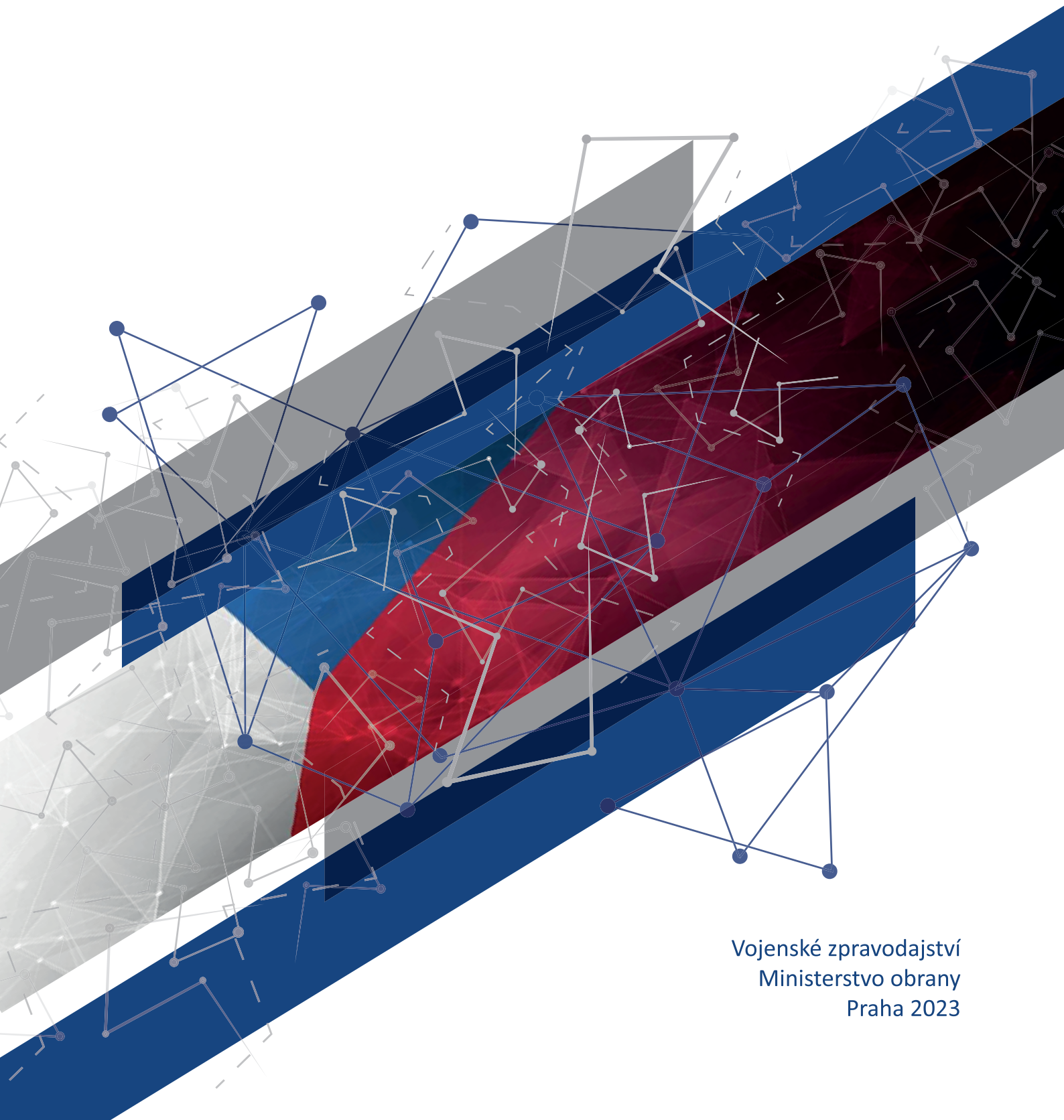
Výroční zpráva Vojenského zpravodajství za rok 2022



Vojenské zpravodajství
Ministerstvo obrany
Praha 2023

ÚVODNÍ SLOVO ŘEDITELE

Vážení čtenáři,

veřejná výroční zpráva o činnosti Vojenského zpravodajství v roce 2022 se primárně věnuje dění na Ukrajině. Vojenská agrese Ruské federace ovlivnila Českou republiku i globální dění a výrazně se promítla do úkolů a činností naší zpravodajské služby.

Základní poslání Vojenského zpravodajství se ve srovnání s předešlými lety nezměnilo. S využitím tradičních zpravodajských disciplín i moderních technologií získáváme informace, které jsou důležité pro obranu a bezpečnost naší země.

Z výše uvedených důvodů nicméně dostala naše práce nový význam, rozměr a intenzitu. Chci na tomto místě všem kolegyním a kolegům poděkovat, protože v nelehké situaci obstáli. Prostřednictvím desítek situačních a analytických výstupů obdrželi zákonní adresáti relevantní informace, které se staly podkladem při jejich rozhodování.

Ve třech tematických kapitolách výroční zprávy jsme se rozhodli zaměřit na oblasti, které jsou pro dění na Ukrajině příznačné. Válka 21. století už totiž zdaleka není pouze konvenční. Kybernetický prostor, bezpilotní prostředky, šíření propagandy. Tyto fenomény se staly neodmyslitelnou součástí konfliktu a jejich význam neustále roste.

Ukrajina ale pochopitelně nebyla naším jediným zájmem. Stejně jako v předešlých letech jsme se i v roce 2022 zaměřovali při sběru informací na místa působení českých vojáků v misích, další krizové regiony, terorismus a extremismus, kybernetické hrozby, nebo zpravodajské aktivity cizí moci na našem území.

