z: https://www.unhcr.org/mid-year-trends
[114] The UN Refugee Agency. *Refugee Data Finder*. [online]. [cit. 18.02.2023]. Dostupné z: https://www.unhcr.org/refugee-statistics/download/?url=F8Wzj7
[115] The UN Refugee Agency. *Operational Data Portal. Refugee Situations.* [online]. [cit. 18.02.2023]. Dostupné z: https://data.unhcr.org/en/situations#_ga=2.118651210.211795433.1676819266-1970285126.1676819266&_gac=1.250116340.1676819266.Cj0KCQiArsefBhCbARIsAP98hXQ5Y93TE2cpl4E8yU2obLJId03H8gWhWYNFetBnnhGcrVwATXQGRE8aAsHMEALw_wcB
[116] MCAULIFFE, M. a A. TRIANDAFYLLIDOU. *World Migration Report 2022.* [online]. Switzerland: International Organization for Migration, 2021. [cit. 18.02.2023]. ISBN 978-92-9268-076-3. Dostupné z: https://publications.iom.int/books/world-migration-report-2022
[117] International Organization for Migration. *Search For Books*. [online]. [cit. 18.02.2023]. Dostupné z: https://publications.iom.int/search
[118] International Organization for Migration. *Latest Research Updates*. [online]. [cit. 19.02.2023]. Dostupné z: https://www.iom.int/iom-research-updates
[119] International Organization for Migration. *Czechia.* [online]. [cit. 19.02.2023]. Dostupné z: https://czechia.iom.int/cs

Frontex

- Každé dva roky publikuje **strategickou analýzu rizik**, kde identifikuje rizika a hrozby, analyzuje a prognózuje budoucí vývoj.[120]
- Interaktivní **mapa migrační situace** zobrazuje trasy všech mezinárodních migračních vln a zároveň tato mapa udává i statistické údaje z jednotlivých států o počtu migrantů a způsobu jejich tras. Dále je zde ke stažení volně dostupná excelová tabulka, která každý měsíc přidává údaje o počtu nelegálních migrantů, jejich národnosti a vybraném způsobu migrační trasy. Tato tabulka spravuje údaje již od ledna roku 2009.[121]
- Frontex monitoruje **7 hlavních migračních tras**, uvádí zde základní informace o migračních trasách a jejich historii v posledních letech.[122]

Eurostat

- Poskytuje **databázi s názvem integrace migrantů a dětí migrantů**. Databáze zahrnuje statistické informace pro jednotlivé hostitelské státy i věkové skupiny o sociálním zařazení migrantů, jejich životní úrovni, zdraví, vzdělání, zaměstnání a o státu původu.[123]
- Dále poskytuje **databázi migrantů** spravující informace o mezinárodní migraci a azylu.[124]

---

[120] Frontex. *Public Register of Documents. Strategic Risk Analysis.* [online]. [cit. 19.02.2023]. Dostupné z: https://prd.frontex.europa.eu/?form-fields%5Bsearch%5D=Strategic%20Risk%20Analysis&form-fields%5Bdate-from%5D&form-fields%5Bdate-to%5D&form-fields%5Bdocument-category%5D%5B0%5D=318&form-fields%5Boffset%5D=0&form-fields%5Bform-post-id%5D=NGVlNzVkMzBiOTY1ODE1NmZmZTEyYzMxMjg5NjE3OGJNVFk0T0E9PTU2MDA0ODI3NTljZjliZTkyZWM3OTBhN2E1NzI1NzMxODA5ZDBkMzMwMjE2OTU1Mjk2&form-fields%5Bmodule-post-id%5D=YjE4MWFjZTc1YjEzMmM5YTZhYzA4MGRkOWMzYzM2MDJNemt3TVE9PTYxODU2MDU1NjRlOTUwYjEwODZhM2IyNmE4ODliMzg3ZjdhMzNiYzFlMzcwMDg5MDM5

[121] Frontex. *Migratory map.* [online]. [cit. 24.02.2023]. Dostupné z: https://frontex.europa.eu/we-know/migratory-map/

[122] Frontex. *Migratory routes.* [online]. [cit. 24.02.2023]. Dostupné z: https://frontex.europa.eu/we-know/migratory-routes/western-mediterranean-route/

[123] Eurostat. *Data Browser – Cross cutting topics.* [online]. [cit. 19.02.2023]. Dostupné z: https://ec.europa.eu/eurostat/databrowser/explore/all/cc?lang=en&subtheme=mi&display=list&sort=category

[124] Eurostat. *Data Browser – Population and social conditions.* [online]. [cit. 19.02.2023]. Dostupné z: https://ec.europa.eu/eurostat/databrowser/explore/all/popul?lang=en&subtheme=migr&display=list&sort=category

European Union Agency for Asylum (EUAA) je organizace zabývající se žadateli o azyl. Na interaktivní mapě vede **statistické údaje o počtech žádostí o azyl** a zemí původu migrantů. Dále zveřejňuje základní informace o současných hlavních migračních důvodech a zemích, odkud lidé migrují.[125]

European Union Agency for Fundamental Rights (FRA) vede databázi zpráv, článků, příruček, průvodců, manuálů a dalších pravidelně doplňovaných informací, které jsou přístupné pod oddílem s názvem *Products.* Pro oblast imigrační politiky je pak zapotřebí použít filtr pro téma *Asylum, migration and borders* a zde se zobrazí veškeré publikace z této oblasti. Dále je pak možné publikace filtrovat podle zemí, jazyků, souvisejících článků Charty EU apod.[126]

3.6 Útoky z kyberprostoru

Kyberprostor je virtuální prostor bez jasně vymezených hranic, který se vyznačuje specifickými znaky odlišnými od reálného světa. Specifičnost kyberprostoru zakládá i specifické nároky na udržení kybernetické bezpečnosti. Útoky z kyberprostoru jsou anonymní, je možné je provést z jakéhokoliv místa na světě, jsou sofistikované, eskalující a boj s nimi je velmi náročný.[127]

Národní bezpečnost mohou ohrozit zejména pokusy o napadení sítí subjektů kritické infrastruktury a státních síťových zařízení. Útoky mohou mít různou podobu i formu, zejména se jedná o hackování, šíření škodlivých virů, únik citlivých nebo utajovaných informací, přetěžování sítě, odpírání přístupu uživatelům, narušení normálního chodu činnosti sítě.[128]

Zpravodajské služby a Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) se podílí na zajišťování kybernetické bezpečnosti České republiky,

[125] European Union Agency for Asylum*. Latest Asylum Trends.* [online]. [cit. 24.02.2023]. Dostupné z: https://euaa.europa.eu/latest-asylum-trends-asylum
[126] European Union Agency for Fundamental Rights. *Products.* [online]. [cit. 24.02.2023]. Dostupné z: https://fra.europa.eu/en/products/search
[127] Vláda České republiky. *Bezpečnostní strategie České republiky 2015.* [online]. Praha: Vláda České republiky, 2015 [cit. 29.10.2022]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf, str. 11.
[128] AKHBAR, Babak, BAYERL, Saskia, SAMPSON, Fraser (Eds.). *Open Source Intelligence Investigation. From Strategy to Implementation.* Canada: Springer International Publishing, 2016. ISBN 978-3-319-47671-1. str. 217-218.

spolupracují při bezpečnostních incidentech v oblasti kyberprostoru a vzájemně si pomáhají při detekci kybernetických útoků a reakcích na ně.[129]

NÚKIB v pravidelných měsíčních intervalech zveřejňuje zprávy *Cyber security incidents from the NÚKIB´s perspective*, kde ve statistických údajích uvádí registrované útoky na veřejnoprávní i soukromoprávní instituce ČR. Oddíl těchto zpráv lze však ve vyhledavači dohledat pouze na anglické verzi stránek NÚKIB.[130]

V roce 2020 byla u většiny kybernetických útoků spáchaných na území ČR zaznamenána snaha o kompromitaci sítí státních institucí či získání dat ze soukromé korespondence státních úředníků. K úniku dat nicméně došlo jen v jednom případu. Nelegálně opatřená data ze soukromých emailových schránek úředníků poskytují hackerům cenné informace o mezilidských vztazích, soukromých názorech osoby na určitá témata, ale také některé osobní údaje, jako např. údaje z naskenovaných dokumentů. Takto získané informace lze následně využít v dezinformační, diskreditační kampani. Dezinformacemi poškozená osoba může lehce ztratit důvěru občanů a její návrat je i v případě prokázání neviny téměř nemožný. Se ztrátou důvěry v osobnost poškozeného může úzce souviset i ztráta důvěry občanů v určité státní instituce nebo politické strany, kde zdiskreditovaná osoba působila.[131] V roce 2021 bylo Bezpečnostní informační službou taktéž potvrzeno, že většina útoků z kyberprostoru na státní instituce byla provedena subjekty, kteří měli vazbu zejména na Ruskou federaci nebo Čínskou lidovou republiku.[132]

---

[129] Národní úřad pro kybernetickou a informační bezpečnost. *Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025.* [online]. Praha: Národní úřad pro kybernetickou a informační bezpečnost, 2021 [cit. 20.02.2023]. Dostupné z: https://www.nukib.cz/download/publikace/strategie_akcni_plany/akcni_plan_2021-2025.pdf, str. 3-7.

[130] Národní úřad pro kybernetickou a informační bezpečnost. *Publications & Reports.* [online]. [cit. 26.02.2023]. Dostupné z: https://www.nukib.cz/en/infoservis-en/publications-reports/

[131] Bezpečnostní informační služba. *Výroční zpráva Bezpečnostní informační služby za rok 2020.* [online]. Praha: Bezpečnostní informační služba, 2021. [cit. 05.11.2022]. Dostupné z: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf, str. 17-18.

[132] Bezpečnostní informační služba. *Výroční zpráva Bezpečnostní informační služby za rok 2021.* [online]. Praha: Bezpečnostní informační služba, 2022. [cit. 05.11.2022]. Dostupné z: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2021-vz-cz-2.pdf, str. 8.

3.6.1 Využití OSINT při útocích z kyberprostoru

Úspěch v boji proti kybernetickým útokům je závislý na dostatečné informovanosti zpravodajských služeb o nových kybernetických hrozbách, bezpečnostních incidentech a hackerských skupinách. V účinné obraně národní bezpečnosti nestačí pouhá reakce na již spáchaný útok. Je zapotřebí vyvinout i proaktivní činnost v předcházení kybernetickým útokům a rozšiřovat vědomosti v souvislosti s vývojem nových sofistikovaných způsobů napadení.[133]

Státy, které prostřednictvím svých zpravodajských služeb shromažďují informace a provádějí kyberšpionáž na veřejnoprávních institucích cizího státu, představují hrozbu pro kritickou infrastrukturu napadeného státu. Jejich cílem může být omezení dodávek vybavení a ekonomické podpory pro armádu, omezení komunikačních technologií nebo např. omezení správného chodu státních sítí.

Kromě států využívajících útočnou informační doktrínu představují další hrozbu pro kybernetickou bezpečnost hackeři, kteří mnohdy útočí na státní instituce jen z důvodu zábavy a výzvy, kterou útok s sebou přináší. Nástroje a způsoby útoků prochází vývojem, stávají se promyšlenější než kdy dříve a jejich použití bývá snazší.

Napadení síťových zařízení může probíhat i úmyslným způsobem ze strany nespokojených pracovníků státní organizace, nebo neúmyslným a neopatrným pracovním postupem zaměstnanců, kteří síť omylem infikují virem.[134]

Otevřené zdroje, které lze využít v boji proti kybernetickým hrozbám lze rozdělit na několik kategorií. První kategorii budou bezpochyby představovat informační weby, které poskytují nejnovější informace z globálního kybernetického prostředí. Tím lze získat přístup k zpravodajsky relevantním informacím o nových vývojových trendech v této oblasti.

---

[133] WAGNER, Thomas, Eds. *Cyber Threat Intelligence Sharing: Survey and Research Directions*. [online]. Birmingham: Birmingham City University, 2019. [cit. 26.02.2023]. Dostupné z: https://www.open-access.bcu.ac.uk/7852/1/Cyber%20Threat%20Intelligence%20Sharing%20Survey%20and%20Research%20Directions.pdf, str. 1-4.

[134] JABBOUR, Kamal T., Erich DEVENDORF. Cyber Threat Characterization. *The Cyber Defense Review*, [online]. 2017, roč. 2, č. 3. [cit. 27.02.2023]. ISSN 2474-2120 Dostupné z: http://www.jstor.org/stable/26267387. str. 80-82

Společnost *Security Week* definuje a popisuje **aktuální bezpečnostní hrozby v oblasti kyberprostoru**. Lze zde dohledat informace z oblasti kybernetické bezpečnosti, způsobech zabezpečení a boje proti kybernetickým útokům. V oddílu *Malware&Threats* jsou dále uveřejňovány informace týkající se kybernetické války mezi státy, kybernetických zločinů, úniků dat, kybernetických útocích na státní instituce z celého světa a ransomwarů.[135] V sekci s názvem *Threat Intelligence* jsou zveřejňovány informace o kybernetických hrozbách a aktérů hrozeb, způsobech útoku a škodlivých následcích.[136]

Na podobném informačním principu existuje řada dalších webových portálů, které lze ve vyhledavači jednoduše dohledat pod názvem „*cyber security news"*. Níže uvedený seznam portálů zveřejňuje novinky z oblasti kybernetické bezpečnosti, dále vydává **zprávy s predikcemi na vývoj kybernetických hrozeb** pro nadcházející rok 2023 a doporučení, jak se dá jednotlivým hrozbám ubránit.

- *CSO Online*[137]
- *Cybersecurity Insiders*[138]
- *Dark reading*[139]
- *GBHackers On Security*[140]
- *HelpNetSecurity*[141]
- *Info Security Magazine*[142]
- *National Institute of Standards and Technology*[143]
- *Security Intelligence*[144]
- *Security affairs*[145]

[135] Security Week. *Malware&Threats.* [online]. [cit. 25.02.2023]. Dostupné z: https://www.securityweek.com/category/malware-cyber-threats/
[136] Security Week. *Threat Intelligence.* [online]. [cit. 25.02.2023]. Dostupné z: https://www.securityweek.com/category/threat-intelligence/
[137] *CSO Online*. [online]. [cit. 25.02.2023]. Dostupné z: https://www.csoonline.com/
[138] *Cybersecurity Insiders.* [online]. [cit. 25.02.2023]. Dostupné z: https://www.cybersecurity-insiders.com/
[139] *Dark reading.* [online]. [cit. 25.02.2023]. Dostupné z: https://www.darkreading.com/
[140] *GBHackers On Security*. [online]. [cit. 26.02.2023]. Dostupné z: https://gbhackers.com/
[141] *HelpNetSecurity*. [online]. [cit. 25.02.2023]. Dostupné z: https://www.helpnetsecurity.com/
[142] *Info Security.* [online]. [cit. 25.02.2023]. Dostupné z: https://www.infosecurity-magazine.com/cybercrime/
[143] *National Institute of Standards and Technology.* [online]. [cit. 25.02.2023]. Dostupné z: https://www.nist.gov/cybersecurity
[144] *Security Intelligence.* [online]. [cit. 25.02.2023]. Dostupné z: https://securityintelligence.com/
[145] *Security Affairs.* [online]. [cit. 25.02.2023]. Dostupné z: https://securityaffairs.com/

- *The Hacker News*[146]

Blogy bezpečnostních techniků a analytiků kybernetické bezpečnosti mohou poskytovat expertní pohledy na nové hrozby, způsoby útoku a postupy. Mezi tuto kategorii otevřených zdrojů se řadí např. blogy od:

- *Daniel Miessler*,[147]
- *Graham Cluley*,[148]
- *Troy Hunt*.[149]

Blogy renomovaných společností jsou další z možností, které lze využít pro rozšíření znalostí v oblasti kybernetické bezpečnosti. K využití plného potenciálu těchto blogů je však již vyžadována vyšší míra odborných znalostí v oboru.

