
Recenzovaný článek

Sociální média jako nástroj profilace potenciálních zdrojů zpravodajských služeb. Jak jsou na tom vojenští studenti?

Social Media as a Tool for Profiling Potential Intelligence Service Sources. How are the Military Students Doing?

Libor Kutěj

Univerzita obrany, Brno, Česká republika

Abstrakt: Článek se zabývá využitím zpravodajství ze sociálních médií (SOCMINT) jako nástroje pro výběr a rekrutaci zdrojů ze strany cizích zpravodajských služeb s důrazem na rizika pro studenty vojenského studia státní vojenské vysoké školy. Analyzuje specifika využívání SOCMINT umožňující cizím rozvědkám efektivně získávat osobní údaje a profilovat potenciální spolupracovníky z veřejných i soukromých informací sdílených online. Výzkum provedený mezi studenty Univerzity obrany a dalších škol ukázal, že studenti vojenských oborů sdílejí na sociálních sítích srovnatelný typ informací jako jejich civilní vrstevníci, což je činí stejně zranitelnými vůči aktivitám cizích rozvědek, ovšem s tím rozdílem, že vojenští studenti se připravují na povolání v oblasti obrany a bezpečnosti, čímž se stávají mnohem atraktivnějším cílem cizích zpravodajských agentur než v případě jiných kategorií zaměstnanců.

Abstract: The article addresses the use of social media intelligence (SOCMINT) as a tool for recruiting and selecting sources by foreign intelligence services, with an emphasis on the risks it poses to students in military studies at national military university. It analyzes the specific ways in which SOCMINT enables foreign intelligence agencies to effectively gather personal data and profile potential collaborators from both public and private information shared online. Research conducted among students of the University of Defense and other institutions revealed that military students share comparable types of information on social networks as their civilian peers, making them equally vulnerable to the activities of foreign intelligence services. However, military students are preparing for careers in defense and security, making them a significantly more attractive target for foreign intelligence agencies than other categories of employees.

Klíčová slova: HUMINT; rekrutace; SOCMINT; zpravodajství z lidských zdrojů; zpravodajství ze sociálních médií.

Keywords: HUMINT; Recruitment; SOCMINT; Human Intelligence; Social Media Intelligence.

ÚVOD

V dynamickém prostředí zpravodajských služeb se stále více využívají nové technologické nástroje a analytické metody pro zlepšení kvality shromažďování a analýzy informací. Jedním z těchto nástrojů je zpravodajství ze sociálních médií (Social Media Intelligence, SOCMINT), kterým se rozumí proces sběru a analýzy dat z veřejných sociálních médií s cílem získat užitečné informace. Je považováno za podobor a součást širšího konceptu zpravodajství z otevřených zdrojů (Open-Source Intelligence, OSINT). Na jeho používání však není nahlíženo tak bezproblémově jako je tomu u klasického OSINT, jelikož při užívání platform sociálních médií je ze strany jejich uživatelů očekávána jistá míra soukromí. SOCMINT využívá také informace nalezené na platformách sociálních médií, které byly určeny jen pro konkrétní publikum. Metody SOCMINT však zahrnují neautorizované připojení k vybrané skupině uživatelů nebo vytvoření falešného účtu k zajištění přístupu k účtu určitého uživatele. SOCMINT zahrnuje všechny platformy sociálních médií, nikoli jen sociálních sítí. Sociální síť jako Facebook nebo LinkedIn představují pouze část platform využitelných ke sběru dat. Dalšími jsou platformy pro sdílení médií, jakými jsou například Instagram, diskusní fóra jako Reddit, weby pro sdílení obrázků jako Pinterest, videí YouTube, mikrobloginovací platformy typu X (dříve Twitter), sociální herní platformy jako Xbox Live a blogy vytvořené pomocí platform typu WordPress (Terrell Hanna and Lutkevich 2025; Hejzlarová, Mouralová, and Štěpánková Štýbrová 2023, 299-302).

Základními typy informací, které lze získat monitoringem platform sociálních médií jsou informace o profilu, které jsou poskytnuté samotným uživatelem a jsou viditelné těm, kteří k profilu přistupují. Na některých specifických platformách (například LinkedIn) to mohou být informace o pracovní zkušenosti a pozici uživatele, jeho profesní historii a kontaktní informace. Dále jsou to data a informace z interakcí uživatelů, které jsou dány členstvím uživatele v některé z uživatelských skupin a zveřejňování či komentování obsahu uveřejněného jinými uživateli. Součástí takových interakcí je též uveřejňování obrázků nebo videí a lajkování či jiné reakce na zveřejňovaný obsah. Významnou část dat představují metadata, tedy informace, které se kontextuálně vztahují k uveřejněnému obsahu jako jsou lokalita a čas kdy byl příspěvek vytvořen či dokonce zařízení, kterým byl snímek pořízen. Obecně lze konstatovat, že prostřednictvím SOCMINT lze získat data vázající se k obsahu příspěvků (textové, obrazové a video příspěvky na sociálních sítích, jejich obsah, emotivní tón, používání hashtagů nebo odkazů), o chování uživatelů (aktivita uživatelů, časy publikací, frekvence interakcí - lajky, komentáře, sdílení), o sociálních vazbách (kdo s kým interaguje, jaké skupiny uživatelé sledují, komu dávají přednost, síťové propojení mezi uživateli), geolokační údaje (pokud je součástí příspěvku polohová

značka, lze zjistit, kde byl příspěvek vytvořen a kdy), demografické údaje (věk, pohlaví, místo pobytu, zájmy nebo profesní zaměření uživatelů), trendy a sentimenty (analýza toho, jak veřejnost vnímá konkrétní téma, jaké jsou aktuální trendy a jak se nálady mění v čase) (Maltego 2024). Množství údajů je závislé na rozsahu jednotlivých sledovaných sociálních sítí, např. X, Facebook, Instagram, YouTube. Sociální sítě poskytují obrovské množství informací, denně se na tyto platformy nahrávají miliardy příspěvků, což umožňuje získat ohromné množství dat, ale samozřejmě také data určité skupiny uživatelů či jednotlivců, na které je sběr informací zaměřen (Terrell Hanna and Lutkevich 2025).

