Bezpečnost nositelného HW v ozbrojených složkách

Bc. Josef Sojka

Diplomová práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Josef Sojka**
Osobní číslo:	**A19433**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Bezpečnost nositelného HW v ozbrojených složkách**
Téma práce anglicky:	**The Security of Wearable HW in Armed Forces**

Zásady pro vypracování

1. Popište současný stav výbavy sesednutého vojáka AČR.
2. Identifikujte hrozby a rizika z hlediska kybernetické bezpečnosti.
3. Prověřte bezpečnost bezdrátové komunikace u pozorovacích přístrojů JIM a MOSKITO.
4. Navrhněte vhodné postupy a nastavení k omezení detekce EB protivníka.
5. Specifikujte odlišné požadavky na technologie pro průzkumné a speciální jednotky.
6. Navrhněte soubor požadavků, které by měly splňovat nově zaváděné technologie do AČR.

Forma zpracování diplomové práce: **Tištěná/elektronická**

Seznam doporučené literatury:

1. COLEMAN, David D. CWSP: certified wireless security professional official study guide. Indianapolis, Ind.: Wiley Pub., c2010. Serious skills. ISBN 0470438916.
2. LU, Zhuo a Cliff WANG. Proactive and Dynamic Network Defense. Imprint: Springer, 2019. Advances in Information Security, 74. ISBN 9783030105976.
3. Overview of Dismounted Soldier Systems [online], 2018. 1. Brusel: STO/NATO [cit. 2020-10-17]. ISBN 978-92-837-2129-1. Dostupné z: https://apps.dtic.mil/sti/pdfs/AD1064371.pdf
4. ČOS 589501, 2019. ČESKÝ OBRANNÝ STANDARD: SPECIFIKACE DEFINUJÍCÍ INTEROPERABILNÍ SÍŤ SPOLEČNÉHO SYSTÉMU SESEDNUTÉHO VOJÁKA. 1. Praha: ÚŘAD PRO OBRANNOU STANDARDIZACI, KATALOGIZACI A STÁTNÍ OVĚŘOVÁNÍ JAKOSTI.
5. Koncepce výstavby Armády České republiky 2030 [online], 2019. 1. Praha: Ministerstvo obrany České republiky – VHÚ Praha [cit. 2020-10-17]. ISBN ISBN978-80-7278-789-0. Dostupné z: http://www.mocr.army.cz/images/id_40001_50000/46088/koncepce___2030.pdf

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **15. ledna 2021**
Termín odevzdání diplomové práce: **17. května 2021**

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN
L.S.

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 15. ledna 2021

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne …….

Josef Sojka v.r.

ABSTRAKT

Tato práce je zaměřena na bezpečnost vojenské komunikace a to konkrétně v oblasti nasazení sesednutého vojska. Současným trendem v ozbrojených složkách je budování schopností C4ISTAR. Tento trend pomáhá vytvářet zcela nový druh kyberprostoru a nutí nás k zamyšlení nad novými hrozbami a nad novými aspekty těch stávajících.

Klíčová slova:

C4ISTAR; kybernetická bezpečnost; komunikační systémy; sesednutý voják;

ABSTRACT

This paper is aimed at cyber security of military communications regarding dismounted soldiers operations. Contemporary armed forces goal is to build C4ISTAR capabilities. This endeavour result in whole new area of cyberspace and make us answer to new threats and risks.

Keywords:

C4ISTAR; cyber security; communication systems; dismounted soldier;

Bez spojení není velení.

Běžně užívané vojenské rčení.

Pozor! Nepřítel naslouchá!

Text umisťovaný na pracoviště operátorů – radistů.

Chtěl bych poděkovat vedoucímu práce Ing. Davidu Malaníkovi Ph.D. za podnětné připomínky a rady.

Chtěl bych poděkovat firmě Pramacom HT za zapůjčení přístroje Moskito TI.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Jako voják z povolání se téměř po dobu patnácti let zabývám komunikačními a informačními systémy (dále jen KIS). Prošel jsem řadou pozic a zabýval se různými aspekty problematiky vojenského spojení od osobní radiové komunikace, přes zabezpečení stálých vojenských sítí, po výstavbu komunikačních uzlů na mobilních místech velení. Zaznamenal jsem výrazný posun ve vývoji technologií i v pojetí vojenské komunikace. Zástupným termínem této proměny by mohla být takzvaná digitalizace bojiště. Význam této fráze není co do používání v rámci odborných kruhů armády pevně ukotven, ale dá se říci, že je symbolem modernizace technologického vybavení armády. Přestože projekty k digitalizaci bojiště nejsou nic nového (AČR měla k dispozici studii zabývající se touto problematikou už v roce 2002 [1]) ani v současné době se nedá hovořit o plně digitalizovaném bojišti. Ani po roce 2020 není možné považovat datovou digitální komunikaci za běžnou součást výbavy každého vojáka. Dynamický vývoj digitálních technologií však rychle proměňuje prostor bojiště a v souladu se současnými trendy v oblasti bezpečnosti komunikací se dá hovořit o nově se formujícím kyberprostoru. Dle mého názoru a odborných zkušeností nejsou mnohé aspekty tohoto prostředí dostatečně popsány a to přes to, že se jich dotýká řada koncepčních dokumentů, zákonů a normativních aktů. Jedním z těchto aspektů je bezpečnost technologií používaných na úrovni sesedlých vojsk. V této práci se zaměřím na popis možných bezpečnostních problémů v nastíněné oblasti. Cílem je zpracovat analýzu, která by mohla najít uplatnění u armádních specialistů zabývajících se akvizicemi, vývojem, správou a zabezpečením KIS, ale i velitelů při přípravě a nasazení vojsk. V neposlední řadě by mé závěry mohly posloužit při zpracování projektu bezpečnosti systému sesednutého vojáka, který je potřebný k akreditaci systému pro zpracování utajovaných informací.

I. TEORETICKÁ ČÁST

1 STANOVENÍ POJMŮ

1.1 Bezpečnost v pojetí této práce

Nositelný hardwaru, může být předmětem mnoha druhů bezpečnosti. Mezi mnohými vzpomenu bezpečnost a ochranu zdraví při práci, bezpečnost výrobků a kybernetickou bezpečnost. V této práci se nemám v úmyslu zabývat bezpečností nositelného HW z hlediska možného způsobení přímé újmy obsluze, životnímu prostředí a podobně. Mým záměrem je prozkoumat problematiku bezpečnosti plynoucí z primární funkce, kterou plní nositelný hardware v pojetí ozbrojených sil a tou je komunikace. Bezpečnost, kterou se na těchto stránkách budu zabývat, bude tedy spadat pod kybernetickou, případně informační bezpečnost.

1.2 Vojenská terminologie

V prvé řadě je nutné seznámit se se specifiky vojenské komunikace. V této kapitole objasním některé termíny běžně neužívané mimo vojenské prostředí, ale také poukážu na specifické užití některých termínů tak, jak budou vnímány v rámci této práce.

1.2.1 C2, C4, C4ISTAR

Název C4ISTAR je vlastně souhrnem jednotlivých funkcionalit systému velení a řízení v armádě. Těmto funkcionalitám odpovídají určité prvky architektury systémů velení a řízení. „Podstatou architektury C4ISTAR je efektivní využití elektromagnetického spektra pro velení (Command), řízení (Control), komunikaci (Communication), zpracování dat (Computer), vojskové zpravodajství (Intelligence), sledování (Surveillance), akvizici cílů (Target Acquisition) a průzkum (Reconnaissance)“ [2]. C4ISTAR je pomyslným vrcholem v rámci evoluce velení a řízení.

C2 (Command, Control) systémy jsou nezbytným základem každé vojenské operace a představují schopnosti velet – předávat rozkazy a řídit – dohlížet nad vykonáním rozkazů a usměrňovat činnost podřízených jednotek.

C4 (Command, Control, Communication, Computer) je rozšířením základní funkce velet a řídit o možnost komunikace (ve smyslu rozšířené schopnosti oboustranného předávání obsáhlejších zpráv a informací, ne jen strohé: „*Proveďte rozkaz 66!*“) a využití počítačů jak ke zpracování dat, tak ke komunikaci.

C4ISTAR pak doplňuje spektrum o další schopnosti, které budu dále popisovat v praktické části.

Je možné se setkat i s jiným zkratkami na stejném principu, které berou v potaz i jiné schopnosti, které logicky náleží do stejného spektra, viz například elektronický článek: „C2 vs. C4ISR vs. C5ISR vs. C6ISR: What's the Difference?" na stránkách výrobce odolných serverů Trenton systems [3]. V AČR se však zpravidla užívá jako vrcholná architektura C4ISTAR.

1.2.2 Situational awareness (SA)

Ve vojenském prostředí se jedná o budovanou schopnost obsáhnout všechny podstatné informace pro vedení operace a distribuovat je potřebným součástem nasazených vojsk. Informace, o kterých hovořím, mohou být hydrometeorologické predikce, pozice vlastních jednotek (v současné době zajišťováno často automatizovanými technologiemi souhrně označovanými jako blue force tracking BFT), zjištěné a předpokládané pozice nepřátelských jednotek, zpravodajské informace ze zájmové oblasti, geografické informace a podobně.

1.2.3 Taktický zobrazovací terminál, displej

Taktický zobrazovací terminál (TZT) je zodolněný přenosný počítač vybavený programovým vybavením, usnadňující taktickou vojenskou komunikaci. Nejběžněji využíván je e-mailový klient a zpravidla specializovaná vojenská aplikace umožňující přehled vlastních i zjištěných nepřátelských jednotek a také práci s digitálními mapovými podklady v rámci takzvaného mapového zákresu.

Taktický zobrazovací displej (TZD) je tablet, phablet nebo smartphone s obdobným softwarovým vybavením, jako je popsáno u TZT.

Obojí musí v případě sesednutého vojáka umožňovat připojení k radiostanici pro taktickou komunikaci, případně k dalším periferiím.

1.2.4 Sesednutý voják (dismounted soldier)

Z hlediska organizační struktury armád se zpravidla jedná o vojáky na úrovních družstev a čet. Od úrovně velitele roty a výše se běžně nesetkáváme s fungováním vojáka v sesedlém režimu. Tento termín se může zdát samozřejmý, nicméně je potřeba poznamenat, že se jedná o termín užívaný v rámci NATO standardizovaně. Je definováno jaké má

v rámci aliance mít sesednutý voják v dané odbornosti (ženisté, průzkum, mechanizovaná pěchota a další) schopnosti a jaké může plnit úkoly. Podobně pak je standardizován Systém sesednutého vojáka – DSS (Dismounted Soldier system). Což je slovy standardu „Všechno co voják nosí, přenáší nebo využívá pro vlastní potřebu na bojišti v taktickém prostředí.“ [4] Jak vyplývá z této definice, součástí DSS jsou mimo KIS i zbraně, výstroj, ochranné pomůcky a další materiál.

Významem standardizace je, aby jednotky napříč státy NATO mohly být vystrojeny a vyzbrojeny kompatibilně a byly používány shodné postupy. V rámci NATO jsou stanovovány normy STANAG, a v AČR normy ČOS dle zákona o obranné standardizaci [5]. Této práce by se měly dotýkat české obrané standardy definující interoperabilní síť sesednutého vojáka pro operace v rámci NATO:

ČOS 589501 - specifikace definující interoperabilní síť společného systému sesednutého vojáka; [4]

ČOS 589502 - specifikace definující interoperabilní síť společného systému sesednutého vojáka – bezpečnost; [4]

ČOS 589503 - specifikace definující interoperabilní síť společného systému sesednutého vojáka – datový model; [6]

ČOS 589504 - specifikace definující interoperabilní síť společného systému sesednutého vojáka – zapůjčená radiostanice; [7]

ČOS 589505 - specifikace definující interoperabilní síť společného systému sesednutého vojáka – mechanismus výměny informací; [8]

ČOS 589506 – specifikace definující interoperabilní síť společného systému sesednutého vojáka – přístup k síti; [9]

Výše uvedené normy by měly implementovat do prostředí AČR normu STANAG 4677 Dismounted Soldier Systems Standards and Protocols for Command, Control, Communications and Computers (C4) Interoperability DSS C4 Interoperability, která stanovuje komunikační standardy, které by měly užívat armády NATO k zajištění vzájemné kompatibility [10]. Bohužel odkazovaný dokument není veřejně přístupný.

1.3 Waveformy

V prostředí vojenské komunikace se stále častěji začíná používat termín waveform (případně počeštěná waveforma) pro označení druhu provozu radiostanic. Většina radiostanic umožňuje vícero druhů provozu na základě zvoleného kmitočtového pásma, druhu modulace, přenosového protokolu a použité kryptografické metody. Přestože by bylo přínosné z hlediska bezpečnosti definovat charakteristiky jednotlivých používaných přenosových protokolů, v této práci se takovou analýzou zabývat nebudu. Vzhledem k množství využívaných waveforem by byl rozsah sám osobě dostačující pro celou diplomovou práci.

Podstatné pro tuto práci je popsat základní charakteristiky, které mohou mít vliv na bezpečnost.

Dělit druhy provozu můžeme na základě výše uvedených charakteristik.

1.3.1 Dělení dle kmitočtového spektra

Na základě frekvence vysílače rozdělujeme provozy dle zákona 423/2017 Plán přidělení kmitočtových pásem rozeznáváme pásma takto:

Tabulka 1 Kmitočtová pásma [11]

Číslo pásma N	Symboly	Rozsah kmitočtů (dolní mez mimo, horní mez včetně	Odpovídající názvy pásem
4	VLF	3 až 30 kHz	myriametrové
5	LF	30 až 300 kHz	kilometrové
6	MF	300 až 3000 kHz	hektometrové
7	HF	3 až 30 MHz	dekametrové
8	VHF	30 až 300 MHz	metrové
9	UHF	300 až 3000 MHz	decimetrové
10	SHF	3 až 30 GHz	centimetrové
11	EHF	30 až 300 GHz	milimetrové
12	---	300 až 3000 GHz	decimilimetrové

V praxi se pak často setkáme s českými termíny

HF = krátké vlny (KV)

VHF = velmi krátké vlny (VKV)

UHF = ultra krátké vlny (UKV)

Vlnová délka (frekvence) má výrazný vliv na šíření elektromagnetické vlny prostorem a její možnosti přenosu informace. Delší vlny se lépe šíří překážkami (zalesněné prostředí, terénní překážky) a dá se využít jejich odrazu od vrstev v atmosféře pro přenos na dlouhé vzdálenosti. Z logiky modulace informace mají naopak krátké vlny větší kapacitu pro přenos informací [12].

V současné době je na vzestupu trend využívání MANET sítí. Tyto sítě umožňují každému rádiu fungovat jako retranslační bod a směrovač pro ostatní rádia, přičemž tyto funkce jsou automatizovány. Jedná se o funkce jako self - forming a self – healing, jak je pojmenovává výrobce PERSISTENT SYSTEMS [13]. Výhody jsou jednoznačně rozšíření dosahu radiostanic a efektivní přenos informace formou broadcastu. Samozřejmě jsou zde také nevýhody, například vyšší nároky na zdroj elektrické energie, neboť stanice vysílají z důvodu optimalizace sítě i bez průchodu uživatelských dat. Tato vlastnost je pak také nevýhodná z hlediska možné detekce protivníkem. Nevýhodou může být v případě využití vyšší frekvence v rozsahu UHF poměrně krátký dosah, z vlastní zkušenosti mohu potvrdit, že v zalesněném terénu se signál u některých typů radiostanic ztrácí často i na vzdálenost 100 metrů mezi jednotlivými stanicemi.

1.3.2 Dle modulace

- Amplitudová
- Frekvenční
- Fázová

1.3.3 Dle šifrování

- Nešifrovaná
- Šifrovaná
- Šifrovaná dle standardu [1]

1.3.4 Dle způsobu torby sítě

- Komunikace na přímou radiovou viditelnost (LOS);

[1] Pro komunikaci na určitém stupni utajení jsou zpravidla stanoveny schválené typy kryptografie pro jejich zabezpečení. Stanovení požadovaných standardů v případě vojenské komunikace vychází pro alianční prostředí NATO z nařízení C-M(2002)49-REV1 SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANIZATION (NATO) [14].

- Satelitní;
- Mobile ad hoc network (MANET);

1.4 Kybernetická válka

Ve vojenském prostředí je stále nedostatečně popsáno, co spadá pod pojem kybernetická bezpečnost. V mnoha státech se v rámci armády vytváří kybernetické síly. Nicméně zatím je minimálně v AČR tato součást ozbrojených sil stále ve vývoji a paleta činnosti kybernetických sil není pevně stanovena. Všichni si dovedeme představit co je kybernetický útok v intencích civilní části státního nebo občanského sektoru, v intencích vojenské operace je tento pojem komplikovanější.

Publikace Univerzity obrany v Brně Kybernetická bezpečnost definuje některé aspekty kybernetického válčení takto:

„Dnešní kybernetické útoky jsou primárně prováděny k získávání informací o diplomatických, ekonomických a vojenských programech. Sekundárním cílem může být ochromení kritické infrastruktury daného státu. … Budoucí možné kybernetické války jsou důvodem k vážnému znepokojení nás všech. … kybernetický útok může přijít jako součást koordinovaného útoku, nebo to může být jen výmysl zlomyslného hackera například s vtipnou myšlenkou. Právě útok na kritickou infrastrukturu může vést k vyřazení sítí, které dále slouží ve prospěch zdravotnictví, vodohospodářství a dalších životně důležitých prvků státu. … Závislost na kybernetickém prostoru může být využita nepřítelem k získání strategické výhody při případném konfliktu. Předpokládá se, že kybernetická válka bude předcházet před konvenční válkou.“ [15, s. 22-26]

V tomto kontextu se zdá, že není předpokládáno zapojení kybernetického boje na samotné bojiště. Souhlasím sice, že kybernetické útoky budou předcházet nasazení kinetických sil, podobně jako průzkum, zároveň ovšem předpokládám, že kybernetické síly se po zahájení operací zaměří na další podporu vojenských operací, podobně jako průzkum. Elektronická encyklopedie Britannica definuje kybernetickou válku trochu rozdílněji: „…vedená v a prostřednictvím počítačů a sítí, které je propojují, vedena státy, nebo jejich prostředníky proti jiným státům. Kybernetiká válka je většinou vedena proti vládním a vojenským

sítím za účelem narušení, zničení nebo odepření jejich užití.“[2] [16]. Z mého pohledu je takováto definice přesnější a je potřeba se zamýšlet nad možnostmi kybernetických útoků i v kybernetickém prostoru armády. Kyberprostor vojenských jednotek je sice hodně specifický, ale s modernizací techniky jde postupně vývoj v této oblasti ve šlépějích toho civilního. Roste propojenost a složitost vojenských komunikačních a informačních sítí. V brzké době se tak můžeme setkat s moderními formami kybernetických útoků i v těchto sítích.

Zajímavé je rovněž rozdělení sfér kyberprostoru dle serveru Britannica. Je rozeznávána fyzická vrstva zahrnující hardware, syntaktická zahrnující softwarovou vrstvu a sémantická vrstva, která sestává z uživatelů a jejich interpretace. Všechny pak mohou být zranitelné: „Útoky kybernetické války mohou být vedeny proti fyzické infrastruktuře kyberprostoru za použití klasických zbraní a bojových metod. Pro příklad počítače mohou být fyzicky zničeny, jejich sítě rušeny, a lidští uživatelé této fyzické infrastruktury mohou být podplaceni, oklamáni nebo zabiti za účelem fyzického přístupu k síti nebo k počítači.“[3] [16]. Tato definice do velké míry koresponduje s mnoha riziky, která jsem identifikoval na základě vlastních zkušeností a znalostí armádní infrastruktury a procesů.