- *Decoded avast.io* nabízí informace a novinky z prostředí hrozeb, které ohrožují mobilní telefony, sítě, počítače a zařízení připojená k internetu. Součástí jednotlivých článků jsou jména subjektů útoku, jejich konkrétní postupy a způsoby útoku. Články této společnosti jsou velmi odborné, podávají přesné postupy provedených útoků, způsoby kódování, šifrování a způsob jejich odhalení, nabízí např. i dešifrovací nástroje.[150] Společnost s pravidelností zveřejňuje i zprávy *Avast Threats Report*. Ve zprávách vždy v období předchozího ročního čtvrtletí shrnuje nové sofistikované útoky, trendy a vývoj malwarových kampaní i poznatky o současném stavu kybernetické bezpečnosti.[151]
- *Welivesecurity* nabízí novinky a poznatky z kyberbezpečnostní komunity.[152] Mezi další blogy by se daly řadit např.:
- *Securelist by Kaspersky,*[153]
- *Trend Micro Blog*.[154]

[146] *The Hacker News.* [online]. [cit. 25.02.2023]. Dostupné z: https://thehackernews.com/
[147] *Daniel Miessler*. [online]. [cit. 25.02.2023]. Dostupné z: https://danielmiessler.com/
[148] *Graham Cluley.* [online]. [cit. 25.02.2023]. Dostupné z: https://grahamcluley.com/about-this-site/
[149] *Troy Hunt.* [online]. [cit. 25.02.2023]. Dostupné z: https://www.troyhunt.com/
[150] *Decoded avast.io.* [online]. [cit. 26.02.2023]. Dostupné z: https://decoded.avast.io/
[151] *Decoded avast.io. Threats.* [online]. [cit. 26.02.2023]. Dostupné z: https://decoded.avast.io/tag/threats/
[152] *Welivesecurity.* [online]. [cit. 26.02.2023]. Dostupné z: https://www.welivesecurity.com/
[153] *Securelist by Kaspersky.* [online]. [cit. 26.02.2023]. Dostupné z: https://securelist.com/
[154] *Trend Micro Blog.* [online]. [cit. 26.02.2023]. Dostupné z: https://news.trendmicro.com/

- Oficiální blog společnosti Google s názvem *Threat Analysis Group.*[155]

Mnohé státy sdílejí výroční, čtvrtletní nebo měsíční zprávy o aktuální kybernetické situaci na jejich území v cizím jazyce. Analýza kybernetických hrozeb jednotlivých států a oficiální sdílení výsledků v cizích jazycích je důležitou prvkem pro udržení globální kybernetické bezpečnosti.[156]

Finské Národní centrum kybernetické bezpečnosti vydává na svých stránkách v oddílu *Cyber Weather* zprávy z kybernetickém prostředí v oblasti bezpečnosti, v kterých popisuje klíčové jevy a incidenty, které se staly na území Finska za uplynulý měsíc. Zprávy rozděluje podle jejich závažnosti na klidné, znepokojivé nebo vážné, a dále je rozděluje dle obsahu.[157]

Na stránkách Německého úřadu pro informační bezpečnost, lze pod slovy *The state of IT security in German"* vyhledat výroční zprávy o kybernetických hrozbách státních a vládních německých institucí.[158]

Podobné informace lze najít i na lotyšských stránkách CERT.LV pod vyhledávacím výrazem *Annual report.*[159]

Kromě informační portálů a zpráv, kde se zpravodajští analytici mohou dozvědět aktuální novinky a informace z globálního kybernetického prostředí, lze na internetu zdarma nebo za poplatek využít i některých nástrojů.

Shodan.io, je **zpoplatněný nástroj** sloužící k rozpoznání různých typů zařízení, které jsou připojeny k internetu, zejména servery, hraniční routery, IP kamery. Nástroj nabízí analýzu zranitelnosti systému a penetrační testování.[160] Mezi další

[155] *Threat Analysis Group.* [online]. [cit. 26.02.2023]. Dostupné z: https://blog.google/threat-analysis-group/
[156] WAGNER, Thomas, Eds. *Cyber Threat Intelligence Sharing: Survey and Research Directions*. [online]. Birmingham: Birmingham City University, 2019. [cit. 26.02.2023]. Dostupné z: https://www.open-access.bcu.ac.uk/7852/1/Cyber%20Threat%20Intelligence%20Sharing%20Survey%20and%20Research%20Directions.pdf, str. 1-4.
[157] Traficom. *Cyber Weather.* [online]. [cit. 26.02.2023]. Dostupné z: https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/cyber-weather?toggle=Cyber%20Weather%202023&toggle=Cyber%20Weather%202022
[158] *Bundesamt für Sicherheit in der Informationstechnik.* [online]. [cit. 26.02.2023]. Dostupné z: https://www.bsi.bund.de/DE/Home/home_node.html
[159] CERT.LV. *Latvijas Republikas Informācijas tehnoloģiju drošības incidentu noveršanas institūcija.* [online]. [cit. 26.02.2023]. Dostupné z: https://cert.lv/en/search?q=annual+report
[160] *Shodan.* [online]. [cit. 27.02.2023]. Dostupné z: https://www.shodan.io/

zpoplatněné nástroje fungující na podobném principu skenování všech zařízení připojených k internetu patří:

- *Censys.io*[161]
- *Binaryedge.io*[162]

Nástroj *DomainTools* je nástroj, který se užívá pro průzkum škodlivých aktivit domén. Škodlivost se udává v číslech na stupnici *Risk score*. Pomocí tohoto nástroje lze vyhledat a identifikovat riziko domén vyskytujících se v síti a zastavit útok ještě před jeho spuštěním.[163]

Virustotal analyzuje podezřelé soubory a poskytuje informace o malware, škodlivých doménách, IP adresách.[164]

Exploit.db je databáze shromažďující informace o všech známých zranitelnostech softwarů.[165] *Google Hacking Database* je stejnou společností spravovaná databáze citlivých informací, které nedopatřením unikly na internet.[166]

Wigle.net shromažďuje informace a ukazuje polohu všech wifi sítích po celém světě, které zobrazuje na interaktivní mapě.[167]

Who.is slouží k zjištění majitele internetové domény a IP adresy.[168]

3.7 Extremismus

Extremismem se rozumí ideologicky vyhraněný postoj, který je zaměřen proti zaručeným demokratickým a ústavním principům státu. Pro extremismus jsou typické projevy násilí, popírání základních práv a svobod minoritních skupin obyvatel, odmítání multikulturalismu, specificky zaměřená nenávist, netolerance a vzbuzování strachu.[169] Krize i sociální napětí jsou okolnosti, které vedou

[161] *Censys.io.* [online]. [cit. 27.02.2023]. Dostupné z: https://censys.io/
[162] *Binaryedge.io.* [online]. [cit. 27.02.2023]. Dostupné z: https://binaryedge.io/
[163] *Domaintools.* [online]. [cit. 27.02.2023]. Dostupné z: https://www.domaintools.com/
[164] *Virustotal.* [online]. [cit. 27.02.2023]. Dostupné z: https://www.virustotal.com/gui/home/upload
[165] *Exploit database.* [online]. [cit. 27.02.2023]. Dostupné z: https://www.exploit-db.com/
[166] *Exploit database – Google Hacking Database.* [online]. [cit. 27.02.2023]. Dostupné z https://www.exploit-db.com/google-hacking-database?category=5
[167] *Wigle. Net. All the networks. Found by everyone.* [online]. [cit. 27.02.2023]. Dostupné z: https://wigle.net/index
[168] *Who.is.* [online]. [cit. 27.02.2023]. Dostupné z: https://who.is/
[169] Ministerstvo vnitra České republiky. *Audit národní bezpečnosti.* [online]. Praha: Ministerstvo vnitra České republiky, 2016. [cit. 06.11.2022]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf, str. 27-28.

ke vzniku sociálně vyloučených skupin. Následně jsou tyto skupiny osob více náchylné k radikalizaci nebo sympatizováním s extremistickými názory a aktivitami.[170] Extremismus je ve svém počátku nebezpečný zejména pro menšiny, pokud se však tato hrozba včas a dostatečně nepodchytí, může představovat hrozbu pro celý státní systém. Z tohoto důvodu je monitorování extrémistických aktivit a činností jedním ze zásadních kroků pro udržení národní bezpečnosti demokratického státu.[171]

Česká extrémistická scéna se již dlouhodobě potýká s problémy, které tkví v nedostatečné vnitřní komunikaci, spolupráci a organizovanosti svých členů. Obecně by se dalo tvrdit, že české extremistické skupiny spíše stagnují. Bezpečnostní informační služba nicméně upozorňuje, že riziko může představovat komunikace českých extrémistických subjektů se zahraničními subjekty. Dalším rizikem pak může být možnost ovlivnění jednotlivce radikálními postoji.[172]

3.7.1 Využití OSINT v boji proti extremismu

Propagandistické materiály extremistických skupin jsou lehce dostupné prostřednictvím webových portálů a sociálních sítí jako je Facebook, Twitter, Tumblr, YouTube, Skype, WhatsApp. Tyto materiály mají mnoho podob. Může se jednat o videa s extremistickou rétorikou, hudební písně, projevy, časopisy, manuály, příručky a další publikace přístupné online nebo vytištěné v papírové podobě.[173]

Vyznavači pravicového extremismu ve Spojených státech se uchylují k náboru mladých studentů v areálech škol nebo na sociálních mediích. Z pohledu demografického složení extremistických skupin tvoří mladí lidé do 30 let většinovou

[170] Vláda České republiky. *Bezpečnostní strategie České republiky 2015*. [online]. Praha: Vláda České republiky, 2015. [cit. 29.10.2022]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf, str. 12; 17, bod 70.

[171] Ministerstvo vnitra České republiky. *Audit národní bezpečnosti.* [online]. Praha: Ministerstvo vnitra České republiky, 2016. [cit. 06.11.2022]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf, str. 27-28.

[172] Bezpečnostní informační služba. *Výroční zpráva Bezpečnostní informační služby za rok 2021.* [online]. Praha: Bezpečnostní informační služba, 2022. [cit. 05.11.2022]. Dostupné z: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2021-vz-cz-2.pdf, str. 9, 19-20.

[173] Counter Extremism Project. *Extremists & Online Propaganda.* [online]. Counter Extremism Project, 2018. [cit. 27.02.2023]. Dostupné z: https://www.counterextremism.com/themes/custom/cep/templates/reports/extremists_online_propaganda/files/Extremists%20and%20Online%20Propaganda_040918.pdf, str. 1-3.

část skupiny, proto se nábor nových členů zaměřuje na mládež, která je i snáze ovlivnitelná.[174]

Pro boj s extremismem je zapotřebí pochopit sociální, kulturní a politické aspekty, které vedou ke vzniku extrémistických postojů ve společnosti, včetně pochopení skutečností, které umožňují extremistickým skupinám vznikat, zvětšovat své členské základny a negativně ovlivňovat veřejné mínění.[175]

Otevřené zdroje zabývající se extremistickou problematikou jsou podstatně rozmanité. Jedním z druhů otevřených zdrojů zabývajících se extremismem jsou webové portály organizací, které bojují s radikálními a násilnickými projevy ve společnosti.

ADL je institucí bojující vůči předsudkům a **nenávisti proti židovské komunitě**. Spravuje databázi nenávistných symbolů a vede přehled analytických zpráv a výzkumů s extremistickou, antisemitskou a nenávistnou tématikou.[176]

Counterextremism je společností, která bojuje s extremismem. Vyvinula technologii, která identifikuje extrémistické aktivity na sociálních sítích a správcům těchto sítí pomáhá tyto skupiny, příspěvky, obrázky a videa odstranit z obsahu sociálních sítí.[177] Organizace *Counterextremism* dále nabízí:

- **Databáze extremistů a teroristů** zveřejňuje všechny známé osobní údaje a další informace o známých teroristických i extrémistických lídrech, rekrutech, propagandistů apod.[178]

[174] Counter Extremism Project. *White Supremacy Groups in the United States.* [online]. Counter Extremism Project, 2023. [cit. 03.03.2023]. Dostupné z: https://www.counterextremism.com/sites/default/files/supremacy_landing_files/U.S.%20White%20Supremacy%20Groups_022323.pdf, str. 1.
[175] SUBEDI, Db. a Bert JENKINS. Preventing and Countering Violent Extremism: Engaging Peacebuilding and Development Actors. *Counter Terrorist Trends and Analyses.* [online]. 2016, roč. 8., č. 10. [cit. 04.03.2023]. ISSN 2382-6444. Dostupné z: http://www.jstor.org/stable/26351459, str. 13-15.
[176] *ADL*. [online]. [cit. 03.03.2023]. Dostupné z: https://www.adl.org/
[177] *Counterextremism.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.counterextremism.com/
[178] *Counter Extremism Project. Terrorists and Extremists Database.* [online]. [cit. 18.02.2023]. Dostupné z: https://www.counterextremism.com/extremists

- **Databáze extrémistických a teroristických skupin** vede evidenci známých radikálních uskupení, jejich názorovou ideologii a hlavních vůdčí osobnosti.[179]
- Zprávy shrnující a popisující teroristickou a extremistickou scénu na území jednotlivých států.[180]

Databáze organizace *European Agency for Fundamental Rights* shromažďuje celosvětové **rozsudky soudů v oblasti trestných činů z nenávisti**.[181]

Mezi další zdroje patří *European Eye on Radicalization* více viz kapitola 3.3.1.[182]

Institute for Strategic Dialogue vydává **analytické zprávy** o extrémistické problematice, jakožto rychle se vyvíjející hrozbě.[183]

International Center for Counter-terrorism je think-tankem poskytujícím průzkumy, poradenství a školení v boji proti extremismu. V oddíle publikací lze nalézt nejnovější publikace společnosti o extremismu ve světě.[184]

Jednotlivci z České republiky vyznávající některou extremistickou ideologii mohou spolupracovat, být ovlivněni, komunikovat nebo se jinak aktivně spojovat se zahraniční extrémistickou scénou. Rizikem může být inspirace a praktikování zahraničních násilnických trendů. Z tohoto důvodu je pro zpravodajské služby klíčové monitorovat a mít přehled o zahraničních extrémistických projevech, skupinách a propagandistickém působení.[185] Následující text bude poskytovat přehled aktivních extremistických blogů, fór a webových stránek ze Spojených států a evropských zemí.

---

[179] *Counter Extremism Project. Extremist Groups.* [online]. [cit. 18.02.2023]. Dostupné z: https://www.counterextremism.com/global-extremist-groups
[180] *Counter Extremism Project. Country Reports: Extremism & Terrorism.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.counterextremism.com/countries
[181] *European Agency for Fundamental Rights. Cases and rulings.* [online]. [cit. 18.02.2023]. Dostupné z: https://fra.europa.eu/en/databases/anti-muslim-hatred/case-law
[182] *European Eye on Radicalization.* [online]. [cit. 03.03.2023]. Dostupné z: https://eeradicalization.com/
[183] *Institute for Strategic Dialogue.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.isdglobal.org/
[184] *International Center for Counter-terrorism.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.icct.nl/
[185] Ministerstvo vnitra České republiky. *Audit národní bezpečnosti.* [online]. Praha: Ministerstvo vnitra České republiky, 2016. [cit. 06.11.2022]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf, str. 28-30.

Pro **americké extrémistické portály**, pravicově orientované, je charakteristická antisemitská tématika, dále odpor k černošské rase, vzbuzování nenávisti a násilí vůči migrantům.[186]

American Renaissance je pravicově zaměřený blog, který podporuje pseudovědecké zprávy, podcasty, videa a novinky o podřadnosti černošské rasy[187]

Identity Evropa je extrémistický americký portál s protiimigrační tématikou.[188]

League of the South je antisemitisticky zaměřená webová stránka šířící nenávist proti jiným než křesťanským náboženství a kulturním odlišnostem.[189]

The National Socialist Movement je neonacistickou skupinou s agresivní rétorikou vůči Židům a dalším minoritním skupinám.[190] K propagandě využívá různé formy šíření nacistického obsahu. Sdílí videa, je aktivní na svých webových stránkách, oslovuje lidi na ulicích pomocí reklamních brožur, pořádá veřejné promluvy, pochoduje po ulicích s vlajkami a megafonem, dále rozvěšuje plakáty, lepí samolepky s QR kódem, které odkazují na hlavní stránky skupiny, tiskne noviny, reklamní papíry a větší nelegální billboardy.[191]

Členové extrémistické skupiny *The Rise Above Movement* trénují bojová umění, které pak využívají při násilných konfliktech. Svou propagandu šíří prostřednictvím webových stránek *Media2Rise.*[192]

Na podobném principu jsou dosud aktivní i:

- *Patriotfront,*[193]

[186] Counter Extremism Project. *White Supremacy Groups in the United States*. [online]. Counter Extremism Project, 2023. [cit. 03.03.2023]. Dostupné z: https://www.counterextremism.com/sites/default/files/supremacy_landing_files/U.S.%20White%20Supremacy%20Groups_022323.pdf, str. 1-112.
[187] *American Renaissance.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.amren.com/
[188] *Identity Evropa.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.identityevropa.com/
[189] *League of the South.* [online]. [cit. 03.03.2023]. Dostupné z: http://leagueofthesouth.com/
[190] *The National Socialist Movement.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.nsm88.org/
[191] *The National Socialist Movement. NSM Year in Review 2022.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.nsm88.org/comment/7740#comment-7740
[192] *Media2Rise.* [online]. [cit. 03.03.2023]. Dostupné z: https://media2rise.com/
[193] *Patriotfront*. [online]. [cit. 03.03.2023]. Dostupné z: https://patriotfront.us/

- *Dailystormer.*[194]

Zahraniční extrémistické skupiny ze Spojených států spravují i některé portály určené k šíření extrémistické propagandy formou žurnalistických stránek, knihkupectví s antisemitskou tématikou, rádií, video a audio vysílacích stanic, blogů. Příkladem z doposud aktivních propagandistických stránek by mohly být:[195]

- *The Barnes Review*,[196]
- *The Occidental Quarterly*,[197]
- *The Occidental Observer*,[198]
- *The Right Stuff*,[199]
- *Rense Radio Network*,[200]
- *RedIce.TV*.[201]

Úspěšný boj s extremisty prokazuje zrušení některých známých extremistických webových stránek jako byly stránky skupin *Atomwaffedivision.org, Bloodandsoil.org, Crew38.com, Hammerskins.net, Ironmarch.org, Siegeculture.biz, Thebase.wordpress.com*.[202]

Další přehled **amerických levicově orientovaných webových portálů** lze dohledat i s obsáhlou popisnou charakteristikou v dokumentu *Far-left Extremist*

[194] Dailystormer. [online]. [cit. 03.03.2023]. Dostupné z https://dailystormer.in/
[195] Counter Extremism Project. *White Supremacy Groups in the United States*. [online]. Counter Extremism Project, 2023. [cit. 03.03.2023]. Dostupné z: https://www.counterextremism.com/sites/default/files/supremacy_landing_files/U.S.%20White%20Supremacy%20Groups_022323.pdf, str. 112-113.
[196] *The Barnes Review. Magazine and Bookstore.* [online]. [cit. 03.03.2023]. Dostupné z: https://barnesreview.org/
[197] *The Occidental Quarterly*. [online]. [cit. 03.03.2023]. Dostupné z: https://www.toqonline.com/
[198] *The Occidental Observer.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.theoccidentalobserver.net/
[199] *The Right Stuff*. [online]. [cit. 03.03.2023]. Dostupné z: https://therightstuff.biz/
[200] *Rense Radio Network.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.renseradio.com/hosts.htm
[201] *RedIce.TV*. [online]. [cit. 03.03.2023]. Dostupné z: https://redice.tv/
[202] Counter Extremism Project. *White Supremacy Groups in the United States.* [online]. Counter Extremism Project, 2023. [cit. 03.03.2023]. Dostupné z: https://www.counterextremism.com/sites/default/files/supremacy_landing_files/U.S.%20White%20Supremacy%20Groups_022323.pdf, str. 3-112.