V oblasti zpravodajství nalézá SOCMINT velmi široké využití. Sledováním trendů a změn v chování uživatelů lze do jisté míry předpovědět, jak se budou vyvíjet různé sociální, politické nebo ekonomické události. Pomocí analýzy sentimentu lze zjistit, jaké emoce lidé spojují s určitou událostí nebo politickým tématem. V reálném čase lze sledovat, jak se šíří informace o krizových situacích (např. přírodní katastrofy, teroristické útoky) a kde se nacházejí hlavní zdroje informací. SOCMINT může sloužit bezpečnostním složkám k monitorování rizikových aktivit, detekci potenciálních hrozeb (např. extremistických skupin nebo plánování zločinů) a analýze zpravodajsky relevantního chování (Kutěj 2021, 28-29).

1 MOŽNOSTI SOCMINT V PRAXI AGENTURNÍHO ZPRAVODAJSTVÍ

Jedním z klíčových a nezastupitelných základních zpravodajských oborů zůstává zpravodajství z lidských zdrojů (Human intelligence, HUMINT), které je postaveno na využívání lidských zdrojů, především pak takových, které jednájí ve prospěch zpravodajské služby. Tyto zdroje (agenti) jsou vybírány přímo v zájmovém prostředí nebo by měly mít možnost si přístup do tohoto prostředí získat (Horák and Kutěj 2016, 19-20). Po celé dekady tvořila významnou část každodenní zpravodajské práce získávání a ověřování údajů o potenciálních zdrojích, což bylo náročné jak na síly, tak prostředky zpravodajské služby. Narůstající množství digitálních dat o osobách uveřejňovaných na platformách sociálních médií vyvolává otázku, jakým způsobem obohatit tradiční metody výběru potenciálních zdrojů HUMINT o metody SOCMINT (Kutěj 2021, 28-29).

Dnes je zřejmé a v praxi ověřené, že využití SOCMINT pro výběr a rekrutaci agentů představuje inovativní přístup, který dokáže efektivně podpořit tradiční metody HUMINT. SOCMINT lze použít ve všech fázích rekrutace agentů, od počátečního výběru vhodných kandidátů až po jejich oslovení a následné monitorování. SOCMINT umožňuje důstojníkům zpravodajských služeb vyhledávat osoby s požadovaným profesním, osobním nebo geografickým profilem. Například při hledání osob s přístupem k citlivým informacím v určité oblasti mohou analytici pomocí vyhledávacích a filtrujících nástrojů identifikovat jedince s odpovídajícím zaměstnáním, vzděláním, kontakty a aktivitami na sociálních platformách. SOCMINT umožňuje získat informace nejen o profesní kvalifikaci, ale i o osobnostních rysech, zájmech, osobních hodnotách a postojích kandidátů. Analýza historie příspěvků, sdíleného obsahu, názorů a sociálních interakcí na platformách jako Facebook nebo Instagram může poskytnout hlubší náhled na to, jak daný jedinec reaguje na různé podněty a jaká je jeho motivace, což může být klíčové při hodnocení jeho

vhodnosti pro určité operace. S využitím SOCMINT lze poznat vlastnosti zájmové osoby, které mohou usnadnit ovlivnění potenciálního kandidáta. To zahrnuje identifikaci osobních nebo finančních problémů, nespokojenost se současnou pracovní pozicí, politickou či sociální frustraci nebo osobní aspirace. Tyto faktory lze zjistit z veřejných příspěvků, diskusí a reakcí na aktuální události. S těmito informacemi je pak možné přesněji definovat přístup k oslovení a nabídku spolupráce, která by rezonovala s potřebami a motivacemi kandidáta. SOCMINT také poskytuje možnost analyzovat sociální vazby jedinců a identifikovat jejich blízké kontakty. Tato analýza může odhalit osobní nebo profesní vztahy, které by mohly mít vliv na rozhodnutí daného jedince přijmout spolupráci nebo by mohly být využity k nepřímému ovlivnění. Mapování vztahů může rovněž odhalit, zda má kandidát vazby na nepřátelské skupiny, konkurenční agentury nebo rizikové subjekty, což je klíčové pro vyhodnocení bezpečnosti samotného rekručního procesu (Kutěj 2021, 62-69).