Problémem pro identifikaci kybernetických rizik by mohl být fakt, že jsou součástí běžných operací jiných složek armády než kybernetických sil. Bude otázkou kam zařadit různé druhy útoků. Jako příklad útoků na pomezí kybernetických a jiných mohu uvést elektromagnetické rušení, které je běžně známo a označováno jako elektronický boj (EB), získání kontroly nad nepřátelským dronem prostřednictvím nějaké formy man in the middle, získání kontroly nad nepřátelským dronem na základě triangulace pozice operátora a fyzického zabrání hardwaru, útok kinetických bojových prostředků s cílem získat přístup k nepřátelské komunikační nebo informační síti a následná implementace malwaru. Využití zbraní, které budou ničit nepřátelskou elektroniku. Takové útoky se podle mých vědomostí zatím nestaly, částečně díky tomu jak vypadá soudobé asymetrické bojiště. Na bojištích v Afghánistánu, Mali, ale i na Ukrajině se setkáváme s armádami, které jsou technologicky na výši a bojují s podstatně hůře vybaveným protivníkem. Zaměření poloh nepřátelských komunikačních prostředků, jejich rušení nebo sofistikovanější napadání není na po-

[2] Vlastní překlad anglického originálu.
[3] Vlastní překlad anglického originálu.

řadu dne a s podobnými scénáři se setkáváme snad jen v rámci žánru science-fiction. Běžně se však stává, že myšlenky prezentované jako sci-fi se staly každodenní realitou.

Ať už bude taková činnost součástí kybernetické války či nikoliv, jedná se o potenciální riziko pro kyberprostor armády.

1.5 Utajovaná informace

Na rozdíl od většiny civilních organizací, které přistupují k ochraně informací na základě vlastního uvážení, případně podle zákona o zpracování osobních údajů č. 110/2019 Sb. [17], Armáda České republiky se ve vztahu k informacím musí řídit dle Zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti 412/2005 Sb.

V souladu se zákonem jsou tak rozeznávány informace ve čtyřech stupních utajení (vyhrazené, důvěrné, tajné a přísně tajné). Případně se můžeme setkat s informacemi podléhajícím utajení mimo Českou republiku, ale v souladu se zákonem jsou označovány podle příslušné organizace například jako NATO SECRET pro informace klasifikované jako tajné v rámci NATO [18].

Paralelně k tomuto označování AČR využívá ještě zvláštní označení informací a to „PRO SLUŽEBNÍ POTŘEBU“. V tomto případě se jedná o informace v zákonném smyslu neutajované. Nicméně jedná se o informace, které například spadají do oblasti Zákona o zpracování osobních údajů nebo, nenaplňují literu zákona, ale zpracovatel předpokládá, že není vhodné jejich obecné šíření. Z mého osobního pohledu se jedná o určitý alibismus, kdy vytvořením vágně definované instituce dokumentu pro služební potřebu obcházejí zpracovatelé povinnosti, které by jim vznikaly vytvářením dokumentů dle zákonů 412/2005 a 110/2019. Významnou roli přitom hraje i nevhodné nastavení vnitřních armádních procesů ve vztahu k utajovaným informacím, které jakoukoli práci s utajovanou informací nadměrně ztěžují. V praxi jsem se setkal, s tím, že vojáci, kteří mají odůvodněnou potřebu seznámit se s utajovanou informací, se s ní neseznámí díky příliš složitému přístupu k ní, případně se vůbec nedozví, že dokument významný pro výkon jejich funkce existuje.

II. PRAKTICKÁ ČÁST

2 SOUČASNÝ STAV VÝBAVY SESEDNUTÉHO VOJÁKA POZEMNÍCH SIL AČR

V této části se zaměřím na obecný popis výbavy vojáků v AČR se zaměřením na elektronická zařízení a to zejména na komunikační prostředky. Dle mých znalostí neexistují žádné podobné popisy a armáda nezveřejňuje počty kusů jednotlivých zařízení ani jejich distribuci v rámci jednotlivých složek. Samozřejmě není možné, aby bylo konkrétně publikováno, které vlnové formy radiostanic, popřípadě jaké SW vybavení a jaké protokoly jsou využívány.

V mnoha případech budu vycházet z vlastních zkušeností z mnohaleté praxe v oboru. Přestože armáda neutajuje, jakou technologii využívá, zároveň platí, že tyto informace nezveřejňuje (s výjimkou počtů bojové techniky, které musí být v rámci mezinárodních úmluv zveřejňovány). Informace o tom, že je konkrétní technika dodávána do armády je zpravidla uváděna jako propagace daného výrobku na stránkách výrobců, případně dodavatelů. Nejsem si ovšem vědom žádného dokumentu, ať už veřejného, či interního v rámci AČR, který by komplexně popisoval problematiku vybavení sesednutého vojáka nebo celé struktury armádního KIS. Z praxe vím, že v mnoha případech jsou v armádě zavedeny radiostanice nebo jiné přístroje v počtech několika kusů (v jednom případu jsem se setkal s jediným kusem radiostanice nekompatibilní s žádnou jinou radiostanicí zavedenou v AČR a pokud vím, nikdy nebyla ve výcviku použita). Není tak možné zahrnout všechny možné varianty a způsoby použití výbavy DSS. Jako podstatné vnímám definovat typy výbavy, způsoby jejich užívání a z těchto odvodit možná rizika a problémy. Z výše uvedeného vyplývá, že nemohou být pokryta rizika do největších podrobností – například zranitelnost konkrétního typu firmwaru určitého typu radiostanice.

2.1 Komunikace C2

Komunikaci je možné považovat v rámci bojiště za naprosto klíčovou schopnost. Ještě v nedávných dobách nebyl tolik brán zřetel na komunikační vybavení jednotlivce. Vojáci nejmenších organizačních vojenských celků – družstev/týmů/skupin. Tyto skupiny o velikosti většinou do deseti osob komunikovali často pouze hlasem. V mnoha případech je tomu tak i dnes. Radiostanice je pak doménou velitelů těchto skupin (případně jim přidělených spojovacích specialistů) a slouží pro komunikaci s nadřízenými prvky. Záměrem moderních armád je však pokrýt elektronickou komunikací všechny vojáky v poli jak ilustruje například jeden ze střednědobých cílů kanadské armády definovaný v dokumentu koncep-

ce v letech 2011 – 2025: „Komunikační systém plně přizpůsobitelný misi, modulární a integrovaný do systému vojáka pro každého jednotlivého vojáka.“ [19] [4]

Z takto definovaného cíle je ovšem zároveň patrné, že zajistit požadované pokrytí komunikačními prostředky není samozřejmostí. Podobně jako u jiných prvků výbavy a výzbroje se i v případě radiostanic setkáváme s postupným vyzbrojováním. V AČR je tento jev významně patrný a můžeme se v jeho důsledku setkat s radiostanicemi mnoha rozdílných typů od řady výrobců. Pro ilustraci uvedu přehled nejrozšířenějších stanic.

2.1.1 Radiostanice DICOM

Starší radiostanice DICOM (RF-13, RF-1301, RF1302) tvoří stále ještě největší část osobních radiostanic pozemních sil. Přesto se dají považovat za výběhové, neboť neumožňují šifrovaný provoz na požadované úrovni a datový provoz s připojením k TZT nebo TZD (viz níže tablet nebo přenosný počítač) je možný jen s pomocí modemu, který je sice ve výzbroji, ale byl softwarově kompatibilní pouze pro operační systém windows do generace XP.

2.1.2 Radiostanice HARRIS

Z důvodu požadavku na zabezpečení šifrovaného provozu a kompatibilních vlnových forem přechází pozemní síly AČR postupně na radiostanice HARRIS. Modely RF-7800S a RF-7850S pro nejjednodušší komunikaci na úrovni řadového vojáka. Pro potřeby spojařů a různých specialistů jsou používány AN/PRC 152 a AN/PRC 117G. Můžeme se rovněž setkat s krátkovlnnými radiostanicemi AN/PRC 150. Většina těchto radiostanic umožňuje dokonce více režimů pro datovou komunikaci prostřednictvím připojených periferií.

2.1.3 Ostatní radiostanice

Ve výbavě jednotek AČR je zastoupeno řada dalších typů od několika výrobců, přičemž nejvýznamnější zastoupení tvoří rádia výrobců PERSISTENT SYSTEMS (MPU5 dodávaná v rámci kompletů C4ISTAR), Rohde & Schwarz a THALES.

[4] Vlastní překlad anglického originálu.

2.2 Počítače C4

Pro zasílání dat jsou vojáci na vybraných funkcích vybavení zvolněnými přenosnými počítači, tablety nebo smartphony v současné terminologii využívané v armádě hovoříme o taktickém zobrazovacím terminálu – TZT v případě zvolněného přenosného PC a taktickém zobrazovacím displeji – TZD v případě tabletu nebo smartphonu. Vojáci vybavení těmito přístroji zpravidla zastávají funkce velitelů družstev/skupin/týmů/čet, spojařů a specialistů v různých oborech jako je průzkum.

Účel počítačů v DSS je poskytnout vojákům v poli informační podporu v rámci SA a umožnit předávat informace k nadřízeným stupňům. Vybaven vhodným softwarem a periferiemi se stává každý voják senzorem na bojišti a může přijímat informace ze všech ostatních senzorů, pokud by to bylo potřeba. To nás vede k jedné z nejsložitějších otázek z hlediska bezpečnosti a to jak takové informace distribuovat.

2.2.1 Operační systém

Přestože preferovaným systémem pro vojenské systémy velení a řízení je stále ještě windows 7 (psáno v únoru 2021), v praxi se v omezené míře můžeme setkat s různými variantami OS windows a Linux a Android. Zatímco v případě windows jsou v armádě přesně stanoveny způsoby nastavení pro jednotlivé verze, pro OS Android, taková direktiva neexistuje. V rámci kompletů ISR, které jsou dodávány, jako funkční celek spoléhá v tomto ohledu plně na externího dodavatele.

2.2.2 Software

Software pro využití v rámci DSS se dá logicky členit do dvou kategorií obslužný software pro periferie a software pro velení a řízení/SA.

V případě obslužného softwaru pro periferie a zpracování dat se jedná zpravidla o software interagující se senzory, jako jsou JIM, JIM compact, Moskito IT, bezpilotními prostředky (UAV a UGV). Obslužný software pak umožňuje jejich nastavení a příjem dat z těchto senzorů. Dále se může jednat o software na úpravu multimediálního obsahu zachyceného senzory. V praxi je pouze malé množství zachycených dat vhodné pro okamžité sdílení na nadřízený stupeň.

Vzhledem k tomu, že moderní komunikační prostředky jsou tzv. softwarová rádia, je nutný také software pro ovládání a nastavení komunikačních prostředků. Softwarové rádio často označované zkratkou SDR (software defined radio) představuje evoluci v rámci radiotech-

niky. Zatímco starší rádia byly tvořeny oddělenými hardwarovými bloky pro modulaci, směšování, zesílení a podobně. Dnes je mnoho z této funkcionality převzato procesorem rádia a řízeno softwarově. To umožňuje větší míru funkcionality například z hlediska používání modulace a kódování, než starší typy rádií, které byly omezeny například fyzikálními vlastnostmi instalovaného modulátoru. Zároveň je ovšem komplikovanější zabezpečit jejich nastavení prostřednictvím přepínačů a tlačítek na samotném těle rádia – proto je potřeba některé parametry nastavovat prostřednictvím obslužného softwaru.

2.2.3 Informační systém

Z hlediska definic zákonů 412/2005 Sb. a 181[5] [20] by měly prostředky v systému sesednutého vojáka být informačním systémem. Informační systém by však měl být jednoznačně popsán, spravován a řízen. Současné použití tomu úplně neodpovídá. Chybí jeho jednoznačný popis a standardizace. Je potřeba si uvědomit, že oproti standardním počítačovým sítím jak je známe dnes, se jedná o nody propojené poměrně pomalými a v mnoha případech i nestálými komunikačními kanály. Výměna informací v takovém prostředí musí být poměrně dobře řízena, aby nedocházelo k zahlcení sítě. Další problematikou je nastavení přístupu v rámci systému – tedy kdo k jakým informacím a k jaké komunikaci má mít přístup, zvlášť pokud by došlo k nasazení DSS v utajovaném režimu. Je rovněž také potřeba definovat důkladně přenosové prostředí, které může sestávat z řady různých prvků, které využívají značně odlišné přenosové protokoly.

2.3 Senzory C4ISTAR

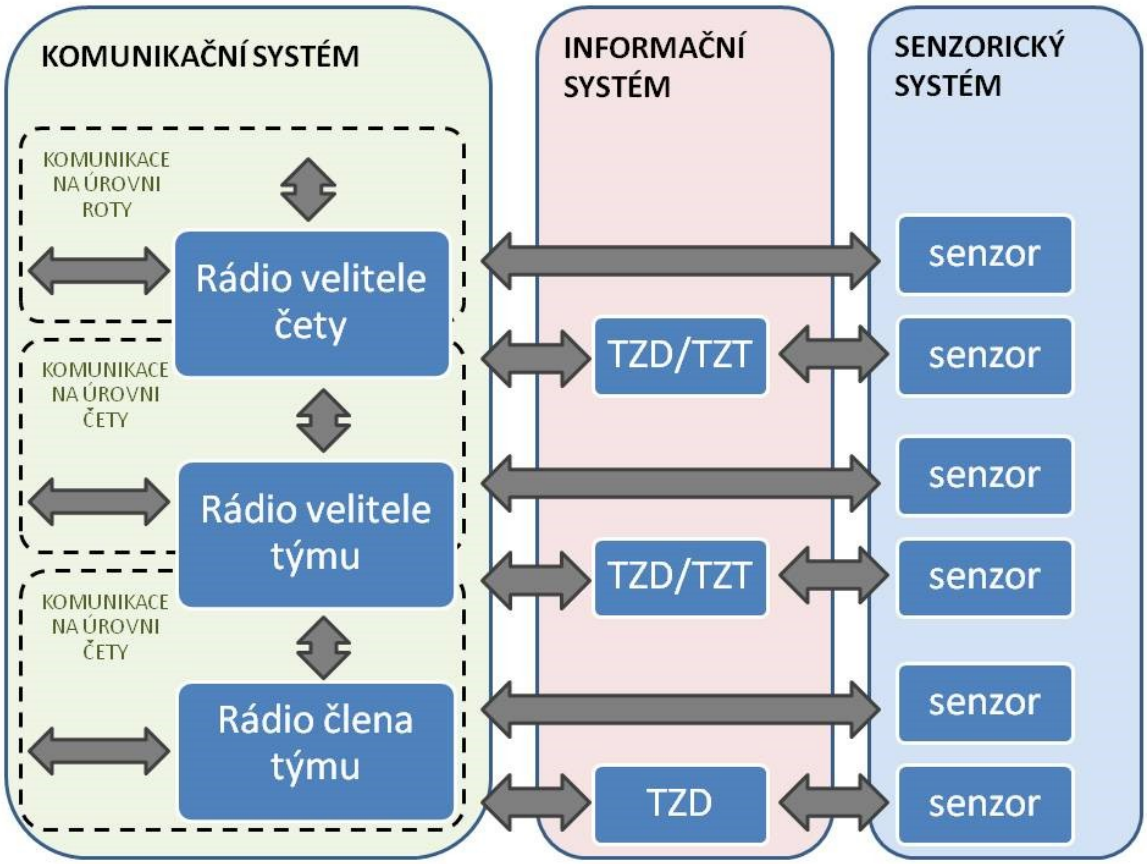
V rámci své činnosti na bojišti využívají vojáci celou řadu různých přístrojů, od prostého dalekohledu, či buzoly po složité pozorovací přístroje schopné zaznamenávat jak termovizní obraz, tak polohu GPS, naměřenou vzdálenost k pozorovanému objektu a tyto informace přenášet pomocí bluetooth nebo IP protokolu přes WIFI či ethernet.

Přestože tyto zařízení umožňují větší efektivitu směrem k SA, znamenají také dodatečnou nesenou zátěž, zvýšené nároky na zdroje elektrické energie a v neposlední řadě také bezpečnostní riziko, neboť se jedná o zařízení, které ukládá informace a je schopno je vysílat v mnoha případech i bezdrátově.

[5] Zákon 181 hovoří primárně o kritické infrastruktuře, kam se nedá DSS jednoznačně zařadit, nicméně logicky bychom některá ustanovení tohoto zákona mohli brát v potaz a vycházet z nich.

2.4 Systém sesednutého vojáka (DSS)

Pomineme-li komponenty nesouvisející s kybernetickou bezpečností, zařízení v rámci DSS, která vyžadují pozornost, tvoří z mého pohledu tři skupiny prvků, které spolu vzájemně interagují. Na Obrázku 1 můžete vidět ideové schéma těchto skupin. Každá šipka reprezentuje určitou formu komunikace, která by měla být přesně definována, co se týče použitých protokolů, přípustných dat, procesů do kterých je tato komunikace zapojena a podobně.



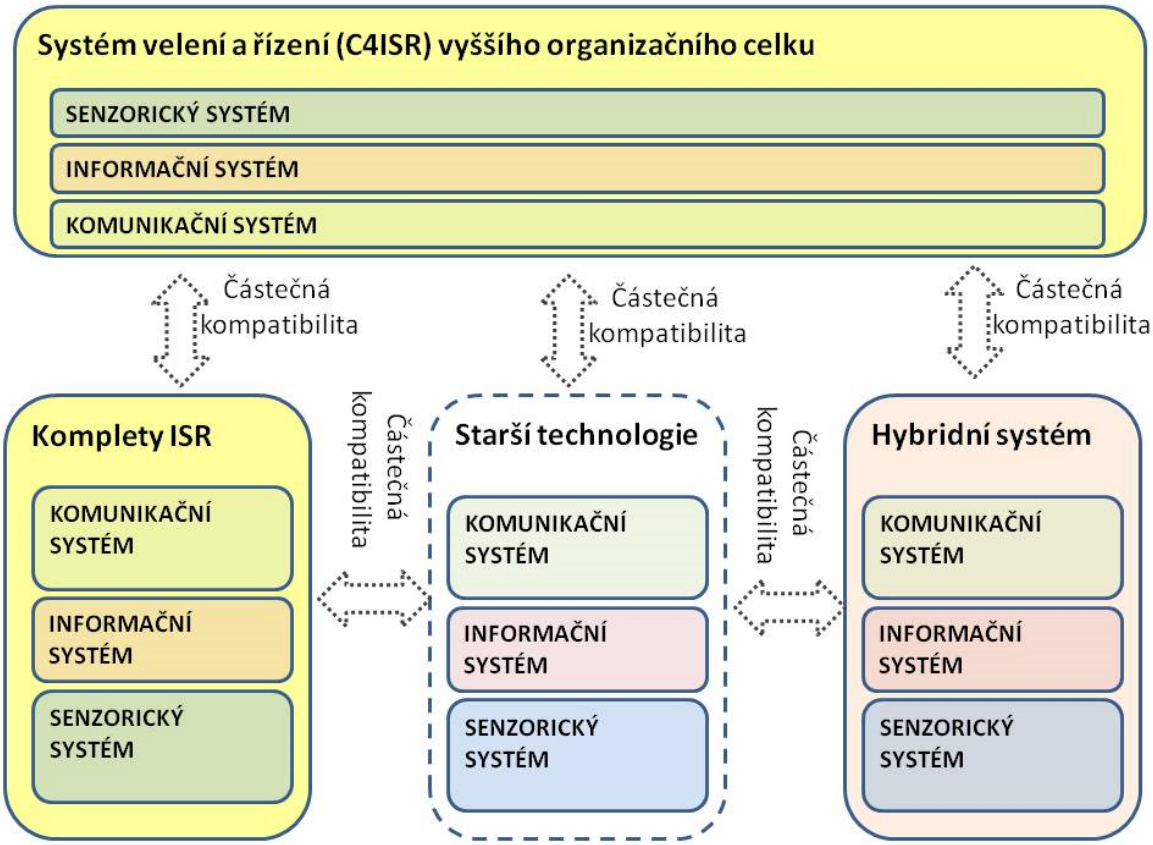
Obrázek 1 Komunikace v rámci DSS

V současné praxi ovšem taková funkční definice v rámci AČR neexistuje. Nenašel jsem ani veřejně ani neveřejně přístupný popis systému sesednutého vojáka pro AČR. Jediným vodítkem je tak soubor Českých obranných standardů, který je ovšem zaměřen na popis interakce systému vojáka jednoho členského státu NATO k systémům vojáka jiného státu v rámci NATO, případně mimo NATO. ČOS se tak zaměřuje především na řešení spojení mezi různými systémy DSS.