Groups in the United States, který je volně přístupný, z již zmiňované webové stránky *Counter Extremism.*[203]

Pro **evropské extrémistické portály** je charakteristické šíření nenávisti vůči minoritním skupinách, především muslimské národnosti, dále pořádání demonstrací a témata týkající se ochrany a udržení evropské kultury.[204]

Alternative für Deutschland je krajně pravicová strana, zejména s proti imigrantskými a protimuslimskými názory, která svou ideologii šíří prostřednictvím webového portálu[205], Facebookových stránek, Instagramu, Twitteru i YouTube.[206]

Generation Identity se snaží zvrátit islamizaci Evropy a negativně vystupuje proti multikulturalismu. Tato skupina spravuje stránky pro Velkou Británii a Irsko[207], Francii[208] a Německo.[209]

Jobbik je maďarská fašistická politická strana, která sama sebe označuje za konzervativní a vlasteneckou. Šíří nenávist vůči Romům, muslimům a Židům.[210]

Satanistická organizace *The Order of Nine Angels* uctívající Adolfa Hitlera má silně antisemitskou rétoriku. Podporuje džihádistický terorismus, sympatizuje s Usamou bin Ládinem, propaguje pedofilii a další zločiny, které podkopávají systematický řád společnosti.[211]

---

[203] Counter Extremism Project. *Far-left Extremist Groups in the United States.* [online]. Counter Extremism Project, 2022. [cit. 03.03.2023]. Dostupné z: https://www.counterextremism.com/sites/default/files/supremacy_landing_files/U.S.%20Far-Left%20Extremist%20Groups_PDF_083122.pdf

[204] Counter Extremism Project. *European Ethno-Nationalist and White Supremacy Groups*. [online]. Counter Extremism Project, 2022. [cit. 03.03.2023]. Dostupné z: https://www.counterextremism.com/sites/default/files/supremacy_landing_files/European%20Ethno-Nationalist%20and%20White%20Supremacy%20Groups_120722.pdf, str. 1-3.

[205] *Alternative für Deutschland*. [online]. [cit. 03.03.2023]. Dostupné z: https://www.afd.de/

[206] Counter Extremism Project. *European Ethno-Nationalist and White Supremacy Groups*. [online]. Counter Extremism Project, 2022. [cit. 03.03.2023]. Dostupné z: https://www.counterextremism.com/sites/default/files/supremacy_landing_files/European%20Ethno-Nationalist%20and%20White%20Supremacy%20Groups_120722.pdf, str. 5-9.

[207] *Generation Identity. United Kingdom and Ireland.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.generation-identity.org.uk/

[208] *Génération Identitaire.* [online]. [cit. 03.03.2023]. Dostupné z: https://generationidentitaire.org/

[209] *Identitäre Bewegung.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.identitaere-bewegung.de/

[210] *Jobbik.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.jobbik.com/

[211] *The Order of Nine Angels.* [online]. [cit. 03.03.2023]. Dostupné z: https://lapisphilosophicus.wordpress.com/

Mezi další aktivní evropské extrémistické webové portály politických stran nebo politicky aktivních skupin patří:

- *Associazione Culturale Veneto fronte Skinheads,*[212]
- *Blood & Honour,*[213]
- *Blood C18 Honour – Hungary,*[214]
- *Der Dritte Weg,*[215]
- *ISD The Voice Of Blood and Honour RECORDS,*[216]
- *Ľudová strana naše Slovensko,*[217]
- *Nationaldemokratische Partei Deutschlands,*[218]
- *Nordic Resistance Movement,*[219]
- *Noua Dreaptă,*[220]
- *RedWatch Poland.*[221]

A fórum *Stormfront.*[222]

Mezi české otevřené zdroje pak lze řadit webové portály skupiny *Antifa,*[223]*DSSS,*[224]*Národní demokracie,*[225]*Generace identity*[226] a *Národní obroda.*[227]

[212] *Associazione Culturale Veneto fronte Skinheads.* [online]. [cit. 03.03.2023]. Dostupné z: http://venetofronteskinheads.org/beta/
[213] *Blood & Honour.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.afd.de/https://www.bloodandhonourworldwide.co.uk/bhww/
[214] *Blood C18 Honour – Hungary*. [online]. [cit. 03.03.2023]. Dostupné z: http://c18hungary.blogspot.com/
[215] *Der Dritte Weg.* [online]. [cit. 03.03.2023]. Dostupné z: https://der-dritte-weg.info/
[216] *ISD The Voice Of Blood and Honour RECORDS.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.isdrecords.com/
[217] Ľudová strana naše Slovensko. [online]. [cit. 03.03.2023]. Dostupné z: http://www.lsnaseslovensko.sk/
[218] *Nationaldemokratische Partei Deutschlands.* [online]. [cit. 03.03.2023]. Dostupné z: https://npd.de/
[219] *Nordic Resistance Movement.* [online]. [cit. 03.03.2023]. Dostupné z: https://nordicresistancemovement.org/
[220] *Noua Dreaptă.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.nouadreapta.org/
[221] *RedWatch Poland.* [online]. [cit. 03.03.2023]. Dostupné z: http://www.redwatch.info/
[222] *Stormfront*. [online]. [cit. 03.03.2023]. Dostupné z: https://www.stormfront.org/forum/
[223] *Antifa.* [online]. [cit. 03.03.2023]. Dostupné z: https https://antifa.cz/
[224] *DSSS.* [online]. [cit. 03.03.2023]. Dostupné z: http://www.dsss.cz/
[225] *Národní demokracie.* [online]. [cit. 03.03.2023]. Dostupné z: https://narodnidemokracie.cz/
[226] *Generace identity.* [online]. [cit. 03.03.2023]. Dostupné z: https://generace-identity.cz/
[227] *Národní obroda.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.narodni-obroda.cz/

4 Využití OSINT z hlediska armády

Zpravodajství z otevřených zdrojů nabízí řadu výhod, které lze z hlediska vojenského plánovaní operací využít. Potenciál OSINT pro armádní účely bude záviset na lokalitě konfliktu a podmínkách ozbrojeného konfliktu. Značné využití bude zejména pro varování, plánování, poskytnutí pomoci a bude sloužit pro rychlou rozhodovací informovanost velitele zásahu. Výhody OSINT pro armádu by se daly rozčlenit na 3 základní úrovně.

Na strategické úrovni je OSINT využitelný z hlediska upozornění o hrozícím nebezpečí nebo nepřátelských motivech proti státnímu území. Předzvěst plánovaného nebezpečí poskytuje významnou vojenskou výhodu. Shromažďování informací z otevřených zdrojů o krizových, mimořádných nebo ozbrojených situacích a jejich následná analýza podává mnohdy hodnotnější a kvalitnější zpravodajské informace než informace od utajovaných zdrojů, jejichž názor může být mnohdy ovlivněn subjektivními pohledy. Otevřené zdroje jsou na strategické úrovni vhodné pro získání informací, které nemohou být jinými zpravodajským odvětvími obecně získány – např. kulturní a demografické podmínky. Informovanost o hrozbách, kterou lze zjistit prostřednictvím otevřených zdrojů může vést k pozitivní změně politického přístupu a lepšímu vybavení a výcviku vojáků.

Na operační úrovni poskytuje OSINT klíčové informace o mapách a satelitních snímcích území, regionálních podmínkách vzduchu, povrchu krajiny, vodních toků, geografických charakteristikách popisující ovzduší, počasí, teploty, přístupnost a kvalitu vodních zdrojů. Důležité budou i charakteristiky týkající se mostů, přístavů, počtu letišť, druhu silnic, civilních úkrytů a bunkrů. Množství těchto informací poslouží veliteli k lepší orientaci v prostředí a rozhodování o účinném využití sil a prostředků k vedení operace.

Na technické úrovni poskytnou informace z otevřených zdrojů většinu údajů potřebných k řízení a koordinaci vzdušných, pozemních a námořních operací.[228]

[228] STEELE, Robert David. Open Source Intelligence: What Is It? Why Is It Important To The Military? *American Intelligence Journal.* [online]. 1996, roč. 17, č. ½. [cit. 06.02.2023]. Dostupné z: http://www.jstor.org/stable/44326547, str. 35–37.

U těch vojenských operací, u kterých není hlavním cílem získat vysoké množství různorodých informací je OSINT nejvíce vhodnou variantou, která nabízí velmi rychlý přísun aktuálních informací. Pro prvotní rozhodování je tento rychlý přísun informací důležitý. Na základě včasně získaných informací si mohou vojenští důstojníci lehce vytvořit základní představu o dané problematice. Následné vytyčení požadavků a úkolů pro zpravodajce pro doplňující sběr informací je pak jednodušší a přesnější.

V porovnání s utajovanými zpravodajskými obory lze prostřednictvím OSINT získat předběžné informace za vynaložení menších finančních prostředků a v kratší době. Sběr volně dostupných informací z otevřených zdrojů je v závažných politických problematikách (terorismus, extremismus, proliferace zbraní atd.) méně rizikový než sběr informací utajovaným způsobem. Pro to je důležité ve vhodných případech vždy nejprve využít toho, co může zpravodajství z otevřených zdrojů nabídnout, následně lze tradiční utajované zpravodajské obory zaměřit na požadavky, které informace je potřeba doplnit nebo které nelze získat jiným způsobem.[229]

Současným příkladem praktického využití OSINT pro vojenské účely je válka mezi Ukrajinou a Ruskem. Satelitní snímky zobrazují ničivou devastaci ukrajinského území. Masová média odhalují technická data o ruském vojenském vybavení a vojenských prostředcích. Obsahy, fotky a videa shromážděné a zveřejněné jednotlivci na sociálních sítích zachycují autentické záběry z ulic. Videa z bitevního pole prezentují kruté podmínky bitevní reality. Celý proces však s sebou nese i šíření falešných a záměrně manipulativních zpráv, proto třídění informací získaných z otevřených zdrojů je pro dostatečnou informovanost klíčové.[230]

Ukrajinští vývojáři vytváří online platformy, které pomáhají přežít v době války, nebo které nahlašují posuny ruských vojsk, informují o ruském vojenském

[229] HORÁK, Oldřich a Ivo PIKNER. Zpravodajství z otevřených zdrojů. *Vojenské rozhledy.* [online]. 2007, č. 3. [cit. 08.10.2022]. ISSN 2336-2995. Dostupné z: https://www.vojenskerozhledy.cz/images/archiv_voj_rozhl/clanky/2007/3/4_zpravodajstvi_z_otevrenych_zdroju.pdf, str. 36-37.
[230] TZ a Tamir HAYMAN. Open-Source Intelligence and the War in Ukraine. *INSS, Insight.* [online]. Institute for National Security Studies, 2023, č. 1678. [cit. 08.10.2022]. Dostupné z: http://www.jstor.org/stable/resrep47006. str. 1-6.

vybavení a nahrávají důkazy o ruských válečných zločinech.[231] Společností *AJAX* byla vytvořena aplikace *Air Alert,* která zachraňuje životy civilistů i ukrajinských vojáků. Aplikace vydává **hlasité varování při aktuálním náletu** nebo jiném nebezpečí v jakékoliv denní době.[232] Způsob, kterým civilisté mohou **nahlašovat pozice ruských vojsk** a vojenské vybavení probíhá přes aplikaci *eVorog*. Tyto informace se následně přeposílají do rukou ukrajinské armády.[233] Webový portál pro hlášení válečných zločinů vojáků Ruské federace na území Ukrajiny umožňuje **nahrávat důkazní videa a fotografie spáchaných trestných činů**.[234] *International Legion Defence of Ukraine* je portál, který náboruje bojovníky pro Ukrajinu pomáhá i radí, jakým způsobem je možné vstoupit na ukrajinské území a doporučuje, které vybavení si vzít s sebou.[235] Evakuační weby pro osoby, které si přejí odejít, přejít nebo přejet z místa na místo, radí, jak tento postup udělat, aby nebyly při přesunu ohroženy na životech.[236] Na podobném principu funguje i portál *Pomich*.[237]

Z těchto příkladů je patrné, že v této digitální válce se může každý civilista stát součástí velké informační skupiny, která pomáhá monitorovat pohyb a aktivity ruských vojsk na Ukrajině a tím usnadňovat práci ukrajinské armádě.[238]

[231] The Washington Post. Democracy Dies in Darkness. *Instead of consumer software, Ukraine's tech workers build apps of war. [*online]. [cit. 01.03.2023]. Dostupné z: https://www.washingtonpost.com/technology/2022/03/24/ukraine-war-apps-russian-invasion/
[232] Ajax. *The Air Alert app is now available for Android and iOS*. [online]. [cit. 01.03.2023]. Dostupné z: https://ajax.systems/blog/zastosunok-povitryana-trivoga/
[233] Telegram. *eVorog*. [online]. [cit. 01.03.2023]. Dostupné z: https://t.me/evorog_bot
[234] *Office of the Prosecutor General.* [online]. [cit. 01.03.2023]. Dostupné z: https://warcrimes.gov.ua/
[235] *International Legion Defence of Ukraine.* [online]. [cit. 01.03.2023]. Dostupné z: https://fightforua.org/
[236] *Ukraine now.* [online]. [cit. 01.03.2023]. Dostupné z: https://www.ukrainenow.org/refuge
[237] *Pomich* [online]. [cit. 01.03.2023]. Dostupné z: https://pomich.org/shippers
[238] TZ a Tamir HAYMAN. Open-Source Intelligence and the War in Ukraine*. INSS, Insight.* [online]. Institute for National Security Studies, 2023, č.1678. [cit. 08.10.2022]. Dostupné z: http://www.jstor.org/stable/resrep47006. str. 1-6.

5 Praktická část

Stěžejním bodem této kapitoly bude praktický příklad zpravodajského cyklu – sběru a analýzy informací, která bude provedena pouze s využitím otevřených zdrojů. Jeho cílem bude zjistit stav zabezpečení Jaderné elektrárny Dukovany a její schopnost odolat různým způsobům teroristického útoku.

5.1 Popis hrozby

Jednou z hrozeb, která ohrožuje národní bezpečnost České republiky, je terorismus. Na tuto skutečnost poukazují výroční zprávy Bezpečnostní informační služby, Bezpečnostní strategie ČR i Audit národní bezpečnosti (více viz kap. 3.3).

S vývojem nových způsobů útoků a nových druhů zbraní by se dalo konstatovat, že terorismus prochází určitou progresivní změnou. Mezi současné trendy terorismu se řadí online seberadikalizace, rostoucí míra radikalizace z důvodů zhoršující se životní úrovně a jaderný terorismus.

Jaderná zařízení jsou atraktivním cílem útoku pro teroristické skupiny nebo vojenský ozbrojený konflikt. Reaktory jsou statické a vůči vnějšímu útoku zranitelné. Pro pracovníky jaderné elektrárny je v případě fyzického napadení nemožné včas odstranit jaderný materiál a zabránit tak možné zkáze. Bezpečnostní experti se shodují na tvrzení, že nově se objevující hrozby jsou závažnější než ty doposud známé, tradiční. Nově vznikající hrozba jaderného terorismu může mít při uskutečněném a zdařilém útoku na jaderná zařízení nepředstavitelné a rozhodně katastrofální následky pro lidstvo.

Při boji s tímto druhem hrozby nelze jen vyčkávat a až následně reagovat na nově nastalou situaci, ale je zapotřebí volit i proaktivní přístup. Osoby odpovídající za zabezpečení jaderných elektráren musí předvídat a aktivně reagovat na nově vznikající rizika. Předpokládá se, že přizpůsobování zabezpečení nově vznikajícím hrozbám bude stále problematičtější. Technologický pokrok může

umožnit vytvoření takových útočných prostředků, jako jsou např. útočné drony, které by mohly obejít standardní obranné systémy.[239]

Cílem útoku se mohou stát reaktory, sklady jaderných paliv a objekty zpracování a sklady radioaktivního odpadu. Jaderný terorismus může usilovat o získání jaderného materiálu pro výrobu radiologických zbraní, což jsou zbraně, které slučují klasickou trhavinu s jaderný materiálem, např. vyhořelým jaderným palivem a při iniciaci nekontrolovatelně šíří radiační záření do ovzduší. Teroristé mohou také usilovat o přerušení provozu elektrárny nebo o vyvolání katastrofického jaderného bezpečnostního incidentu narušením ochranné vrstvy některého z jaderných zařízení.

Ačkoliv je pro teroristy opatření jaderného materiálu pro výrobu radiologických zbraní značně složité a přímý útok hlavních teroristických organizací na státní instituce České republice aktuálně nehrozí, nelze tento fakt s jistotou do budoucna vyloučit.[240]

5.2 Cíl analýzy

Jaderná elektrárna Dukovany (JEDU) je objekt, který by se mohl stát předmětem zájmu sabotážního útoku teroristických uskupení nebo ozbrojených vojenských operací. Na provedené praktické ukázce sběru informací z otevřených zdrojů budou prezentovány varianty informací, které lze dohledat o zabezpečení jaderné elektrárny Dukovany. Výhody, které otevřené zdroje poskytují zpravodajským důstojníkům v množství dohledatelných informací totiž poskytují stejné množství informací i nepřátelským subjektům.