Na základě zjištěných informací lze připravit přesně cílené komunikační strategie, které využívají online prostředí k navázání kontaktu způsobem, který minimalizuje podezření. SOCMINT například může pomoci zjistit, jaké kanály jsou pro komunikaci s kandidátem vhodné a předejít tím nežádoucí pozornosti nebo odhalení. Po výběru vhodného kandidáta a jeho získání ke spolupráci se zpravodajskou službou lze SOCMINT použít ke kontinuálnímu sledování jeho aktivit na sociálních sítích, aby se zjistilo, zda nedochází k nevysvětlitelným projevům v jeho chování, které by mohly znamenat bezpečnostní riziko, signalizovat změnu loajality nebo snahu o ukončení spolupráce. Takto získané informace umožňují pružně reagovat na aktuální situaci a přizpůsobit metody řízení agenta v procesu jeho používání (Kutěj 2021, 69-70).

Celkově SOCMINT umožňuje zpravodajské službě personalizovaný přístup k rekrutaci agentů, který vychází z analýzy dat a chování na sociálních sítích. Integrace SOCMINT do procesu výběru a rekrutace tak zvyšuje efektivitu zpravodajských operací a bezpečnost celého výběru, získávání a řízení agenturní práce.

2 CHARAKTER INFORMACÍ PŘÍNOSNÝCH PRO TIPOVÁNÍ POTENCIÁLNÍHO ZDROJE

Data získaná využitím SOCMINT o vybraných osobách ty jsou nezastupitelná především ve fázi tipování vhodné osoby ke spolupráci se zpravodajskou službou. Mimo údajů o potenciálu určité osoby plnit úkoly ve prospěch zpravodajské služby jsou rozhodujícími takové informace, které mají zpravidla osobní povahu a vypovídají o motivaci jedince spolupracovat se zpravodajskou službou, což může významným způsobem ovlivnit rekruční proces (Termann 1997, 160). Samotné hodnocení motivace je pro rozvedku obtížné a pokud se jedná o budování zdroje ve významné oblasti zpravodajského zájmu je k vyhodnocení zjištěných poznatků zpravidla přizván operativní psycholog. Široce sdílené údaje v sociálních médiích rozšiřují možnost kvalifikovaného hodnocení motivačních faktorů. Ty jsou poté nezřídka využity také v samotné fázi získávání ke spolupráci a při kontrole serióznosti zdroje ve fázi jeho používání. Některé uveřejňované informace např. o oblíbeném jídle a nápojích a oblíbeném oblečení mohou nezřídka vypovídat o

požívačnosti, oblibě luxusu, touze experimentovat, snaze vyniknout a podobných projevech bezprostředně souvisejících s prezentací jedince v určité společenské skupině. Poznání těchto vlastností se dá zpravodajskou službou velmi výhodně využít formou přípravy pozitivních motivačních pobídek (Termann 1997, 161; Kutěj 2020, 68).

3 METODOLOGIE

Cílem výzkumu bylo prozkoumat možnosti využití SOCMINT pro získání údajů využitelných cizími zpravodajskými službami k efektivnímu tipování a rekrutaci agentů ve prospěch HUMINT a zjistit nakolik jsou takto využitelné informace uveřejňovány na platformách sociálních médií budoucími vysokoškolsky vzdělanými důstojníky Armády České republiky.

Pro dosažení cílů výzkumu byly stanoveny dvě hypotézy:

1. Studenti vysoké vojenské školy uveřejňují na platformách sociálních médií typově a charakterově odlišné informace, než studenti jiných vybraných škol z bezpečnostním či mezinárodněvztahovým zaměřením studia.
2. Studenti vysoké vojenské školy jako uživatelé sociálních médií uveřejňují na těchto platformách údaje, které jsou využitelné v procesu tipování a rekrutace ze strany cizích zpravodajských služeb.

K ověření platnosti uvedených hypotéz byl proveden smíšený výzkum kombinující kvalitativní a kvantitativní metody (Hendl 2012, 58-59, 273). Pro vymezení kategorií údajů a informací, jejichž uveřejnění v sociálních médiích umožňuje cizím zpravodajským službám budování agenturních pozic bylo využito empiricko-deduktivní metody a metody abduktivní logiky společenskovedního výzkumu, které umožnily zprostředkovat obecné metody zpravodajské činnosti v souladu s potřebou stanovení kritérií zpravodajské využitelnosti dat sdílených na sociálních platformách (Hendl 2012, 34).

V části výzkumu věnované uveřejňování informací specificky vhodných pro budování agenturních pozic cizích rozvědek v ozbrojených silách ČR bylo pracováno pouze se vzorkem studentů Univerzity obrany (86 % vojenské studium a 16 % civilní studium).

Na základě více než dvacetileté zpravodajské empirie autora v oblasti HUMINT bylo vytipováno šest oblastí, které mají či mohou mít vliv na hodnocení motivace zdroje ke spolupráci s cizí rozvědkou:

- užívání omamných a psychotropních látek;
- finanční situace;
- závislosti;
- sexuální orientace;
- oblíbené jídlo a nápoje;
- oblíbené oblečení.

Proces přípravy potenciálního zdroje před jeho získáním ke spolupráci s cizí zpravodajskou službou je charakteristický snahou této služby získat co největší množství informací, které operativnímu pracovníkovi umožní se k této osobě přiblížit, tedy vytvořit přímý či zprostředkovaný kontakt. Součástí je získat natolik hluboké poznání osobnosti a zvyků

zájmové osoby, že rozvědka může připravit formu a obsah získávacího pohovoru (Kutěj 2020, 67-69).

V tomto smyslu jsou nejvíce užitečné informace z následujících oblastí:

- režim dne;
- zvyky;
- kontakty (konkrétní osoby, obsah a forma interpersonálních vztahů);
- rodinné a partnerské zázemí;
- zájmy a záliby;
- touhy, přání, ambice v soukromém životě.