Nejblíže k popisu systému mají popisy kompletů ISR, které dodává do armády firma PRAMACOM – HT [2]. Tyto komplety mají sloužit jako celistvý systém pro sesednuté jednotky v různých provedeních dle zaměření/odbornosti jednotek (komplet pro průzkum, letecké návodčí (FAC), bojové družstvo). Samy o sobě tyto komplety fungují, jako DSS obsahují radiostanice, senzory, power-management systém, batohy, TZD a TZT už vybavené softwarem včetně Pramacomem vyvinutého softwaru MyVector pro velení a řízení a SA. Jedná se ovšem o izolované komplety – nejsou ve výbavě celé armády a není popsána kompatibilita s dalšími prvky, které nejsou součástí těchto kompletů (dle mých informací tato kompatibilita nebyla ani požadována). Nejpodstatnější je neexistující propojení se softwarovými produkty nasazenými v rámci systému velení a řízením vyšších stupních organizačního řetězce AČR. Pro pozemní síly AČR dodává softwarové aplikace pro velení a řízení firma ICZGROUP [21], která mimo jiné dodává i software pro sesednutého vojáka určený pro TZD na bázi OS android – BADIAN, který ovšem není kompatibilní se softwarem MyVector. V praxi se pak můžeme setkat s různými kombinacemi nasazeného hardwaru a softwaru, který je však často pouze částečně kompatibilní. Zpravidla se dá zjednodušit situace na tři varianty.

- Jednotky jsou nasazeny s kompletním dedikovaným DSS systémem (zpravidla komplety firmy PRAMACOM)
- Jednotky jsou nasazeny se starším vybavením často pouze s komunikací na bázi jednoduchých radiostanic neumožňujících sofistikované šifrování ani datové přenosy. Je otázkou zda v se v tomto případě dá hovořit o DSS.
- Jednotky jsou nasazeny s kombinovaným systémem, kdy jsou využity komponenty z kompletů určených pro DSS a různé komponenty, které nejsou součástí žádného dedikovaného systému, případně se dají využívat mimo svůj určený systém. Pro představu se může jednat o družstvo vybavené starými typy radiostanic umožňujícími pouze hlasovou komunikaci na úrovni týmu, pozorovacím přístrojem z kompletu ISR a přenosným PC s radiostanicí umožňující datový přenos na nadřízeného, obé vyjmuto z vozidla.

Samozřejmě při nasazení velkých celků dochází ke kombinaci všech těchto variant naráz a vznikají různé varianty propojení a použití na základě okamžité potřeby. Automatizace datových přenosů v takovém případě není možná a na místě velení musí dojít k manuálnímu přenosu získaných údajů do jednoho systému. Detailní popis těchto řešení není v podstatě možný, neboť se neustále mění podle aktuálních možností a potřeb.



Obrázek 2 Současný stav KIS sesednutého vojáka v AČR

Nezjistil jsem, že by byl někde detailně popsán systém, jakým způsobem by měla data prostupovat celým systémem, jaké formáty dat jakým uživatelům náleží a podobně. Určitým způsobem musela být analýza rozpracována, alespoň částečně, neboť software společnosti ICZGROUP umožňuje pracovat s přednastavenými typy uživatelů, kteří mají k dispozici různé typy definovaných formulářů k vytváření zpráv a obsahu v rámci samotného softwaru.

Zároveň dokument ČOS obsahuje definici zpráv, které by měly být vyměňovány mezi jednotlivými DSS aliančních stran participujících na společné operaci, k čemuž by ovšem měla sloužit tzv brána JDSS. JDSS gateway má být zařízení nebo software umístěný logicky mezi systémy DSS spolupracujících stran, jejich datové formáty tedy nemusí být kompatibilní přímo:

„Brána JDSS poskytuje funkce pro výměnu následujících informací:

• Pozice;

• Identifikace;

• Kontaktní hlášení;

• Všeobecné informace;

• CASEVAC požadavek;

• CBRN zprávy;

• Zákres;

• Další vrstvy (volitelně).

Výměna interoperabilních informací JDSS musí být chráněna stupněm utajení NATO Restricted. Některé členské státy NATO nemají národní bezpečnostní ekvivalent pro klasifikační stupeň NATO Restricted. Průvodce národních ekvivalentů stupňů utajení je uveden v ČOS 589502 – Bezpečnost.“ [4, s. 12, 15]

Zároveň je ovšem patrné, že armáda nedokázala nadefinovat výměnu informací mezi systémy a to ani ve vlastní výbavě. Software firem ICZ Group a Pramacom si nedokáže vyměňovat zprávy ani sdílet informace, přestože takový prostup není nemožný, a dle mé profesní zkušenosti ani příliš složitý. Mohlo by se jednat o pouhé standardizování formulářů pro stanovená hlášení uvedená výše a to včetně definice jejich podoby a způsobu přenosu na všech vrstvách modelu OSI. Ideální by byla přímá implementace standardizovaného formátu datové zprávy dle STANAG 5525, na kterou odkazuje ČOS 589501 [4, s. 9] a měl by zajistit kompatibilitu v rámci NATO. U NATO taková standardizace evidentně existuje a krom zmíněného STANAGu je popsána i protokoly APP-11 a ADatP-3 [22].

V tuto chvíli se zdá, že zmiňovaný soubor norem ČOS není dostatečným popisem problematiky – zabývá se propojením různých DSS, a ne vlastní definicí DSS. Zároveň však nedochází k jeho důsledné implementaci v rámci systémů AČR. Jeho vhodná implementace by mohla sloužit k propojení mezi vlastními technologiemi. Současně mezi vlastními systémy nemáme žádnou kompatibilitu a informace se mezi systémy manuálně přepisují.

2.5 Bezpečnost

V této sekci nemohu podat o mnoho víc než vlastní zkušenosti. Přestože existuje řada dílčích požadavků na bezpečnost komunikace na úrovni sesedlého vojáka. Celý systém je dle mých zkušeností u pozemních sil v neurčitém stavu. V rámci ČOS 589502 je odkazována řada dokumentů, které by mohly sloužit jako východisko pro definování bezpečnosti, mezi

jinými se jedná o studii NIAG Study SG123 Annex B, která definuje bezpečnost v interoperabilním prostředí a dokument AC/35-D/1020 „Přehled základních hrozeb a slabých míst CIS“, který je bohužel utajovaný. ČOS také definuje požadavek ze strany NATO, aby systémy DSS měly v rámci aliance schopnost přenášet informace minimálně o stupni utajení vyhrazené [6, s. 9]. Jinými slovy je požadován systém akreditován příslušným úřadem (v našem případě NBÚ a NÚKIB) pro přenos utajované informace do stupně utajení vyhrazené. V praxi máme radiostanice akreditované pro přenos utajované informace. Máme rovněž akreditované informační systémy velení a řízení pro zasazení na velitelstvích. Chybí ovšem akreditovaný systém sesedlého vojáka s TZT nebo TZD, které by byly schopny přenášet a zobrazovat utajované informace a poskytovat spojení s utajovanými systémy míst velení. Sesedlý voják tak může z bojiště přenášet utajovanou informaci pouze hlasovým kanálem. Přes všechny dostupné dokumenty zpracované z úrovně NATO nebo EDA není AČR schopna zpracovat návrh architektury vlastního DSS k akreditaci na příslušný stupeň utajení. Bohužel nejsou volně dostupné a jak jsem zmiňoval již výše způsob distribuce zvláště utajovaných informací v AČR je nedostatečný.

Samozřejmě bezpečnost v rámci DSS je aplikována a existuje celá řada organizačních a technických opatření, k zachování bezpečnosti komunikačních a informačních systémů, které tvoří součásti DSS, ale nejsem si vědom existence souhrného popisu systému, který by popisoval architekturu, stanovoval role a procesy v rámci DSS AČR.

DO Českého obraného standardu je zakomponován požadavek, aby vždy při plánování operace byla dohodnuta činnost na možné nepředvídatelné události a jako příklad jsou uvedeny následující případy:

- „Ztráta nebo narušení brány JDSS/zapůjčené radiostanice;
- Nefunkční brána JDSS/zapůjčená radiostanice;
- Výběr zpráv, u kterých budeme vyžadovat potvrzení;
- Starost o spolehlivost sítě.“ [4]

Rovněž je zde spousta bezpečnostních restrikcí ve spojovacích příručkách, které vychází z imperativu „Nepřítel naslouchá“. Například je zakázáno v otevřené řeči přenášet komunikačními prostředky jakékoliv citlivé informace o počtech, pozicích, úkolech a podobně. Za tímto účelem jsou používány různé způsoby kódových označení a jednoduchých šifer založených často na transpozici.

Bezpečnost je tedy evidentně brána v potaz, v praxi se však setkávám s nedůslednou aplikací takovýchto zásad. Jejich aplikace totiž není tak jednoznačná jak by se zdálo na první pohled. Standardizovaný postup u moderních stanic, které zpravidla využívají zabezpečení spojení prostřednictvím kryptografických algoritmů se sdílenými kryptografickými klíči je, že voják, jemuž bude hrozit zajetí, popřípadě bude muset zanechat stanici například v poškozeném vozidle, provede nouzové vymazání uložených klíčů a provozních údajů. Takový postup je považován za bezpečný. V praktickém výcviku se ovšem takové scénáře cvičí velmi zřídka a pro vojáky je problematické takové vymazání provést ve správnou dobu. Vymazání nelze provádět při prvním kontaktu s protivníkem – pořád je potřeba spojení. Při zajetí nebo vážném zranění je ovšem pozdě. Smazání stanice se mi tak jeví jako dobrá možnost, ale ne dostačující bezpečnostní prvek a k němu navázaný proces.

V případě použití TZT nebo TZD je vyžadováno šifrování HDD, ale například v případě android zařízení je šifrování HDD složitější. V rámci bezpečnosti sesedlého vojáka je komplikované navrhnout nezávadný systém s ohledem na možnost zajetí vojáka i s veškerým vybavením. V takovém případě je možné využít mučení k zjištění hesla do systému a šifrování bude bez efektu. Zajímavou možností by bylo použití šifrovacího systému, který by umožňoval při zadání speciálního hesla systém smazat. Nemám ovšem na mysli smazání prostřednictvím zadání chybného hesla, které je implementováno například v některých zařízeních apple. Mluvím o systému, kdy je uživateli vydávána dvojice hesel, jedno heslo pro autentizaci druhé pro smazání, tzv panické, případně duress heslo. Takové systémy jsou známy a mohou využívat různých principiálních schémat fungování, viz studie: „Panic Passwords: Authenticating under Duress“ [23]. Podobný postup je u armád zaveden v rámci hlasové komunikace, kdy užití speciálního kódu nebo fráze voják signalizuje protistanici, že vysílá pod donucením nepřítele.

2.6 Shrnutí kapitoly

Je patrné, že současný stav je neuspokojující vzhledem k požadavkům partnerů a vlastních stanovených cílů. Ze všeho nejvíc je ovšem potřeba v rámci DSS pro AČR zpracovat koncepci, která by pokrývala všechny požadavky a to jak funkční tak bezpečnostní. Současný stav, kdy probíhá živelné ad hoc kompletování různých technologií může určitým způsobem plnit funkce, nicméně nelze zachovat vyžadovanou bezpečnost.

3 HROZBY A RIZIKA DSS Z HLEDISKA KYBERNETICKÉ BEZPEČNOSTI

V této části se budu zabývat možnými riziky a to prostřednictvím fault tree analýzy. Tato analýza nám umožňuje hledat kořenové příčiny problému. V pojetí této práce můžeme stanovit několik základních hrozeb, které vychází z účelu samotného systému DSS. Těmito základními hrozbami jsou ztráta funkce, kompromitace systému a kompromitace utajované informace.

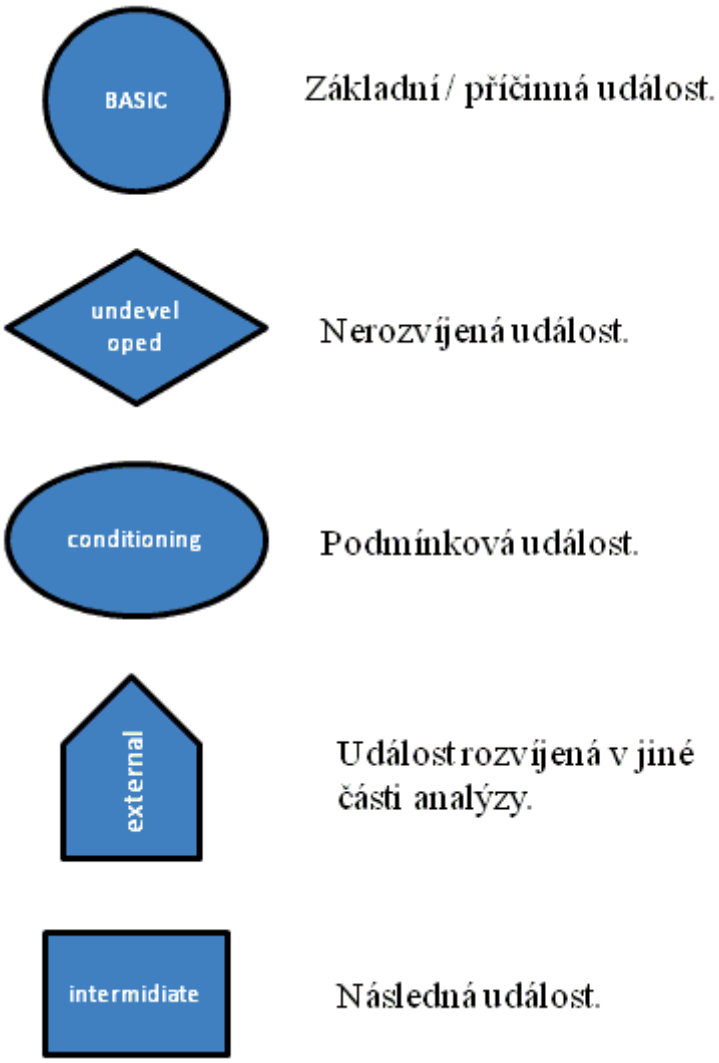
Vzhledem k neuspořádanému současnému stavu, kdy nelze určit jednoznačnou architekturu systému, je mnou prováděná analýza zaměřena obecněji. Předpokládám, že v rámci návrhu architektury DSS bude nutné provést detailnější analýzu rozpracovanou až k jednotlivým přenosovým protokolům, konkrétním zařízením a činnostem.

3.1 Fault tree analýza

K identifikaci možných závad nebo havarijních stavů je možné využít analýzu stromu poruch. Principem této analýzy je logicky odvodit možné příčiny nežádoucího stavu a prostřednictvím logických operátorů je graficky popsat. Pro tuto práci jsem se rozhodl použít FTA pro identifikaci rizik systému sesednutého vojáka.

Po prostudování mnoha variant jsem zjistil, že používané symboly u tohoto typu analýzy se mírně liší, ale základní operátory OR a AND, kruh pro základní (případně příčinnou událost) a obdélník pro rozvíjené události jsou neměnné. Pro mé účely jsem se rozhodl zahrnout i symboly pro nerozvíjenou událost, podmínkovou událost a událost rozvíjenou v jiné části analýzy.

3.1.1 Druhy událostí



3.1.2 Druhy operátorů

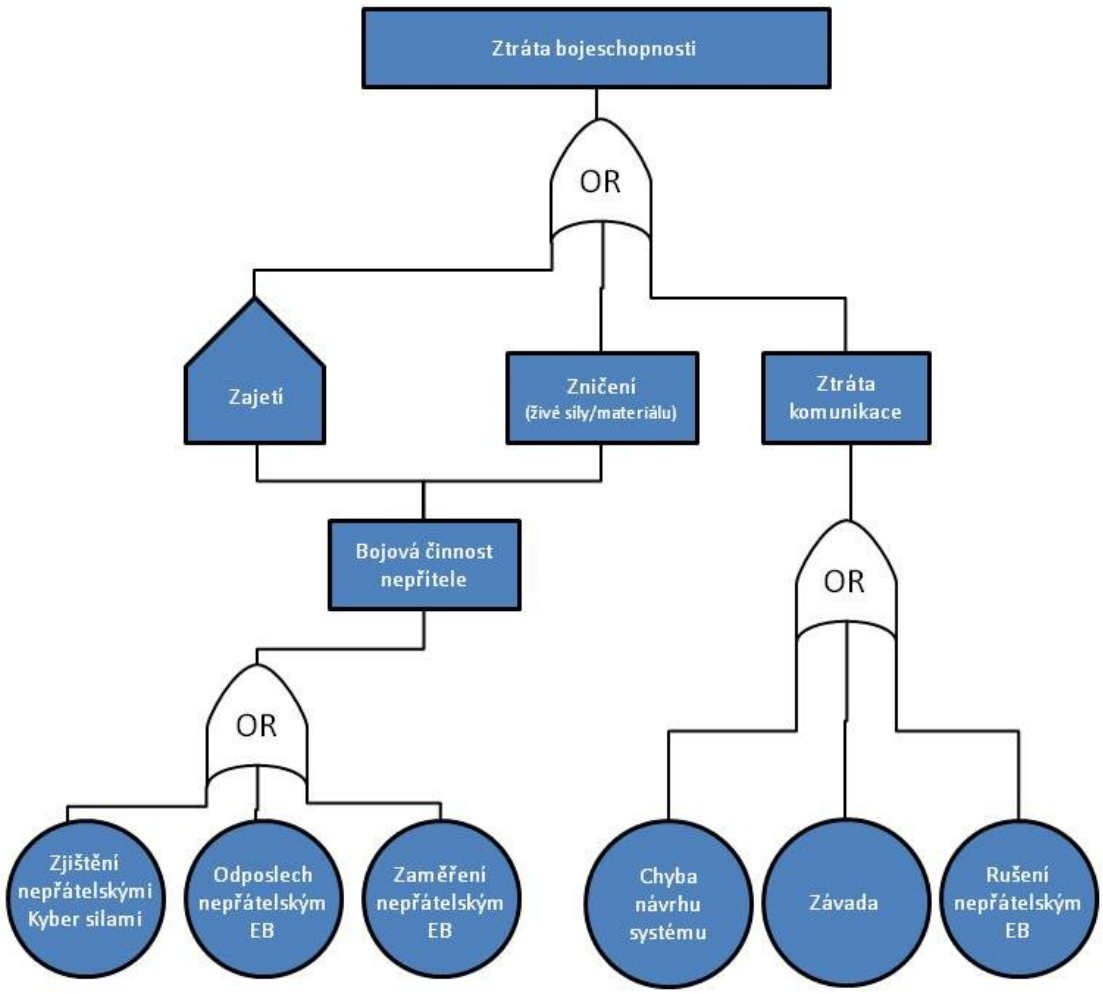
Logický součin.

Událost na výstupu existuje pokud nastanou všechny události vstupu.

Logický součet.

Událost na výstupu existuje pokud nastane jedna z událostí na vstupu.

3.2 Hrozba ztráty funkce



Ztráta funkce je zde myšlena ve vztahu k celému systému a tím pádem i k bojeschopnosti (schopnosti plnit stanovený úkol) vojsk užívajícího tento systém. Ztráta funkce pozorovacího přístroje tak nutně nemusí znamenat ztrátu bojeschopnosti.

Může být důsledkem činnosti, nepřítele, závady, nevhodného použití, nebo kombinací.

Může být ztracena funkcionalita části systému, nebo celého systému co se týče jednotlivce nebo celku. Dle mého názoru můžeme rozlišit několik základních scénářů.

- Je ztracena funkcionalita části vybavení, ale zachována schopnost plnit stanovený úkol a komunikovat. Je možnost potvrdit splnění úkolu, zpřesňovat úkol a obdržet nové úkoly.
- Je ztracena funkcionalita části vybavení, včetně komunikace, ale zachována možnost plnit stanovený úkol – je nemožné potvrdit, zda byl úkol splněn, případně obdržet nové úkoly.