[239] YALÇINKAYA, Haldun a Elif Merve DUMANKAYA. *Emerging Threats in Terrorism*. [online]. Ankara: Centre of Excellence Defence Against Terrorism, 2022. [cit. 04.03.2023]. ISBN 978-605-74376-3-1. Dostupné z: https://www.coedat.nato.int/publication/researches/13-Emerging_ThreatsinTerrorism.pdf, str. 15-40.

[240] DURDIAK, Jaroslav et al. *Zbrane hromadného ničenia – aktuálna bezpečnostná hrozba.* [online]. Bratislava: Ministerstvo obrany Slovenskej republiky, Inštitút bezpečnostních a obranných štúdií, 2005. [cit. 05.02.2023]. ISBN 978–80–88842–76–X Dostupné z: https://inis.iaea.org/collection/NCLCollectionStore/_Public/40/100/40100341.pdf, str. 14-15, 103-108.

Získaná data budou tříděna a analyzována. Analýzou získaných informací bude zhodnocena míra rizikovosti těchto veřejně dostupných informací, s cílem poukázat na význam a potenciál tohoto zpravodajského oboru.

Pro získávání informací, bude využito prohledávání jednotlivých webových portálů, veřejně dostupných publikací, satelitních map, sociálních sítí, novinových článků a souvisejících fotografií.

5.3 Vytyčení požadavků

OSINT analýza objektu JEDU si klade za cíl zjistit míru zabezpečení tohoto areálu pomocí otevřených zdrojů. Vyhledávané informace se budou zaměřovat pouze na zabezpečení objektu, a na další informace, které by mohly zajímat nepřátelské subjekty. Cílem bude zjistit co nejvíce relevantních informací o:

- plánu areálu, popisu budov a vnitřních prostorech budov,
- fyzické ostraze objektu, jejich vybavení, prostředcích a výcviku,
- technickém zabezpečení areálu.

V případě, že by terorističtí aktéři získali v době plánování způsobu provedení útoku některé z výše uvedených informace, výrazně by tyto poznatky pomohly zvýšit pravděpodobnost úspěšného dokončení útoku a dosažení požadovaného záměru.

Získání informací o plánu areálu a účelu jednotlivých budov mohou vést k ulehčení orientace v areálu a vytyčení cílových budov, které budou určeny k zneškodnění nebo narušení. Některé budovy představují pro teroristy atraktivní cíl i z hlediska jaderných materiálů v nich uskladněných. Tyto budovy pak mohou být již v přípravné fázi útoku označeny za cíl k vniknutí a vykradení.

Informace o fyzické ostraze mohou sloužit k přípravě na útok, pořízení konkrétního vybavení tak, aby útočníci nebyli připraveností a výbavou ostrahy elektrárny překvapeni.

Získání základních informací o zabezpečení jaderné elektrárny může vést k odhalení slabin v bezpečnostním systému areálu a zaútočení na ně. Informace o technickém zabezpečení pomohou v předstihu připravit prostředky na překonání

zábranných překážek a naplánovat vhodný útok, který by zvládl obejít instalované obranné bezpečnostní systémy.

5.4 Sběr informací, předběžná analýza, doplňování informací

V této kapitole bude představen možný postup sběru dat v případě zjišťování míry zabezpečení objektu jaderné elektrárny.

Výchozím bodem bude **nalezení webových stránek společnosti, popř. jiných profilů na sociálních sítích.**

Oficiální webové stránky organizace spravuje společnost *ČEZ*. Na stránkách lze dohledat základní informace o elektrárně, je zde přístupná virtuální prohlídka areálu a uvedeny určité informace o zabezpečení.[241]

Jaderná elektrárna Dukovany, je i poměrně aktivní na svém facebookovém profilu *„Infocentrum JE Dukovany*“, kde sdílí aktuality týkající se dění v elektrárně v pravidelných intervalech, min. však 1x týdně.

Podrobnou historickou analýzou zveřejněných příspěvků lze zjistit např.:

- jména některých zaměstnanců, kteří byli tímto profilem zveřejněni z důvodu jejich úspěšného kariérního postupu nebo výkonu,
- fotografie hasičů a hasičské techniky, a to, že mají základnu přímo v areálu,
- fotografie některých strážníků fyzické ostrahy v uniformách s nápisem M2C,
- fotografie zaměstnanců při kupování jídla v jídelně, včetně ne zcela detailního obrazu jejich visaček.

[241] Skupina ČEZ. *Jaderná elektrárna Dukovany.* [online]. [cit. 07.02.2023]. Dostupné z: https://www.cez.cz/cs/o-cez/vyrobni-zdroje/jaderna-energetika/jaderna-energetika-v-ceske-republice/edu

Na základě poznatků získaných z oficiálních stránek je zapotřebí provést sběr dat ve dvou oblastech.

- Zjištění plánu areálu: prohlédnutí areálu pomocí virtuální prohlídky, utvoření si reálných představ o prostorech, orientace v prostoru, vytyčení možných atraktivních cílů.
- Informace o ostraze, výstroj, výzbroj, pracovní doba a zjištění významu zkratky M2C.

Prvním krokem bude **zjištění plánu areálu, rozmístění budov, popř. účel jednotlivých budov na základě virtuální prohlídky.**

Na oficiálních stránkách JEDU je areál objektu zpracován do kvalitně a detailně propracované virtuální prohlídky. Prostřednictvím tohoto virtuálního průvodce lze vstoupit do vnitřních prostor 8 budov.

- budova, kde jsou umístěny diesel generátory
- sklady použitého paliva
- reaktorový sál
- vstup, chodba i výstup z kontrolovaného pásma
- prádelna
- jídelna
- strojovna i prostor hlavního parního kolektoru
- centrální čerpací stanice vody

Dále jsou zde zobrazeny a popsány další místa, nikoliv však jejich vnitřní prostory.

- úložiště nízko a středně radioaktivního odpadu
- vyvedení elektrického výkonu
- chladící věže
- prostory mezi chladícími věžemi a před a za hlavní bránou[242]

Poznatky z virtuální prohlídky poskytnou částečný vizuální přehled o vnitřním prostředí areálu JEDU, vnitřních prostorech a vybavení budov. Doplňujícím krokem

[242] Skupina ČEZ. *Virtuální prohlídky.* [online]. [cit. 07.02.2023]. Dostupné z: http://virtualniprohlidky.cez.cz/cez-dukovany/

může být využití satelitních map společnosti *Google* nebo *Mapy.cz*. Při pohledu ze satelitních map je na první pohled patrné, že areál Dukovany je rozlehlý a tvořen několika desítkami budov, skladů, komínů i chladících věží. Jedna z budov je v aplikaci „*Google maps*“ označena jako úložiště jaderného odpadu[243], účel zbylých budov však z map rozpoznat nejde.

Virtuální prohlídka poskytuje v rozlehlém areálu skládajícím se z desítek budov informace o přesné poloze i vnitřních prostorech důležitých budov, tedy reaktorových sálů, skladů použitého paliva, úložišť radioaktivního odpadu, vyvedení elektrického výkonu, chladících věží. Poškození nebo útok na jednu z těchto budov, narušení jejího ochranného pásma, její vyřazení z provozu může představovat cíl útoku teroristické organizace. Sklady použitého paliva pak mohou představovat teroristický záměr o vniknutí a odcizení jaderného materiálu. Účel zbylých budov nicméně z virtuální prohlídky nevyplývá.

Prostřednictvím virtuální prohlídky si lze vytvořit částečný plán areálu s popisy důležitých budov, orientační představu ve vnitřních prostorech, a to vše bez fyzického navštívení areálu a obhlédnutí místa.

Ve vyhledavači *Google* lze dohledat podle fotek sdílených pod místem JEDU dále tyto prostory:

- vnitřní prostory dozorny bloku číslo 1,
- dukovanská vinice v okolí chladících věží,
- vnitřní prostory infocentra.[244]

[243] Google maps. *Úložiště radioaktivních odpadů Dukovany.* [online]. [cit. 04.03.2023]. Dostupné z: https://www.google.com/maps/place/%C3%9Alo%C5%BEi%C5%A1t%C4%9B+radioaktivn%C3%ADch+odpad%C5%AF+Dukovany/@49.082222,16.1563535,17z/data=!4m6!3m5!1s0x4712a7c5ceef6d3f:0xc04d85864ad4a139!8m2!3d49.081682!4d16.1584848!16s%2Fg%2F11fjxr0jpj

[244] Google maps. *Jaderná elektrárna Dukovany.* [online]. [cit. 04.03.2023]. Dostupné z: https://www.google.com/maps/place/Jadern%C3%A1+elektr%C3%A1rna+Dukovany/@49.0850898,16.1500925,3a,75y,90t/data=!3m8!1e2!3m6!1sAF1QipNqseoN-LmzeWTPqlyzloOG8ByaNkw1TE1Np9j5!2e10!3e12!6shttps:%2F%2Flh5.googleusercontent.com%2Fp%2FAF1QipNqseoN-LmzeWTPqlyzloOG8ByaNkw1TE1Np9j5%3Dw441-h298-k-no!7i2000!8i1350!4m8!3m7!1s0x4712a782b94a8bdd:0xe7b03895595a5567!8m2!3d49.0850898!4d16.1500925!14m1!1BCgIgAQ!16zL20vMGNqNjl4

Ostraha areálu

Na facebookovém profilu *Infocentrum JE Dukovany* byly na fotografiích zveřejněny obličeje strážných, kteří v černých uniformách s nápisem M2C kontrolují osoby vstupující do areálu. Další oblastí sběru dat bude vyhledat informace o ostraze.

Oficiální webové stránky společností neuvádějí informace týkající se fyzické ostrahy. Při vyhledání termínu *„ostraha Dukovany“* prostřednictvím vyhledavače *Google* se zobrazily odkazy na pracovní inzeráty pro pozici ostrahy JE Dukovany.

Na portále *flek.cz* lze dohledat inzerát na 5 pracovních míst pro pozici strážného jaderné elektrárny Dukovany. Fyzická ostraha objektu je zajišťována firmou *Mark2 Corporation Czech, a.s.*, což odpovídá zkratce M2C a potvrzuje zjištění z Facebooku. Z popisu pozice vyplývá, že ostraha slouží ve směnném provozu ranní/noční směny. Ostraha se tedy na hlídání areálu podílí pravděpodobně nepřetržitě, nicméně tento fakt bude zapotřebí dále prověřit. Dále z inzerce vyplývá, že vlastnění zbrojního průkazu je nepovinný požadavek, což znamená, že někteří strážní mohou sloužit i bez střelné zbraně. K náplni práce ostrahy patří prověřování poplachů elektronické zabezpečovací signalizace a poplachových zabezpečovacích a tísňových systémů. Ostraha dále provádí pochůzkovou činnost.[245] Z inzerátu nevyplývá, že ostraha ovládá či monitoruje kamerové systémy objektu, řeší bezpečnostní incidenty, kontroluje osoby vstupující do areálu nebo do areálu vjíždějící zásobovací vozidla dodavatelů. Toto zjištění poukazuje na skutečnost, že tyto povinnosti musí mít na starost jiný subjekt.

V inzerátu, v popisu pracovní náplně strážného, není ani uvedena kontrola vstupujících osob, tato aktivita byla nicméně zachycena na fotografii z facebookového profilu u osoby oblečené v uniformě M2C. To může nasvědčovat tomu, že firma M2C nabízí ještě další pracovní pozice ostrahy areálu, které již nejsou na inzertních stránkách *flek.cz* zveřejněny.

[245] Flek na správném místě. *Ostraha pro JADERNOU ELEKTRÁRNU DUKOVANY.* [online]. [cit. 07.02.2023]. Dostupné z: https://flek.cz/nabidka/ostraha-pro-jadernou-elektrarnu-dukovany-naborovy-prispevek-30-000-kc/413327?utm_source=jooble&utm_medium=cpc&utm_campaign=allvacancies

Získané poznatky vedou k vyhledání webových stránek firmy M2C, která zajišťuje fyzickou ostrahu areálu. Na těchto stránkách lze v souvislosti s JE Dukovany dohledat popis práce dalších pracovních pozic fyzické ostrahy:

- strážný JE Dukovany,[246]
- člen zásahové jednotky JE Dukovany,[247]
- operátor řídícího centra,[248]
- manažer bezpečnosti.[249]

Z popisu náplně jednotlivých pozic fyzické ostrahy M2C si lze udělat komplexní představu o činnosti ostrahy v areálu JEDU. Domněnka o nepřetržitosti provozu fyzické ostrahy byla prostřednictvím těchto stránek potvrzena, jelikož se zde přiznávají příplatky za noční, víkendové a sváteční směny. Strážní jsou situováni na vrátnici a provádějí základní obchůzkovou činnost po areálu. Zásahová jednotka provádí zásahy při bezpečnostních incidentech a provádí kontrolu vstupu osob a vjezdu vozidel. Operátor řídícího centra obsluhuje kamerové systémy a zabezpečovací systémy, řídí činnost strážných v areálu. Manažer bezpečnosti řídí tým, organizuje školení a koordinuje bezpečnost.

Pro doplňující informace lze na facebookovém profilu společnosti M2C nalézt video, které popisuje činnost zásahové jednotky JE Dukovany. Jeden z členů zde uvádí: *„Řídící centrum nám nahlásí krizovou událost, my vyjedeme na zásah, abychom zjistili, zda se jedná o technickou poruchu nebo narušení prostoru.“* Na videu je tento člen zásahové jednotky oblečen do žlutočerné uniformy a na vestě má připevněnou vysílačku zn. Motorola, pomocí které se pravděpodobně spojuje s řídícím centrem. Na opasku se nevyskytuje zbraň a její

[246] M2C kariéra. *Ostraha pro JE Dukovany.* [online]. [cit. 07.02.2023]. Dostupné z: https://kariera.m2c.eu/pracovni-pozice/ostraha-pro-je-dukovany-naborovy-prispevek-30-000-kc/
[247] M2C kariéra. *Člen zásahové jednotky JE Dukovany.* [online]. [cit. 07.02.2023]. Dostupné z: https://kariera.m2c.eu/pracovni-pozice/clen-zasahove-jednotky-nabor-prispevek-30-000-kc-je-dukovany/
[248] M2C kariéra. *Operátor řídícího centra.* [online]. [cit. 07.02.2023]. Dostupné z: https://kariera.m2c.eu/pracovni-pozice/operator-ka-ridiciho-centra-naborovy-prispevek-120-000-kc/
[249] M2C kariéra. *Manažer bezpečnosti.* [online]. [cit. 07.02.2023]. Dostupné z: https://kariera.m2c.eu/pracovni-pozice/manazer-bezpecnosti-m-z-jaderne-elektrarny/

obrysy nejsou viditelné ani pod oblečením.[250] Tento člen zásahové jednotky není tedy pravděpodobně zbraní vyzbrojen.

Na základě získaných informací si lze udělat souhrnnou představu o činnosti, povinnostech, způsobech komunikace a vzájemných vztazích jednotlivých pracovních oddělení na ostraze. V případě podezření z narušení perimetru jsou členové zásahové jednotky vyslání k fyzickému prověření poplachu. Ačkoliv členové zásahové jednotky M2C mají v popisu práce povinnost udržení dobré fyzické kondice, tyto atributy pro ochranu areálu před závažnějším bezpečnostním incidentem – teroristickým útokem nejsou dostačující.

Pro doplnění informací o fyzické ostraze areálu JEDU bude zapotřebí zjistit, zda zde existuje pohotovostní ochrana v případě ozbrojeného a organizovaného útoku na areál JEDU. Ačkoliv na oficiálních webových stránkách i facebookovém profilu není o této informaci zmínka, vyhledavač Google při hledaném výrazu *„ozbrojený útok na jadernou elektrárnu Dukovany“* zobrazí mnoho článků, které odkazují na **Speciální jednotku Dukovany (SJD) PČR.**

SJD je policejní zásahová jednotka, která sídlí přímo v areálu JEDU a je primárně určená k ochraně areálu proti útoku z vnějšího prostředí. Z článku na stránkách Policie ČR vychází, že k výbavě této jednotky patří speciální páčidlo, speciální sluchátka s ochranou a výbušniny.[251]

Na stránkách *UTON* lze dohledat, že policisté z této speciální jednotky, mají ve výbavě bojové nože s názvem *TIGER*. Nůž je 275 mm dlouhý, s jednostranným ostřím, zubatým ostřím a na rukojeti hrotem k rozbíjení skla.[252]

Na stránkách obce Jaroměřice nad Rokytnou je z fotogalerie patrné, že k výbavě policistů dále patří pistole, samočinné střelné zbraně, pumpovací brokovnice,

[250] M2C. *Zásahová jednotka očima zaměstnance M2C.* [online]. [cit. 07.02.2023]. Dostupné z: https://www.facebook.com/m2c.cz/videos/568693217410400/
[251] Policie České republiky. *Jadernou elektrárnu střeží speciální jednotka.* [online]. [cit. 07.02.2023]. Dostupné z: https://www.policie.cz/clanek/jadernou-elektrarnu-strezi-specialni-jednotka.aspx
[252] UTON. *TIGER – zásahová jednotka Dukovany.* [online]. [cit. 07.02.2023]. Dostupné z: https://www.uton.cz/noze-pcr/tiger-2/

odstřelovací puška s optikou, pyrotechnický oblek. Na fotografiích lze rozpoznat i tváře třech policistů.[253]

V roce 2020 bylo vybavení policistů rozšířeno o střelecké brýle, moderní dorozumívací zařízení a speciální maskovací obleky, které dle přiložené fotogalerie zahrnují zimní maskování.[254]

Na počátku roku 2023 byl tento tým vybaven taktickými ochrannými oděvy a zatepleným oblečením. Nově pak policisté dostali střelecké brašny a defibrilátory. V článku se uvádí i jméno velitele SJD. Policisté prochází pravidelně množstvím odborných výcviků a kurzů, např. Antiterror Academy, SAFEGUARD.[255]

Konkrétní údaje k policistům sloužících v SJD PČR

Počet policistů sloužících v SJD není možné z otevřených zdrojů dohledat. Jediná informace o jejich stavu je z roku 2016, kdy se uvádí, že z důvodu zvyšujícího se rizika teroristického útoku byla blíže neurčená kapacita sloužících příslušníků navýšena o jednu třetinu z původního počtu.[256]

Speciální jednotka Dukovany má vlastní facebookový profil, nicméně ten obsahuje pouze určité fotografie a videa z výcviků. Tváře policistů jsou zde vždy zahalena výstrojí. Tento profil je bez fanoušků a komentátorů příspěvků. Žádní uživatelé tak s touto stránkou nejsou v interakci, a proto zjištění jejich členů nebylo tímto způsobem možné dohledat.