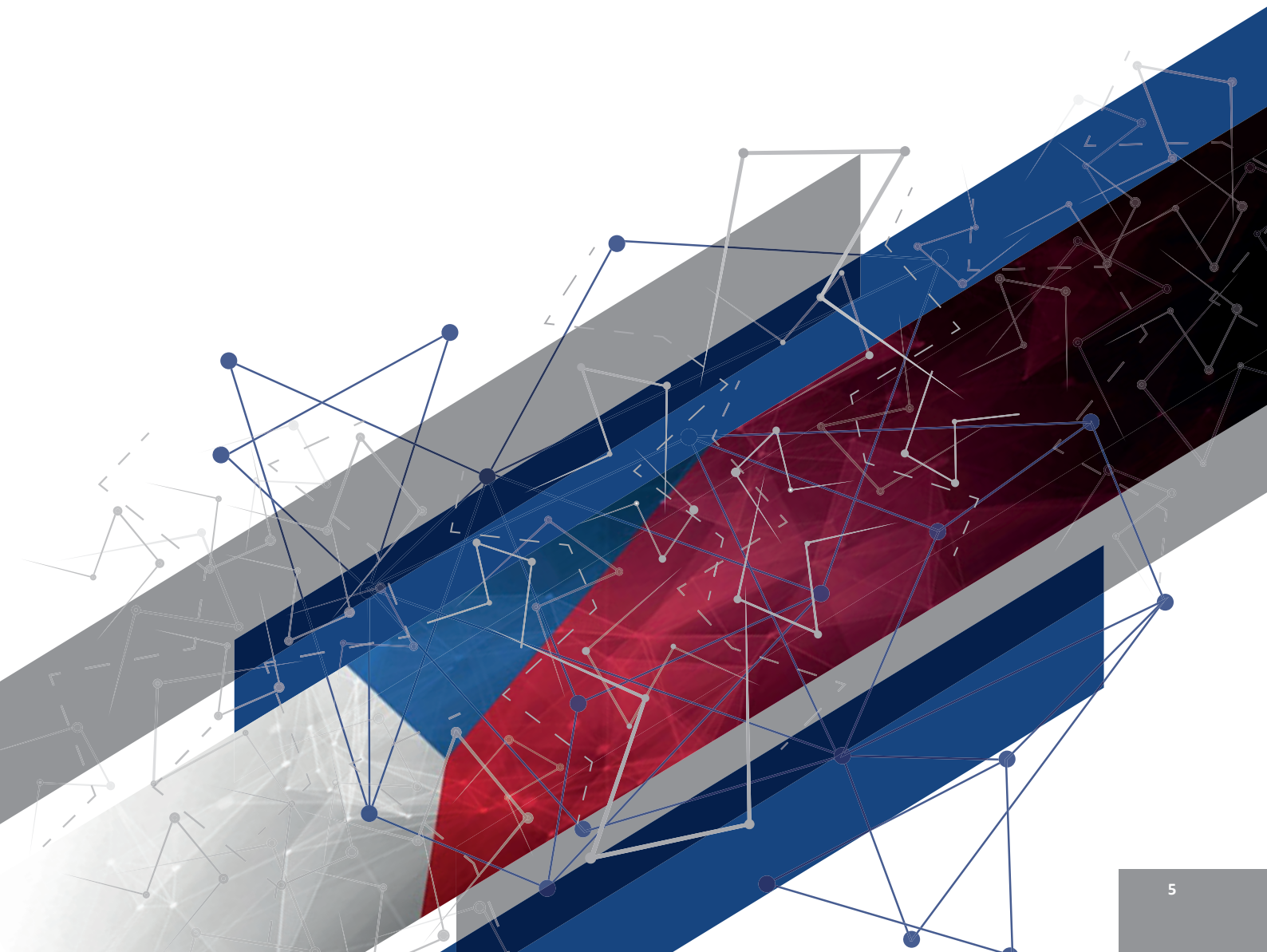
V souvislosti s rokem 2022 nemohu nezmínit ještě jednu skutečnost. Poprvé a v nelehké době předsedala Česká republika prostřednictvím naší služby Vojenskému zpravodajskému výboru NATO. Což mimo jiné v souvislosti s Ukrajinou znamenalo nutnost rychlé a efektivní koordinace. Jsem rád, a zde tlumočím také názor zahraničních partnerů, že i v této roli jsme obstáli na výbornou.

Dámy a pánové, těší mě, že si Vojenské zpravodajství doma i v zahraničí udržuje renomé respektované instituce. Ujišťuji vás, že budeme vždy připraveni hájit zájmy České republiky a přispívat k bezpečnosti všech jejích občanů.

S úctou

Ředitel Vojenského zpravodajství
generálporučík Ing. Jan Beroun

OBSAH



K VÝVOJI SITUACE V ROCE 2022

Narůst celosvětové nestability a nepředvídatelnosti dalšího vývoje vyústily v roce 2022 svým rozsahem i intenzitou v největší vojenský konflikt současnosti, navíc na evropském kontinentu a v relativní blízkosti České republiky – na Ukrajině. Vyvrcholil tím proces opomíjející principy a mechanismy, které ve většině případů a po velmi dlouhé období umožňovaly předcházet bezpečnostním krizím i otevřeným vojenským konfliktům. Dialog a ochota ke kompromisu byly vytěsněny sebestředným monologem a prosazováním vlastních názorů a stanovených cílů.

Vojenské zpravodajství opakovaně upozorňovalo na některé negativní jevy a tendence, které k tomu nevyhnutelně vedly. Snažilo se je identifikovat, pojmenovat, vyhodnotit a interpretovat do budoucna, a to jako varování před přípravou vojenského konfliktu i v celosvětovém měřítku. Již ve své veřejné Výroční zprávě za rok 2019 zdůraznilo, že se svět přiblížil konfliktu v důsledku narůstající polarizace zájmů, názorů a rozdílných postojů, pokračující proměny dosavadního velmocenského uspořádání, prohlubující se multipolarity a úpadku principů mezinárodního práva. Upozornilo na skutečnost, že chybí standardní dialog a posiluje konfrontace jako způsob řešení narůstajících problémů a rozporů. Došlo ke zpochybňování role mezinárodních institucí, vojenských aliancí, odzbrojovacích dohod resp. záruk a jistot, které deklarovaly a poskytovaly. Další vývoj pak tyto tendence jen prohloubil.

Byly tak relativizovány i samotné jistoty dosavadního uspořádání světa, který se nyní ocitl v tíživé realitě otevřené a rozsáhlé vojenské konfrontace s významným potenciálem jejího možného rozvinutí a zcela fatálními potenciálními důsledky do budoucna. Přístup aktérů zapojených do tohoto střetu vyústil do hospodářské krize a velmi pravděpodobně i dlouhodobější ekonomické nestability, jejichž projevem je aktuálně nedostatek a nárůst cen nezbytných surovin, významné inflační tlaky a snižování životní úrovně značné části populace. Dočasná mocenská unipolarita ustupuje intenzivnímu tlaku na nahrazení bipolaritou respektive potenciálně problematickou multipolaritou, což je provázeno ztrátou důvěry ve většinově dosud respektované mezinárodní garance, systémy bezpečnosti a jejich mechanismy.