- Je ztracena funkcionalita části vybavení, včetně komunikace není možné plnit úkol ani potvrdit, že nedojde k jeho splnění.
- Je ztracena funkcionalita části vybavení, ale zachována schopnost komunikace. Je možnost potvrdit nesplnění úkolu, a obdržet nové úkoly.

Tyto scénáře ilustrují důležitost komunikace a mohou nás vést návrhem DSS tak, aby byla pojištěna funkcionalita technických prvků, které jsou nezbytné pro zachování požadovaných schopností. Samozřejmě pro různé typy úkolů bude podstatné zachovat jiné schopnosti. Komunikace se ovšem rozhodně jeví jako základní a nezbytný prvek a celá logika systémů jako C4ISTAR je postavena na základě rozvíjení C2 dále.

3.2.1 Ztráta funkce činností nepřítele

Elektronický boj má jako jeden z hlavních cílů narušení schopností nepřítele prostřednictvím elektromagnetického rušení. To může mít za následek:

- Neschopnost komunikace nebo její omezení;
- Ztrátu možnosti navigace GPS, GLONAS…;
- Ztrátu funkce elektronických systému zaměřování a navádění;

3.2.2 Závada

DSS může být značně komplikovaný, což představuje velké množství možných poruch. Je potřeba si uvědomit, že se jedná o systémy, které vojáci přenášejí v batozích, nosných systémech na vestách a vykonávají s nimi celou řadu činností včetně seskoku padákem. V některých případech dochází k opakovanému připojování a odpojování konektorů, ukládání kabelů do kapes a pouzder. Zároveň mohou být vojáci v poli dlouhou dobu a může dojít k vyčerpání zdrojů elektrické energie. Technika i obsluha musí fungovat v extrémních teplotách a v různých světelných podmínkách. Pokud jste někdy v noci po tmě tápali při připojení nabíjecího kabelu telefonu, představte si, že musíte být schopni připojovat různé typy zařízení po tmě v hlubokém mrazu a časové tísni.

Příklady možných rizik poškození a závad:

- Poškození neopatrnou manipulací;
- Poškození nárazem při přepravě;
- Opotřebení užíváním – například zlomení kabelu opětovným ohýbáním;
- Koroze kovových součástí;

- Zkrat v důsledku přítomnosti vody (přestože zařízení splňují normu IP 67 může dojít k poškození konektoru nebo celého zařízení pokud se dostane voda nebo vzdušná vlhkost do spojů koncovek);
- Nedostatečné napájení.

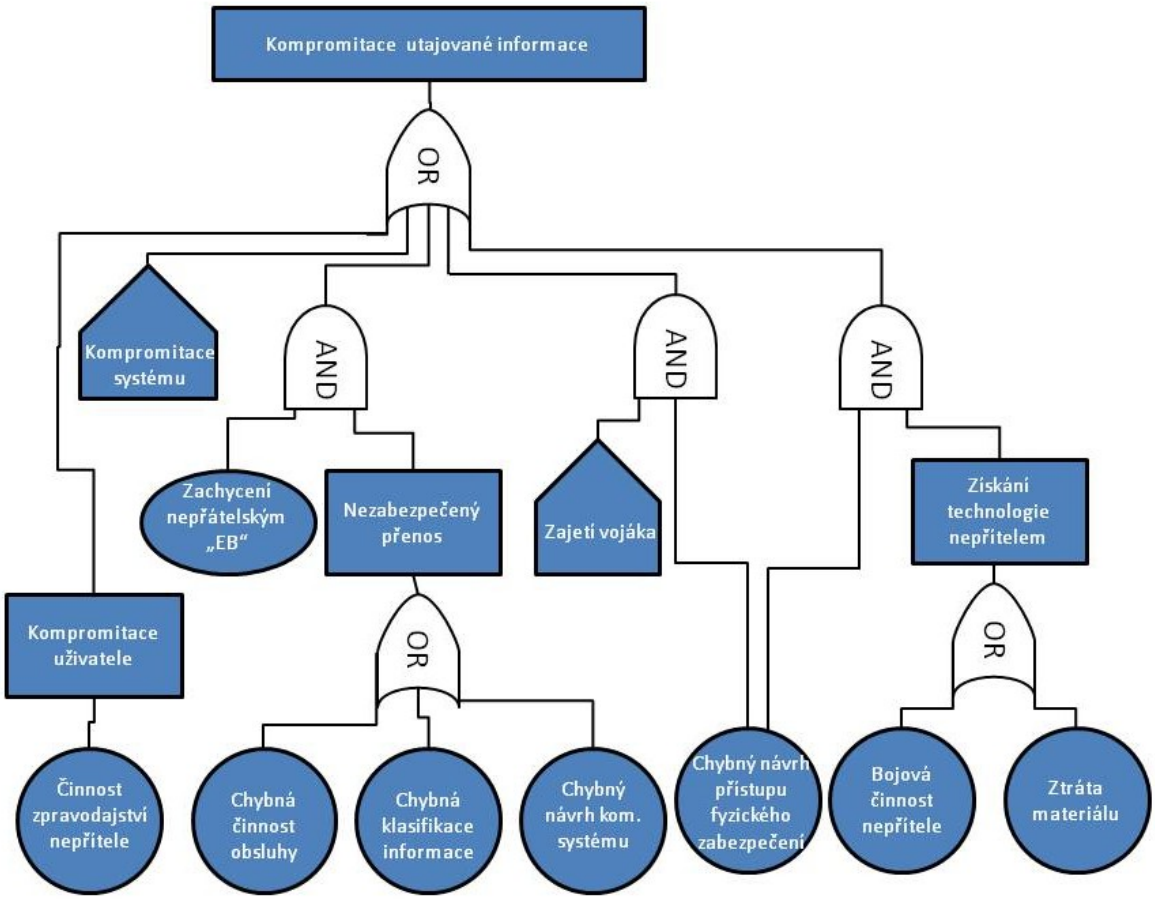
3.2.3 Riziko „decreased reality“

Zatímco velké množství koncepcí moderního vybavení vojáka počítala s nějakou variantou koncepce rozšířené reality, v praxi by mohlo docházet k opačnému efektu. Praktická zkušenost specialistů zabývajícím se C4ISTAR s výcvikem s novým vybavením byla, že vojáci byli omezováni díky výbavě. Na začátku výcviku se smartphony s taktickou aplikací, kde mohli sledovat své vzájemné polohy, postupovali při přesunech velmi pomalu, neboť věnovali přílišnou pozornost displejům s modrými tečkami označujícími na mapě polohu jejich kolegů, přestože by ve většině situací stačilo sledovat vizuálně své okolí a nejbližší spolubojovníky. Vzhledem k omezené senzorické kapacitě člověka je otázkou nakolik může docházet ke skutečnému zlepšení výkonu a na kolik je reálné riziko sníženého výkonu na základě senzorického zahlcení. V určitých ohledech odkazuji na podobný princip, jako můžeme shledat u autonehody způsobené nepozorností při přelaďování rádia.

Druhým aspektem, na který bych chtěl upozornit je, že příliš složitý systém vyžadující rozsáhlý výcvik ubírá na výcviku z jiných oblastí. Mluvíme-li o sesedlém vojákovi bavíme se o člověku, který musí zvládnout poměrně rozsáhlou paletu dovedností, většinu z nich je potřeba pravidelně aktivně udržovat. V případě speciality C4ISR musí nepočítaje udržování fyzické kondice zvládnout střelbu z více typů zbraní, topografii, taktiku, dovednosti v oblasti přežití, skrytého pohybu, pohybu v noci, znalost techniky a uniforem cizích armád, práce s výbušninami, ovládání několika typů radiostanic, práce v os windows, linux a android a potřebným sw (který se samozřejmě mírně liší mezi jednotlivými OS), několika typy pozorovacích přístrojů, základní ovládání bezpilotních prostředků, výsadkovou přípravu, velká část z těchto vojáku také řízení vozidel v terénu. Takový objem znalostí a dovedností představuje rozsáhlou přípravu a neustálé opakování. Riziko je tedy:

- Neschopnost vykonávat požadované činnosti při častém střídání personálu.
- Neschopnost ovládat technologie, při časté technologické obměně.

3.3 Hrozba kompromitace utajované informace



Ztráta, či prozrazení utajované informace je bezpečnostním incidentem dle zákona 412/2005 Sb. a z něj odvozených směrnic v rámci AČR. Krom tohoto faktu se jedná o hrozbu pro probíhající operace, ostatně to je důvodem pro utajení informace. Utajované informace, se kterými se může setkat sesednutý voják, jsou informace o vlastních jednotkách, informace o plánovaných činnostech, ale také informace, které jsou součástí samotného DSS – provozní údaje v radiostanicích, IP adresy zařízení, přístupové údaje a podobné.

Mým předpokladem je, že tak jako je při zajetí nepřátelského vojáka jednou z procedur jeho výslech, do budoucna se stane běžnou procedurou analýza veškerého vybavení a pokus o extrakci dat. Cílem mohou být zprávy uložené v TZT, nebo TZD, polohy vlastních jednotek uložené v rámci taktických aplikací, provozní údaje a další. V tomto případě je naprosto nevhodné používat k zabezpečení OS otisk prstu nebo rozpoznání obličeje. Přesto, že je takové zabezpečení stále běžnější při civilním užití pro vojenské účely je naprosto nevhodné, neboť může sloužit k odemčení zařízení i v případě zabití vojáka, nehledě na

nepraktičnost spojenou s užíváním různých ochranných pomůcek jako jsou brýle, rukavice a přilby.

V případě získání kompletního přístupu k vybavení je samozřejmě možný pokus o kompromitaci nepřátelského systému. Moderní systémy jsou konstruovány tak aby měly funkci nouzového vymazání paměti, která by měla zajistit, že se nepřítel nedostane k provozním údajům a použitým šifrám. Jak už je zmíněno výše, je potřebné, aby byli vojáci cvičeni k nouzovému výmazu, případně destrukci jakéhokoliv materiálu, který by mohl obsahovat citlivé údaje a to včetně materiálu mrtvých spolubojovníků, případně v opuštěných vozidlech. Materiál, který nejde smazat nebo vzít sebou lze zničit úderem pažby, prostřelením nebo výbušninou.

V případě zajetí má voják možnost stanici smazat, pokud mu stanici okamžitě nezabaví. Zvlášť v případě umístění stanice ve vestě.

V případě, že ke kompromitaci klíče dojde, je poměrně složité takovou skutečnost zjistit. Nejvhodnější možnost je pravidelná obměna sdílených kryptografických klíčů a jejich vhodná distribuce. Rozdílné jednotky by měly ideálně používat různé kryptografické řetězce. Vize velkých MANET sítí je z hlediska rizika získání radiostanice nepřítelem problematická. Čím víc radiostanic v síti bude, tím bude síť robustnější, spolehlivější pro přenos informace po celém bojišti a odolnější proti rušení, ale také zranitelnější v případě ztráty jediné stanice. S rostoucí velikostí sítě bude také složitější jakýkoliv havarijní scénář, kdy by docházelo k obměně kryptografických řetězců.

Nezbývá tedy než důležité informace chránit ve dvou vrstvách. Šifrování přenosu je minimálním požadavkem, utajená informace by se dala chránit v případě hlasové komunikace dobře známým použitím dopředu dohodnutých transpozičních kódů a kódových slov. Datová komunikace by se dala chránit šifrováním v rámci programového vybavení. Vhodné provedení by bylo, aby komunikační software pro přenos zpráv umožnil definovat klasifikaci zprávy a pokud by se jednalo o utajovanou zprávu, byla by zpráva zašifrována pro přenos například veřejným klíčem příjemce. Zašifrována by pak měla být i v úložišti zpráv tak aby nebyla ani pro původce přístupná bez další úrovně autentizace. Takovou autentizací by mohl být například certifikát na nosiči oddělitelném od zařízení (smart card, USB paměťové médium). Voják by jej používal pouze při odesílání a přijímání hlášení prostřednictvím TZT a TZD. Při jiných činnostech by jej měl uložen na dostupném místě tak, aby jej v případě zajetí mohl zahodit, případně zničit ve vhodnou chvíli. Riziko, že v případě

zajetí nebo zabití protivníkem budou získány všechny potřebné komponenty ke kompromitaci utajované informace, by se tak značně snížilo.

Pokud by byl do systému zaveden princip asymetrických šifer, kdy každý příjemce a odesílatel by měli privátní a veřejný klíč, při zajeti by protivník získal pouze přístup ke zprávám pro příjemce, kterého zajal a zároveň jej může vyslýchat a při umístění na externí nosič, jak je zmíněno výše by i riziko získání bylo nízké. Při odebrání zabitému vojáku by pak v kombinaci s potřebou zadat heslo do zařízení TZD nebo TZT, byl průnik k informacím nepravděpodobný.

3.3.1 Unik informací sociálními sítěmi

Mírně mimo tématiku této práce je pak riziko sdílení nějaké informace prostřednictvím zařízení, které nespadá do samotného systému DSS. V rámci nařízení Ministerstva obrany mají vojáci zakázáno pořizovat fotografie a jakékoliv GPS záznamy v průběhu služební činnosti. Toto nařízení reaguje na fakt, že aplikace jako Strava nebo Garminconnect mohou poskytovat data o poloze vojáků. Na tento fakt upozornila média na počátku roku 2018 v souvislosti s odhalením cest na vojenských základnách v Afghanistánu, Sýrii a dalších prostřednictvím aplikace Strava.

V současné době jsou vojáci dostatečně poučeni, aby nepoužívali chytré sporttestery k zaznamenávání tras v rámci operací. Nicméně vzhledem k neustále rostoucí složitosti kybernetického prostoru bude čím dál komplikovanější uchránit citlivé informace před sofistikovanou činností kybernetických sil. Zpravodajský sběr informací z otevřených zdrojů může být cenným zdrojem informací, které poskytnou vojáci nevědomě.

V průběhu jednoho mezinárodního cvičení v roce 2019, jsem zkoušel prohledávat internet a využíval jsem různé metody vyhledávání podle relevantních řetězců, podle místa sdílení a podobně. Na webu picuki.com, který umožňuje nepřihlášeným uživatelům prohlížet obsah sociální sítě Instagram jsem našel fotku slovenského vojáka s radiostanicí. Obrázek mám uložený v počítači, nicméně se mi jej znovu nepodařilo dohledat přesné URL. Na fotce sice není čitelná frekvence na displeji, ale vidíme USB, které značí Uper Side Band. Máme tedy znalost o typu používané radiostanice a částečně o modulaci signálu. Informace, které můžeme korelovat s dalšími zjištěními ze senzorů EB.

Obrázek 3 OSINT [24]

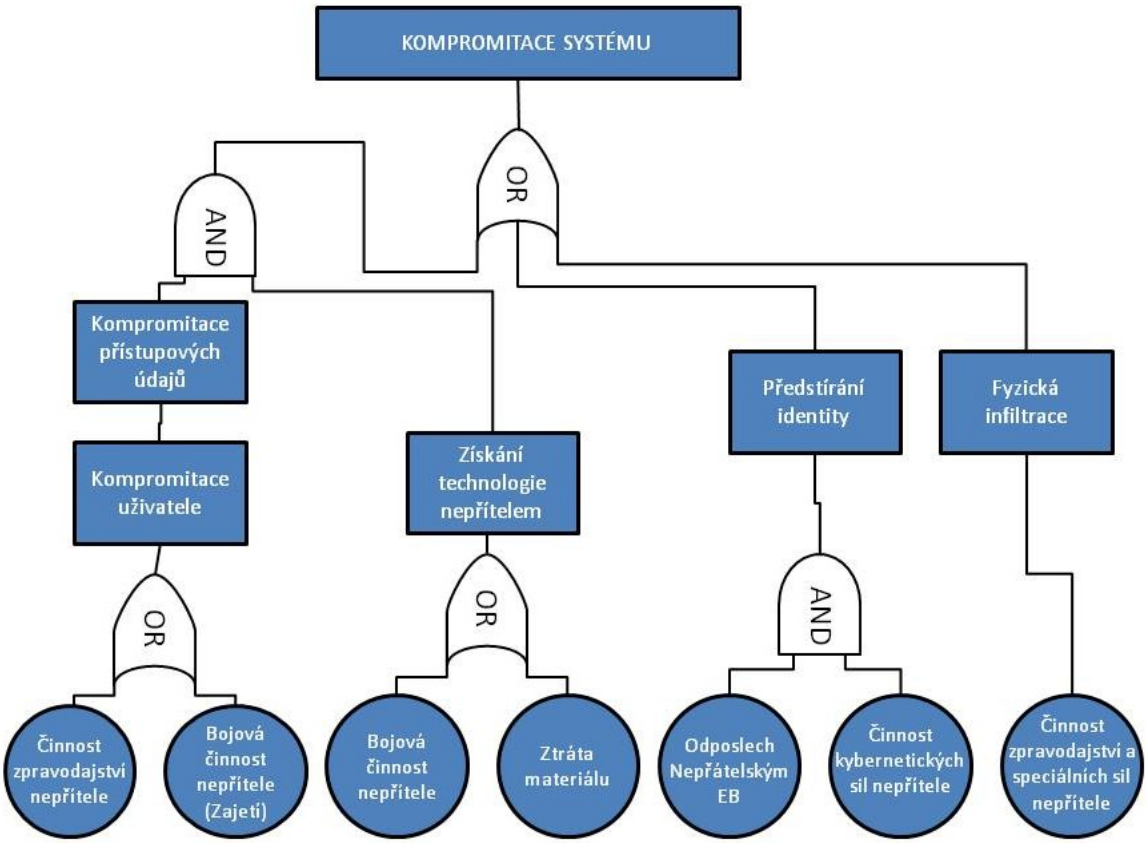
Toto je však příliš jednoduchý příklad. Kybernetický boj se může zaměřit na dlouhodobé sledování profilů vojáků na sociálních sítích a vytvářet pokročilé korelace z různých údajů. Sociální sítě například umožňují zobrazovat přibližnou polohu příspěvků. Naprosto nevinné příspěvky tak mohou vést ke kompromitaci informace o přesunu jednotky.

Kompromitované zařízení vojáka (například mobilní telefon s malwarem umožňujícím záznam zvuku) přítomné při přípravě nasazení může být rovněž problematické, i kdyby nebyly probírány utajované informace per se. Vojáci mohou diskutovat o trase, výzbroji počtu mužů a podobně. Do budoucna tak bude nutné, aby byly ošetřeny i tyto otázky – veškerá zařízení, která se připojují k veřejným sítím, budou muset být oddělena od jakých-

koli prostor, kde jsou probírány služební záležitosti, případně aby veškerá tato zařízení byla součástí vojenských sítí a byla monitorována důkladněji, než jsou osobní zařízení jednotlivých vojáků. V současné době se taková opatření dělají pouze u stupně utajení tajné a výše, ne každá citlivá informace je ovšem tajná. A z praxe vím, že je poměrně složité oddělit, co by mělo být utajováno a co ne.

Problém je také, že je poměrně těžké oddělit služební a osobní kyberprostor. Dokud jediný kontakt mimo vojenskou základnu byla pro vojáky telefonní linka. Bylo jednoduché se na několik minut soustředit na to, aby jednotlivec nemluvil o služebních záležitostech a bylo snazší provádět případnou kontrolu narušení bezpečnosti. Telefonní místnost byla prostorově oddělena od ostatních prostor a rozhodně nebyla místem, kde by se probíraly služební záležitosti. V současné době je na velkých základnách běžné, že mají vojáci vlastní elektroniku a dost příležitostí jak se připojit k internetu a všichni jsme zvyklí vše sdílet na sociálních sítích. Přítomnost elektroniky je tak běžná v našem životě, že je složité vytvářet návyky pro její omezení při vykonávání služebních činností. V případě nasazení do zahraniční operace by bylo ideálním řešením úplné omezení přístupu k jakékoliv osobní elektronice a elektronické komunikace prostřednictvím sociálních sítí po celou dobu nasazení. Takový postup je však těžko představitelný.