Jediný krok s pozitivním výsledkem směřující k získání pravděpodobných jmen příslušníků SJD byl v případě prohledání již zmiňovaného facebookového profilu *Infocentrum JE Dukovany.* Po znovu provedeném prohledání profilu, byly nalezeny

[253] Jaroměřice nad Rokytnou. *Den s policií 18.9.2010.* [online]. [cit. 07.02.2023]. Dostupné z: https://jaromericenr.cz/vismo/galerie2.asp?id_galerie=8385&pocet=24&stranka=1
[254] Deník. *Ostraha i zásahová jednotka. Policisté z elektrárny Dukovany mají nové vybavení.* [online]. [cit. 07.02.2023]. Dostupné z: https://www.denik.cz/regiony/tohle-je-specialni-jednotka-dukovanske-elektrarny-podivejte-se-20200201.html
[255] Noviny VM. *Nové vybavení pro tým policistů ze Speciální jednotku Dukovany.* [online]. [cit. 07.02.2023]. Dostupné z: https://www.novinyvm.cz/22742-nove-vybaveni-pro-tym-policistu-ze-specialni-jednotku-dukovany.html
[256] Atominfo.cz – aktuálně o jádru. *Policejní jednotka v JE Dukovany zvýšila stav o třetinu.* [online]. [cit. 07.03.2023]. Dostupné z: https://atominfo.cz/2016/04/policejni-jednotka-v-je-dukovany-zvysila-stav-o-tretinu/

příspěvky týkající se aktualit o Speciální jednotce. Jednotlivé příspěvky měly průměrně zhruba 150 interakcí v podobě vyjádření „To se mi líbí“. Při rozkliknutí „lajkujících“ uživatelů, prohledání jejich příspěvků, fotografií, přátel a sledovaných stránek šlo s určitou mírou pravděpodobnosti určit pár příslušníků PČR, kteří mohou sloužit u SJD. Jedná se však pouze o domněnku, kterou nelze zcela potvrdit. Z důvodu ochrany osobních údajů nejsou uvedena jména těchto osob, ani přesné odkazy na příspěvky, z nichž autorka vycházela.

S jistotou lze potvrdit pouze jméno vedoucí odboru SJD PČR, který se v článcích vyjadřuje k problematice výcviku SJD. Jeho facebookový profil, fotografie nebo bližší osobní údaje se autorce však nepodařilo dohledat.

Fyzická ostraha areálu JE Dukovany je tedy zabezpečena soukromou bezpečnostní agenturou M2C, která zařizuje standardní bezpečnostní provoz areálu a pro případ ohrožení je zřízena speciální jednotka Policie ČR, která je určena pro odvrácení útoku vedeného proti jaderným zařízením nebo osobám.

Na vnější obraně areálu se v případě útoku v součinnosti s fyzickou ostrahou podílejí složky Armády ČR, vojenské policie a Policie ČR. Pro připravenost proti teroristickým útokům se v pravidelných intervalech konají cvičení všech zmíněných složek. Cvičení zahrnuje přípravu na teroristický útok v bezprostřední blízkosti kritických prostor elektrárny a deaktivace nástražných výbušných systémů profesionálními pyrotechniky.[257] Činnost je koordinována z operačního střediska elektrárny. Armádní síly zde nacvičují používání vojenských vrtulníků Mi-24 i obsazování strategických míst k obraně vnějšího perimetru. Cvičení obvykle trvají

[257] SKUPINA ČEZ. *V rámci cvičení SAFEGUARD budou Dukovany chránit vojáci ze zálohy.* [online]. [cit. 05.03.2023]. Dostupné z: https://www.cez.cz/cs/pro-media/tiskove-zpravy/v-ramci-cviceni-safeguard-budou-dukovany-chranit-vojaci-ze-zalohy-166132

4 dny, účastní se jich přes 200 příslušníků a poslední cvičení byla provedena v letech 2016[258], 2018[259], 2022.[260]

Pro doplnění kompletních informací o fyzické ostraze areálu JEDU bude zapotřebí získat informace o:

- umístění zásahové jednotky M2C
- umístění řídícího centra ostrahy
- umístění SJD PČR

Tyto informace, z již provedené virtuální prohlídky nevyplývaly, nicméně na stránkách společnosti ČEZ lze pod poměrně složitým postupem dohledat soubor, který je určen jako školení pro vstup dodavatelů do jaderné elektrárny. Na hlavních stránkách společnosti ČEZ je zapotřebí vybrat oddíl s názvem „o společnosti“, dále se pak vybírají následující odkazy „pro dodavatele“ – „informace a požadavky pro dodavatele JE“ – „pokyny pro vstup do jaderných elektráren“ – „vstupní školení pro samostatný vstup do střeženého prostoru“ – „EDU“ – „ke stažení“ – „příručka pro vstupní školení do jaderné elektrárny“.

Příručka obsahuje některé velmi významné informace. V úvodní části příručky lze nalézt plánek celého areálu, který popisuje umístění 44 budov. Na tomto plánku lze dohledat některé dosud neznámé lokace budov, např. umístění vrátnice ostrahy M2C, řídícího centra ostrahy, Hasičského záchranného sboru, budovy superhavarijních čerpadel a záložní vjezd do areálu.

Na tomto orientačním plánu areálu se nevyskytuje popis umístění základny Speciální jednotky Dukovany PČR. Neuvedení jejich základy možná mohlo být i záměrem, nicméně při detailním prozkoumání celé příručky se zde o 4 kapitoly

[258] Znojmo. *Útok na jadernou elektrárnu odražen. Cvičení SAFEGUARD Dukovany 2016 prověřilo součinnost vojáků, policistů a společnosti ČEZ při ochraně JE Dukovany.* [online]. [cit. 05.03.2023]. Dostupné z: https://www.znojmocity.cz/utok-na-jadernou-elektrarnu-dukovany-odrazen-cviceni-safeguard-dukovany-2016-proverilo-soucinnost-vojaku-policistu-a-spolecnosti-cez-pri-ochrane-je-dukovany/d-51748

[259] Třebíč. *Vojáci, policisté, hasiči a energetici společně cvičili ochranu Jaderné elektrárny Dukovany.* [online]. [cit. 05.03.2023]. Dostupné z: https://www.trebic.cz/vojaci-policiste-hasici-a-energetici-spolecne-cvicili-ochranu-jaderne-elektrarny-dukovany/d-39020

[260] SKUPINA ČEZ. *V rámci cvičení SAFEGUARD budou Dukovany chránit vojáci ze zálohy.* [online]. [cit. 05.03.2023]. Dostupné z: https://www.cez.cz/cs/pro-media/tiskove-zpravy/v-ramci-cviceni-safeguard-budou-dukovany-chranit-vojaci-ze-zalohy-166132

dále nachází plán areálu s popisem budov pro fyzickou bezpečnost, kde se už přesná lokace SJD PČR vyskytuje.[261]

Dle autorky práce jsou v příručce obsaženy velmi citlivé údaje týkající se zabezpečení areálu. Pro případný ozbrojený útok na jadernou elektrárnu, který by byl teroristickou organizací dopředu plánovaný, jsou informace o umístění jednotek, které zajišťují fyzickou ostrahu klíčové. V případě útoku se totiž tato stanoviště mohou stát prvotním cílem určenému k zneškodnění. Nepřítel, může být dále prostřednictvím otevřených zdrojů obeznámen s vybavením SJD PČR, stejně tak jako s jejich specializací a výcvikem. Pomocí virtuální prohlídky, plánků z příručky a satelitních map si může vytvořit zcela přesnou představu o vnitřních prostorech areálu a účelů jednotlivých budov, což dopomůže k orientaci a urychlení pohybu v areálu objektu.

Varianty útoků mohou být různé, nicméně v případě zneškodnění elektrického vyvedení a záložních diesel generátorů, které jsou na plánech taktéž zaznamenány by zabezpečení a další přístroje závislé na elektrické energii mohly zůstat nefunkční.

[261] SKUPINA ČEZ. *Vstupní školení do Jaderné elektrárny ETE a EDU.* [online]. ČEZ, 2018. [cit. 04.03.2023]. Dostupné z: https://www.cez.cz/webpublic/file/edee/2022/04/skripta_a1_2021_v5.pdf, str. 14-16, 35-45.

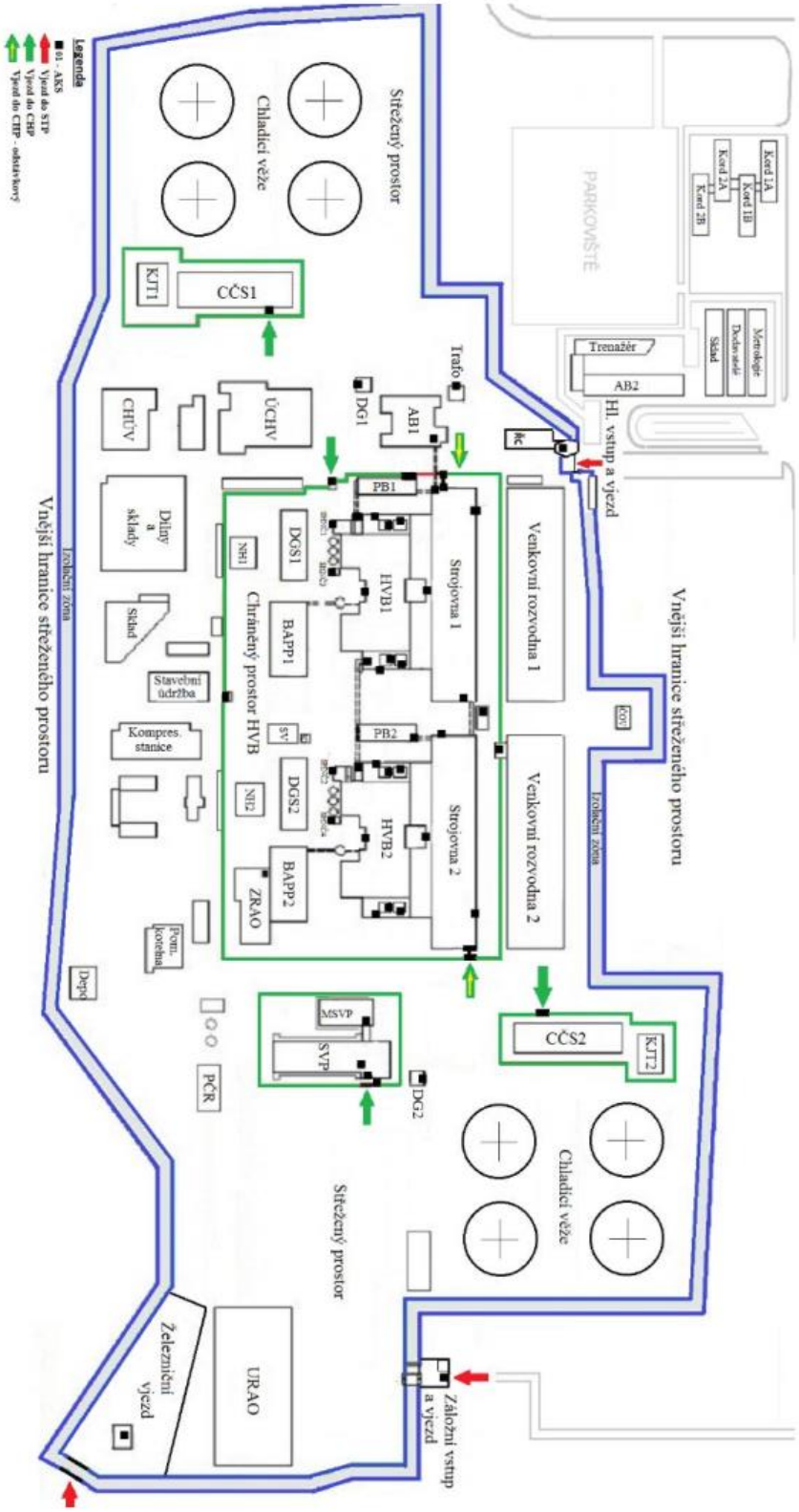
Technická ochrana objektu

Dle zmiňované příručky je prostor areálu členěn na střežený, chráněný a životně důležitý prostor. Areál JEDU je podél perimetru zabezpečen železobetonovým oplocením s technickým vybavením, které v případě narušení vyhlásí poplach. Uvnitř tohoto střeženého prostoru se nachází tzv. chráněný prostor, který je ohraničen pletivovým oplocením vybaveným elektronickou signalizací pro případ narušení. Životně důležité prostory se nachází uvnitř budov chráněného prostoru a jsou zabezpečeny mechanickými zábrannými prostředky a bezpečnostními systémy.

Vstup do chráněných a životně důležitých prostor je umožněn pouze přes vyhrazená místa, která podléhají kontrolám vstupu. Tyto kontrolní úseky jsou vybaveny rámovými detektory kovu, rentgenovými přístroji na kontrolu zavazadel, biometrickým snímačem otisku prstu a turnikety, které reagují na vstupní čipové karty.[262] Pro násilné vniknutí do těchto prostor by se tedy vyžadovalo překonání mechanických zábranných systémů v podobě oplocení, nebo turniketů. Ačkoliv životně důležité prostory nejsou na plánku zaznamenány, z příručky jasně vyplývá, že se nachází v chráněných prostorech, které jsou na plánu zřetelně vyobrazeny.

Na obr. 2 jsou v modrém poli zaznamenané střežené prostory, zelené pole odpovídá chráněným prostorům. Životně důležité prostory se pak nacházejí uvnitř zeleně vyznačených chráněných prostor. Barevné šipky na plánu jsou určeny k vyznačení hlídaných vstupních koridorů do jednotlivých prostor. Bystré oko si právě na této mapě všimne i lokace základny PČR.

[262] SKUPINA ČEZ. *Vstupní školení do Jaderné elektrárny ETE a EDU.* [online]. ČEZ, 2018. [cit. 04.03.2023]. Dostupné z: https://www.cez.cz/webpublic/file/edee/2022/04/skripta_a1_2021_v5.pdf, str. 35-45.



Členění prostor EDU z hlediska fyzické ochrany

Obrázek 2 Areál jaderné elektrárny Dukovany, rozčleněn dle typů střežených prostor (zdroj: ČEZ)

V roce 2019 bylo investováno 400 milionů korun do modernizace technického zabezpečení areálu. Ochrana perimetru byla vybavena ostnatými dráty, čidly detekce pohybu, osvětlením a modernizovaným kamerovým systémem. Prostory pro vjezd vozidel byly doplněny o mechanické zábranné systémy.

Nad celým areálem elektrárny platí bezletová zóna.[263] V případě narušení letového prostoru je jaderná elektrárna informována operačním centrem Ministerstva obrany ČR.[264] Areál je vybaven vzdušným monitorovacím systémem laserů, určeným k ochraně vzdušného prostoru. Tento systém vysílá každou vteřinu zhruba 70 000 paprsků do prostoru, pokud by nad areálem letěl jakýkoliv objekt, paprsek se od něj odrazí, vrátí k vyhodnocení do detektoru a objeví se operátorovi v řídícím centru.[265] Odrazit útok ze vzdušného prostoru, včetně útočných dronů by měli být schopni policisté z SJD, kteří jsou k tomu vybaveni i odpovídající technikou.[266]

5.5 Souhrnná analýza informací

Shromážděné informace o zabezpečení jaderné elektrárny Dukovany nyní představují kompletní soubor pro analytické zpracování a zodpovězení počátečně stanovených požadavků.

Cílem bylo zjistit co nejvíce relevantních informací o:

- plánu areálu, popisu budov a vnitřních prostorech budov,
- fyzické ostraze objektu, jejich vybavení, prostředcích a výcviku,
- technickém zabezpečení areálu.

[263] ESTAV.cz. *Zvýšení zabezpečení jaderných elektráren bude stát 1,2 miliardy*. [online]. [cit. 06.03.2023]. Dostupné z: https://www.estav.cz/cz/7664.zvyseni-zabezpeceni-jadernych-elektraren-bude-stat-1-2-miliardy

[264] SKUPINA ČEZ. *Vstupní školení do Jaderné elektrárny ETE a EDU.* [online]. ČEZ, 2018. [cit. 06.03.2023]. Dostupné z: https://www.cez.cz/webpublic/file/edee/2022/04/skripta_a1_2021_v5.pdf, str. 44.