Západ je bezprostředně konfrontován s rozporováním jím prosazovaných univerzálních hodnot a principů, s nimiž se významná část nezápadního světa neidentifikuje a odmítá je přebírat. To přispělo k vytvoření vysoce toxického prostředí vytvářeného na základě ideových a ideologických východisek, která mohou být velkou hrozbou při naplňování stanovených cílů. Ideologie má navíc zcela fatální destruktivní schopnost ovlivňovat racionální hodnocení možností a disponibilních schopností všech stran potenciálního otevřeného konfliktu. Ta část světa, reprezentovaná zejména Ruskem a Čínou, vůči které se Západ vymezuje, pak chápe aktuální vývoj zejména jako svou mimořádnou příležitost ke změně dosavadního globálního uspořádání a možnost využít dynamiku vývoje k prosazení deklarovaných cílů. K tomu přispívá i skutečnost, že se jedná o politické režimy autoritativního charakteru s možností efektivního stanovování a naplňování strategických cílů a značného urychlení rozhodovacích procesů.

Stojíme tak před novým rozdělením světa, kterému nebude na základě řady kritérií jako doposud jednoznačně dominovat Západ, ale prosazují se v něm kromě Číny také dynamicky se rozvíjející země tzv. globálního jihu. Otázkou zůstává, zda nepůjde o takové světové mocenské uspořádání, které učiní mezinárodní bezpečnostní situaci ještě mnohem nestabilnější a nepředvídatelnou. Navíc se bude jednat o vysoce konkurenční prostředí vyžadující nutnost mobilizovat zdroje a úsilí, pokusit se obnovit ty atributy západní civilizace, které jí již v minulosti zajistily převahu a prvenství. Kromě tradičního individualismu a svobod jednotlivce šlo o inovativní přístupy a možnost konkurence v prostředí s minimální regulací.

Konflikty nového typu v takto utvářeném světě jsou příznačné zejména různorodostí domén, ve kterých probíhají, variabilitou prostředků a nástrojů, jimiž budou uskutečňovány. Hrozí tak

přerůst v nekontrolovatelné a značně nepřehledné soupeření, kterému bude Západ nucen bezprostředně čelit. Stále významnější roli zde budou hrát moderní technologie, nové technické prostředky a jejich dříve zcela nepředstavitelné kvantitativní i kvalitativní nasazení. To pak bude logicky odrážet nejen ekonomický a intelektuální potenciál, ale současně schopnost efektivity řízení a rozhodování zainteresovaných aktérů.

Vojenské zpravodajství bude ve své činnosti nuceno čelit zcela novým a netradičním výzvám, které bude muset i samo předvídat, odhadovat, pojmenovávat a soustřeďovat svůj pohled na vývoj do budoucna. Aby tak přispělo k připravenosti České republiky na řadu ještě neznámých nebo spíše jen tušených budoucích hrozeb a z nich plynoucích existenciálních rizik.

KYBERNETICKÝ KOMPONENT VÁLKY NA UKRAJINĚ

STRATEGICKÉ HODNOCENÍ

Projevy kybernetického působení v souvislosti s válkou na Ukrajině zcela neodpovídaly předválečným predikcím. Kybernetické útoky ruských aktérů přes vysokou incidenci nedosáhly předpokládané míry sofistikovanosti a uzpůsobení konkrétním cílům. Pozorovaný modus operandi spíše naznačuje, že mezi klíčové faktory válečného nasazení ofenzivních kybernetických schopností patřily operační potřeby ruských ozbrojených sil, poměr dostupných kapacit vůči počtu požadavků na způsobení kybernetických efektů či dostupné příležitosti, které původci hrozby mohli využít.

Masové nasazení destruktivních schopností způsobilo rozsáhlé škody postiženým organizacím, z vojenského hlediska však dosud na vývoj války na operační či strategické úrovni nemělo významný vliv. Kybernetické útoky ruských aktérů kromě vojenských cílů směřovaly především proti ukrajinským vládním institucím, důležitým sektorům kritické infrastruktury (energetika, doprava), telekomunikacím a médiím, případně jejich dodavatelům a poskytovatelům IT služeb.

Pravděpodobným cílem těchto útoků bylo narušování služeb kritických pro potřeby ukrajinských ozbrojených sil, výkon státních institucí, zabezpečení základních potřeb ukrajinských obyvatel a vytváření zmatku, paniky a nepřehledných situací, kdy potřební nemají včasný přístup k přesným a životně důležitým informacím.

Tyto cíle se nejspíše podařilo naplnit jen částečně – v průběhu války se míra intenzity kybernetického působení v čase vyvíjela, přičemž skutečné dopady způsobených útoků lze vzhledem k chybějícím datům i kinetickému působení ruských ozbrojených sil i s odstupem hodnotit jen složitě. Vrcholné intenzity kybernetický komponent konfliktu dosáhl nejprve v období od počátku invaze do konce jara 2022 a následně během podzimní kampaně kinetických i kybernetických útoků proti ukrajinské energetické infrastruktuře, cílící pravděpodobně na podrytí morálky ukrajinských vládních představitelů, ozbrojených sil i obyvatelstva.

Kybernetické kampaně Ruské federace s přihlédnutím k doktríně informační konfrontace zároveň často zahrnují aspekt psychologického či vlivového působení, kdy kromě samotných způsobených efektů, které působí svým cílům, zamýšlenému obecenstvu adresují i specifickou zprávu či narativ.

OPERAČNÍ POTŘEBY VYTVÁŘEJÍ TLAK NA HORIZONTÁLNÍ APLIKOVATELNOST PROSTŘEDKŮ

Kybernetických útoků na míru uzpůsobených konkrétním cílům bylo v průběhu roku 2022 pozorováno spíše poskrovnu. Ve vyšší míře ze strany ruských aktérů na počátku invaze nedošlo k očekávanému kombinovanému nasazení sofistikovaných kybernetických efektů proti kritické infrastruktuře, které by sloužily jako násobitel efektu kinetických operací ruských ozbrojených sil.

Narušení služeb kritické infrastruktury bylo patrné v počátcích invaze i během podzimní kampaně proti ukrajinské energetice, většinu výpadků však způsobilo fyzické poškození infrastruktury vlivem kinetického působení ruských ozbrojených sil. Kybernetické útoky, které vysoce pravděpodobně souvisely s operačními potřebami a zájmy ruských ozbrojených sil, nabývaly spíše podoby rozsáhlého nasazení tzv. wiperů proti ukrajinským organizacím v zájmových sektorech.