3.4 Hrozba kompromitace systému



Dobře známé útoky jsou falešné vysílání (v případě zjištění nepřátelských frekvencí a volacích znaků prostřednictvím EB), případně vysílání pod nátlakem (v případě zajetí vojáka), tyto můžeme považovat za jednoduché kybernetické útoky. Možnosti složitějších kybernetických útoků prostřednictvím komunikačních a informačních sítí vojsk nejsou příliš prozkoumány. Například riziko, že někdo odešle virus v prostředí taktické komunikace, bylo vždy považováno za minimální, polní komunikace končila u radiostanice a tablet nebo počítač v poli byl doménou speciálních sil. S rozšiřováním těchto zařízení se musíme připravit na rizika, která vychází z možnosti kompromitace některého z koncových zařízení vojáka v poli. Kompromitace systému by pak mohla vypadat různým způsobem, od zasílání falešných zpráv po infekci sofistikovaným malwarem. Přestože si nejsem vědom nějakého napadení systému vojenské taktické nebo strategické komunikace podobným způsobem, musíme s takovými hrozbami počítat. Předpoklad bezpečnosti na základě izolace je zde chybný - schopnost kompromitovat zdánlivě uzavřený systém existuje a byla ilustrována na příkladu stuxnetu [25].

3.1 Hrozby spojené s budoucími možnostmi EB

Závažným problémem by mohlo být nasazení prostředků schopných ničit elektronická zařízení. V současné době se s nasazením takových prostředků nesetkáváme, ale musíme předpokládat, že se stanou realitou. Dokladem může být analýza schopností Ruské federace k roku 2025, kde je uveden předpoklad vývoje prostředků se silným elektromagnetickým vyzařováním na bázi specializované munice a mobilních systémů [26]. Taková schopnost by byla velmi ceněná na bojišti stále více ovlivňovaném elektronikou. Představa zbraně ničící/zneschopňující elektroniku snadno dopravitelná kamkoliv na bojiště, je děsivá. Mnoho jednotek by bylo rázem učiněno nebojeschopnými. Takový bojový scénář má v určitých ohledech ještě větší dopad než přímé ničení živé síly. Často se zmiňuje, že v případě pěchotních min je jejich konstrukce zaměřena spíše na zranění, než zabití vojáka. Zraněného vojáka musí někdo nést, poskytnout mu lékařskou pomoc. Podobné by to mohlo být, pokud by velení náhle ztratilo veškerou komunikaci s jednotkami v určité oblasti a dotčené jednotky by nemohly komunikovat mezi sebou. Byly by zneschopněny některé zaměřovací systémy, moderní zbraňové a řídicí systémy vozidel – zmatek.

Jak se s takovou formou projevu EB vypořádat? Vyrobit komunikační prostředek nereagující na extrémní EM impulsy je velmi náročné, ne li nemožné. Jednotky by měly být vybaveny nějakou formou nouzového komunikačního zařízení schopného odolat jakýmkoliv poruchám EM spektra. Mohlo by jít o obyčejný satelitní telefon vybavený přenosným pouzdrem, které by fungovalo jako faradayova klec svého druhu. V případě poškození běžně používaného rádia by pak mohli vojáci vyjmout nouzové rádio z ochranného obalu a začít jej používat. Na rozdíl od klasického rušení by destruktivní EM prvky nemohly fungovat kontinuálně kvůli přílišné energetické náročnosti.

3.2 Shrnutí hrozeb a rizik v rámci DSS

Stanovení hrozeb a rizik je klíčové pro jakoukoliv bezpečnostní analýzu. Vždy bude otázkou jak detailně rozpracovat jednotlivé body. Mnou zvolená metoda stromu poruch nebyla pravděpodobně nejvhodnější pro daný problém, neboť existuje příliš mnoho vzájemných vazeb a závislostí, které je problematické znázornit, grafické znázornění tak ztrácí na přehlednosti.

Uvědomuji si, že mnou předestřené hrozby je možné rozpracovat do větších detailů – jedná se o skupiny hrozeb a rizik. Pro bezpečnostní analýzu návrhu systému DSS bude potřeba rozpracovat analýzu detailněji s ohledem na konkrétní architekturu. Rovněž bude nutné

jednotlivá rizika vyhodnotit. Metody hodnocení jako FMEA ovšem pracují například s pravděpodobností výskytu. Vzhledem ke specifičnosti tohoto systému a nemožnosti určit jak intenzivní nebo častá může být činnost kybernetických sil, bych se neodvážil sám některé hodnoty definovat. Osobně bych doporučoval mnou rozpracované rizika použit jako výchozí bod pro FMEA, kterou by vyplnila oslovená skupina odborníků v oblasti vojenských komunikací, EB a zpravodajství s požadavkem na vyhodnocení a případné doplnění. Následné zprůměrování bych považoval za směrodatné.

Důležité je uvědomit si, že aktivum život může být v pohledu armády v určitých případech podřízeno zachování funkce. Mohou být případy, kdy může být vědomě ignorováno riziko vedoucí k ohrožení života, aby byl splněn stanovený úkol. Například riziko: *zaměření polohy nepřátelským EB na základě zachycení EM emisí;* může být vědomě ignorováno, pokud jednotka vyhodnotí, že vysílání informace je důležité dostatečně na to, aby riskovali ohrožení vlastního života. Takové situace však nelze standardizovat a je potřeba při návrhu systému usilovat o minimalizaci všech rizik.

Tabulka 2 Hrozba ztráty funkce

HROZBA	RIZIKO	AKTIVA			
		život	Materiál	utajovaná informace	funkce
Hrozba ztráty funkce	Narušení činnosti v důsledku zaměření EB;	X	X	X	X
	Ztráta materiálu obsahujícího utajované informace;		X	X	X
	Snížení výkonu operátorů v důsledku senzorického zahlcení.				X
	Neschopnost operátorů ovládat v plném rozsahu DSS v důsledku nedostatečného výcviku.		X		X
	Neschopnost operátorů ovládat v plném rozsahu DSS v důsledku změn systému.		X		X
	Poškození neopatrnou manipulací;		X		X
	Poškození nárazem při přepravě;		X		X
	Opotřebení užíváním;		X		X
	Koroze kovových součástí;		X		X
	Zkrat v důsledku přítomnosti vody (přestože zařízení splňují normu IP 67 může dojít k poškození konektoru nebo celého zařízení pokud se dostane voda nebo vzdušná vlhkost do spoje);		X		X
	Nedostatečné napájení;				X
	Vzájemná nekompatibilita s vlastními nebo koaličními systémy;				X
	Rušení komunikačních sítí;				X
	Detekce/odposlech vysílání nepřátelským EB;				X
	Zaměření polohy nepřátelským EB na základě zachycení EM emisí;	X	X		X

Tabulka 3 Hrozba kompromitace systému

HROZBA	RIZIKO	AKTIVA			
		život	Materiál	utajovaná informace	funkce
Hrozba kompromitace systému	Narušení integrity systému falešným účastníkem nepřátelského EB a/nebo zpravodajských sil;			X	X
	Infikování systému malwarem na základě chyby uživatele;			X	X
	Infikování systému malwarem na základě kompromitace uživatele (vydírání, podplacení…);			X	X
	Infikování systému malwarem na základě zpravodajské / diverzní činnosti;			X	X
	Zneužití systému po konfiskaci hardwaru na bojišti. (ztráta, zabrání, zajetí);			X	X
	Získání přístupu ke kryptografickým klíčům nebo jiným provozním a přístupovým údajům;			X	
	Dešifrování / dekódování zabezpečení komunikačních systémů;			X	

Tabulka 4 Hrozba kompromitace utajované informace

HROZBA	RIZIKO	AKTIVA			
		život	Materiál	utajovaná informace	funkce
Hrozba kompromitace utajované informace	Dešifrování / dekódování zachycené zprávy;			X	
	Získání utajovaných informací kompromitací systému;			X	
	Získání utajovaných informací prostřednictvím konfiskaci hardwaru na bojišti;			X	
	Únik utajované informace při zajetí;			X	
	Únik utajované informace přenášené nezabezpečeně;			X	
	Únik utajované informace nevhodným sdílením mimo systém;			X	
	Únik utajované informace na základě kompromitace uživatele (vydírání, podplacení…);			X	
	Neoprávněné sdílení informace chybou obsluhy (porušení need to know);			X	
	Neoprávněné sdílení informace nevhodným nastavením systému (porušení need to know);			X	

4 NÁVRH VHODNÉHO POSTUPU A NASTAVENÍ K OMEZENÍ DETEKCE EB PROTIVNÍKA

Dle koncepce pro rok 2030 má být AČR schopna „..vedení nepřetržitého skrytého rádiového a radiotechnického průzkumu, zjišťování všech druhů radiolokátorů, identifikačních prostředků a navigačních zařízení. Budou schopny sofistikovaného zaměřování, identifikace a rušení spojovacích, datových a informačních sítí a navigačních systémů, včetně zajištění ochrany osob, vozidel, letounů a ostatních prostředků AČR. Bude dosažena schopnost vedení EB v oblasti navigačního válčení. V oblasti elektronického působení bude zabezpečena součinnost s KS, dosaženo schopnosti rušení nekomunikačních signálů a působení směrovanou energií.“ [27, s. 21]

Můžeme předpokládat, že schopnosti, které v rámci elektronického boje chceme dosáhnout my, bude dosahovat i potencionální nepřítel a v mnoha případech může dosáhnout vyšší úrovně schopností. Samozřejmě, ne všechny konflikty jsou vedeny proti technicky vyspělým oponentům, budování schopností by však mělo vždy vycházet z očekávání nejhoršího.

V této kapitole se budu zabývat primárně detekcí vysílače, tedy odhalením vysílání, určením jeho polohy a případnou korelací s dalšími vysílači ve stejné síti. To je základní schopností EB a umožňuje určit polohu, velikost a do určité míry i typ jednotek protivníka. EB a do budoucna i kybernetické síly mohou také usilovat o narušení integrity a důvěrností obsahu nepřátelských KIS. Prvotním krokem však bude pravděpodobně vždy detekce.

V následujícím textu se vyjádřím k jednotlivým činnostem nepřátelského EB dotýkajících se sesednutého vojáka a možnými opatřeními před působením na vlastní síly Zároveň bych rád poznamenal, že požadavky na ochranu před EB nebudou vždy shodné u různých druhů jednotek.

4.1 Zaměřování, identifikace spojovacích sítí

Jedna z nejběžnějších a nejstarších metod EB. Zaměření je prováděno různým způsobem například na základě triangulace změřeného signálu z různých přijímačů nebo na základě měření z jediného bodu pomocí specializovaných anténních těles a senzorů. V dnešní době se tyto technologie nespecializují výhradně na armádu, ale slouží i pro vyhledávání rušivých signálů v prostředích citlivých na vyzařování v elektromagnetickém spektru. Zajímavý přehled zařízení k zaměření elektromagnetického vyzařování byl zpracován jako průzkum trhu pro úřad Vnitřní bezpečnosti USA v roce 2019 [28].

Pro detekci vysílání je podstatné, jaký výkon bude mít vysílaný výkon od sesednutého vojáka na přijímači detekčního systému a samozřejmě citlivost tohoto přijímače. Výkon jaký bude vyslán na dané místo je závislý na volbě antén, poloze jednotlivých prvků vůči sobě a vlastnostem vysílaného signálu. Matematicky jsou tyto proměnné popsané v radiokomunikační rovnici:

$$P_{dp} = \frac{\mathrm{P_v G_v G_p}}{\mathrm{L_R}} |F|^2$$

P_{dp} – dosažitelný výkon na přijímané anténě;

P_v – vysílaný výkon;

G_v – zisk vysílací antény;

G_p - zisk přijímací antény;

F – činitel tlumení;

Lr – útlum volného prostoru $L_R = \left(\frac{4\pi R}{\lambda}\right)^2$;

R – vzdálenost od zdroje vysílání a přijímačem vysílání;

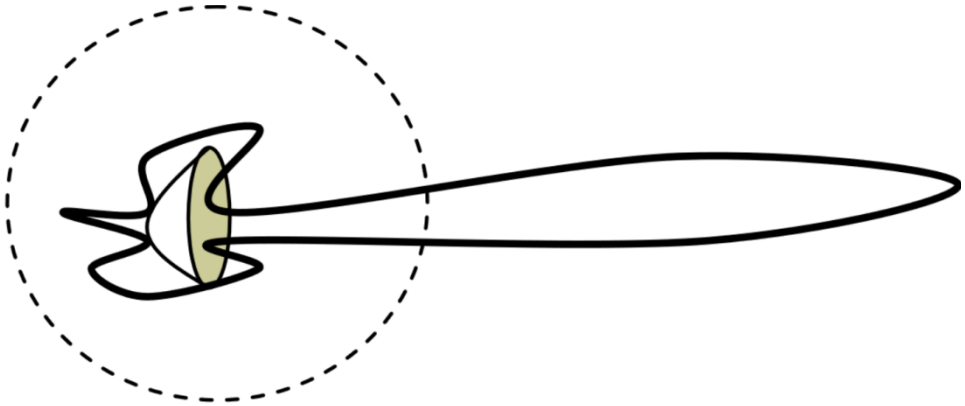
λ – vlnová délka; [29]

P_{dp} pro nás bude výkonem na přijímači nepřátelského EB. P_v výkon vysílaný nějakým z našich prostředků. Pro snížení pravděpodobnosti detekce je nutné docílit snížení P_{dp}. Zaměříme se tedy na proměnné, které můžeme ovlivnit.

Námi vysílaný výkon můžeme měnit do té úrovně, kdy nám ještě dostačuje k zabezpečení komunikace. Většina radiostanic umožňuje volbu výkonu uživatelem alespoň ve dvou úrovních. Pro minimalizaci možné detekce je tedy vhodné začínat vysílání na nejnižším možném výkonu a v případě, že spojení není navázáno vysílaný výkon navyšovat dokud nebude spojení navázáno. Bohužel manuálně je tento postup zdlouhavý a některé radiostanice umožňují nastavovat výkon například jen ve dvou úrovních (jmenovitý, snížený). V případě, že bude EB hrát větší roli v budoucích konfliktech, může být výhodné implementovat waveformy s progresivním řízením výkonu – tak, aby bylo dosaženo minimálního možného výkonu pro udržení spojení. Takové řešení by bylo ideální v případě MANET sítí, kdy by pokročilé směrování mezi stanicemi ve spolupráci s inteligentním řízením výkonu umožnilo snížit maximální úroveň výkonu, kterou radiostanice vyzáří. V rámci ma-

pování sítě by radiostanice mohly začínat broadcastem na minimálním výkonu a ten postupně navyšovat pokud se nepodaří navázat spojení s ostatními stanicemi. Předpokládám, že většina výrobců používá postup, kdy pro mapování sítě používají radiostanice broadcast na jmenovitém či maximálním výkonu a poté případně výkon snižují – takový postup vede k rychlejší formaci sítě.

Zisk vysílací antény můžeme ovlivnit volbou antény a v případě závěsných drátových antén i způsobem jejich sestavení. Nicméně zatímco ze vztahu vyplývá závislost přímá – zvýšíme-li zisk antény, zvýší se výkon na přijímači, v praxi EB to úplně neplatí. Je potřeba si uvědomit, že zisk antény G je poměr v jakém anténa dokáže vysílanou elektromagnetickou energii vyslat v požadovaném směru oproti anténě, která by vysílala elektromagnetickou energii všemi směry. Vhodným konstrukčním řešením antény se dosahuje směrovost antény, viz obrázek 4.



Obrázek 4 Charakteristika vyzařování směrové antény [29]

Zisk G_v je největší v ose antény (na obrázku se jedná o dlouhý lalok směřující doprava) u směrových antén se dá hovořit o jmenovitém zisku. V ostatních směrech je zisk antény naopak snížen oproti všesměrové anténě. Při použití směrové antény tak podstatně klesá možnost detekce nepřátelského EB, jehož přijímače by se nacházely mimo osu vyzařování antény.

Antény s takovými vlastnostmi využíváme k zvýšení dosahu a omezení rušení v případě, že spojujeme dva stacionární vzdálené body, případně s použitím automatického natáčení můžeme spojit pohybující se předmět se stacionárním – využívá se u dopravních prostředků. Takový systém je nevýhodný pro pěší vojáky komunikující za pohybu. Výhodné by takové řešení mohlo být pro jednotky komunikující při zastávce, nebo ze zaujatého prostoru na místo velení - které má stálou polohu.

Útlum volného prostoru měnit jednoduše nelze, do určité míry jej můžeme ovlivnit volbou vhodného kmitočtu – útlum volného prostoru roste s kmitočtem. Kmitočty však nelze jednoduše přizpůsobovat potřebám z hlediska EB. Nehledě na fakt, že se snižováním kmitočtu logicky klesá kapacita přenosu dat, která je přímo závislá na frekvenci.

Činitel tlumení sice nelze měnit změnou vlastností prostředí, nicméně je možné ovlivnit volbu stanoviště pro komunikaci. V praxi asi každý člověk zažil, že ztratil signál v rokli nebo v tunelu – činitel tlumení okolního prostoru byl příliš velký než aby propustil elektromagnetické vlny. Vhodnou volbou stanoviště tedy můžeme značně ovlivnit, jak a kam se náš signál bude šířit. Takováto volba není možná vždy. Může však být například zohledněna při volbě stanoviště pozorování průzkumných jednotek. Je vhodné volit stanoviště tak, aby terén poskytoval přirozené překážky ve směru předpokládaného stanoviště nepřátelského EB a zároveň umožňoval přímou radiovou viditelnost v požadovaném směru spojení.

Další z možností jak se bránit detekci by mohlo být zahlcení nepřátelského EB velkým množstvím signálů. Pokud bude bojiště dostatečně zahlceno v elektromagnetickém spektru, stane se pro EB problematické jakkoli provoz třídit a vyhodnocovat možné cíle. Dosáhnout toho lze dvěma způsoby.

První varianta je využití MANET sítí o velkých počtech účastníků. Díky neustálému mapování sítě je generován velký objem provozu, který je ve spojení se šifrováním poměrně složité pro nepřátelský EB třídit. Při využití automatických retranslačních bezpilotních prostředků UAV jako je například hoverfly [30] k retranslaci a zvýšení dosahu MANET sítě tak vznikají další body v síti, které zároveň mohou působit jako klamné cíle. V případě využití autonomních systémů ve stejné komunikační síti, jako využívá DSS, vyvstávají nové problémy. Například roste riziko, že by se vysílač mohl dostat do rukou nepřátel. V případě MANET sítí takové riziko musíme předpokládat a volit řešení, která budou odolná proti DDOS útokům. Tento požadavek u radiových sítí je ostatně uveden i v ČOS 589502.

Druhou variantu nám nabízí studie schopností EB Ruské federace k roku 2025. Jedním z cílů je „představit způsoby imitace falešné elektronické situace a dezinformování nepřátelských systémů C2 a zbraňových systémů.“ [26]. Tento cíl pod sebou skrývá vícero možností implementace. Falešnou elektronickou situaci lze vytvořit prostřednictvím falešného vysílání. Toto by v současné době mohla být poměrně zajímavá možnost – falešné vysílače stacionární a na robotických nosičích i mobilní by mohly představovat poměrně dostupnou

možnost jak vytvořit falešný obraz. Vysílání se dá poměrně jednoduše nasimulovat a vysílač ani případný robotický nosič by nemusel být military grade technologie – cena by pak nebyla závratně vysoká.

4.2 Rušení spojovacích sítí.

Rušení sítí bývá prováděno jako vysílání šumového signálu v odpovídajícím frekvenčním rozsahu o velké elektromagnetické intenzitě do cílového prostoru. Jakékoliv vysílání ve stejném frekvenčním rozsahu o nižší intenzitě elektromategnického pole než je ta způsobena rušením v dané oblasti nebude úspěšné.