V souladu s cílem výzkumu bylo vytipováno pět tematických okruhů sdílených na sociálních sítích, které mají či mohou mít vypovídací hodnotu o shora uvedených zájmových oblastech:

- rodina;
- přátelské vztahy;
- intimní vztahy;
- způsob trávení volného času;
- fotografie z navštívených míst.

Pro zjištění charakteru sdílených informací ze strany vzorku respondentů výzkumu bylo využito elektronického dotazování v rámci kvantitativní metody sběru dat ke zjištění primárních informací a jejich následnému statistickému zpracování použitím analytických nástrojů zpracování dat (Červenka a Kunštát 2006, 47-66). Srovnání mezi jednotlivými vzorky respondentů bylo provedeno komparativní metodou.

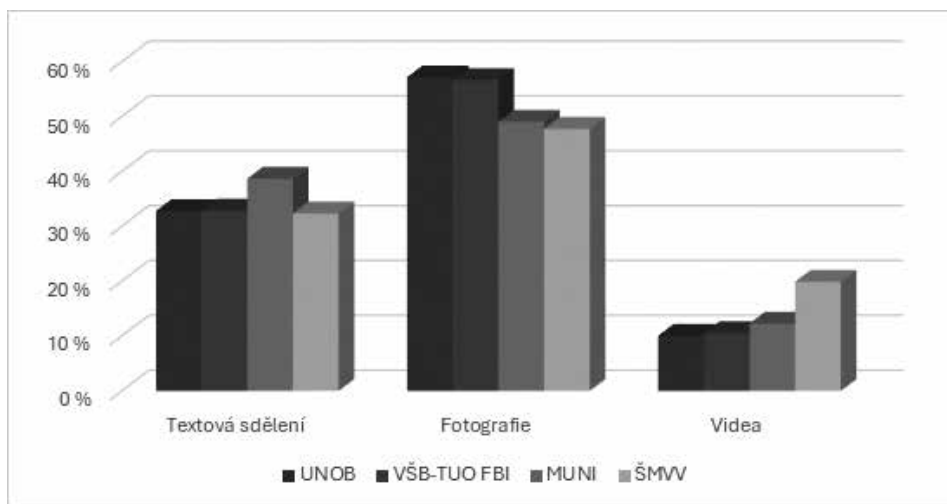
Respondenti kvantitativní fáze výzkumu (celkový počet 881) byli náhodně vybráni mezi studenty tří vysokých a jedné střední školy se zřejmou či předpokládanou (nicméně vzájemně odlišnou formou) vazbou na prostředí obrany a bezpečnosti. První vzorek respondentů představovali studenti prezenčního a kombinovaného studia Univerzity obrany v Brně. Předmětná škola byla zvolena s ohledem na její postavení jako jediné vojenské vysoké školy v ČR. Výkon práce jejich absolventů má zpravidla přímé spojení s činností ozbrojených sil ČR, většinou pak ve služebním poměru vojáků z povolání. Vzorek respondentů Univerzity obrany (UNOB) byl tvořen 498 studenty. Druhý vzorek respondentů byl tvořen studenty Fakulty bezpečnostního inženýrství Vysoké školy báňské – Technické univerzity Ostrava (VŠB-TUO) a jednalo se o 214 respondentů. Třetím vzorkem byli studenti programu „Mezinárodní vztahy a evropská studia“ a „Bezpečnostní a strategická studia“ Fakulty sociálních studií Masarykovy univerzity (MUNI), přičemž vzorek představoval 66 respondentů. Čtvrtým vzorkem byli studenti Školy mezinárodních a veřejných vztahů Praha (SMVV) oboru „Mezinárodní studia a diplomacie“ a čítal 103 respondenty.

Kvantitativní část výzkumu s uvedenými vzorky respondentů byla provedena formou dotazníkového šetření umožňující rychlý sběr řady dat. V části šetření zaměřené na zjištění platform sociálních médií, která jsou jednotlivými skupinami respondentů využívána a v jaké míře, byla v dotazníkovém šetření použita forma vícenásobné odpovědi. Otázky byly voleny jako identifikační a uzavřené. Jejich formulace byla volena tak, aby neumožňovala zkreslení významu, sugestivní zabarvení, hypotetické odpovědi, stereotypní sugesce a otázky obsahující najednou dva a více problémů. Žádná z formulovaných otázek nesměřovala k identifikaci politických a ideologických preferencí respondentů.

4 VÝSLEDKY

V poměru uživatelů sociálních médií k celkovému množství respondentů nebyl zjištěn rozdíl představovaný pohlavím respondentů, jejich příslušností k ozbrojeným silám nebo bezpečnostním sborům ČR a stupni studované školy v rámci vzdělávacího systému. Ve všech vzorcích respondentů je podíl aktivních uživatelů sociálních sítí téměř nebo zcela 100 %. Toto číslo plně podporuje obecně sdílený předpoklad, že naprostá většina populace příslušníků tzv. generace Z se aktivně projevuje na sociálních médiích. Dílčí rozdíly byly zjištěny mezi nejvyužívanějšími platformami sociálních médií. U vzorků UNOB a VŠB-TUO nejvíce respondentů využívá Facebook a jako druhé médium Instagram. U vzorků MUNI a ŠMVV je nejoblíbenější platformou Instagram následovaný Facebookem.