Wipery přepisují a mažou data a záznamy na paměťových úložištích postižených organizací. Přestože jsou tyto nástroje v kybernetických útocích používány dlouhodobě, mimo jiné i pro mazání stop za jinou škodlivou aktivitou, míra a frekvence jejich nasazení v rámci války na Ukrajině byla v roce 2022 bezprecedentní. Ruští a proruští aktéři vytvořili hned několik paralelních rodin těchto nástrojů, které byly nasazovány v různých časových obdobích a které využívaly specifických funkcí. Řada těchto nástrojů byla využita pro konkrétní kampaň útoků a následně opuštěna, dlouhodobě probíhal vývoj pouze u několika vybraných.

Nasazení těchto schopností pravděpodobně vychází z logiky vojenské účelnosti i potřeb útočníků. Wipery jsou poměrně agnostické vůči systémům, na nichž jsou nasazeny. Je poměrně jednoduché je vytvořit, mohou také zneužívat nativně přítomné funkce operačních systémů. Jednoduchost těchto nástrojů zároveň znamená, že v případě jejich úspěšné detekce a analýzy a následné zavedení protiopatření ze strany obránců sice jejich efektivita významně klesá, pro útočníky se však jedná o komparativně nižší ztrátu, než v případě na míru šitých nástrojů určených k exploataci konkrétního cíle – jsou proto postradatelné.

Napadení organizace wipery může způsobit významné škody skrze rozsáhlou ztrátu dat,[1] nenávratné poničení paměťových médií, ztrátu přístupu ke klíčovým službám, náklady spojené s vyřešením incidentu či ušlé příležitosti a reputační škody. V ukrajinském kontextu se navíc vyskytly případy několikanásobného napadení již dříve postižených organizací, což se následně odráží v morálce zaměstnanců, odborného personálu snažícího se zabezpečit systémy i třetích stran, které postihuje výpadek služeb. Z vojenského hlediska však takový útok má výrazný efekt především v případě, kdy se například způsobený výpadek důležité služby v čase překrývá s její okamžitou potřebou nebo kdy má ztráta dat implikace pro kritické operace typu přesunů jednotek či zabezpečování logistické podpory.

Naopak vytvoření na míru šitého synergického efektu v konkrétním čase a prostoru pro účely postupu či působení ozbrojených sil je pro kybernetického původce hrozby o poznání složitější z hlediska výzkumu

[1] Především v případě absentujících záloh, z nichž by organizace ztracená data mohla obnovit.

a vývoje příslušné schopnosti i složitosti jejího nasazení, koordinace a integrace do vojenské operace. Ač takový útok může mít významné dopady, typicky není jednoduše přenositelný do jiného kontextu. I v případě, že útočníci použijí modulární malware, jsou nuceni funkcionalitu uzpůsobit konkrétní konfiguraci systémů provozovaných cílovou entitou, což výrazně zvyšuje nároky na průzkum zájmové infrastruktury a komplikuje frekventované nasazení schopností tváří v tvář vysokému operačnímu tempu a počtu požadavků na operace proti zájmovým cílům. Další nároky s sebou přináší nutnost koordinace způsobených efektů s manévry ozbrojených sil v místě a čase během vzájemného působení s protivníkem.

V průběhu války na Ukrajině v roce 2022 jsou veřejně známy dvě kauzy na míru šitých útoků, které mohly sloužit jako násobitel efektu operací ruských ozbrojených sil. V prvním, úspěšném případě způsobili útočníci kybernetický efekt v satelitní síti KA-SAT provozované společností Viasat. Byť se i v tomto případě jednalo o masové nasazení wiperů, cílem byla satelitní síť, již měly využívat ukrajinské ozbrojené síly, přičemž efekt byl proveden v souběhu s ruským překročením ukrajinských hranic v počátku invaze. Téměř jistě byl útok proveden za účelem narušení jedné z komunikačních platforem obránců.

V druhém případě se pak téměř jistě ruští kybernetičtí původci hrozby měli pokusit o napadení elektrických rozvoden vysokého napětí malwarem Industroyer2.[2] Ukrajinské veřejné instituce však ve spolupráci se soukromými kyberbezpečnostními společnostmi tomuto útoku dokázaly předejít. V případě, že by byl útok úspěšný, by se jednalo o již třetí kyberneticky způsobený blackout na Ukrajině.

Neúspěch této operace může sloužit jako argument ve prospěch plošného nasazení méně sofistikovaných, postradatelných kybernetických nástrojů se širokou využitelností. Přestože by v případě úspěchu nasazení Industroyer2[2] mohlo mít významné dopady vlivem dočasného přerušení dodávek elektřiny v zájmové oblasti, náklady z hlediska vývoje, výzkumu i přípravy a realizace operace by byly vysoce pravděpodobně hodnoceny jako vysoké i v případě jejího úspěchu.[3] Nejistá pravděpodobnost dosažení efektu může vyústit v preferování kinetických forem působení proti zvoleným cílům.

Nezodpovězenou otázkou zůstává také skutečná úroveň integrace kybernetických operací do působení ruských ozbrojených sil. Přestože Vojenské zpravodajství disponuje poznatky o kybernetických operacích, které téměř jistě sloužily k podpoře ruských ozbrojených sil, nejednalo se tolik o přímé působení efektů jako spíše o informační podporu. Přestože v určitých obdobích války docházelo k působení proti identickým množinám cílů kinetickými i kybernetickými prostředky zároveň, mohlo se v těchto případech jednat o duplicitní působení na základě jednotného zadání.

ŠPIONÁŽ KLÍČOVOU SOUČÁSTÍ KYBERNETICKÉHO PŮSOBENÍ

Kromě vysoce frekventovaných kybernetických útoků byla v roce 2022 pozorována celá řada kybernetických špionážních kampaní, která cílila na veřejné instituce zemí zapojených do válečného konfliktu či jejich podporovatelů. Mezi nejaktivnější původce kybernetických hrozeb v souvislosti s válkou kromě ruských patřili ti čínští či běloruští, přičemž kampaně zasahovaly i země EU a NATO (včetně České republiky) či významné hráče mezinárodního systému, například země BRICS či další země globálního Jihu, o jejichž mezinárodní podporu Ruská federace usilovala. Motivací útočníků kromě sběru zpravodajských informací byly snahy o zjištění pozic a reakcí daných zemí vůči válce na Ukrajině, poznatky k dodávkám zbraní a humanitárního materiálu, rozličné makroekonomické ukazatele apod.

[2] Předchozí verze tohoto malwaru byla použita stejným původcem hrozby za účelem způsobení blackoutu v Kyjevě v prosinci 2016. Totožný aktér je vysoce pravděpodobně odpovědný za výpadek také v ivano-frankivské oblasti v prosinci 2015.