Bránit se takovému rušení se dá několika způsoby:

- Využití provozu se skokovou změnou kmitočtu;
  Při dostatečné rychlosti přelaďování vysílače o výrazné kmitočtové kroky nebude možné provádět rušení, neboť rušič je také vysílačem, který vysílá na určitém nosném kmitočtu s určitou šířkou pásma. Konstrukce rušiče, který by dokázal detekovat vysílač se skokovou změnou kmitočtu je teoreticky možné, ale poměrně komplikované a energeticky velmi náročné. Naopak použití skokové změny kmitočtu je nevýhodné z důvodu alokace velkého množství kmitočtů na jeden komunikační kanál.
- Využívání záložních kanálů s jiným kmitočtem;
  Nejsnazší metoda jak se vypořádat s rušením, ale také nejméně trvalá. Jakmile je detekován provoz na nově použitém kmitočtu může být rušič přeladěn a rušit jej.
- Využívání sítí MANET;
  Při nasazení velkého počtu radiostanic dostatečně blízko u sebe může být efektivní proti rušení. Radiostanice blízko u sebe mohou produkovat dostatečně silný signál, aby si dokázali vyměňovat pakety i při rušení. Přeposíláním paketů pak může být spojení navázáno i se vzdálenými nody v síti. Samozřejmě v tomto případě značně roste počet přeposílaných paketů a je degradována propustnost sítě.

4.3 Možnost zachycení obsahu při přenosu

Krom zaměření polohy vysílání a rušení může být v rámci EB prováděn i odposlech radiových přenosů. Současné možnosti šifrování ovšem umožňují dostatečně zabezpečit přenos proti dešifrování. V rámci ozbrojených složek existují předpisy k použití šifrování v rámci přenosů a je popsáno jaké šifrovací algoritmy jsou přípustné pro zabezpečení podle stupně

utajení. Dle mých zkušeností je tato oblast jediná, která je relativně dobře popsaná a funguje jak v rámci komunikačních sítí jednotlivých národů, tak v mezinárodních operacích pod hlavičkou NATO.

5 SPECIFIKACE ODLIŠNÝCH POŽADAVKŮ NA TECHNOLOGIE PRO PRŮZKUMNÉ A SPECIÁLNÍ JEDNOTKY

Jednotky mechanizované pěchoty (7. Mechanizovaná brigáda) nebo jednotky typu komando (dříve 4. Brigáda rychlého nasazení, dnes 43. Výsadkový pluk) operují často ve velkých celistvých skupinách, často společně s dalšími prvky. V takových případech je SA zpravidla částečně sdílena minimálně v podobě sledování polohy vlastních sil (BFT). Cílem je dosažení sdíleného obrazu bojiště v reálném čase (nebo alespoň blízkého reálnému času).

Speciální síly a průzkumné jednotky naproti tomu operují v malých skupinách, které potřebují utajit vlastní postup a to často i před vlastními silami. Takový přístup vychází z jednoho ze základních imperativů zákona 412/2005 Sb. často adresovaného jako „need to know“ a tedy, že s informacemi spadajícími do kterékoliv kategorie utajení se seznamují pouze ti, kteří tyto informace potřebují pro výkon své funkce. Jednotky sdílející bojiště v rámci společného úkolu mají potřebu znát svou vzájemnou polohu a do určité míry i úkoly, které plní. Speciální jednotky a průzkumné jednotky plní často úkoly, které jsou nezávislé na ostatních jednotkách. Často operují v hloubce na území protivníka. Praxe je často taková, že neudávají svou přesnou polohu ani přímým nadřízeným.

5.1 Speciální síly

Speciální síly plní řadu rozdílných úkolů a je problematické stanovit jednotné požadavky, které by odpovídaly všem typům operací. Při úkolu spojeném s dlouhodobějším skrytým působením bude potřeba minimalizovat jakoukoliv elektromagnetickou stopu, podobně jako u průzkumných jednotek. V případě skrytého působení pak nebude vhodné využití radiových provozů typu MANET. MANET komunikace v rámci neustálé kontroly stavu sítě a konfigurace tras mezi jednotlivými nody vysílá i v případě, že sítí neproudí informace uživatelů. Riziko odhalení a zaměření se v takovém případě zvyšuje.

U úkolů kde dochází k rychlému a krátkodobému nasazení jako byla například akce k eliminaci Usámy bin Ladina, bude důraz kladen na kvalitu a spolehlivost spojení i za cenu možného odhalení nepřátelským EB, které pravděpodobně prozatím nedokáže reagovat v řádu jednotek minut. V případě, kdy je potřeba například vizuálního potvrzení cíle na místo velení bude také rozhodující datová propustnost používaného kanálu. Většina vojenských komunikačních technologií není vyvinuta pro real-time stream videa na velké vzdálenosti. Speciální síly jsou jakýmsi high-endem ve většině oblastí a proto je potřeba

neustále zvažovat inovace. V současné době většina výrobců vojenských komunikačních technologií jako jsou THALES [31], AIRBUS [32], GENERAL DYNAMICS [33] a další pracují na variantách 4G, LTE a dokonce 5G sítí pro vojenské využití. Koncept je stále málo přijímán v armádních kruzích, ale představuje zajímavou variantu. Například ve spojení s dedikovaným smarthonem jako je Galaxy S20 Tactical edition [34] představuje i možnost jak snížit náklady – omezila by se potřeba poměrně drahých taktických radiostanic. Pro většinu současných armád by však znamenal značnou výchozí investici, neboť postrádá potřebnou infrastrukturu a neposkytuje kompatibilitu s klasickými radiostanicemi. Nasazení komunikačních sítí tohoto typu představuje budování polních základnových stanic (BTS) a vybavení vozidel BTS moduly. Oproti klasickým radiostanicím postrádají zpětnou kompatibilitu – se 4G smartphonem navážete spojení s VHF nebo UHF radiostanicí pouze pomocí nějakého typu hlasové brány. Oproti tomu nové typy radiostanic mají možnost navazovat spojení i se staršími typy stejného určení (pro osobní vojenskou komunikaci jsou většinou určeny radiostanice, které umožňují vkv FM provoz kompatibilní napříč všemi výrobci a modelovými řadami).

5.2 Průzkumné jednotky

Průzkumné jednotky zpravidla působí skrytě, zároveň je ovšem pro jejich činnost klíčový přenos informace zpět k velení. Specifické je ovšem to, že při řadě průzkumných úkolů není podstatné odeslat informaci okamžitě. Některé úkoly mohou mít podobu například propátrat určitou oblast, nebo pozorovat dění v zájmovém objektu. Pokud při takovém úkolu nedoje k důležité události, průzkumná jednotka zasílá pouze souhrné hlášení za určitou dobu, případně pouze hlášení o vlastním stavu. Hlášení jsou často vyžadována i v případě, že průzkum nezjistil žádné zájmové informace - velení potřebuje v pravidelných intervalech vědět, že je jednotka namístě a provádí stanovený úkol. Bez nastavení pravidelného hlášení by panoval stav neurčitosti (nepřítomnost hlášení by mohla znamenat, že jednotka neplní úkol, ale také, že úkol plní, ale v zájmové oblasti není aktivita nepřítele). Do určité míry je tedy výhodné hlásit, že se v zájmové oblasti nic neděje – neboť i to může být žádaná informace. Za předpokladu intenzivní činnosti EB protivníka je ovšem výhodné zvážit vzhledem k povaze úkolu nakolik častá taková hlášení musí být a v určitých případech pravidelná hlášení úplně vynechat.

V případě podávání hlášení jen v určených časových intervalech je vhodné plánování tohoto spojení tak, aby byla minimalizovaná možnost odhalení prostřednictvím EB.

Průzkumné jednotky mohou vybrat stanoviště, které bude mít vhodné terénní uspořádání tak, aby byl omezeno vysílání signálu nežádoucím směrem. Rovněž je vhodné využití směrových antén, na rozdíl od bojových jednotek průzkum většinou nevysílá za pohybu, kdy by byly směrové antény nevýhodné.

Pokud EB zjistí opakující se vysílání na vlastním území ze stejné polohy, existuje riziko navedení palby na zjištěné souřadnice, případně vyslání jednotek k prověření situace. Minimalizace takového rizika by mohla být dosažena (pokud to okolnosti dovolují - nutnost skrytého přesunu) vysíláním mimo místo, kde se průzkumná jednotka nachází. A v případě dlouhodobého setrvání v jedné oblasti vysílací stanoviště případně i časy měnit.

V případě vzdušné nadvlády a budoucího nárůstu počtu UAV by bylo možné využít retranslace prostřednictvím blízkého UAV. Signál ke spojení s UAV ve vzdálenosti například 2 km nerušený povrchovými překážkami by mohl být řádově nižšího výkonu než signál potřebný ke spojení na 20 km zalesněnou oblastí s terénními překážkami.

6 VYHODNOCENÍ BEZPEČNOSTI JIM A MOSKITO.

V rámci vojenských komunikačních a informačních systémů je zpravidla zakázáno využití wifi, bluetooth a veškerých podobných technologií. Přesto nakupované prostředky tyto komunikační rozhraní většinou mají a je pouze na určité úrovni zakázáno. Tento zákaz je odvozen na základě §9 vyhlášky 523/2005 Sb, která definuje, že „Přenos utajované informace komunikačním kanálem vedeným mimo objekt musí být zabezpečen certifikovaným kryptografickým prostředkem, který je certifikován nejméně pro stejný stupeň utajení jako přenášená utajovaná informace.“ Objektem v této definici je prostor akreditovaný pro zpracování utajované informace. Při přenosu bezdrátovými technologiemi pak není možné zabezpečit, že přenosový kanál bude omezen na objekt. Zároveň platí, že wifi a bluetooth adaptéry nesplňují požadavek certifikované kryptografické ochrany.

Nicméně stejný paragraf definuje:

„Během certifikace informačního systému může Úřad, na základě předložené analýzy rizik, přijatých specifických bezpečnostních opatření pro detekci narušení bezpečnosti komunikačního kanálu a opatření pro snížení důsledků útoku, schválit odlišný systém zabezpečení informačního systému, než je uveden v odstavcích 4 a 6.“ [35].

V této části práce poskytnu podklady pro příslušnou analýzu.

6.1 Charakteristika přístrojů

V obou případech se jedná o vojenské pozorovací přístroje společnosti SAFRAN. Přístroje umožňují krom standardního pozorování dalekohledem zobrazení termovizního obrazu, měření vzdálenosti laserem, dopočítání pozice pozorovaného objektu (v případě Moskito za předpokladu, že je instalován GPS přijímač, který je volitelný).

V obou případech je možný sdílení video obrazu do připojených zařízení. Podporované periferie jsou USB 2,0, Ethernet, RS – 232, volitelně bluetooth. Přístroj JIM pak nabízí variantu wifi nebo bluetooth [36].

6.2 Použití přístrojů.

Pozorovací přístroje tohoto typu jsou využívány především u průzkumných a speciálních jednotek, při zřizování pozorovacích stanovišť. Je možné umístit přístroj na vhodné místo (volitelným doplňkem je trojnožka) se zaměřením na pozorovaný objekt a samotný operátor může s využitím streamovaného obrazu využít lepšího skrytu mimo přímou viditelnost

od pozorovaného objektu. Oproti pozorování s klasickým dalekohledem se při vhodném využití snižuje možnost detekce průzkumníka termovizními, nebo IR přístroji. Variantou použití je, že je pozorovací přístroj využíván jedním operátorem, který může odeslat stisknutím spouště obraz do TZD, nebo TZT dalšího operátora. V takovém případě je výhodné bezdrátové připojení, které umožňuje větší vzdálenost mezi pozorovacím přístrojem a TZD nebo TZT.

6.3 Rizika použití přístrojů.

6.3.1 Informační bezpečnost

I v případě použití přístrojů v rámci DSS s určitým stupněm utajení, informace, které by byly přenášeny mezi pozorovacím přístrojem a TZD nebo TZT pravděpodobně nebudou spadat mezi utajované informace a dle mého názoru by se mohlo jednat o taktickou informaci. Musíme také přihlédnout k faktu, že samotná detekce průzkumných skupin může být vnímána jako kompromitace informace. V situacích, kdy by využití bluetooth snížilo riziko fyzické detekce, je v určitých případech (předpoklad nízké nebo žádné aktivity EB v oblasti) dostatečným odůvodněním pro jeho využití.

6.3.2 Detekce ozáření

Velké množství moderních bojových prostředků využívá nějakou formu detekce ozáření laserovými dálkoměry nebo zaměřovači (viz například LAWAREC od firmy EVPÚDEFENCE [37]). Použití přístrojů JIM nebo Moskito k měření vzdálenosti, nebo zaměření polohy některých typů techniky může v případě jejich vybavení detektorem ozáření vést k odhalení přítomnosti průzkumu.

6.3.3 Narušení integrity přenášené informace

V případě odhalení vysílání nepřítelem by mohlo dojít k nějaké formě útoku typu Man in the middle obraz přenášený do TZT nebo TZD by mohl být změněn a například vysílán ve smyčce. Průzkumné jednotky by pak mohly získávat nepřesné informace. Nicméně takový útok by vyžadoval, aby nikdo přímo nesledoval obraz v optice přístroje, neboť ten by zůstal nepozměněn. Horším případem by bylo vložení škodlivého kódu do fotografie. Riziko takového útoku můžeme považovat za poměrné malé. V první řadě by byla potřeba detekce vysílání, následně jeho analýza, dekódování a případné dešifrování, a pak umístit vysílač dostatečně blízko, aby dokázal přehlušit právoplatné vysílání bluetooth nebo wifi.

Umístění vysílače v blízkosti průzkumných jednotek se z logiky činnosti průzkumu jeví jako nepraktické řešení.

Jak wifi, tak bluetooth umožňuje šifrování, přičemž bluetooth je zranitelné hlavně při párování, nicméně to by neprobíhalo v době nasazení jednotky. V případě, že by útočník chtěl bluetooth komunikaci narušit, musel by se pokusit o odpárování zařízení.

6.3.4 Detekce vysílání

Riziko odhalení prostřednictvím EB je pro průzkumné jednotky z hlediska kybernetické bezpečnosti asi nejpodstatnější.

Teoretická detekce EB wifi se dá poměrně dobře dopočítat za předpokladu šíření signálu volným prostorem. Vysílaný výkon u standardních zařízení nesmí překročit 100 mW (maximální povolený vyzářený výkon pro 2,4 - 2,483 GHz wifi). Citlivosti uváděné u detektorů, ve výše zmíněném průzkumu trhu jsou až -134 dB (-104dBm nebo cca $3{,}98\text{x}10^{-11}$mV). Zisk přijímací antény se dá odhadovat kolem 10 dB (10 násobné zvýšení výkonu), což je podle mých zkušeností poměrně standardní zisk běžných směrových antén. Vyjádříme-li z radiokomunikační rovnice ($P_{dp} = \frac{\mathrm{P_v G_v G_p}}{\left(\frac{4\pi R}{\lambda}\right)^2}|F|^2$) vzdálenost R, dostaneme:

$$R = \sqrt{\frac{\mathrm{P_v G_v G_p}\lambda^2}{(4\pi)^2 P_{dp}}|F|^2}$$

Zisk vysílací antény můžeme zanedbat, neboť budeme uvažovat, že přístroje vysílají wifi všesměrově. Problém je zjistit jaké budou ztráty v přenosovém prostředí, pokud je pro náš výpočet zanedbáme, teoretická detekce ve volném prostředí by byla možná na[6]:

$$R \cong 49854\text{m}$$

Téměř 50 km za laboratorních podmínek, při maximálním výkonu, který může dle českého telekomunikačního úřadu [38] wifi vysílat. Nejsou započítány žádné ztráty prostředí ani rušení způsobené jinými sítěmi, které v daném pásmu působí. V praxi jsem zkoušel měřit sílu signálu přicházejícího od radiostanice vozidla při konstantní vzdálenosti a při různé

[6] Existuje řada nástrojů, které tyto propočty simulují. Například web rfwireless-world.com nabízí kalkulátor, který umožňuje zadat všechny hodnoty a to včetně ztrát v prostředí vedení a dalších. Při zadání výše zadaných hodnot odpovídá výsledek mému propočtu.

orientaci vozidla s prutovou anténou umístěnou na kapotě. Toto měření mělo za účel ukázat prakticky vojákům, jak je vhodné orientovat vozidlo vzhledem ke směru vysílání a bylo pouze orientační. Nebylo zaznamenáváno ani ověřováno v různých polohách a vzdálenostech tak, aby byl omezen vliv prostředí (hlavně odrazy od okolí). Při orientaci vozidla zadní částí k měřícímu přístroji, kdy mezi přijímací anténou měřícího přístroje a vysílací anténou radiostanice částečně stínila kabina vozidla, byla opakovaně naměřena nižší hodnota a to v rozmezí 3 - 8 dB. Snížení vysílaného výkonu o 3 dB by v rámci našeho propočtu znamenalo zkrácení dosahu možné detekce na zhruba 35 km. V reálném prostředí pak podobných překážek ovlivňujících šíření signálu existuje mnoho – vegetační porost, terénní nerovnosti, stavby, nehledě na poměrně velké množství dalších signálů v pásmu wifi, které mohou způsobovat rušení a snižovat dosah. Pro srovnání standardní wifi moduly mají citlivost přijímače podstatně nižší cca -84dBm a antény mají nižší zisk cca 5dB [7]. Pro uvedený wifi modul by byl dosah volným prostorem 2,8 km. Z praxe všichni víme, že standardně v budovách mají wifi AP dosah v řadech desítek metrů. Takové snížení oproti teoretickému dosahu je způsobeno dvěma faktory a to, že v reálných podmínkách je daleko více ztrát než ve volném prostoru a také, že takto pojatý výpočet nám říká, že signál o dané síle bude detekován. Rovnice nepočítá s různými vlastnostmi modulace signálu na šíření prostorem (Při velkém zjednodušení se dá říci, že bude rozdíl, pokud bude vysíláno 100mW na jeden bit informace nebo na 1 kbit informace. V prvním případě bude mnohem větší energetická špička a tedy rozdíl mezi signálem a šumem). Odhaduji, že reálný dosah/detekovatelnost signálu bude oproti teoretickému o řád nižší. Maximální vzdálenost, na kterou by bylo možné zachytit wifi s citlivostí přijímače -134 dBbm v reálných podmínkách bude přibližně 5 km.

Bluetooth operuje ve stejném frekvenčním rozsahu a maximální výkon vysílače může být 100 mW u zařízení třídy 1, stejně jako u wifi. Zařízení třídy 1 ovšem musí mít řízení výkonu a jejich minimální vysílaný výkon je 1mW [39].

Při vysílání výkonem 1mW by teoretický přijímač EB v ideálním prostředí detekoval signál na vzdálenost zhruba 5 km. Pokud bychom pro reálné prostředí snížili tento výkon o řád, dostali bychom detekovatelnou vzdálenost vysílání při 1mw rovnající se 500m.

---

[7] Například wifi modul dostupný na:
https://www.adsnotef.com/index.php?main_page=product_info&products_id=77771

Je potřeba si uvědomit, že tyto výkony jsou poměrně malé oproti výkonům vysílání radiostanic, které se pohybují v jednotkách watů, ale vysílání probíhá v případě zapnutého přístroje připojeného k TZD nebo TZT téměř nepřetržitě.

Ze způsobu nasazení přístrojů je patrné, že průzkumné jednotky si vybírají stanoviště, které je dobře skryto, ale zároveň musí poskytovat dobrý výhled na pozorovaný objekt, který nemůže být příliš daleko (optický dosah samotných přístrojů se pohybuje podle způsobu pozorování v jednotkách kilometrů). Za předpokladu, že bude pozorovaným objektem rozsáhlá základna, kde se může nacházet přijímač systému EB, riziko detekce bude potřeba brát v potaz a pro propojení je vhodné využít kabel. V případě pozorování objektu, kde není pravděpodobnost přítomnosti EB v blízkém okruhu, případně byla jeho přítomnost průzkumnou činností falzifikována, bude riziko zanedbatelné.

Je potřeba si uvědomit, že průzkum bude s velkou pravděpodobností schopný odhalit přítomnost prvků EB (například na základě přítomnosti anténních systémů) v podobné vzdálenosti, na jakou bude EB schopno lokalizovat vysílání wifi nebo bluetooth.