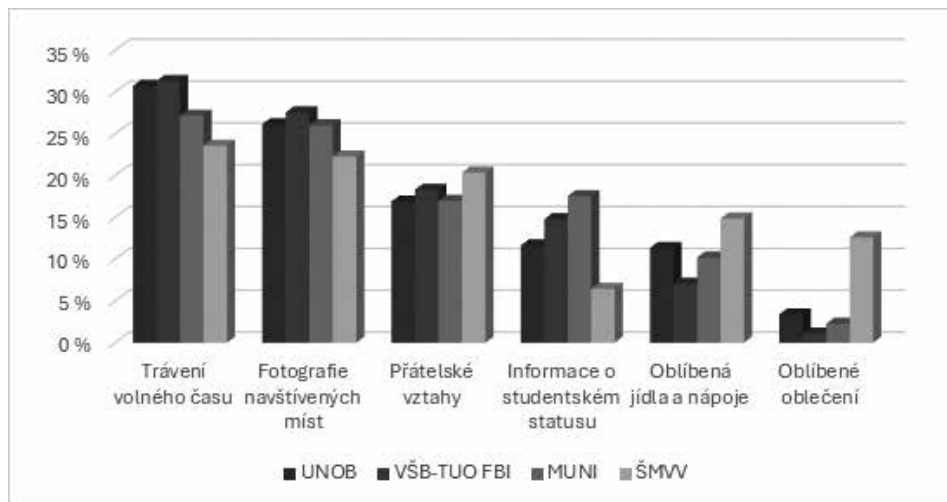
Při zkoumání forem příspěvků uveřejňovaných na sociálních sítích byly zohledněny textové zprávy a komentáře, fotografie a videa. Je evidentní (viz obrázek 1), že ve všech případech je fotografie převládající formou využívanou k uveřejnění. Okolo třetiny respondentů uveřejňuje příspěvky mající charakter textového sdělení a asi desetina (v případě ŠMVV se však jedná o celou pětinu respondentů) publikuje videozáznamy.



Obrázek 1: Podíl forem uveřejňovaných příspěvků

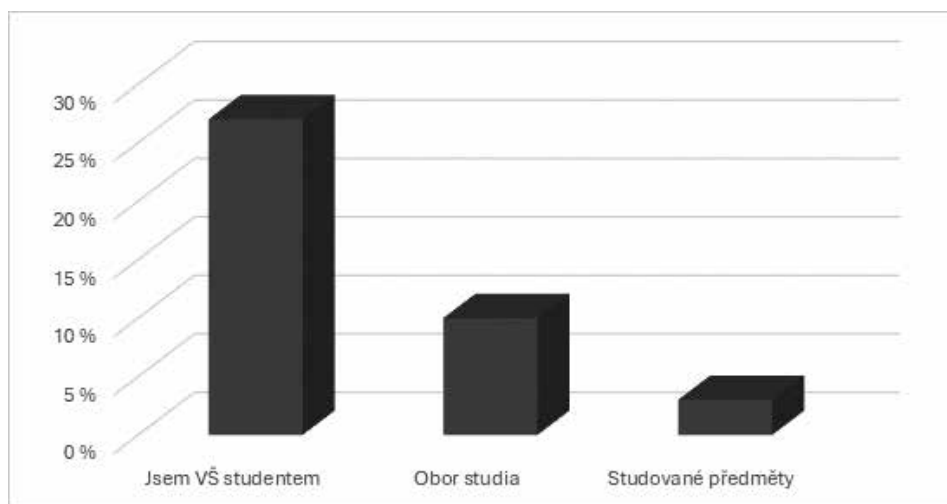
Stran charakteru příspěvků na sociálních sítích byly v případě skupin respondentů ze všech tří vysokých škol zjištěny čtyři převládající oblasti, které jsou předmětem prezentace na sociálních sítích (viz obrázek 2). Nejvíce se jedná o způsob trávení volného času (UNOB 70 %, VŠB-TUO FBI 71 % a MUNI 75 %), dále fotografie navštívených míst (UNOB 60 %, VŠB-TUO FBI 62 % a MUNI 72 %), přátelské vztahy (UNOB 39 %, VŠB-TUO FBI 41 % a MUNI 47 %) a informace o skutečnosti, že uživatelé jsou vysokoškolskými studenty (UNOB 27 %, VŠB-TUO FBI 33 % a MUNI 48 %). Poměrně početnou kategorií

uveřejňovaných příspěvků jsou oblíbená jídla a nápoje (UNOB 26 %, VŠB-TUO FBI 16 % a MUNI 28 %).



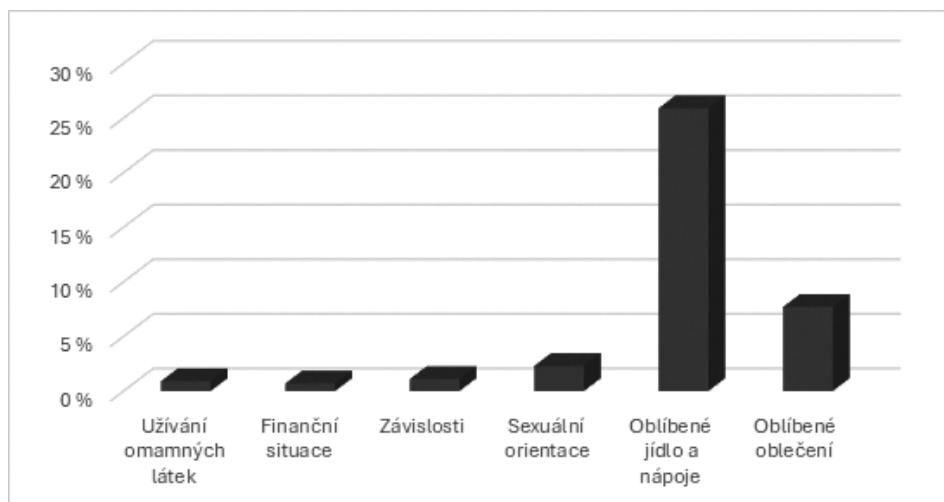
Obrázek 2: Podíl charakteru příspěvků ve vybraných kategoriích u respondentů VŠ