[3] Nemusí se zde jednat přímo o náklady finanční, jako spíše o počet alokovaných lidských sil a hodin strávených přípravou útoku, jakkoliv byl Industroyer2 vyvíjen jako modulární malware.

Ruští kybernetičtí aktéři zároveň v roce 2022 prováděli průzkumné kybernetické operace proti západním cílům. Záměrem těchto operací mohl být sběr informací, předvýzkum pro následné útoky, příprava operačního prostředí či strategická komunikace ve smyslu varování před další podporou Ukrajiny. Zaměření sběru poznatků u jednotlivých aktérů korespondovalo s dlouhodobými úkoly jejich pravděpodobných sponzorů v ruském bezpečnostním aparátu.

Na taktické a operační úrovni probíhala špionáž zaměřená na podporu činnosti ruských ozbrojených sil na Ukrajině.

OMEZENÁ PŘÍTOMNOST NESTÁTNÍCH AKTÉRŮ

Do konfliktu na obou stranách vstupují také nestátní aktéři, kteří se soustředí především na provádění ofenzivních operací. Jejich dopad však dosud byl zřetelný spíše v oblasti informačního či vlivového působení, kdy byly některé operace či za ně odpovědné entity předmětem mediálního zájmu, přičemž pro tyto účely i z důvodu koordinace dobrovolníků samotní aktéři často provozují profily na veřejně dostupných sociálních sítích.

Aktivity nestátních aktérů působících ve prospěch jak Ukrajiny, tak Ruské federace se sestávaly především z kybernetických útoků určených k odepření do internetu vystavených služeb veřejných institucí i komerčních entit, neautorizovaných změn obsahů webových stránek a veřejných prezentací, rozličných informačních operací typu změn obsahu rozhlasového či televizního vysílání, případně tzv. hack & leak operací. V nich útočníci získají neautorizovaný přístup k citlivým, neveřejným databázím, které následně zveřejňují. V několika případech za účelem dosažení vlivového efektu byly dokonce „zveřejněny“ již dříve uniklé databáze, případně tyto byly sestaveny z veřejně dostupných údajů.

Přestože v počátcích konfliktu byla podpora především Ukrajiny, ale i Ruské federace ze strany nestátních aktérů poměrně živelná, postupně dochází ke konsolidaci. Jednotliví participující nestátní aktéři v mnoha případech udržují různě blízké vazby s veřejnými institucemi, přičemž skutečně aktivní po téměř roce konfliktu zůstávají především aktéři s vazbami na obě země nebo dokonce na jejich bezpečnostní instituce. Proukrajinští hackeři se v některých případech netají vazbami na ozbrojené síly či bezpečnostní instituce Ukrajiny, proruští hackeři se ke spolupráci s bezpečnostním aparátem Ruské federace nevyjadřují nebo jej popírají. Ukrajinští bezpečnostní představitelé i americká komerční společnost podnikající v oblasti kybernetické bezpečnosti však některá proruská uskupení dokonce obvinili z toho, že udržují významné vazby s ruskými zpravodajskými službami nebo jsou jimi přímo sponzorována.

Přes svůj typicky východoevropský původ se proti očekáváním ve významné míře do konfliktu nezapojila kriminální uskupení provozující ransomwarové operace. V období před konfliktem byli ransomwarem zasaženi někteří provozovatelé kritické infrastruktury v Německu a v Nizozemí, v roce 2021 byly ransomwarové útoky kvůli dopadům na infrastrukturu Spojených států dokonce projednávány na nejvyšší úrovni prezidenty USA a Ruské federace. Přestože po ruské invazi na Ukrajinu některá ransomwarová uskupení zaujala ke konfliktu konkrétní veřejně deklarovaný postoj, neobjevily se ve vyšší míře významné případy politicky motivovaného nasazení kriminálního ransomwaru. V případě alespoň jedné ransomwarové organizované kriminální skupiny válka měla dokonce přivodit vnitřní rozpad skupiny poté, co údajně insider ukrajinské národnosti zveřejnil interní komunikaci skupiny z důvodu jejího zaujetí proruského postoje.

Některé struktury kybernetického zločinu však do konfliktu zasahují jako tzv. zprostředkovatelé přístupu, kdy neautorizovaně pronikají do počítačových sítí zájmových organizací, načež tento přístup následně odprodávají třetím stranám. Ty po zisku přístupu mohou postiženou síť informačně vytěžit nebo ji napadnout za účelem způsobení nežádoucího efektu, například ransomwarem či wiperem.

VYSOKÝ POTENCIÁL RE-ESKALACE

Přestože Vojenské zpravodajství v roce 2022 nepozorovalo vyšší množství pokusů o způsobení nežádoucích kyberfyzických efektů v souvislosti s válkou na Ukrajině, re-eskalační potenciál je hodnocen jako vysoký. Destruktivní aktéři operující ve prospěch Ruské federace a jejích ozbrojených sil dosud operují ve vysokém tempu se zaměřením na podporu vojenských operací. Tyto operace pravděpodobně konzumují značnou část dostupných kapacit. Situace je pravděpodobně komplikována množství požadavků na provedení operací či sběr zpravodajských informací, případně postupným vyčerpáváním odpovědného personálu.

Výskyt destruktivních kybernetických útoků však nemusí korelovat s intenzitou konfliktní dynamiky, zamýšlené efekty aktéři mohou odložit a způsobit je případně i ex post, až se kapacity uvolní. Podobné případy již byly pozorovány v období let 2015 až 2017, kdy destruktivní kybernetické útoky proti ukrajinským i dalším cílům následovaly až s odstupem po událostech roku 2014, kdy vyvrcholily demonstrace Euromajdan, rozhořel se separatistický konflikt na Donbasu s ruskou účastí a došlo k mezinárodně neuznané anexi Krymu.

Kybernetičtí útočníci museli v průběhu roku 2022 vážit na jedné straně mezi svými zadáními a potřebami, širokým spektrem cílů, které nejlépe mohou ovlivnit skrze široce nasaditelné, jednoduché a postradatelné nástroje, a potenciálnímu soustředění se na sofistikované útoky, které mohou přinést déletrvající a významnější efekt, ovšem za cenu vyšších nákladů, nižšího množství postižených cílů a vyššího rizika neúspěchu v případě, že konkrétní přístup nebude úspěšný. Dostupné poznatky dosud indikují, že se poplatní původci hrozeb rozhodli jít cestou diverzifikace svých nástrojů a cílů; toto rozhodnutí však mohou s časem přehodnotit spolu s případným uvolněním rukou v případě poklesu intenzity konfliktu.