[265] Třebíčský deník.cz. *Neproklouzne ani vrabec. Jadernou elektrárnu Dukovany chrání lasery i před drony.* [online]. [cit. 06.03.2023]. Dostupné z: https://trebicsky.denik.cz/zpravy_region/neproklouzne-ani-ptacek-jadernou-elektrarnu-dukovany-chrani-lasery-i-pred-drony.html

[266] Atominfo.cz – aktuálně o jádru. *Policejní jednotka v JE Dukovany zvýšila stav o třetinu.* [online]. [cit. 07.03.2023]. Dostupné z: https://atominfo.cz/2016/04/policejni-jednotka-v-je-dukovany-zvysila-stav-o-tretinu/

Požadavek č. 1 - plán areálu

Informace o plánu areálu vyplývající ze satelitních map, virtuální prohlídky a příručky pro vstupní školení do jaderné elektrárny lze využít pro zcela přesné zpracování dispozičního plánu areálu, které zahrnuje počet budov, jejich využití a přesné umístění. Informace z těchto zdrojů se vzájemně doplňovaly a jednotlivá zjištění spolu souhlasila. Kvalitu a věrohodnost zjištěných informací lze proto předpokládat vysokou.

Velmi významným zjištěním byly v tomto smyslu informace o umístění budov, které představují atraktivní cíle pro teroristické organizace z hlediska:

- napadení: reaktorové sály, chladící systémy, budovy určené ke zpracování radioaktivních odpadů, diesel generátory, elektrické vyvedení.
- vniknutí a odcizení materiálu k výrobě radiologické zbraně: mezisklady a sklady použitého jaderného paliva, úložiště nízko a středně radioaktivního odpadu.
- strategických stanovišť: umístění základny SJD PČR, vrátnice a sídla strážných M2C, operačního střediska.

Z otevřených zdrojů byl zjištěn účel téměř všech cca 50 budov vyskytujících se v areálu a alespoň částečná představa o vnitřních prostorech 10 budov. Současně byly zjištěny i všechny příjezdové a vstupní trasy do areálu a následně i vstupní místa do jednotlivých chráněných prostor, které jsou po obvodu svých hranic ohraničeny oplocením a zabezpečovací technikou.

Požadavek č. 2 – fyzická ostraha

Jak již bylo uvedeno výše, areál je střežen soukromou bezpečnostní agenturou M2C, která má na starosti standardní bezpečnostní provoz, propustkovou kontrolní činnost, obchůzkovou činnost a prověřování bezpečnostních incidentů. Speciální jednotka Dukovany PČR sídlí v areálu a řeší závažné bezpečnostní incidenty a krizové situace. V součinnosti s ostatními bezpečnostními složkami státu se podílí na ochraně a obraně areálu. Pro případ teroristického útoku je SJD vycvičena na zvládání situací proti zvlášť nebezpečným a ozbrojeným pachatelům, stejně tak jako proti útoku teroristické skupiny. Pro účely přímého útoku v podobě

fyzické penetrace je Speciální jednotka vybavena odstřelovacími puškami, samočinnými střelnými zbraněmi i balistickou ochranou. V případě akutního odstranění nástražného výbušného systému v perimetru objektu je jednotka vybavena i pyrotechnickou výstrojí.

Z uvedeného by se dalo usuzovat, že prvotní zásah i následná součinnost všech bezpečnostních složek by měla efektivně zvládnout odvrácení teroristického útoku.

Rizikovým zjištěním z hlediska bezpečnosti by mohl být poznatek o tom, že ostraha společnosti M2C je v podstavu. Chybějí místa na pozice strážného, člena zásahové jednotky, operátora řídícího centra i bezpečnostního manažera. Někteří členové ostrahy nemusí mít zbrojní průkaz a nemusí tak být při výkonu strážní služby vyzbrojeni zbraní. Tento poznatek je podpořen i videoukázkou z facebookového profilu společnosti M2C, kde na uniformě jednoho zaměstnance M2C nelze viditelně rozpoznat nošenou zbraň.

Jednou z pracovních povinností členů zásahové jednotky M2C je i prověřovat bezpečnostní incidenty možného narušení perimetru. I za předpokladu, že by byl zaměstnanec ozbrojen krátkou střelnou zbraní nelze zcela předpokládat účinný zákrok proti připravenému a ozbrojenému útočníkovi.

Požadavek č. 3 – technické zabezpečení areálu

Z hlediska prostředků určených k ochraně perimetru byly zjištěny informace o mechanických zábranných systémech, zejména typu oplocení, existenci systému zabraňujícímu násilný vjezdu vozidel a zábranné prostředky proti násilnému vstupu osob do areálu.

Technické zabezpečení je zajištěno kombinací kamerových systémů, elektronických kontrol vstupu, biometrických čteček, turniketů, vibračních čidel detekující pohyb a vzdušeného monitorovacího systému.

Objekt je dále v příručce členěn do 3 typů prostor. Ke každému prostoru byla nalezena charakteristika a přísné požadavky na prostředky, které zabraňují vstup nepovolaným osobám. Kdokoliv, kdo si tuto příručku prohlédne je obeznámen s informacemi, které budovy jsou dle JEDU považovány za chráněné a taktéž

s tím, v kterých budovách se zákonitě vyskytují důležité objekty patřící do tzv. životně důležitých prostor areálu.

5.6 Shrnutí a doporučení

Z pročtených článků vyplývá, že si společnost ČEZ uvědomuje zranitelnost objektu v návaznosti na nově vznikající hrozby a do zabezpečení areálu investuje nemalé finanční částky. V průběhu posledních několika let se zlepšila a rozšířila výstroj i výzbroj SJD PČR, zvětšila se kapacita policistů a zvýšily se platy. Instalovala se nová technická zabezpečovací zařízení. Vše dle podávaných informací svědčí o proaktivním přístupu v oblasti zvyšování zabezpečení.

V závěru zpravodajského cyklu by se dalo konstatovat, že informace týkající se plánu areálu, umístění a účelu jednotlivých budov byly téměř ve všech případech zjištěny. Subjekty fyzické ostrahy, jejich princip činnosti, vzájemná spolupráce, komunikace, výstroj a výzbroj byly také vcelku podrobně zjištěny.

Technické zabezpečení bylo zjištěno pouze do omezené míry. V obecné rovině bylo zjištěno technické zabezpečení a umístění mechanických zábranných prostředků ochrany perimetru. Přesné umístění a počet kamerových systémů, čidel a jiných bezpečnostních systémů však zjištěn nebyl. Tato část by mohla být určena k doplnění. Jednou z možností je opakování procesu a zaměření shromažďování informací na technické zabezpečení. Další možností by pak mohlo být doplnění informací jinými zpravodajskými obory – pravděpodobně přímá fyzická obhlídka místa nebo využití exkurzních aktivit přímo v areálu. Ze zjištěných informací však například i vyplývá, že prohlídku areálu pomocí dronu s cílem zjistit umístění a počet prostředků technického zabezpečení by nebylo možné provést. Dron by byl vzdušným monitorovacím systémem rychle odhalen a SJD zneškodněn.

Stav celkového zabezpečení působí velmi dobře. Vyhledáváním informací z otevřených zdrojů bylo nicméně zjištěno pár poznatků, které můžou představovat důležité informace pro nepřítele.

Primárním doporučením autorky práce by bylo zavedení omezeného přístupu k jinak veřejně dostupné příručce pro vstupní školení do jaderné elektrárny. Ta dle názoru autorky obsahuje překvapivě citlivé údaje umístění důležitých budov a konkrétních informací o technickém i fyzickém zabezpečení areálu. Příručka má

být dle uvedených informací určena dodavatelům pro lepší orientaci a informovanost o chodu areálu. Z tohoto důvodu by mohla být přístupná pouze vybraným dodavatelům.

Dále by bylo možné polemizovat nad nutností veřejného zpřístupnění virtuální prohlídky vnitřních prostor reaktorových sálů, místností s jaderným palivem, skladů použitého paliva, diesel generátorů, místností zpracování radioaktivních odpadů a čerpací stanice surové vody. Vizuální přehled vnitřních prostor těchto teroristicky atraktivních budov může z hlediska bezpečnosti působit jako rizikový faktor.

Ačkoliv situace na trhu práce je zjevně nelehká, další oblast ke zdokonalení bezpečnosti by mohla spočívat v kladení větších požadavků na potenciální zájemce na pozici člena ostrahy M2C. Zbrojní průkaz na pozici člena ostrahy je doposud pouze výhodou, nikoli povinností. A může se tak stát, že areál budou střežit nevyzbrojené osoby.

Speciální jednotka Dukovany PČR nejeví z pohledu autorky slabá místa, až na dohledatelnost lokace jejich základny v areálu.

Závěr

Prostudováním strategických dokumentů ČR byly autorkou vytyčeny a vybrány aktuální bezpečnostní hrozby. Na základě zejména zahraniční literatury byly charakterizovány novinky a trendy jednotlivých hrozeb, dále byly popsány i nové sofistikované metody vedení útoků, použití prostředků a propagandistického působení. K jednotlivě uvedeným hrozbám byl vytvořen přehled a způsob využití možných zdrojů OSINT.

Praktická část se zaměřila na provedení praktické ukázky zpravodajského cyklu v oblasti zabezpečení jaderné elektrárny v kontextu obrany proti jadernému terorismu. Cílem tohoto postupu bylo získat zpravodajsky relevantní informace o míře zabezpečení jaderné elektrárny Dukovany a zhodnotit míru rizikovosti těchto zveřejněných informací. 2 ze 3 stanovených požadavků byly po obsahové stránce naplněny dostatečně. Třetí požadavek bylo možno zpracovat jen v omezené míře. V závěrečné části praktické práce byly shrnuty subjektivní doporučení autorky, týkající se možností zlepšení zabezpečení a způsobů odstranění rizikových faktorů.

Při práci s otevřenými zdroji a shromažďováním dat je zapotřebí pracovat i s mírou věrohodnosti získaných informací. Mnohé informace zde mohou být uvedeny úmyslně upravené nebo lživé pro vyvolání strachu, ovlivnění veřejného mínění nebo zmatení zpravodajců. Autorka práce se domnívá, že v následujících letech bude manipulací s pravdivostí informací přibývat. Velmi náročný krok pak bude pro zpravodajce představovat posouzení, zda získané informace jsou pravdivé nebo zdali se jedná o dezinformace. Boj s dezinformacemi nebude mnohdy lehkým úkolem. Sofistikovaných způsobů šíření dezinformací přibývá a současná situace ve světě poukazuje na skutečnost, že některé i médii zveřejňované informace vycházejí z dezinformačních zdrojů. Dezinformace již mění svou podobou a nevyskytují se pouze na známých dezinformačních webech, ale nyní i na sociálních sítích, v mediálním prostoru a v oficiálních zprávách některých státních aktérů.

Schopnost vyhledání a porozumění pravdivých informací se bude stávat opravdovou profesionální dovedností.

Z množství relevantních a důležitých informací, které se dají prostřednictvím otevřených zdrojů vyhledat vyplývá, že OSINT je nedílnou součástí zpravodajské práce a jeho význam pro včasnou informovanost je nesporný.

Dynamický vývoj všech bezpečnostních hrozeb poukazuje na potřebu aktivního působení bezpečnostních sborů a státních institucí v boji s těmito hrozbami. Česká republika bude muset stále rychleji rozvíjet prostředky k zabezpečení obrany proti kybernetickým a hybridním útokům, posilovat obranu před terorismem a zamezovat šíření dezinformačních kampaní. To předpokládá stále vyspělejší obranné technologie, na jejichž vývoj bude nutné vynakládat odpovídající finanční zdroje.

Seznam použité literatury

Monografie

1. American Foreign Policy Council. *World Almanac od Islamism.* [online]. [cit. 15.02.2023]. Dostupné z: https://almanac.afpc.org/almanac
2. AKHBAR, Babak, BAYERL, Saskia, SAMPSON, Fraser (Eds.). *Open Source Intelligence Investigation. From Strategy to Implementation*. Canada: Springer International Publishing, 2016. ISBN 978-3-319-47671-1.
3. Bezpečnostní informační služba. *Výroční zpráva Bezpečnostní informační služby za rok 2018.* [online]. Praha: Bezpečnostní informační služba, 2019. [cit. 22.10.2022]. Dostupné z: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2018-vz-cz.pdf.pdf
4. Bezpečnostní informační služba. *Výroční zpráva Bezpečnostní informační služby za rok 2019*. [online]. Praha: Bezpečnostní informační služba, 2020. [cit. 22.10.2022]. Dostupné z: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf
5. Bezpečnostní informační služba. *Výroční zpráva Bezpečnostní informační služby za rok 2020.* [online]. Praha: Bezpečnostní informační služba, 2021. [cit. 22.10.2022]. Dostupné z: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf
6. Bezpečnostní informační služba. *Výroční zpráva Bezpečnostní informační služby za rok 2021.* [online]. Praha: Bezpečnostní informační služba, 2022 [cit. 03.02.2023]. Dostupné z: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2021-vz-cz-2.pdf
7. *Bezpečnostní výzvy současného světa: Security challenges of the world of today.* Praha: Policejní akademie České republiky v Praze, 2020. ISBN 978-80-7251-498-4.
8. Counter Extremism Project. *European Ethno-Nationalist and White Supremacy Groups.* [online]. Counter Extremism Project, 2022. [cit. 03.03.2023]. Dostupné z: https://www.counterextremism.com/sites/default/files/supremacy_landing_files/European%20Ethno-Nationalist%20and%20White%20Supremacy%20Groups_120722.pdf
9. Counter Extremism Project. *Extremists & Online Propaganda.* [online]. Counter Extremism Project, 2018. [cit. 27.02.2023]. Dostupné z: https://www.counterextremism.com/themes/custom/cep/templates/reports/

extremists_online_propaganda/files/Extremists%20and%20Online%20Propaganda_040918.pdf

10. Counter Extremism Project. *Far-left Extremist Groups in the United States.* [online]. Counter Extremism Project, 2022. [cit. 03.03.2023]. Dostupné z: https://www.counterextremism.com/sites/default/files/supremacy_landing_files/U.S.%20Far-Left%20Extremist%20Groups_PDF_083122.pdf

11. Counter Extremism Project. *White Supremacy Groups in the United States.* [online]. Counter Extremism Project, 2023. [cit. 03.03.2023]. Dostupné z: https://www.counterextremism.com/sites/default/files/supremacy_landing_files/U.S.%20White%20Supremacy%20Groups_022323.pdf

12. DURDIAK, Jaroslav et al. *Zbrane hromadného ničenia – aktuálna bezpečnostná hrozba.* [online]. Bratislava: Ministerstvo obrany Slovenskej republiky, Inštitút bezpečnostních a obranných štúdií, 2005. [cit. 05.02.2023]. ISBN 978–80–88842–76–X Dostupné z: https://inis.iaea.org/collection/NCLCollectionStore/_Public/40/100/40100341.pdf

13. Eurobarometr. *Public opinion on the war in Ukraine.* [online]. [cit. 20.02.2023]. Dostupné z: https://www.europarl.europa.eu/at-your-service/cs/be-heard/eurobarometer/public-opinion-on-the-war-in-ukraine

14. Europol. *European Union Terrorism Situation and Trend report 2022. (TE-SAT).* [online]. [cit. 20.02.2023]. Dostupné z: https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2022-te-sat

15. Freedom House. *Freedom in the World 2022, The Global Expansion of Authoritarian Rule.* [online]. [cit. 06.02.2023]. Dostupné z: https://freedomhouse.org/report/freedom-world/2022/global-expansion-authoritarian-rule

16. GANOR, Boaz. Understanding the Motivations of 'Lone Wolf' Terrorists: The 'Bathtub' Model. *Perspectives on Terrorism.* [online] 2021, roč. 15, č. 2. [cit. 05.02.2023]. ISSN 2334-3745. Dostupné z: https://www.jstor.org/stable/27007294

17. CHRISS, Pallaris. Center For Security Studies. *Open Source Intelligence: A strategic enabler of national security.* [online]. 2008, roč. 3, č. 32 [cit. 08.10.2022]. ISSN 2296-0244. Dostupné z: https://www.files.ethz.ch/isn/50169/css_analysen_nr%2032-0408_E.pdf

18. HORÁK, Oldřich a Ivo PIKNER. Vojenské rozhledy. *Zpravodajství z otevřených zdrojů.* [online]. 2007, č. 3 [cit. 08.10.2022]. ISSN 2336-2995. Dostupné z: https://www.vojenskerozhledy.cz/images/archiv_voj_rozhl/clanky/2007/3/4_zpravodajstvi_z_otevrenych_zdroju.pdf

19. JABBOUR, Kamal T., Erich DEVENDORF. Cyber Threat Characterization. *The Cyber Defense Review*, [online]. 2017, roč. 2, č. 3. [cit. 27.02.2023]. ISSN 2474-2120 Dostupné z: http://www.jstor.org/stable/26267387

20. JANDA, Jakub. *The Lisa Case STRATCOM Lessons for European states.* Security Policy Working Paper. [online]. 2016, č. 11. [cit. 02.02.2023]. Dostupné z: https://www.baks.bund.de/sites/baks010/files/working_paper_2016_11.pdf JONGMAN, Berto. Recent Online Resources for the Analysis of Terrorism and Related Subjects. *Perspectives on Terrorism*. [online]. 2021, roč. 15, č. 3. [cit. 03.03.2023]. ISSN 2334-3745. Dostupné z: https://www.jstor.org/stable/27030911

21. MCAULIFFE, M. a A. TRIANDAFYLLIDOU. *World Migration Report 2022*. [online]. Switzerland: International Organization for Migration, 2021. [cit. 18.02.2023]. ISBN 978-92-9268-076-3. Dostupné z: https://publications.iom.int/books/world-migration-report-2022

22. MICHÁLEK, Luděk. *Základy zpravodajské činnosti.* Praha: PAČR v Praze, 2011. ISBN 978-80-7251-360-4.

23. MICHÁLEK, L., POKORNÝ, L., STIERANKA, J., MARKO, M., VAŠKO, A., *Zpravodajské služby a zpravodajská činnost.* Praha: Wolters Kluwer ČR, 2021.ISBN 978-80-7598-725-9.