Pro perspektivní výběr potenciální zdrojové báze jsou významné především informace o samotném vojenském vysokoškolském studiu a specializaci studia, ze které lze usuzovat další směr kariérního růstu ve vybraném druhu ozbrojených sil. Podíl respondentů ve vzorku UNOB ve vztahu k uveřejňování tohoto typu informací prezentuje obrázek 3.



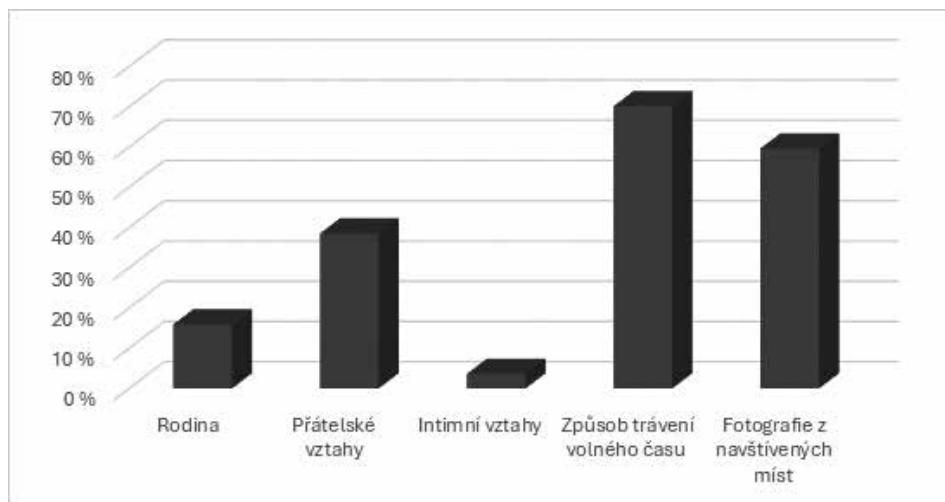
Obrázek 3: Podíl respondentů skupiny UNOB uveřejňujících informace o studiu a jeho specializaci

Výsledky dotazování na oblast uveřejňování takových informací, které mohou být cizími speciálními službami využity pro hodnocení motivace jedince k práci pro rozvědku cizího státu znázorňuje obrázek 4.



Obrázek 4: Podíl respondentů skupiny UNOB uveřejňujících informace o vybraných osobnostních parametrech

Část výzkumu zaměřená na uveřejňování informací umožňujících cizí zpravodajské službě získat natolik hluboké poznání osobnosti a zvyků zájmové osoby, že jí usnadní přípravu formy a obsahu získávacího pohovoru ukázala (viz obrázek 5), že ve vzorku respondentů UNOB jsou nejvíce zveřejňovány údaje ke způsobu trávení volného času a fotografií z navštívených míst. Méně než polovina respondentů prezentuje přátelské vztahy a jen něco více než 10 % uvádí údaje o rodině. Minimálně je komunikováno o intimních vztazích.



Obrázek 5: Podíl respondentů skupiny UNOB uveřejňujících informace osobního charakteru

5 DISKUSE

V poměru uživatelů sociálních médií k celkovému množství respondentů nebyl zjištěn rozdíl představovaný pohlavím respondentů, jejich příslušností k ozbrojeným silám nebo bezpečnostním sborům ČR a stupni studované školy. Ve všech vzorcích respondentů je podíl aktivních uživatelů sociálních sítí téměř nebo zcela 100 %. Toto číslo plně podporuje poznání, kdy naprostá většina populace příslušníků tzv. generace Z se aktivně projevuje v sociálních médiích.

Byly zjištěny dílčí rozdíly mezi využívanějšími platformami sociálních médií. U vzorků UNOB a VŠB-TUO nejvíce respondentů využívá Facebook a jako druhé médium Instagram. U vzorků MUNI a ŠMVV je nejoblíbenější platformou Instagram následovaný Facebookem. Z provedeného výzkumu není možné usuzovat, čím je dán uvedený rozdíl v oblíbenosti. Nabízí se otázka, zda se jedná o rozdíl daný studiem škol technického zaměření, resp. společenskovedního směru, nicméně zde nelze dospět k uspokojivé odpovědi a pro dosažení cíle výzkumu se nejedná o relevantní problém. Obdobně by bylo možné spekulovat o tom, zda generace dnešních vysokoškolských studentů je uvklá více konfiguraci a funkcím Facebooku a generace středoškolských studentů již více na novější platformu Instagram. Nicméně se opět s ohledem na cíl výzkumu nejedná o relevantní zjištění.