V takovém případě mohou hrozit i další kybernetické útoky proti zemím NATO, kdy by ruskou motivací bylo přerušení dodávek vojenské a humanitární pomoci Ukrajině či msta za již poskytnutou podporu i trvající režim sankcí uvalených proti Ruské federaci.

Případný pokles kybernetických aktivit s Ruskou federací spojených původců hrozeb bude v příštím roce nutno hodnotit a interpretovat opatrně, neboť operační přestávky bývají využívány také k obměně arzenálu používaných nástrojů. Podobný vývoj byl pozorován na přelomu léta a podzimu 2022, kdy byly ruskými kybernetickými aktéry opuštěny některé nástroje, přičemž v následujících měsících byly následně nasazeny nástroje nové.

LEKCE PRO SYSTÉM KYBERNETICKÉ OBRANY

Kybernetické působení v průběhu války Ruské federace proti Ukrajině skýtá cenné lekce pro systém kybernetické obrany, neboť nabízí reflexi institucionálních odpovědností, provádění strategických protiopatření či specifik kybernetické obrany za válečného stavu. Mezi ta například patří i rozhodnutí, do jaké míry centralizovat či decentralizovat systém i pracoviště kybernetické obrany či plány jak se vypořádat se situacemi, kdy agresor dokáže postupovat územím a okupovat regionální centra včetně administrativních budov a počítačových systémů a sítí veřejných institucí.

Významným aspektem kybernetické obrany Ukrajiny byla privatizace bezpečnosti a využití služeb komerčních subjektů, které zásadním způsobem podpořily a navýšily obranný potenciál ukrajinských veřejných institucí. Ukrajina od roku 2014 podnikla řadu kroků k navýšení svého obranného potenciálu. Navíc jí po invazi poskytlo své služby několik předních západních komerčních společností podnikajících v kybernetické bezpečnosti. Díky tomu a díky upřené pozornosti dalších entit směrem k očekávaným kybernetickým útokům z Ruské federace tak došlo k znásobení potenciálu ukrajinských kybernetických obránců.

Kybernetické působení v průběhu války na Ukrajině dokládá potřebu rekrutace a přípravy dostatečného množství odborníků na kybernetickou bezpečnost už za mírového stavu. V případě rozsáhlé krize či dokonce válečného stavu je nutno již operovat s kostrou personálu, přičemž pro krizové situace je nutno počítat také s faktorem jeho únavy, nutností jej rotovat či doplňovat.

Zároveň, pokud již za mírového stavu nepostačují státní kapacity pro potřeby kybernetické obrany, je nutno hledat cesty, jak tyto doplnit pro zmiňované případy nastalých krizových situací či válečného stavu. Příležitostmi mohou být jak rozvoj spolupráce se soukromým sektorem, tak cílené budování kybernetických záloh či uvážení případné alokace expertů na informační technologie či přímo kybernetickou bezpečnost v krizových situacích v rámci konskripce. Cenné mohou být také zkušenosti spojenců a partnerů s integrací aktivit dobrovolníků do kybernetické obrany státu. Ponaučení musí zároveň reflektovat také státní krizové plány a plány managementu rizik na různých úrovních, případně hospodářská opatření pro krizové stavy.

Dalším kritickým aspektem ukrajinské kybernetické obrany byla mezinárodní spolupráce transatlantického a evropského společenství, jednak ve prospěch Ukrajiny, kdy například spojenecká země Ukrajině ještě před invazí poskytla týmy kybernetických obránců, kteří po dobu více než dvou měsíců pomáhali zabezpečit některé prioritní systémy a sítě, jednak autonomně, kdy bezpečnostní aparáty zemí NATO spolupracovaly například na rozbití rozsáhlého botnetu operujícího ve prospěch Ruské federace.

Jeho narušení, které se časově překrývalo s invazí ruských vojsk, mělo pravděpodobně dopady na ofenzivní potenciál ruských kybernetických kampaní. V neposlední řadě by lekce z kybernetického komponentu konfliktu měly zahrnovat poučení, že v operační doméně kyberprostoru by se zpravodajská výměna informací měla blížit více principu need-to-share než need-to-know, přičemž kromě zintenzivnění výměny zpravodajských poznatků podléhajících utajením je především nutno podpořit výměnu neutajovanou technických poznatků a indikátorů kybernetických incidentů, a to i se soukromou sférou.

ZÁVĚR

Kybernetický komponent války ilustruje způsoby vojenského využití kybernetických operací a nástrojů v ozbrojeném konfliktu. Ruští kybernetičtí aktéři si dle zjištění komerčních kyberbezpečnostních společností připravovali své operační prostředí již v roce 2021. Následně vyvinuli tlak na ukrajinskou politickou reprezentaci i populaci v týdnech okamžitě předcházejícím zahájení invaze, během níž pak podporovali a doplňovali aktivity ruských ozbrojených sil kybernetickými útoky zaměřenými na zničení či dočasné vyřazení svých cílů, případně kybernetickou špionáží zaměřenou na sběr hodnotných poznatků na taktické, operační i strategické úrovni.

Soustředěná pozornost a defenzivní operace ukrajinských obránců spolu s podporou západních bezpečnostních institucí a komerčních společností podnikajících v kybernetické bezpečnosti vysoce pravděpodobně pomohla omezit útočný potenciál ruských původců kybernetických hrozeb – skrze degradaci a narušování infrastruktury útočníků, sdílení informací o používaných nástrojích či praktik, jak předcházet konkrétním kybernetickým incidentům.

Pozorované destruktivní útoky způsobily rozsáhlé škody postiženým organizacím. Z vojenského hlediska však tyto aktivity pravděpodobně významným způsobem neovlivnily průběh ozbrojeného konfliktu v návaznosti na ilegální invazi ozbrojených sil Ruské federace do Ukrajiny. Vojenské zpravodajství přesto varuje před podceněním situace v příštích dvou letech a poukazuje na nezanedbatelný potenciál další kybernetické eskalace konfliktu, která nutně nemusí korelovat s intenzitou konfliktní dynamiky. V případě zamrznutí konfliktu či přesunu ruského působení směrem k asymetrickému způsobu vedení boje může dokonce role kybernetických operací dále nabývat na důležitosti.