24. Ministerstvo vnitra České republiky. *Audit národní bezpečnosti.* [online]. Praha: Ministerstvo vnitra České republiky, 2016 [cit. 06.11.2022]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf

25. Národní úřad pro kybernetickou a informační bezpečnost. *Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025.* [online]. Praha: Národní úřad pro kybernetickou a informační bezpečnost, 2021 [cit. 20.02.2023]. Dostupné z: https://www.nukib.cz/download/publikace/strategie_akcni_plany/akcni_plan_2021-2025.pdf

26. Ministerstvo obrany České republiky – VHÚ Praha. *Národní strategie pro čelení hybridnímu působení: National strategy for countering hybrid interference*. Praha: Ministerstvo obrany České republiky – VHÚ Praha, 2021. ISBN 978-80-7278-827-9.

27. KERNAR, F. William. *NATO Open Source Intelligence Handbook*. [online]. USA, 2001. [cit. 01. 10. 2022]. Dostupné z: https://archive.org/details/NATOOSINTHandbookV1.2/page/n5/mode/2up

28. POST Jerrold, *Military Studies in the Jihad Against the Tyrants: The Al-Qaeda Training Manual.* Maxwell Air Force Base, Alabama: USAF Counterproliferation Center, 2004. ISBN 9781907521249.

29. *SIPRI Year Book, World Nuclear Forces*. [online]. Stockholm International Peace Research Institute, 2022. [cit. 15.02.2023]. Dostupné z: https://sipri.org/sites/default/files/YB22%2010%20World%20Nuclear%20Forces.pdf

30. SKUPINA ČEZ. *Vstupní školení do Jaderné elektrárny ETE a EDU.* [online]. ČEZ, 2018. [cit. 04.03.2023]. Dostupné z: https://www.cez.cz/webpublic/file/edee/2022/04/skripta_a1_2021_v5.pdf

31. Stockholm International Peace Research Institute. *SIPRI Yearbook 2022. Armaments, Disarmament and International Security.* [online]. Oxford University Press, 2022. [cit. 15.02.2023]. ISBN 978-0-19-197961-3. Dostupné z: https://sipri.org/sites/default/files/2022-06/yb22_summary_en_v2_0.pdf

32. United Nations Office on Drugs and Crime. *The illicit market in firearms.* [online]. Vienna: United Nations Office on Drugs and Crime, 2019. [cit. 19.02.2023]. Dostupné z: https://www.unodc.org/documents/e4j/Module_04_-_The_Illicit_Market_in_Firearms_FINAL.pdf

33. ÜNVER, H. Akın. *Digital Open Source Intelligence and International Security: A Primer.* [online]. Oxford: Centre for Economics and Foreign Policy Studies, 2018. [cit. 06.02.2023]. Dostupné z: http://www.jstor.org/stable/resrep21048

34. Vojenské zpravodajství. *Výroční zpráva Vojenského zpravodajství za rok 2021.* [online]. Praha: Vojenské zpravodajství, Ministerstvo obrany, 2022 [cit. 10.11.2022]. Dostupné z: https://www.vzcr.cz/uploads/41-Vyrocni-zprava-2021.pdf

35. VEJVODOVÁ, Petra a Miloš GREGOR. *Analýza manipulativních technik na vybraných českých serverech. Výzkumná zpráva.* [online]. 2016. [cit. 02.02.2023]. Dostupné z: https://www.academia.edu/26046763

36. Vláda České republiky. *Bezpečnostní strategie České republiky 2015*. [online]. Praha: Vláda České republiky, 2015. [cit. 29.10.2022]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

37. WAGNER, Thomas, Eds. *Cyber Threat Intelligence Sharing: Survey and Research Directions*. [online]. Birmingham: Birmingham City University, 2019. [cit. 26.02.2023]. Dostupné z: https://www.open-access.bcu.ac.uk/7852/1/Cyber%20Threat%20Intelligence%20Sharing%20Survey%20and%20Research%20Directions.pdf

38. WISKID, Claire. *Lone Wolf Terrorism and Open Source Jihad: An Explanation and Assessment.* [online]. International Institute for Counter-

Terrorism, 2016. [cit. 05.02.2023]. Dostupné z: https://www.ict.org.il/UserFiles/ict-lone-wolf-osint-jihad-wiskind.pdf

39. YALÇINKAYA, Haldun a Elif Merve DUMANKAYA. *Emerging Threats in Terrorism*. [online]. Ankara: Centre of Excellence Defence Against Terrorism, 2022. [cit. 04.03.2023]. ISBN 978-605-74376-3-1. Dostupné z: https://www.coedat.nato.int/publication/researches/13-Emerging_ThreatsinTerrorism.pdf
40. YOUNAS, Muhammad Ahsan. Digital Jihad' and Its Significance to Counterterrorism*. Counter Terrorist Trends and Analyses.* [online]. 2014, roč. 6, č. 2. [cit. 03.02.2023]. ISSN 2382-6444. Dostupné z: https://www.jstor.org/stable/26351231
41. ZRŮN, Michal a Lucie ŘEHOŘOVÁ. *Úvod do zpravodajství.* Praha: PAČR v Praze, 2007. ISBN 978-80-7251-252-2.

Časopisecké články

1. HORÁK, Oldřich a Ivo PIKNER. Zpravodajství z otevřených zdrojů. *Vojenské rozhledy.* [online]. 2007, č. 3. [cit. 08.10.2022]. ISSN 2336-2995. Dostupné z: https://www.vojenskerozhledy.cz/images/archiv_voj_rozhl/clanky/2007/3/4_zpravodajstvi_z_otevrenych_zdroju.pdf
2. MUNTEANU, Nicoleta Annemarie. Illegal migration approach from the perspective of open source intelligence. *Research and Science Today*. [online]. 2019, roč. 18, č. 2 [cit. 21.02.2023]. ISSN 2285-9632. Dostupné z: https://www.rstjournal.com/?mdocs-file=3826
3. STEELE, Robert David. Open Source Intelligence: What Is It? Why Is It Important To The Military? *American Intelligence Journal.* [online]. 1996, roč. 17, č. ½. [cit. 06.02.2023]. Dostupné z: http://www.jstor.org/stable/44326547
4. SUBEDI, Db. a Bert JENKINS. Preventing and Countering Violent Extremism: Engaging Peacebuilding and Development Actors. *Counter Terrorist Trends and Analyses.* [online]. 2016, roč. 8., č. 10. [cit. 04.03.2023]. ISSN 2382-6444. Dostupné z: http://www.jstor.org/stable/26351459

5. TZ a Tamir HAYMAN. Open-Source Intelligence and the War in Ukraine. *INSS, Insight*. [online]. Institute for National Security Studies, 2023, č. 1678. [cit. 08.10.2022]. Dostupné z: http://www.jstor.org/stable/resrep47006

Právní předpisy

1. Ústavní zákon č. 110/1998 Sb., *o bezpečnosti České republiky*, v posledním znění
2. Prováděcí nařízení Rady EU č. 2022/1230 ze dne 18. července 2022, kterým se provádí čl. 2 odst. 3 nařízení (ES) č. 2580/2001 o zvláštních omezujících opatřeních namířených proti některým osobám a subjektům s cílem bojovat proti terorismu a kterým se zrušuje prováděcí nařízení (EU) č. 2022/147
3. Rozhodnutí Rady (SZBP) č. 2020/1132 ze dne 30. července 2020, kterým se aktualizuje seznam osob, skupin a subjektů, na něž se vztahují články 2, 3 a 4 společného postoje 2001/931/SZBP o uplatnění zvláštních opatření k boji proti terorismu, a kterým se zrušuje rozhodnutí (SZBP) č. 2020/20
4. Zákon č. 153/1994 Sb., *o zpravodajských službách České republiky,* v posledním znění
5. Zákon č. 289/2009 Sb., *o Vojenském zpravodajství*, v posledním znění
6. Zákon č. 154/1994 Sb., *o Bezpečnostní informační službě*, v posledním znění

Webové stránky a elektronické zdroje

1. *AC24.* [online]. [cit. 05.02.2023]. Dostupné z: https://www.ac24.cz/
2. *ACSRT/CAERT.* [online]. [cit. 04.02.2023]. Dostupné z: https://caert.org.dz/
3. *ADL.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.adl.org/
4. *Aeronet.* [online]. [cit. 05.02.2023]. Dostupné z: https://aeronet.news/
5. Ajax. *The Air Alert app is now available for Android and iOS.* [online]. [cit. 01.03.2023]. Dostupné z: https://ajax.systems/blog/zastosunok-povitryana-trivoga/
6. ALSULAMI, Mohammed. *Europe and the Challenge of Dual-Use Technology Transfer to Iran.* [online]. [cit. 18.02.2023]. Dostupné z:

https://rusi.org/explore-our-research/publications/commentary/europe-and-challenge-dual-use-technology-transfer-iran

7. *Alternative für Deutschland.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.afd.de/
8. *American Renaissance.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.amren.com/
9. *Antifa.* [online]. [cit. 03.03.2023]. Dostupné z: https https://antifa.cz/
10. *Army Recognition.* [online]. [cit. 18.02.2023]. Dostupné z: https://armyrecognition.com/
11. *Associazione Culturale Veneto fronte Skinheads.* [online]. [cit. 03.03.2023]. Dostupné z: http://venetofronteskinheads.org/beta/
12. Atominfo.cz – aktuálně o jádru. *Policejní jednotka v JE Dukovany zvýšila stav o třetinu.* [online]. [cit. 07.03.2023]. Dostupné z: https://atominfo.cz/2016/04/policejni-jednotka-v-je-dukovany-zvysila-stav-o-tretinu/
13. *Binaryedge.io.* [online]. [cit. 27.02.2023]. Dostupné z: https://binaryedge.io/
14. Blackdot solutions. *OSINT Sources: What Are The Different Types of Open Source Data?* [online]. [cit. 25.02.2023]. Dostupné z: https://blackdotsolutions.com/blog/osint-sources/
15. Blogging guide. *Best Open Source Blogging platforms.* [online]. [cit. 25.02.2023]. Dostupné z: https://bloggingguide.com/best-open-source-blogging-platforms/
16. *Blood & Honour.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.afd.de/https://www.bloodandhonourworldwide.co.uk/bhww/
17. *Blood C18 Honour – Hungary*. [online]. [cit. 03.03.2023]. Dostupné z: http://c18hungary.blogspot.com/
18. *Bundesamt für Sicherheit in der Informationstechnik.* [online]. [cit. 26.02.2023]. Dostupné z: https://www.bsi.bund.de/DE/Home/home_node.html
19. BŘEŠŤAN, Robert. Hlídací pes. *Pojďte k nám na vysokou, vábí Rusko Čechy. BIS i Černínský palác to „silně nedoporučují“*. [online]. [cit. 01.02.2023]. Dostupné z: https://hlidacipes.org/pojdte-k-nam-na-vysokou-vabi-rusko-cechy-bis-i-cerninsky-palac-to-silne-nedoporucuji/
20. *Censys.io.* [online]. [cit. 27.02.2023]. Dostupné z: https://censys.io/

21. CERT.LV. *Latvijas Republikas Informācijas tehnoloģiju drošības incidentu noveršanas institūcija.* [online]. [cit. 26.02.2023]. Dostupné z: https://cert.lv/en/search?q=annual+report

22. *Counterextremism.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.counterextremism.com/

23. *Counter Extremism Project. Country Reports: Extremism & Terrorism.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.counterextremism.com/countries

24. *Counter Extremism Project. Extremist Groups.* [online]. [cit. 18.02.2023]. Dostupné z: https://www.counterextremism.com/global-extremist-groups

25. *Counter Extremism Project. Terrorists and Extremists Database.* [online]. [cit. 18.02.2023]. Dostupné z: https://www.counterextremism.com/extremists

26. *Counter Extremism Project. Terrorists On Telegram.* [online]. [cit. 18.02.2023]. Dostupné z: https://www.counterextremism.com/terrorists-on-telegram

27. *CSO Online.* [online]. [cit. 25.02.2023]. Dostupné z: https://www.csoonline.com/

28. *Cybersecurity Insiders.* [online]. [cit. 25.02.2023]. Dostupné z: https://www.cybersecurity-insiders.com/

29. *CZ24 News.* [online]. [cit. 05.02.2023]. Dostupné z: https://cz24.news/

30. *Czech free press.* [online]. [cit. 05.02.2023]. Dostupné z: https://www.czechfreepress.cz/

31. *Dailystormer.* [online]. [cit. 03.03.2023]. Dostupné z https://dailystormer.in/

32. *Daniel Miessler.* [online]. [cit. 25.02.2023]. Dostupné z: https://danielmiessler.com/

33. *Dark reading.* [online]. [cit. 25.02.2023]. Dostupné z: https://www.darkreading.com/

34. *Decoded avast.io.* [online]. [cit. 26.02.2023]. Dostupné z: https://decoded.avast.io/

35. *Decoded avast.io. Threats.* [online]. [cit. 26.02.2023]. Dostupné z: https://decoded.avast.io/tag/threats/

36. Deník. *Ostraha i zásahová jednotka. Policisté z elektrárny Dukovany mají nové vybavení.* [online]. [cit. 07.02.2023]. Dostupné z: https://www.denik.cz/regiony/tohle-je-specialni-jednotka-dukovanske-elektrarny-podivejte-se-20200201.html

37. *Der Dritte Weg.* [online]. [cit. 03.03.2023]. Dostupné z: https://der-dritte-weg.info/

38. *Domaintools.* [online]. [cit. 27.02.2023]. Dostupné z: https://www.domaintools.com/

39. *DSSS.* [online]. [cit. 03.03.2023]. Dostupné z: http://www.dsss.cz/

40. *Důležité 24.* [online]. [cit. 05.02.2023]. Dostupné z: https://zpravy.dt24.cz/

41. ESTAV.cz. *Zvýšení zabezpečení jaderných elektráren bude stát 1,2 miliardy.* [online]. [cit. 06.03.2023]. Dostupné z: https://www.estav.cz/cz/7664.zvyseni-zabezpeceni-jadernych-elektraren-bude-stat-1-2-miliardy

42. *European Agency for Fundamental Rights. Cases and rulings.* [online]. [cit. 18.02.2023]. Dostupné z: https://fra.europa.eu/en/databases/anti-muslim-hatred/case-law

43. *European Eye on Radicalization.* [online]. [cit. 18.02.2023]. Dostupné z: https://eeradicalization.com/

44. European Union Agency for Asylum. *Latest Asylum Trends*. [online]. [cit. 24.02.2023]. Dostupné z: https://euaa.europa.eu/latest-asylum-trends-asylum

45. European Union Agency for Fundamental Rights. *Products.* [online]. [cit. 24.02.2023]. Dostupné z: https://fra.europa.eu/en/products/search

46. European Union. *New requirements to travel to Europe.* [online]. [cit. 24.02.2023]. Dostupné z: https://travel-europe.europa.eu/etias/what-etias_en

47. Eurostat. *Data Browser – Cross cutting topics.* [online]. [cit. 19.02.2023]. Dostupné z: https://ec.europa.eu/eurostat/databrowser/explore/all/cc?lang=en&subtheme=mi&display=list&sort=category

48. Eurostat. *Data Browser – Population and social conditions.* [online]. [cit. 19.02.2023]. Dostupné z: https://ec.europa.eu/eurostat/databrowser/explore/all/popul?lang=en&subtheme=migr&display=list&sort=category

49. *Exploit database.* [online]. [cit. 27.02.2023]. Dostupné z: https://www.exploit-db.com/

50. *Exploit database – Google Hacking Database.* [online]. [cit. 27.02.2023]. Dostupné z https://www.exploit-db.com/google-hacking-database?category=5

51. Flek na správném místě. *Ostraha pro JADERNOU ELEKTRÁRNU DUKOVANY.* [online]. [cit. 07.02.2023]. Dostupné z:

https://flek.cz/nabidka/ostraha-pro-jadernou-elektrarnu-dukovany-naborovy-prispevek-30-000-kc/413327?utm_source=jooble&utm_medium=cpc&utm_campaign=allvacancies

52. Frontex. *Migratory map.* [online]. [cit. 24.02.2023]. Dostupné z: https://frontex.europa.eu/we-know/migratory-map/

53. Frontex. *Migratory routes.* [online]. [cit. 24.02.2023]. Dostupné z: https://frontex.europa.eu/we-know/migratory-routes/western-mediterranean-route/

54. Frontex. *Public Register of Documents. Strategic Risk Analysis.* [online]. [cit. 19.02.2023]. Dostupné z: https://prd.frontex.europa.eu/?form-fields%5Bsearch%5D=Strategic%20Risk%20Analysis&form-fields%5Bdate-from%5D&form-fields%5Bdate-to%5D&form-fields%5Bdocument-category%5D%5B0%5D=318&form-fields%5Boffset%5D=0&form-fields%5Bform-post-id%5D=NGVlNzVkMzBiOTY1ODE1NmZmZTEyYzMxMjg5NjE3OGJNVFk0T0E9PTU2MDA0ODI3NTljZjliZTkyZWM3OTBhN2E1NzI1NzMxODA5ZDBkMzMwMjE2OTU1Mjk2&form-fields%5Bmodule-post-id%5D=YjE4MWFjZTc1YjEzMmM5YTZhYzA4MGRkOWMzYzM2MDJNemt3TVE9PTYxODU2MDU1NjRlOTUwYjEwODZhM2IyNmE4ODliMzg3ZjdhMzNiYzFlMzcwMDg5MDM5