Šetření nepotvrdilo rozdíly v charakteru příspěvků uveřejňovaných na sociálních sítích u respondentů z řad studentů vysokých škol. Ve středoškolského vzorku ŠMVV byl zjištěn vyšší důraz položený na prezentaci „sebe sama“ (oblíbené jídlo a nápoje, oblíbené oblečení) a nižší na prezentaci profesní (jsem studentem a typ studované školy). Těžko

dovozovat na důvod nízkého zájmu středoškoláků prezentovat informace vztahující se ke studiu; pro spekulaci se nabízí nižší míra profesní vyhraněnosti při studiu „zatím“ střední školy a nízké soustředění na profesní budoucnost. Nebyly zjištěny zásadní rozdíly ve formách uveřejňovaných příspěvků. Převládají fotografie, poté textová sdělení a následně videozáznamy. Ve všech vzorcích respondentů byly jako nejvíce publikovaná témata zjištěny způsob trávení volného času, sdílení fotografií z navštívených míst a přátelské vztahy. Mezi vzorky respondentů nebyly zjištěny relevantní rozdíly v podílu uživatelů, kteří si nastavují soukromí svých uživatelských účtů. Souhrnně lze konstatovat, že na základě dat zjištěných u stanovených kategorií šetření nebyly zjištěny relevantní rozdíly mezi jednotlivými skupinami respondentů.

V kontextu cíle výzkumu lze tvrdit, že studenti Univerzity obrany nemají odlišný způsob a rozsah aktivního využívání sociálních médií než studenti mimo resort obrany, jakkoli s vazbami na prostředí obrany, bezpečnosti, resp. mezinárodních vztahů. Skutečnost, že studenti Univerzity obrany jsou zpravidla ve služebním poměru vojáka z povolání (86 % respondentů) a připravují se na výkon práce v oblasti obrany ČR, tuto realitu nijak neovlivňuje. Chování těchto budoucích velitelů a manažerů resortu obrany na sociálních sítích je stejné jako u jiných studujících této generace bez ohledu na specifický charakter studia a budoucího povolání.

Výzkum ukázal, že studenti Univerzity obrany na svých sociálně-mediálních účtech sdílejí informace, které mohou být zahraničními rozvědkami využity při tipování vhodných spolupracovníků. V oblasti informací o samotném vojenském vysokoškolském studiu a specializaci studia respondenti vzorku UNOB vykazují standardní míru otevřenosti srovnatelnou s jinými vysokými školami. Mezi těmito dokonce prezentují svou profesní afilaci nejméně (vzorek UNOB 27 %, vzorek VŠB-TUO 33 % a vzorek MUNI 48 %). Nicméně jen samotné sdílení informace o studiu Univerzity obrany nemůže být vnímáno negativně, a naopak je možné je využít např. marketingově ve prospěch propagace studia vojenských oborů.

U sdílení informací umožňujících poznání osobnosti a zvyků zájmové osoby vzorek respondentů Univerzity obrany opět nijak nevybočuje z typů a rozsahu sdíleného obsahu ve srovnání s respondenty z dalších vysokých škol. Je ovšem skutečností, že na podkladě toho, co respondenti z řad studentů Univerzity obrany na sociálních sítích sdílejí, si lze poměrně jednoduše vytvořit obrázek o jejich zálibách, způsobu trávení volného času a také o charakteru a kvalitě přátelských vztahů. Taková míra je pro cizí zpravodajskou službu dostatečná pro přípravu nejvhodnější formy kontaktu a případně kompletaci motivační pobídky.

Na základě výsledků provedeného výzkumu lze konstatovat, že stanovená hypotéza, podle které studenti vysoké vojenské školy uveřejňují na platformách sociálních médií typově a charakterově odlišné informace, než studenti jiných vybraných škol z bezpečnostním či mezinárodněvztahovým zaměřením studia se nepotvrdila. Je evidentní, že typ a charakter informací uveřejňovaných na sociálních sítích je v zásadě stejný jako v případě studentů jiných vybraných vysokých škol a specifický charakter vojenského studia nemá na možnou odlišnost vliv.

Naopak tvrzení, podle kterého studenti vysoké vojenské školy jako uživatelé sociálních médií uveřejňují na těchto platformách údaje, které jsou využitelné v procesu tipování a

rekrutace ze strany cizích zpravodajských služeb se ukázalo jako pravdivé. Bez ohledu na specifický charakter vojenského studia a budoucí zařazení jeho absolventů v ozbrojených silách ČR existují vhodné podmínky pro využití SOCMINT k tipování a rekrutaci zdrojů z profesního prostředí obrany ČR ke spolupráci s cizí zpravodajskou službou.

ZÁVĚR

V současné době více než dvě miliardy lidí po celém světě používají účet na Facebooku nebo na jiné platformě nehledě na profesní účty na LinkedIn a podobných platformách. SOCMINT tak může být velmi účinným nástrojem činnosti cizích výzvědných agentur, stejně tak se však může stát instrumentem kontrarozvědných složek ke zpravodajské ochraně. Na profesních platformách, jako např. LinkedIn, lidé sdílejí ohromující množství informací o jejich pracovním zařazení, obsahu jejich práce, detailech jejich dosavadní kariéry, zařazení v rámci korporátní hierarchie, údaje o klientské bázi, data o zaměstnavateli, vojenské službě, stupni bezpečnostního prověření a další a další údaje, které by mimo sociální média zpravodajské služby shromažďovaly dlouhé měsíce, přičemž řada z těchto údajů by pro cizí rozvědky nebyla dostupná nikdy. (Gioe 2017, 217-218)