Ruské ofenzivní snahy na Ukrajině podporovala také kybernetická špionáž a kyberneticky umožněné či amplifikované informační operace. Především kybernetická špionáž na taktické, operační i strategické

úrovni bude provozována i v následujícím období za účelem zisku informační převahy, která by se následně překlopila do postupu ozbrojených sil či diplomatických a ekonomických úspěchů na strategické úrovni.

Významným rizikem je i pravděpodobnost přelití efektu kybernetických útoků proti kritické infrastruktuře Ukrajiny a sousedních zemí do infrastruktury zemí EU a NATO, či dokonce přímé působení nežádoucích efektů proti této infrastruktuře kybernetickými útoky ze strany destruktivních aktérů. Náznaky možné přípravy operačního prostředí ze strany ruských aktérů byly pozorovány napříč rokem 2022, přičemž výpadky satelitních služeb v evropských zemích v návaznosti na ruský útok na satelitní síť KA-SAT zároveň ilustruje možné dopady kybernetického působení proti mezinárodně sdílené infrastruktuře. Země EU a NATO i nadále budou představovat prioritní cíle zpravodajských operací a sběru zpravodajských poznatků ruských služeb.

Masové nasazení jednoduchých wiperů ruskými aktéry může představovat alternativní způsob válečného nasazení kybernetických schopností, kdy kybernetické ofenzivní operace nebude nutně potřeba integrovat s operacemi a manévry ostatních typů ozbrojených sil (pozemních, vzdušných atd.) s cílem sofistikovaného vyřazování citlivých systémů a operačních technologií. Útočníci místo toho budou obránce zahlcovat vysokým počtem nepříliš sofistikovaných, ale široce využitelných nástrojů, přičemž se místo vyřazení operačních technologií, skrze něž bývají ovládány průmyslové systémy, budou soustředit na narušení kontinuity každodenních operací svých cílů skrze vyřazení jejich informačních technologií.

BEZPILOTNÍ PROSTŘEDKY V KONFLIKTU NA UKRAJINĚ

Obr. 1 Ukrajinský Bayraktar TB2

Ozbrojené konflikty v uplynulých deseti letech potvrdily, že bezpilotní prostředky (UAV[4]) mají své nezastupitelné místo ve výzbroji ozbrojených sil, a to k plnění průzkumných i bojových misí. Aktuální ozbrojený konflikt na Ukrajině jednoznačně potvrdil tuto tezi, poukázal na některé nové způsoby taktického použití UAV, na perspektivy ve vývoji bojových variant těchto prostředků (UCAV[5]) a na důležitost obrany před UAV protivníka.

Používání UAV, průzkumných za účelem korigování palby dělostřelectva nebo víceúčelových se schopností používat palubní zbraně proti pozemním cílům, se stalo běžnou rutinou zejména v asymetrických konfliktech nebo v konfliktech menšího rozsahu. Pro konflikt na Ukrajině je charakteristická bojová činnost v podmínkách působení silné protivzdušné obrany (PVO), využívání prostředků pro vedení elektromagnetického boje (EB) a nasazení velkého počtu UAV na taktické úrovni. V první etapě války ukrajinské ozbrojené síly používaly víceúčelové UAV tureckého původu kategorie MALE[6] typu Bayraktar TB2 (obr. 1), které útočily na ruskou bojovou techniku v kolonách. Tyto bojové mise byly úspěšné, avšak pouze po dobu nedostatečného krytí těchto jednotek ruskou PVO. Po její konsolidaci bylo používání ukrajinských TB2 z důvodu velkých ztrát omezeno.

[4] UAV – Unmanned Aerial Vehicle; synonymem UAV je dron.
[5] UCAV – Unmanned Combat Aerial Vehicle.
[6] MALE – Medium Altitude Long Endurance (pro střední výšky s velkou vytrvalostí).


Iranprimer.usip.org

Obr. 2 Shahed-136 ve vypouštěcím zařízení (vlevo) a za letu (vpravo)


Newsweek.com

Při nasazení víceúčelových UAV kategorie MALE se ukázalo, že prostředky osvědčené v asymetrických konfliktech nebyly obdobně efektivní v konfliktu na Ukrajině. Zde, v podmínkách silné PVO, se naproti tomu osvědčily UCAV s jednorázovým použitím (LM[7]), které jsou v žurnalistické rétorice označovány jako „sebevražedné". Pro ruskou stranu bylo charakteristické používání LM typu Shahed-136 (obr. 2) íránského původu, které byly zavedeny do výzbroje ruských ozbrojených sil v průběhu konfliktu pod označením Geraň-2. Tyto relativně levné útočné prostředky byly koordinovaně nasazovány primárně k ničení ukrajinské energetické infrastruktury a sekundárně k oslabování schopností ukrajinské PVO v důsledku spotřeby skladových zásob účinných, ale nákladných protiletadlových řízených střel.

V průběhu konfliktu na Ukrajině byly, obdobně jako v jiných konfliktech v uplynulých deseti letech, používány komerčně dostupné UAV kategorie „mikro"[8] a „mini"[9] k průzkumu i k útokům na pozemní cíle. K tomuto účelu byla využita provizorně vyrobená munice na bázi ručních granátů nebo munice do automatických granátometů, alternativně také upravené minometné střely. Ve srovnání s předcházejícími konflikty byla tato činnost praktikována v masovém měřítku pod kontrolou pravidelných ozbrojených sil, a to oběma válčícími stranami.

Novým trendem zaznamenaným v konfliktu na Ukrajině bylo používání rychlostních dálkově řízených UAV z pohledu první osoby (FPV[10]) s nákladem výbušnin k přímým útokům na pozemní cíle. Tyto UCAV na bázi technologie FPV (obr. 3) patří rovněž do kategorie LM a jsou vyráběny provizorně s významným přispěním amatérských modelářů, kteří stavbu a létání s FPV provozují jako své hobby.


Armyinform.com.ua


Armyinform.com.ua

7 LM – Loitering Munition; synonymem je OWA UAV – One Way Attack UAV.
8 Mikro UAV – maximální vzletová hmotnost do 5 kg.
9 Mini UAV – maximální vzletová hmotnost v intervalu 5 až 30 kg.
10 FPV – First Person View.[5] UCAV – Unmanned Combat Aerial Vehicle.