Dalším podstatným faktem je, že pro určení polohy zachyceného signálu je nutné porovnat zachycený signál z několika přijímačů EB (na podobném principu funguje určení polohy GPS, ale logika je obrácená - jeden přijímač porovnává signál několika vysílačů). Jediný přijímač je schopen určit maximálně směr sledovaného vysílání (pokud využívá vhodné anténní prvky). Pro alespoň přibližnou detekci polohy by tedy musel být vysílač v dosahu minimálně dvou přijímačů EB.

Samotné zachycení vysílání ještě neznamená nutně odhalení přítomnosti. Wifi a bluetooth signály jsou dnes všudypřítomné a EB by muselo konkrétní zachycený signál identifikovat a označit jako nepřátelský. Pravděpodobnost identifikace je těžké určit a bude závislá na množství signálů v daném spektru, v tomto ohledu hraje významnou roli charakteristika a osídlení oblasti. V místech s nízkou nebo žádnou populací, případně v oblastech s obyvatelstvem s minimálním technologickým vybavením bude pravděpodobnost zachycení a identifikace mnohonásobně vyšší, než v oblastech hustě osídlených technologicky vybaveným obyvatelstvem.

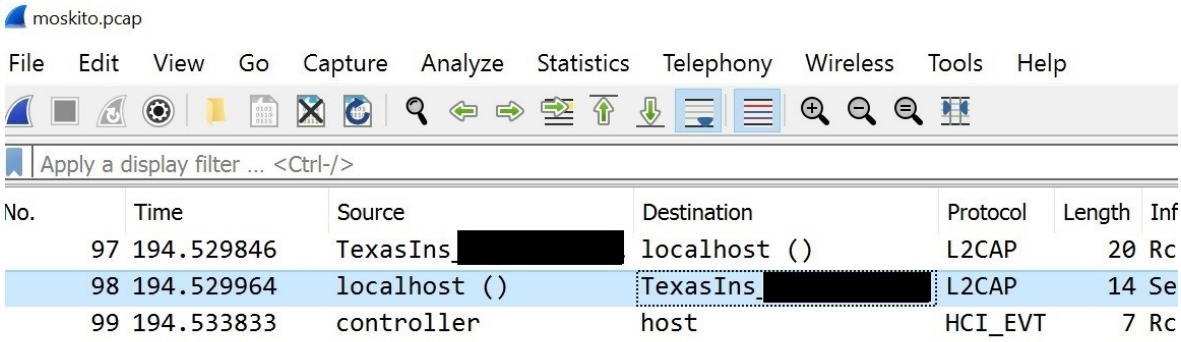
6.4 Penetrační test

Od firmy Pramacom HT jsem zapůjčil přístroj Moskito TI s bluetooth modulem. V domácím prostředí jsem se pokusil za pomocí linuxové forenzní a penetrační distribuce prověřit bezpečnost bluetooth přenosu mezi přístrojem Moskito TI a smartphonem.

6.4.1 Identifikace

Z již výše uvedených údajů jsem považoval za podstatné zjistit, zda bude útočník schopen přístroj identifikovat. U přístroje můžeme nastavit bluetooth rozhraní na vypnuto nebo zapnuto, dále nastavíme jméno, jakým se bude ohlašovat při párování a provádět samotné párování. Další nastavení bezdrátového adaptéru Moskito uživateli neumožňuje.

Adresa adaptéru, kterou se hlásí, patří pod výrobce Texas Instruments (obrázek 5), který se řadí mezi větší výrobce na trhu. Dohledat tak Moskito TI, případně JIM bude bez bližší znalosti problematické a vyžadovalo by v prostředí s více vysílači mnoho času.



Obrázek 5 Mac adresa bluetooth adaptéru Moskito TI

6.4.2 Sestava pro testování

Testovaný scénář bylo Moskito TI propojené pomocí bluetooth se starším mobilním telefonem (Xiaomi Mi A2). Přístroj Moskito jsem pojmenoval TEST UTB.

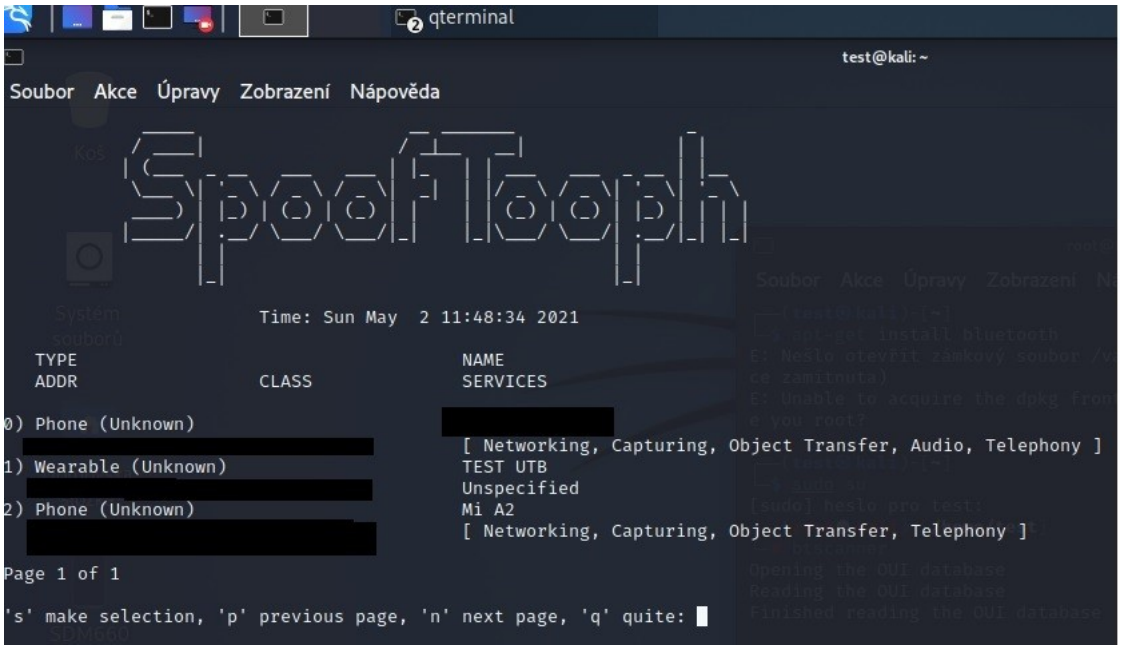
K testování jsem využil linuxovou distribuci Kali instalovanou na starší přenosný PC.

6.4.3 Průběh testu

Jako první jsem začal sledovat bluetooth zařízení pomocí nástroje spooftooph, který umožňuje klonování naskenovaných zařízení.

Při zapnutém nástroji jsem posílal záběry z Moskita do telefonu Mi A2. Nicméně nástroj spooftooph odhalil pouze zařízení Mi A2.

Pokusil jsem se obě zařízení odpárovat a znovu spárovat. V tomto bodě se mi povedlo zachytit oba přístroje (zachytil jsem navíc svůj vlastní telefon).

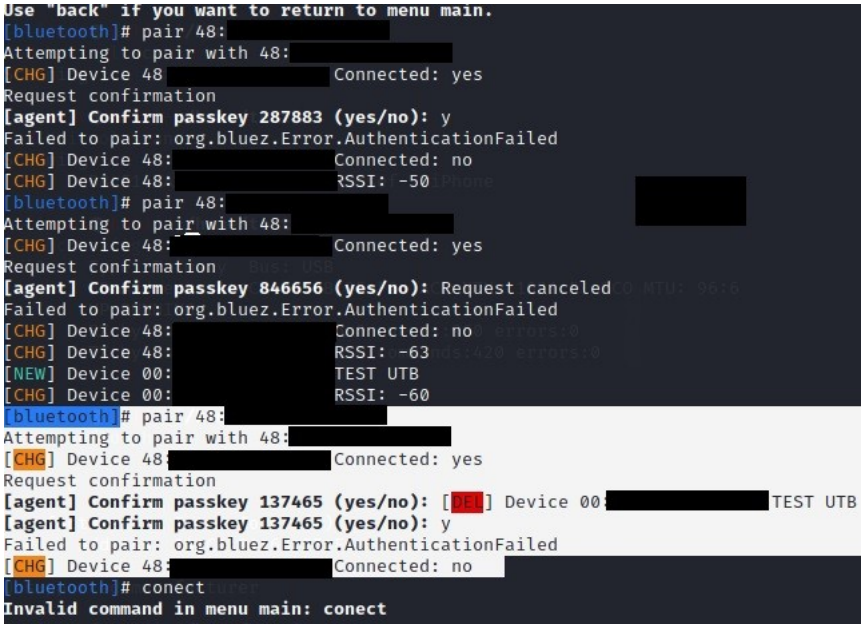


Obrázek 6 Spooftooph

Za povšimnutí stojí, že zařízení se hlásí jako wearable a nic kromě jména ho nemůže nijak zvlášť prozradit.

Dalším testem bylo vyzkoušet, zda se dokážu připojit k přístroji nebo k telefonu, pokud naklonuji jejich protějšky, za předpokladu, že jsou zařízení už spárována. Přirozeně by v polních podmínkách zařízení byla už spárována a nové párování by nastalo pouze v případě závady nebo případného kybernetického útoku na některé ze zařízení.

V případě klonování Mi A2 a pokusu o připojení k Moskitu byl pokus opakovaně neúspěšný. Moskito bylo pro párování nedostupné.



Obrázek 7 Pokus o párování

Opačný postup naklonování Moskita a pokus o spárování s Mi A2 se dostal o krok dále, k potvrzovacím kódům. Zde jsem potvrdil kódy jak v linuxu, tak na displeji telefonu[8], nicméně párování nebylo úspěšné a nepodařilo se mi nahradit spárované Moskito za klon.

6.4.4 Závěry testování

Mnou prováděné pokusné testy patřily k těm nejjednodušším z repertoáru možného útočníka, nicméně prokázaly, že v případě spárované sestavy Moskito – přístroj operátora nebude jednoduché v poli bluetooth napadnout a útočník bude pravděpodobně nucen pokusit se nejprve o rozpárování zařízení. Moskito během celého několikahodinového skenování okolních bluetooth signálů nebylo viditelné a to ani při zapínání a vypínání, nebo při odesílání dat do telefonu. U telefonu tomu tak nebylo a pravidelně při příjmu/potvrzování dat byl viditelný, nicméně se nejednalo o telefon zařazený do výbavy AČR.

Útočník, který by dokázal rozpárovat zařízení a měl by zautomatizováno klonování zařízení, by mohl uspět v určité formě útoku. Takový útok by však byl poměrně komplikovaný s přihlédnutím ke všem specifikům použití pozorovacích přístrojů.

[8] Riziko takového scénáře považuji za malé, je pravděpodobné, že člověk znalý základů kybernetické bezpečnosti by nepotvrdil párování, které neočekává.

6.5 Závěry hodnocení přístrojů

Rizika použití přístrojů v režimu bezdrátové konektivity jsou závislá na prostředí, ve kterém budou použity.

Riziko detekce prostřednictvím EB nelze na základě teoretických propočtů zcela zanedbat v oblastech s nízkým pokrytím sítěmi wifi a bluetooth. Nicméně pro přesné zhodnocení dosahu bych doporučoval v rámci výcviku EB vyzkoušet prakticky na jakou vzdálenost je možné zachycení bluetooth a wifi v různých prostředích.

Riziko detekce protivníkem v případě použití laserového zaměřovače/dálkoměru na moderní prostředky (vozidla, tanky) protivníka se jeví jako poměrně velké a doporučil bych zvážit jeho použití dle situace, případně volit alternativní cíl měření (například zaměřit vedle stojící budovu, případně jiný objekt, v případě kolony volit vozidlo pravděpodobně neosazené senzory jako je nákladní vůz).

Z hlediska zranitelnosti bluetooth přenosu se jeví přístroje jako relativně bezpečné. Bluetooth sám o sobě umožňuje po spárování poměrně kvalitní zabezpečení (proměnlivé frekvence, šifrování). Firmware přístroje je evidentně napsán bezpečněji, než v případě testovaného telefonu a pozorovací přístroj sám o sobě nezasílá žádný nadbytečný advertisement. Při párování pak při vhodném pojmenování nebude evidentní, o jaké zařízení se jedná.

7 SOUBOR POŽADAVKŮ, KTERÉ BY MĚLY SPLŇOVAT TECHNOLOGIE ZAVÁDĚNÉ DO AČR

V této práce jsem se dotknul řady témat, která by měla být brána v potaz při tvorbě architektury DSS. Rozsah problematiky DSS je příliš velký, abych byl schopen adekvátně pokrýt toto téma v rozsahu, který by představoval úplný soubor požadavků. Požadavky, které definuji na základě mého zkoumání, jsou z mého pohledu nezbytné, ale nemohou být požadavky dostačujícími pro specifikaci technologií a tvorbu architektury.

7.1 Implikace zákonů

7.1.1 Problematika definice toku informací

Vzhledem k tomu, že systém sesednutého vojáka má umožňovat zpracování informací podléhající určitému stupni utajení, musí splňovat kritéria předepsaná zákonem 412/2005 Sb. a vyhláškou 523/2005 Sb „o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor“. V těchto publikacích je uveden základ pro návrh systémů nakládajících s utajovanými informacemi.

V případě zpracování utajované informace systém sesednutého vojáka spadá jak do definice informačního systému v § 34: „jeden nebo více počítačů, jejich programové vybavení, k tomu patřící periferní zařízení, správa tohoto informačního systému a k tomuto systému se vztahující procesy nebo prostředky schopné provádět sběr, tvorbu, zpracování, ukládání, zobrazení nebo přenos utajovaných informací.“ [18]

Zároveň však komunikační prvky spadají pod definici komunikačního systému v § 35: „Komunikačním systémem nakládajícím s utajovanými informacemi (dále jen"komunikační systém") se pro účely tohoto zákona rozumí systém zajišťující přenos těchto informací mezi koncovými uživateli a zahrnující koncové komunikační zařízení, přenosové prostředí, kryptografické prostředky, obsluhu a provozní podmínky a postupy.“ [18]. Dále je potřeba, aby byl prostřednictvím NÚKIB IS certifikován a pro KS byl schválen projekt bezpečnosti komunikačního systému.

Krom definice a popisu potřebného zabezpečení je popsáno i prostředí pro používání utajovaných systémů. Zákon 412/2005 Sb. Hlava V, fyzická bezpečnost, § 24 stanovuje, způsoby zpracování utajované informace. Je zde požadavek, aby byla utajovaná informace

projednávána a zpracovávána v určeném objektu nebo zabezpečené oblasti. V polních podmínkách taková oblast stanovit nelze, ale:

„d) v odůvodněných případech s písemným souhlasem odpovědné osoby nebo bezpečnostního ředitele mimo objekt, pokud je zajištěno, že k utajované informaci nemá přístup neoprávněná osoba.“ [18]

Vyhláška 523/2055 Sb dále stanovuje:

„§ 13 Požadavky na ochranu mobilních a přenosných informačních systémů

(1) Pro mobilní a přenosné informační systémy se v analýze rizik posuzují i rizika, která jsou u mobilních informačních systémů spojená s dopravním prostředkem, a u přenosných informačních systémů s prostředími, ve kterých budou tyto informační systémy používány.“ [35].

Samotný zákon stanovuje řadu věcí pouze obecně a často ve formátu, kdy nechává otevřené možnost navrhnout systém dle vlastních specifikací a předložit tento návrh ke schválení.

„§ 12 Možnost nahrazení prostředků počítačové bezpečnosti

Zajištění některých bezpečnostních funkcí informačního systému prostředky počítačové bezpečnosti lze v odůvodněných případech nahradit zvýšeným použitím prostředků personální nebo administrativní bezpečnosti, fyzické bezpečnosti informačních systémů anebo organizačních opatření. Při nahrazení prostředků počítačové bezpečnosti náhradním bezpečnostním mechanismem nebo skupinou mechanismů, které mají zajišťovat určitou bezpečnostní funkci, musí být plně realizována bezpečnostní funkce a zachována kvalita a úroveň bezpečnostní funkce.“ [35].

Zákon 412/2005 Sb. ovšem stanovuje také taktickou informaci:

„(1) Taktickou informací se pro účely tohoto zákona rozumí utajovaná informace s krátkou dobou trvání důvodu utajení. Taktická informace se zpracovává v informačním nebo komunikačním systému a při přenosu se chrání kryptografickou ochranou.

(2) Ochrana taktické informace do stupně utajení Tajné může být zabezpečena též souborem opatření stanovených na základě vyhodnocení rizik. Podmínky odlišné manipulace s taktickou informací upravuje bezpečnostní standard.“ [18]

Pro účely systému sesednutého vojáka by pravděpodobně bylo dostačující, aby zpracovával pouze taktické informace. Bohužel, v tomto ohledu by musel být definován požadavek

z úrovně velení, jak má vypadat informační tok mezi jednotlivými prvky armády a to do úrovně klasifikace utajení jednotlivých předávaných hlášení a stanovení uživatelů, kteří mohou mít přístup. Až na základě informačního toku by bylo možné stanovit, v jakém technickém prvku by se zpracovávaly nebo ukládaly utajované informace a mohlo by dojít k vyhodnocení rizik a návrhu bezpečnostních opatření sytému, na základě standardu. Bohužel tento standard je utajovaný jak definuje vymezení pojmů: „j) bezpečnostním standardem utajovaný soubor pravidel, ve kterém se stanoví postupy, technická řešení, bezpečnostní parametry a organizační opatření pro zajištění nejmenší možné míry ochrany utajovaných informací," [18]

Domnívám se, že jeden z důvodů proč se stále v rámci AČR nepodařilo zasadit utajovaný systém sesednutého vojáka je, že chybí rozpracování informačního toku a definice jaké informace budou proudit kam v jakém stupni utajení. Dle mých zkušeností velká část pracovníků KIS a část velitelských struktur v armádě vyjadřuje potřebu, aby systémy pro sesednutého vojáka byly utajovány až do stupně tajné. Tato potřeba vychází ze zkušeností ze zahraničních operací, kde takové systému u jiných armád existují. Nicméně nikdo mi nedokázal odpovědět jednoznačně na otázku, jakého typu by byly tajné informace předávané v rámci DSS. Jediný konkrétní typ informace, který byl vzpomenut je bojový rozkaz. Ten v určitých případech opravdu nabývá utajení tajné, nicméně dle mého názoru by se mohlo jednat o taktickou informaci a bylo by možné v rámci systému nastavit taková opatření, aby se taková informace neuchovávala po dlouhou dobu.

7.1.2 Zákonné požadavky

Jediný jednoznačně nezbytný technický požadavek definovaný zákonem 412/2005 Sb. je, že utajovaná informace musí být při přenosu kryptograficky ochráněna. Zároveň platí, že prostředky zajišťující kryptografii musí být certifikovány z úrovně NBÚ nebo NÚKIB a tento certifikát musí být obnovován.

Ve vyhlášce 523/2005 Sb jsou bezpečnostní požadavky uvedeny v § 7 Minimální bezpečnostní požadavky v oblasti počítačové bezpečnosti.

Přičemž pro systém nakládající s informacemi do úrovně vyhrazené musí splňovat následující:

„- jednoznačnou identifikaci a autentizaci uživatele, přičemž musí zajistit ochranu důvěrnosti a integrity autentizační informace,

- volitelné řízení přístupu k objektům informačního systému na základě rozlišování a správy přístupových práv uživatele

- nepřetržité zaznamenávání událostí, které mohou ovlivnit bezpečnost informačního systému do auditních záznamů a zabezpečení auditních záznamů před neautorizovaným přístupem.

- Možnost zkoumání auditních záznamů a stanovení odpovědnosti jednotlivého uživatele, bezpečnostního správce nebo správce informačního systému,

- ochranu důvěrnosti dat během přenosu mezi zdrojem a cíle.“ [35].

Pro systém nakládající s informacemi od úrovně důvěrné výše musí splňovat ještě další požadavky:

„- volitelné řízení přístupu k objektům informačního systému na základě rozlišování a správy přístupových práv uživatele

- ošetření paměťových objektů před jejich dalším použitím, zejména před přidělením jinému subjektu informačního systému, které znemožní zjistit jejich předchozí obsah,

- ochranu důvěrnosti dat během přenosu mezi zdrojem a cíle.“ [35].