V návaznosti na uvedené je potřeba vnímat společenskou realitu dnešní doby. Jak ukazují výsledky provedeného průzkumu, generace dnešní mládeže je v zásadě plně přítomna na sociálních sítích a není předpoklad, že by se tato situace kdykoli v budoucnu změnila. Je charakteristická rychlým životním stylem, z něž velkou část zabírá on-line přítomnost. Ta jí umožňuje rychlé sdílení myšlenek a názorů na různá témata prostřednictvím řady sociálních médií a technologických produktů. Je vyspělá v počítačových technologiích, jelikož se již narodila do doby, ve které se komputelizace stala masovou záležitostí. Již z podstaty věci je tedy nemožné, aby se příslušníci této generace chovali odlišně, a to bez ohledu na určitá specifika, která s sebou přináší vojenské povolání a působení v bezpečnostním systému státu.

Rostoucí dostupnost a veřejná povaha informací na sociálních sítích představují významná rizika, která mohou být cizími zpravodajskými službami snadno využita pro výběr a rekrutaci potenciálních spolupracovníků. Přestože uživatelé sociálních médií obvykle očekávají určitý stupeň soukromí, tato očekávání se často míjejí s realitou, jelikož zahraniční zpravodajské služby mohou snadno přistupovat k osobním detailům jako jsou zájmy, kontakty, či dokonce emocionální a profesní postoje uživatelů. Tyto údaje lze následně využít nejen k tipování vhodných kandidátů, ale i k vytvoření strategie ovlivňování a oslovování, přičemž takto získané poznatky mohou významně usnadnit budování vztahu s daným kandidátem tajné spolupráce.

Je samozřejmé, že také studenti Univerzity obrany na svých sociálně-mediálních účtech sdílejí informace, které mohou být zahraničními rozvědkami využity při tipování vhodných spolupracovníků. Je realitou, že na podkladě toho, co respondenti z řad studentů Univerzity obrany na sociálních sítích sdílejí, si lze poměrně jednoduše vytvořit obrázek o jejich zálibách, způsobu trávení volného času a také o charakteru a kvalitě přátelských vztahů. Taková míra je pro cizí zpravodajskou službu dostatečná pro přípravu nejvhodnější formy kontaktu a případnou kompletaci motivační pobídky.

Studenti vojenského studia na Univerzitě obrany by si měli být této hrozby vědomi zvláště intenzivně. Navzdory jejich specifickému profesnímu zaměření a přípravě na práci v oblasti obrany a vnější bezpečnosti státu však výzkum ukázal, že ne vždy přikládají bezpečnostním aspektům dostatečnou váhu. Tato skutečnost podtrhuje potřebu zvyšování informovanosti o rizicích spojených se sdílením osobních údajů online, zejména mezi těmi, jejichž profesní budoucnost se bude týkat státní obrany a bezpečnosti. Zvláštní důraz by měl být kladen na hrozby spojené s možnou rekrutací cizími zpravodajskými službami, přičemž organizačně nejjednodušším a zároveň nejefektivnější formou řešení by bylo začlenění této problematiky do vojenské odborné přípravy. Vhodné by bylo rovněž zakomponování těchto témat do nově připravovaných studijních programů, aby studenti získali potřebné znalosti k ochraně před zpravodajskými hrozbami již v průběhu svého vzdělávání.

Tento článek vznikl na základě výzkumu podpořeného poskytovatelem Ministerstvem obrany České republiky, Univerzitou obrany a projektem Fakulty vojenského leadershipu „LANDOPS“.

Autor prohlašuje, že není ve střetu zájmů v souvislosti s publikováním tohoto článku a při jeho přípravě akceptoval všechny etické normy požadované vydavatelem.

SEZNAM ZDROJŮ

Červenka, Jan a Daniel Kunštát, eds. 2006. České veřejné mínění: výzkum a teoretické souvislosti. Praha: AV ČR. Sociologický ústav.

Gioe, David V. 2017. 'The More Things Change': HUMINT in the Cyber Age. In: Dover, Robert, Huw Dylan a Michael Goodman (eds.). *The Palgrave Handbook of Security, Risk and Intelligence*. London: Palgrave Macmillan.

Hejzlarová, Eva M., Magdalena Mouralová, and Martina Štěpánková Štýbrová, eds. 2023. *Fantastická data ve veřejné politice a jak je využít*. Praha: Nakladatelství Karolinum.

Hendl, Jan. 2012. Kvalitativní výzkum: základní teorie, metody a aplikace. Praha: Portál.

Kutěj, Libor. 2020. *Zdrojové možnosti HUMINT a CI/HUMINT v operacích*. Praha: Powerprint.

Kutěj, Libor. 2021. "Zpravodajství ze sociálních médií při budování agenturních pozic z pohledu zabezpečování zpravodajské ochrany." Habilitační práce, Univerzita obrany.

Maltego. 2024. „Everything About Social Media Intelligence (SOCMINT) and Investigations“. 18.10.2024. Everything About Social Media Intelligence (SOCMINT) and Investigations (maltego.com)

Termann, Stanislav. 1997. *Operativní psychologie*. Praha: Ministerstvo obrany ČR.

Terrell Hanna, Katie, and Ben Lutkevich. "What is social media?" <https://www.techtarget.com/whatis/definition/social-media>