55. *GBHackers On Security.* [online]. [cit. 26.02.2023]. Dostupné z: https://gbhackers.com/

56. *Generace identity*. [online]. [cit. 03.03.2023]. Dostupné z: https://generace-identity.cz/

57. *Génération Identitaire.* [online]. [cit. 03.03.2023]. Dostupné z: https://generationidentitaire.org/

58. *Generation Identity. United Kingdom and Ireland.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.generation-identity.org.uk/

59. Google maps. *Jaderná elektrárna Dukovany.* [online]. [cit. 04.03.2023]. Dostupné z: https://www.google.com/maps/place/Jadern%C3%A1+elektr%C3%A1rna+Dukovany/@49.0850898,16.1500925,3a,75y,90t/data=!3m8!1e2!3m6!1sAF1QipNqseoN-LmzeWTPqlyzloOG8ByaNkw1TE1Np9j5!2e10!3e12!6shttps:%2F%2Flh5.googleusercontent.com%2Fp%2FAF1QipNqseoN-LmzeWTPqlyzloOG8ByaNkw1TE1Np9j5%3Dw441-h298-k-no!7i2000!8i1350!4m8!3m7!1s0x4712a782b94a8bdd:0xe7b03895595a5567!8m2!3d49.0850898!4d16.1500925!14m1!1BCgIgAQ!16zL20vMGNqNjl4

60. Google maps. *Úložiště radioaktivních odpadů Dukovany.* [online]. [cit. 04.03.2023]. Dostupné z: https://www.google.com/maps/place/%C3%9Alo%C5%BEi%C5%A1t%C4%9B+radioaktivn%C3%ADch+odpad%C5%AF+Dukovany/@49.082222,16.1563535,17z/data=!4m6!3m5!1s0x4712a7c5ceef6d3f:0xc04d85864ad4a139!8m2!3d49.081682!4d16.1584848!16s%2Fg%2F11fjxr0jpj
61. *Graham Cluley.* [online]. [cit. 25.02.2023]. Dostupné z: https://grahamcluley.com/about-this-site/
62. *GTD – Global Terrorism Database.* [online]. [cit. 04.02.2023]. Dostupné z: https://www.start.umd.edu/gtd/
63. *HelpNetSecurity.* [online]. [cit. 25.02.2023]. Dostupné z: https://www.helpnetsecurity.com/
64. *Identitäre Bewegung.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.identitaere-bewegung.de/
65. *Identity Evropa.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.identityevropa.com/
66. *Info Security.* [online]. [cit. 25.02.2023]. Dostupné z: https://www.infosecurity-magazine.com/cybercrime/
67. *Institute for Strategic Dialogue.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.isdglobal.org/
68. *Interactive map: Russia's Invasion of Ukraine. Institue for the Study of War, 2023.* [online]. [cit. 06.02.2023]. Dostupné z: https://storymaps.arcgis.com/stories/36a7f6a6f5a9448496de641cf64bd375
69. *International Center for Counter-terrorism.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.icct.nl/
70. *International Crisis Group.* [online]. [cit. 06.02.2023]. Dostupné z: https://www.crisisgroup.org/
71. *International Legion Defence of Ukraine*. [online]. [cit. 01.03.2023]. Dostupné z: https://fightforua.org/
72. International Organization for Migration. *Czechia.* [online]. [cit. 19.02.2023]. Dostupné z: https://czechia.iom.int/cs
73. International Organization for Migration. *Latest Research Updates.* [online]. [cit. 19.02.2023]. Dostupné z: https://www.iom.int/iom-research-updates

74. International Organization for Migration. *Search For Books.* [online]. [cit. 18.02.2023]. Dostupné z: https://publications.iom.int/search
75. *ISD The Voice Of Blood and Honour RECORDS.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.isdrecords.com/
76. *ISW – Institue for the Study of War.* [online]. [cit. 06.02.2023]. Dostupné z: https://www.understandingwar.org/
77. Skupina ČEZ. *Jaderná elektrárna Dukovany.* [online]. [cit. 07.02.2023]. Dostupné z: https://www.cez.cz/cs/o-cez/vyrobni-zdroje/jaderna-energetika/jaderna-energetika-v-ceske-republice/edu
78. Skupina ČEZ. *Virtuální prohlídky.* [online]. [cit. 07.02.2023]. Dostupné z: http://virtualniprohlidky.cez.cz/cez-dukovany/
79. *Janes.* [online]. [cit. 18.02.2023]. Dostupné z: https://www.janes.com/
80. Jaroměřice nad Rokytnou. *Den s policií 18.9.2010.* [online]. [cit. 07.02.2023]. Dostupné z: https://jaromericenr.cz/vismo/galerie2.asp?id_galerie=8385&pocet=24&stranka=1
81. *Jobbik.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.jobbik.com/
82. *League of the South.* [online]. [cit. 03.03.2023]. Dostupné z: http://leagueofthesouth.com/
83. *Liveuamap.* [online]. [cit. 06.02.2023]. Dostupné z: https://liveuamap.com/
84. Ľudová strana naše Slovensko. [online]. [cit. 03.03.2023]. Dostupné z: http://www.lsnaseslovensko.sk/
85. M2C kariéra. *Člen zásahové jednotky JE Dukovany.* [online]. [cit. 07.02.2023]. Dostupné z: https://kariera.m2c.eu/pracovni-pozice/clen-zasahove-jednotky-nabor-prispevek-30-000-kc-je-dukovany/
86. M2C kariéra. *Manažer bezpečnosti.* [online]. [cit. 07.02.2023]. Dostupné z: https://kariera.m2c.eu/pracovni-pozice/manazer-bezpecnosti-m-z-jaderne-elektrarny/
87. M2C kariéra. *Operátor řídícího centra.* [online]. [cit. 07.02.2023]. Dostupné z: https://kariera.m2c.eu/pracovni-pozice/operator-ka-ridiciho-centra-naborovy-prispevek-120-000-kc/

88. M2C kariéra. *Ostraha pro JE Dukovany.* [online]. [cit. 07.02.2023]. Dostupné z: https://kariera.m2c.eu/pracovni-pozice/ostraha-pro-je-dukovany-naborovy-prispevek-30-000-kc/
89. M2C. *Zásahová jednotka očima zaměstnance M2C.* [online]. [cit. 07.02.2023]. Dostupné z: https://www.facebook.com/m2c.cz/videos/568693217410400/
90. *National Institute of Standards and Technology.* [online]. [cit. 25.02.2023]. Dostupné z: https://www.nist.gov/cybersecurity
91. *Nationaldemokratische Partei Deutschlands.* [online]. [cit. 03.03.2023]. Dostupné z: https://npd.de/
92. *Národní demokracie.* [online]. [cit. 03.03.2023]. Dostupné z: https://narodnidemokracie.cz/
93. *Národní noviny.* [online]. [cit. 05.02.2023]. Dostupné z: https://www.narodni-noviny.cz/
94. *Národní obroda*. [online]. [cit. 03.03.2023]. Dostupné z: https://www.narodni-obroda.cz/
95. Národní úřad pro kybernetickou a informační bezpečnost. *Publications & Reports.* [online]. [cit. 26.02.2023]. Dostupné z: https://www.nukib.cz/en/infoservis-en/publications-reports/
96. *Nordic Resistance Movement.* [online]. [cit. 03.03.2023]. Dostupné z: https://nordicresistancemovement.org/
97. *Noua Dreaptă.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.nouadreapta.org/
98. *Nová republika.* [online]. [cit. 05.02.2023]. Dostupné z: https://www.novarepublika.online/
99. Noviny VM. *Nové vybavení pro tým policistů ze Speciální jednotku Dukovany.* [online]. [cit. 07.02.2023]. Dostupné z: https://www.novinyvm.cz/22742-nove-vybaveni-pro-tym-policistu-ze-specialni-jednotku-dukovany.html
100. NSI. *CNS Global Incidents and Trafficking Database Archived Reports and Graphics.* [online]. [cit. 03.03.2023]. Dostupné z

https://www.nti.org/analysis/articles/cns-global-incidents-and-trafficking-database-archived-reports-and-graphics/

101. *Media2Rise.* [online]. [cit. 03.03.2023]. Dostupné z: https://media2rise.com/

102. *Office of the Prosecutor General.* [online]. [cit. 01.03.2023]. Dostupné z: https://warcrimes.gov.ua/

103. *Parlamentní listy.* [online]. [cit. 05.02.2023]. Dostupné z: https://www.parlamentnilisty.cz/

104. *Patriotfront.* [online]. [cit. 03.03.2023]. Dostupné z: https://patriotfront.us/

105. Policie České republiky. *Jadernou elektrárnu střeží speciální jednotka.* [online]. [cit. 07.02.2023]. Dostupné z: https://www.policie.cz/clanek/jadernou-elektrarnu-strezi-specialni-jednotka.aspx

106. *Pomich.* [online]. [cit. 01.03.2023]. Dostupné z: https://pomich.org/shippers

107. PRIO – *The Peace Research Institute Oslo*. [online]. [cit. 06.02.2023]. Dostupné z: https://www.prio.org/

108. *Protiproud.* [online]. [cit. 05.02.2023]. Dostupné z: https://protiproud.info/

109. Recorded Future. *What Is Open Source Intelligence and How Is IT Used?* [online]. [cit. 25.02.2023]. Dostupné z: https://www.recordedfuture.com/open-source-intelligence-definition

110. *RedIce.TV.* [online]. [cit. 03.03.2023]. Dostupné z: https://redice.tv/

111. *RedWatch Poland.* [online]. [cit. 03.03.2023]. Dostupné z: http://www.redwatch.info/

112. *Rense Radio Network.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.renseradio.com/hosts.htm

113. Rewards for Justice. *Intelligence-Driven Law Enforcement. Terrorism Reward Offers.* [online]. [cit. 04.02.2023]. Dostupné z: https://rewardsforjustice.net/index/?jsf=jet-engine:rewards-grid&tax=crime-category:1070%2C1071%2C1073%2C1072%2C1074

114. Royal United Services Institute. *Sanctions.* [online]. [cit. 18.02.2023]. Dostupné z: https://rusi.org/explore-our-research/topics/sanctions#latest-publications
115. *Securelist by Kaspersky.* [online]. [cit. 26.02.2023]. Dostupné z: https://securelist.com/
116. *Security Affairs.* [online]. [cit. 25.02.2023]. Dostupné z: https://securityaffairs.com/
117. *Security Intelligence.* [online]. [cit. 25.02.2023]. Dostupné z: https://securityintelligence.com/
118. Security Week. *Malware&Threats.* [online]. [cit. 25.02.2023]. Dostupné z: https://www.securityweek.com/category/malware-cyber-threats/
119. Security Week. *Threat Intelligence.* [online]. [cit. 25.02.2023]. Dostupné z: https://www.securityweek.com/category/threat-intelligence/
120. *Shodan.* [online]. [cit. 27.02.2023]. Dostupné z: https://www.shodan.io/
121. SKUPINA ČEZ. *V rámci cvičení SAFEGUARD budou Dukovany chránit vojáci ze zálohy.* [online]. [cit. 05.03.2023]. Dostupné z: https://www.cez.cz/cs/pro-media/tiskove-zpravy/v-ramci-cviceni-safeguard-budou-dukovany-chranit-vojaci-ze-zalohy-166132
122. *START – Study of Terrorism and Responses to Terrorism.* [online]. [cit. 04.02.2023]. Dostupné z: https://www.start.umd.edu/
123. Statista. *Most popular social networks worldwide as of January 2023, ranked by number of monthly active users.* [online]. [cit. 25.02.2023]. Dostupné z: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
124. Stockholm International Peace Research Institute. *SIPRI Databases.* [online]. [cit. 15.02.2023]. Dostupné z: https://sipri.org/databases
125. Stockholm International Peace Research Institute. *SIPRI Year Book Online.* [online]. [cit. 15.02.2023]. Dostupné z: https://www.sipriyearbook.org/

126. *Stormfront.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.stormfront.org/forum/
127. Telegram. *eVorog.* [online]. [cit. 01.03.2023]. Dostupné z: https://t.me/evorog_bot
128. The Barnes Review. *Magazine and Bookstore.* [online]. [cit. 03.03.2023]. Dostupné z: https://barnesreview.org/
129. *The Hacker News. [online].* [cit. 25.02.2023]. Dostupné z: https://thehackernews.com/
130. *The National Socialist Movement.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.nsm88.org/
131. The National Socialist Movement. *NSM Year in Review 2022.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.nsm88.org/comment/7740#comment-7740
132. *The Occidental Observer.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.theoccidentalobserver.net/
133. *The Occidental Quarterly.* [online]. [cit. 03.03.2023]. Dostupné z: https://www.toqonline.com/
134. *The Order of Nine Angels.* [online]. [cit. 03.03.2023]. Dostupné z: https://lapisphilosophicus.wordpress.com/
135. *The Right Stuff.* [online]. [cit. 03.03.2023]. Dostupné z: https://therightstuff.biz/
136. The UN Refugee Agency. *Global Trends.* [online]. [cit. 18.02.2023]. Dostupné z: https://www.unhcr.org/globaltrends
137. The UN Refugee Agency. *Mid-Year Trends*. [online]. [cit. 18.02.2023]. Dostupné z: https://www.unhcr.org/mid-year-trends
138. The UN Refugee Agency. *Operational Data Portal. Refugee Situations.* [online]. [cit. 18.02.2023]. Dostupné z: https://data.unhcr.org/en/situations#_ga=2.118651210.211795433.1676819266-1970285126.1676819266&_gac=1.250116340.1676819266.Cj0KCQiArsefBhCbARIsAP98hXQ5Y93TE2cpl4E8yU2obLJId03H8gWhWYNFetBnnhGcrVwATXQGRE8aAsHMEALw_wcB

139. The UN Refugee Agency. *Refugee Data Finder.* [online]. [cit. 18.02.2023]. Dostupné z: https://www.unhcr.org/refugee-statistics/download/?url=F8Wzj7

140. The Washington Post. Democracy Dies in Darkness*. Instead of consumer software, Ukraine's tech workers build apps of war*. [online]. [cit. 01.03.2023]. Dostupné z: https://www.washingtonpost.com/technology/2022/03/24/ukraine-war-apps-russian-invasion/

141. *Threat Analysis Group.* [online]. [cit. 26.02.2023]. Dostupné z: https://blog.google/threat-analysis-group/

142. *TRACK. Tracking Terrorism.* [online]. [cit. 18.02.2023]. Dostupné z: https://trackingterrorism.org/

143. Traficom. *Cyber Weather.* [online]. [cit. 26.02.2023]. Dostupné z: https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/cyber-weather?toggle=Cyber%20Weather%202023&toggle=Cyber%20Weather%202022

144. *Trend Micro Blog*. [online]. [cit. 26.02.2023]. Dostupné z: https://news.trendmicro.com/

145. *Troy Hunt.* [online]. [cit. 25.02.2023]. Dostupné z: https://www.troyhunt.com/

146. Třebíč. *Vojáci, policisté, hasiči a energetici společně cvičili ochranu Jaderné elektrárny Dukovany.* [online]. [cit. 05.03.2023]. Dostupné z: https://www.trebic.cz/vojaci-policiste-hasici-a-energetici-spolecne-cvicili-ochranu-jaderne-elektrarny-dukovany/d-39020

147. Třebíčský deník.cz. *Neproklouzne ani vrabec. Jadernou elektrárnu Dukovany chrání lasery i před drony.* [online]. [cit. 06.03.2023]. Dostupné z: https://trebicsky.denik.cz/zpravy_region/neproklouzne-ani-ptacek-jadernou-elektrarnu-dukovany-chrani-lasery-i-pred-drony.html

148. *UCDP – Upsala Conflict Data Program.* [online]. [cit. 06.02.2023]. Dostupné z: https://ucdp.uu.se/encyclopedia

149. *Ukraine now.* [online]. [cit. 01.03.2023]. Dostupné z: https://www.ukrainenow.org/refuge

150. United Nations Register of Conventional Arms. *Transparency in the global reported arms trade.* [online]. [cit. 16.02.2023]. Dostupné z: https://www.unroca.org/

151. *Ústav mezinárodních vztahů Praha.* [online]. [cit. 06.02.2023]. Dostupné z: https://www.iir.cz/

152. UTON. *TIGER – zásahová jednotka Dukovany.* [online]. [cit. 07.02.2023]. Dostupné z: https://www.uton.cz/noze-pcr/tiger-2/

153. *Virustotal.* [online]. [cit. 27.02.2023]. Dostupné z: https://www.virustotal.com/gui/home/upload

154. *Welivesecurity.* [online]. [cit. 26.02.2023]. Dostupné z: https://www.welivesecurity.com/

155. *Who.is.* [online]. [cit. 27.02.2023]. Dostupné z: https://who.is/

156. Wigle. Net. *All the networks. Found by everyone.* [online]. [cit. 27.02.2023]. Dostupné z: https://wigle.net/index

157. Znojmo. *Útok na jadernou elektrárnu odražen. Cvičení SAFEGUARD Dukovany 2016 prověřilo součinnost vojáků, policistů a společnosti ČEZ při ochraně JE Dukovany.* [online]. [cit. 05.03.2023]. Dostupné z: https://www.znojmocity.cz/utok-na-jadernou-elektrarnu-dukovany-odrazen-cviceni-safeguard-dukovany-2016-proverilo-soucinnost-vojaku-policistu-a-spolecnosti-cez-pri-ochrane-je-dukovany/d-51748

Seznam obrázků