7.1.3 Požadavky na radiostanice dle ČOS

„Požadavek 17

Všechny bezdrátově přenášené informace ze zapůjčené radiostanice musí být chráněny proti předpokládaným bezpečnostním hrozbám v radiovém prostředí pomocí COMSEC a TRANSEC opatření, v souladu s pravidly a pokyny pro NATO Restricted.

Požadavek 18

Bezpečnostní hrozby související s bezdrátovým přenosem v interoperabilní síti musí být ošetřeny v zapůjčené radiostanici.

Požadavek 19

Zapůjčená radiostanice musí být pro manipulaci certifikována na utajovaný stupeň NATO Restricted nebo ekvivalentní národní klasifikační stupeň, viz AC/35-D/1034.

Požadavek 20

Zabezpečující stát poskytující zapůjčenou radiostanici, musí být odpovědný za nastavení a správu těchto radiostanic. Při nasazení má být odpovědný za bezpečnost užívání radiosta-

nice v interoperabilní síti JDSS rovněž zabezpečující stát, viz AC/35-D/2001, AC/35-D/2002 a AC/35-D/1014.

TRANSEC

Požadavek 21

Zapůjčená radiostanice má být odolná proti rušení, zamezit detekci a čelit DoS útokům.

Požadavek 22

Zapůjčená radiostanice má být vybavena funkcí radiový klid.

COMSEC

Požadavek 23

Zapůjčená radiostanice musí poskytovat ochranná opatření COMSEC k ochraně neporušenosti obsahu informací.

Požadavek 24

COMSEC opatření musí být založeny na šifrování radiového přenosu (na vysílací i přijímací straně).

Požadavek 25

Zapůjčená radiostanice musí mít mazací (nulovací) funkci, která odstraní šifrovací klíče a nastavené parametry rádiové sítě.

Požadavek 26

Zapůjčená radiostanice má být vybavena ochranou, která smaže šifrovací klíče a nastavené parametry radiové sítě při nedovolené fyzické manipulaci se zařízením, viz AC/322-D(2005)0040.

Požadavek 27

Zapůjčená radiostanice má mít schopnost indikace, pokud bylo se zařízením nedovoleně fyzicky manipulováno, viz AC/322-D(2005)0040.

Požadavek 28

Pokud je zařízení vybaveno funkcí, která hlídá nedovolenou fyzickou manipulaci se zařízením, musí být tato funkce v činnosti s i bez připojeného napájení.

TEMPEST

Informace nacházející se mimo šifrovanou sekci zapůjčené radiostanice mají být chráněny před nežádoucím radiovým přenosem informací. Nejsou stanovena žádná TEMPEST omezení pro zařízení zpracovávající NATO Restricted informace,

viz AC/35-D/1034.“ [6]

7.2 Požadavky vyvstávající ze závěrů této práce a z vlastních zkušeností

- Radiostanice pro průzkumné jednotky pořizovat s všesměrovými i se směrovými anténami.
- Veškeré prvky implementované do DSS musí být kompatibilní s powermanagement systémem, případně musí být dodán s redukcí/adaptérem.
- Je nutné standardizovat používané konektory a rozhraní.
- V případě využití bezdrátového přenosu typu wifi nebo bluetooth požadovat možnost řízení vysílaného výkonu.
- V případě zařízení bluetooth zajistit aby nevysílalo s výjimkou párování žádné informace mimo zabezpečené kanály (žádná komunikace v rámci discovery, nebo advertisement protokolů)
- Jakákoliv technologie plánovaná pro integraci do DSS musí být předem popsána v rámci systému a v případě utajovaného systému by měl být zpracován návrh projektu bezpečnosti s implementovaným prvkem a požádat o schválení příslušným úřadem.
- Pokud se bude jednat o prostředek poskytující kryptografickou ochranu, musí být certifikován, případně musí být zajištěna certifikace v rámci procesu akvizice.
- V případě, že zaváděný předmět potřebuje akreditaci nebo certifikaci, vždy v rámci akvizice vyhledávat již certifikované/ akreditované výrobky.
- Systém by měl umožnit vícevrstvé šifrování pro zprávy utajovaného charakteru. Šifrován by měl být jak kanál, tak tělo zprávy.
- Programové vybavení (především taktické aplikace) musí umožňovat zprávy definované na základě standardů například NATO STANG 5525 a potažmo ČOS 589501 (příkladem může být APP-11) a musí být stanoven přesný datový formát zprávy tak aby byla zajištěna kompatibilita zpráv mezi různými aplikacemi.
- Z důvodu nemožnosti využití online aktualizací doporučuji využití softwaru a OS s minimální nutností aktualizací – příkladem může být windows LTSC.

7.3 Doporučený postup návrhu systému

Vzhledem k řadě již existujících koncepcí by bylo vhodné prozkoumat varianty a návrhnout vlastní architekturu systému. Vhodným vzorem by mohl být projekt GOSSRA [40], (Generic Open Soldier Systems Reference Architecture), který má za cíl vytvářet otevřenou architekturu systému vojáka. Tento projekt je podporován prostřednictvím Evropské Obranné Agentury (EDA) a participuje na něm 6 členských států EU (a potažmo NATO). Vzhledem k rozsahu potřeb AČR by přistoupení k podobnému programu mohlo být výhodnější než samostatný vývoj, který v současném stavu sestává z několika částečně kompatibilních celků.

8 ZÁVĚR

V této práci byly prozkoumány základy bezpečnosti systému sesednutého vojáka, z hlediska kybernetické bezpečnosti. Problematika celého systému je poměrně složitá a nelze jednoduše zvažovat bezpečnost jednotlivých hardwarových prvků. Pro fungování DSS v režimu utajení je potřebné sestavit projekt bezpečnosti systému. K sestavení projektu bezpečnosti je nutné definovat základní architekturu systému a to v ideálním případě včetně veškerých vstupujících procesů a jejich vlastníků a uživatelů. V současné době takový popis pokud vím, neexistuje a pokud ano, AČR prozatím nedokázala jednotlivé komponenty DSS do tohoto systému implementovat.

Pro zajištění interoperability bude nutné vybudovat informační a komunikační systém sesednutého vojáka schopný nasazení v utajovaném režimu. Pro takové nastavení je pak nutný důkladný popis systému a jeho způsobu použití tak aby bylo možné systém akreditovat příslušnými úřady.

Problém, se kterým jsem se setkával při konzultaci s kolegy je neznalost samotných odborníků, kteří mi nebyli schopni odpovědět na řadu zdánlivě prostých otázek ani mě navést k dokumentům, které by je zodpovídali. Krásným příkladem je taktická informace zmiňovaná v zákonu 412/2005 Sb.. Bylo velmi problematické dohledat dokument, který ji popisuje, přičemž řada příslušníků armády, kteří se utajovanými systémy zabývají, neví, že takový dokument existuje. Tento dokument je utajovaný a pro tuto diplomovou práci by nebyl využitelný. Nicméně vzhledem k mé potřebě tyto problémy řešit v rámci pracovní náplně by mohl být důležitý a měl bych opodstatněnu potřebu znát jeho obsah. Utajení některých informací se zdá být příliš dokonalé.

Dle mého názoru jsem dostatečným způsobem poukázal na hrozby a rizika vyvstávající z jednotlivých technologických řešení. Nicméně jednotlivé technologie nebyly popsány dostatečně podrobně, aby bylo možné jednoznačně definovat problémy do té úrovně, kdy bylo možné přímo navrhnout technologická řešení architektury systému. Jednotlivé oblasti bude nutné rozpracovat do úrovně jednotlivých přenosových protokolů, kryptografických algoritmů a nastavení tak, aby byla zajištěna bezpečnost v rámci systémů sesednutého vojáka. Tato práce však může posloužit jako výchozí analýza pro zpracování projektu bezpečnosti systému sesednutého vojáka. V tomto bodě bude ovšem značně problematické jak přistoupit k nestejnorodým technologickým prostředkům ve výbavě vojsk. Jak už bylo poukázáno i v této práci.

SEZNAM POUŽITÉ LITERATURY

[1] Program digitalizace bojiště pro Armádu České republiky. *Technologická agentura ČR* [online]. Praha: TA ČR, c 2019 [cit. 2021-4-17]. Dostupné z: https://starfos.tacr.cz/cs/result/RIV%2F60162694%3AG10__%2F02%3A00000009#result-main

[2] Jednotné prostředí C4ISTAR. *Pramacom Optics and Communications* [online]. Praha: Pramacom-HT, c2016 [cit. 2021-4-17]. Dostupné z: http://www.infrared.cz/domains/infrared.cz/cz/projekty/istar.html

[3] C2 vs. C4ISR vs. C5ISR vs. C6ISR: What's the Difference? *Trenton systems* [online]. Lawrenceville: Trenton systems, c 2020, 16 Dec 2020 [cit. 2021-4-17]. Dostupné z: https://www.trentonsystems.com/blog/c2-c4isr-c5isr-c6isr-differences

[4] ČOS 589501. *Specifikace definující interoperabilní síť společného systému sesednutého vojáka*. Praha: Úřad pro obrannou standardizaci, katalogizaci a státní ověřování jakosti, 2019.

[5] ČESKÁ REPUBLIKA. Zákon o obranné standardizaci, katalogizaci a státním ověřování jakosti výrobků a služeb určených k zajištění obrany státu a o změně živnostenského zákona. In: *Sbírka zákonů*. Praha: Tiskárna Ministerstva vnitra, 2000, ročník 2000, částka 85, číslo 309. Dostupné také z: https://www.psp.cz/sqw/sbirka.sqw?cz=309&r=2000

[6] ČOS 589502. *Specifikace definující interoperabilní síť společného systému sesednutého vojáka – bezpečnost*. Praha: Úřad pro obrannou standardizaci, katalogizaci a státní ověřování jakosti, 2019.

[7] ČOS 589503. *Specifikace definující interoperabilní síť společného systému sesednutého vojáka – datový model*. Praha: Úřad pro obrannou standardizaci, katalogizaci a státní ověřování jakosti, 2019.

[8] ČOS 589504. *Specifikace definující interoperabilní síť společného systému sesednutého vojáka – zapůjčená radiostanice*. Praha: © Úřad pro obrannou standardizaci, katalogizaci a státní ověřování jakosti, 2019.

[9] ČOS 589505. *Specifikace definující interoperabilní síť společného systému sesednutého vojáka – mechanismus výměny informací*. Praha: © Úřad pro obrannou standardizaci, katalogizaci a státní ověřování jakosti, 2019.

[10] NATO - STANAG 4677. *Engineering 360* [online]. Albany: GlobalSpec, c 2021 [cit. 2021-4-25]. Dostupné z: https://standards.globalspec.com/std/9968493/STANAG%204677

[11] ČESKÁ REPUBLIKA. Vyhláška, kterou se mění vyhláška č. 105/2010 Sb., o plánu přidělení kmitočtových pásem: (národní kmitočtová tabulka). In: *Sbírka zákonů*. Praha: Tiskárna Ministerstva vnitra, 2017, ročník 2017, částka 150, číslo 423.

[12] Elektromagnetické záření. *Gymnázium, Český Krumlov* [online]. Český Krumlov: Gymnázium, Český Krumlov, c 2012 [cit. 2021-4-25]. Dostupné z: https://www.gymck.cz/storage/1364980243_sb_2s_4o_34_35_elmag_vlneni_01.pdf

[13] MPU5. *Persistent systems* [online]. New York: Pulse-creative, 2021 [cit. 2021-4-25]. Dostupné z: https://www.persistentsystems.com/mpu5/

[14] C-M(2002)49-REV1 SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANIZATION (NATO) dostupné z https://www.nbu.cz/download/C-M_2002_49_REV1_znackaNBU.pdf.

[15] HRŮZA, Petr. *Kybernetická bezpečnost II*. Brno: Univerzita obrany, 2013. ISBN 978-80-7231-931-2.

[16] SHELDON, John B. Cyberwar. *Britannica* [online]. Chicago: Encyclopædia Britannica, c 2021 [cit. 2021-4-26]. Dostupné z: https://www.britannica.com/topic/cyberwar

[17] ČESKÁ REPUBLIKA. Zákon č. 110/2019 Sb. Zákon o zpracování osobních údajů. In: *Sbírka zákonů*. Praha: Tiskárna Ministerstva vnitra, 2019, ročník 2019, částka 47, číslo 110. Dostupné také z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=33840

[18] ČESKÁ REPUBLIKA. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. In: *Sbírka zákonů*. Praha: Tiskárna Ministerstva vnitra, 2005, ročník 2005, částka 143, číslo 412. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-412/zneni-20201211

[19] DEPARTMENT OF NATIONAL DEFENCE. *SOLDIER SYSTEMS TECHNOLOGY ROADMAP: CAPSTONE REPORT AND ACTION PLAN*. Ottawa, 2013. Dostupné také z: https://www.defenceandsecurity.ca/UserFiles/File/pubs/capstone_e_05_high_quality-%233243236-v1-OTT_LSTL.PDF

[20] ČESKÁ REPUBLIKA., Zákon 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), 2014. In: *Sbírka zákonů*. ročník 2014, číslo 181. Dostupné také z: https://www.nbu.cz/download/pravni-predpisy/181_2014.pdf

[21] C4ISTAR Ground Force Systems. *ICZ* [online]. Pra: poctivaagentura [cit. 2021-5-1]. Dostupné z: https://www.iczgroup.com/en/products-and-services/defense/c4istar-ground-force-systems/

[22] APP-11 and ADatP-3. *Systematic* [online]. Aarhus: systematic [cit. 2021-4-28]. Dostupné z: https://systematic.com/defence/capabilities/c2/interoperability/app-11-and-adatp-3/

[23] CLARK, Jeremy a Urs HENGARTNER. Panic Passwords: Authenticating under Duress. *Usenix* [online]. Berkeley: Giant Rabbit, c 2021 [cit. 2021-4-28]. Dostupné z: https://www.usenix.org/legacy/event/hotsec08/tech/full_papers/clark/clark.pdf

[24] Instagram post. *Picuki* [online]. California: Picuki, c 2021 [cit. 2019-29-10]. Dostupné z: https://www.picuki.com

[25] ZETTER, Kim. *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. New York: Crown Publishers, 2014. ISBN 978-077-0436-193.

[26] MCDERMOT, Roger N. *Report Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum* [online]. Tallinn: International Centre for Defence and Security, 2017 [cit. 2021-4-28]. ISBN 978-9949-9972-0-6. Dostupné z: https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf

[27] *Koncepce výstavby Armády České republiky 2030* [online]. 1. Praha: Ministerstvo obrany České republiky - VHÚ Praha, 2019 [cit. 2020-10-17]. ISBN ISBN978-80-7278-789-0. Dostupné z: http://www.mocr.army.cz/images/id_40001_50000/46088/koncepce__2030.pdf

[28] SHAHID, Hasan. Radio Frequency Detection, Spectrum Analysis, and Direction Finding Equipment. *Homeland security* [online]. New York: National Urban Security Technology Laboratory, 2019 [cit. 2021-4-28]. Dostupné z: https://www.dhs.gov/sites/default/files/saver-msr-rf-detection_cod-508_10july2019.pdf

[29] KOVÁŘ, Pavel. Základy rádiové digitální komunikace. *Katedra radioelektroniky K13137* [online]. Praha: ČVUT FEL, 2021 [cit. 2021-4-28]. Dostupné z:

http://poseidon2.feld.cvut.cz/courses/E37EAA/materialy.php?akce=dlf&zdroj=vpm&fkey=18&xtgt=2f686f6d652f53657276696365732f7777772f68746d6c2f6564755f6465706f742f2f593337424b53

[30] Hoverfly Technologies chooses unmanned ad-hoc networking from Persistent Systems for tethered UAV. *Military & aerospace electronics* [online]. Nashville: Endeavor Business Media, c 2021, 20 mar 2019 [cit. 2021-4-28]. Dostupné z: https://www.militaryaerospace.com/unmanned/article/16721951/hoverfly-technologies-chooses-unmanned-adhoc-networking-from-persistent-systems-for-tethered-uav

[31] LTE: When the soldier's battlefield phone can only be the best. *Thales* [online]. Gothenburg: Thales group, 2021, 1.9.2019 [cit. 2021-4-29]. Dostupné z: https://www.thalesgroup.com/en/worldwide/defence/magazine/lte-when-soldiers-battlefield-phone-can-only-be-best

[32] ERWIN, Sandra. Airbus to build 'combat cloud' • Major developments in strategic nuclear systems • Senate panel targets EELV. *Https://spacenews.com/* [online]. Alexandria: Pocket Ventures, 2018, 25 July 2018 [cit. 2021-4-29]. Dostupné z: https://spacenews.com/sn-military-space-airbus-to-build-combat-cloud-%E2%80%A2-major-developments-in-strategic-nuclear-systems-%E2%80%A2-senate-panel-targets-eelv/

[33] LTE. *General dynamics: Mission Systems* [online]. Fairfax: General Dynamics Mission Systems, c 2021 [cit. 2021-4-29]. Dostupné z: https://gdmissionsystems.com/communications/lte

[34] Galaxy S20 tactical edition. *Samsung* [online]. San Jose: SAMSUNG ELECTRONICS AMERICA, c 1995-2021 [cit. 2021-4-29]. Dostupné z: https://www.samsung.com/us/business/solutions/industries/government/tactical-edition/

[35] ČESKÁ REPUBLIKA. Vyhláška o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor. In: *Sbírka zákonů*. Praha: Tiskárna Ministerstva vnitra, 2011, ročník 2005, částka 155, číslo 523. Dostupné také z: https://nukib.cz/download/bezpecnost_informacnich_systemu/legislativa/523-2005.pdf

[36] *SAFRAN* [online]. Heerbrugg: Safran Vectronix, c2017 [cit. 2021-4-5]. Dostupné z: https://www.safran-vectronix.com/

[37] Systém detekce laserového a radarového ozáření LAWAREC. *EVPÚDEFENCE* [online]. Uherské Hradiště: machin.cz, c 2021 [cit. 2021-4-29]. Dostupné z: https://www.evpudefence.com/cs/p-system-detekce-laseroveho-a-radaroveho-ozareni-lawarec

[38] PRAVDA, Lukáš. Seminář pro provozovatele Wi-Fi zařízení a sítí. *Český telekomunikační úřad* [online]. Praha: ČTÚ, c 2018 [cit. 2021-5-1]. Dostupné z: https://www.ctu.cz/cs/download/seminare/rok_2014/seminar-wifi_prezentace-02_podminky-vyuzivani-kmitoctoveho-spektra_vo-r_12-09_2010-12.pdf

[39] MIKÉSKA, Zdeněk. Radio Specification of the Bluetooth System. *Elektrorevue* [online]. Brno: International Science and Engineering Society, c 2013 [cit. 2021-4-30]. Dostupné z: http://www.elektrorevue.cz/clanky/04003/english.htm

[40] *Generic Open Soldier system reference Architecture* [online]. Ismaning: GOSSRA Consortium, c 2019 [cit. 2021-4-30]. Dostupné z: https://gossra.net/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AP	Access Point
BFT	Blue Force Tracking
BTS	Base Transceiver Station
C2	Command, Control
C4ISTAR	Command, Control, Communication, Computer, Intelligence, Surveillance, Target Acquisition, Reconnaissance
DSS	Dismounted Soldier System
EB (EW)	Elektronický Boj (Electronic Warfare)
EDA	European Defence Agency
LOS	Line Of Sight
MANET	Mobile Ad Hoc NETwork
NATO	North Atlantic Treaty Organization
SA	Situational Awareness
SDR	Software defined radio
SIEM	Security information and event management
TZD	Taktický Zobrazovací Displej
TZT	Taktický Zobrazovací Terminál
UAV	Unmaned Aerial Vehicle
UGV	Unmaned Ground Vehicle
UHF	Ultra High Frequency
UKV	Ultra Krátké Vlny
VHF	Very High Frequency
VKV	Velmi Krátké Vlny

SEZNAM OBRÁZKŮ

SEZNAM TABULEK