Zkušenosti z konfliktu ukázaly, že současná protivzdušná obrana (PVO) musí být z důvodu masového nasazení UAV kategorií „mikro“ a „mini“ doplněna o další výkonové prvky. Standardní PVO není schopna se s tímto typem prostředků vzdušného napadení (PVN) efektivně vypořádat. Prvním důvodem je složitá detekce cíle, druhým účinnost jeho eliminace, kdy využívání sofistikovaných protiletadlových raketových prostředků je mnohdy technicky nemožné, ale především z hlediska finančních nákladů a proporcionality neefektivní. Cena protiletadlových střel je totiž v příkrém nepoměru k hodnotě ničeným PVN. Naopak jako účinné se ukázaly systémy pro vedení EB, které působí proti PVN nekineticky v různých částech elektromagnetického spektra.[11] Jedná se především o přenosné nebo mobilní prostředky používané oběma stranami konfliktu, jejichž vývoj intenzivně pokračuje.

MOŽNOSTI SOUČASNÝCH PROPAGANDISTICKÝCH KAMPANÍ S DŮRAZEM NA BEZPEČNOSTNÍ PROBLEMATIKU

HYBRIDNÍ PŮSOBENÍ A MORÁLNÍ PANIKA

V posledním desetiletí do veřejné debaty stále intenzivněji proniká téma tzv. dezinformací a propagandy. Zřetelný zlom v tomto ohledu přineslo obsazení Krymu Ruskou federací v roce 2014 a následné boje na východní Ukrajině, kdy část veřejnosti začala tyto události chápat jako výsledek dlouhodobého ruského „hybridního působení“, jehož hlavní složku měla představovat intenzivní propaganda.[12] Ačkoliv hybridní vojenské akce a rozsáhlé propagandistické aktivity nejsou ničím novým a provázejí organizovaná lidská společenství od jejich počátků, měla podle těchto představ nyní Ruská federace disponovat zcela inovativním a mimořádně efektivním konceptem těchto akcí – tzv. Gerasimovovou doktrínou.[13]

Část obyvatelstva členských zemí EU a NATO se tedy ocitla ve stavu jakési morální paniky, neboť získala pocit, že této údajné hrozbě ze strany Ruské federace nedokáže čelit. Tento fakt, spolu se skutečností, že konkrétní propagandistické kanály nebylo ve většině případů možné přesně identifikovat, a tím, že výsledky jejich působení byly jen obtížně kvantifikovatelné, měl za následek mimo jiné masivní nadužívání pojmů s touto problematikou spojených (např. „hybridní válka“, „propaganda“ či „dezinformace“). Ty tak především v laickém diskursu ztratily pro popis a chápání uvedených fenoménů jakýkoliv význam a začaly se užívat spíše pro dehonestaci názorových protivníků a radikálně zjednodušující vysvětlení komplexních jevů,[14] což jejich detailní analýzu a případné řešení problémů, jichž byly odrazem, spíše znesnadňovalo.

Prohlubující se vágnost a významová neurčitost zmíněných termínů přitom vedla i k případům, kdy je někteří političtí a společenští aktéři začali používat i pro označení pravdivých informací, jenž však nebyly v souladu s jimi prosazovanými idejemi, a kdy dokonce docházelo ke spojování kritiky vládních politik s propagandistickým působením cizí moci, což mohlo vést k vyčlenění části do té doby legitimních hlasů z politické debaty.

---

11 Detekce je prováděna v radiolokační, viditelné, infračervené a akustické části elektromagnetického spektra.

12 V této souvislosti se přitom coby jakési synonymum pro propagandistická poselství začal užívat termín dezinformace, jehož obsahová náplň je však poněkud odlišná.

13 Zmíněný ruský doktrinální dokument byl v českých i světových médiích často komentován, ačkoliv fakticky neexistoval. V této souvislosti často zmiňovaný článek ruského náčelníka generálního štábu V. V. Gerasimova Ценность науки в предвидении totiž představuje pouze shrnutí jeho názorů na způsob, jakým asymetrický způsob válčení používají protivníci Ruské federace, především USA. Z historického hlediska tak je možno snahy čelit „Gerasimovově doktríně“ připodobnit k několika staletí trvajícímu boji církevních autorit proti ateistickému traktátu O třech podvodnících, který měl údajně ohrožovat základy hlavních náboženství – ačkoliv ve skutečnosti neexistoval.

14 Například tzv. brexit, volba Donalda J. Trumpa prezidentem USA či rozvrat veřejné debaty v některých členských státech EU a NATO.

PROPAGANDISTICKÉ PŮSOBENÍ V INFORMAČNÍM VĚKU

Přes toto zmatení je však zároveň třeba odmítnout snahy vliv propagandistických kampaní/hybridního působení cizích mocností zcela marginalizovat. Současné výpočetní technologie totiž umožňují veřejnou debatu a nálady širokých vrstev obyvatelstva ovlivňovat mnohem snáze než v předcházejících dekádách, kdy byly zahraniční propagandistické kampaně odkázány výhradně na kanály, jejichž zajištění bylo logisticky náročné (letákové kampaně), daly se snadno narušit (rozhlasové a televizní vysílání), anebo byly ze své podstaty značně nespolehlivé („šeptanda"), přičemž šíření propagandy bylo poměrně nákladné i z časového hlediska.

Internet, sociální sítě a mobilní aplikace však umožňují masivní šíření informací již v řádech hodin, přičemž při sdílení a přeposílání propagandistických poselství existuje řádově nižší riziko jejich nežádoucího zkreslení, jako tomu bylo například u ústního předávání. Zároveň je pro státní orgány demokratických zemí výrazně obtížnější zamezit jejich šíření, neboť takováto akce vyžaduje rozsáhlou aktivitu a spolupráci s provozovateli internetových domén či sociálních sítí. Uvedené zásahy (i vzhledem k tomu, že se jedná o automatizovaný proces, který v budoucnosti bude zřejmě probíhat plně na bázi umělé inteligence) přitom zřejmě postihnou i uživatele, jež se na propagandistických aktivitách ve skutečnosti nepodílí, ale budou mezi její šiřitele zařazeni na základě veřejnosti zcela nesrozumitelných algoritmů. Je zřejmé, že mnohý takovýto neoprávněný zásah bude silně medializován a ve svém důsledku povede k dalšímu poklesu důvěry veřejnosti nejen v tyto procesy, ale i v dané sociální sítě a ve státní správu jako takovou.

Moderní technologie rovněž umožňují propagandistické kampaně zaměřit na konkrétní cílové skupiny, a tak lépe využívat existujících štěpení ve společnosti. Informační působení cizí moci totiž dosahuje největších úspěchů, akcentuje-li stávající rozpory ve společnosti, takže například oslovuje skupinu obyvatel, jež se považuje za diskriminovanou či ohroženou stávající státní mocí či jí propagovaným diskursem. Zahraniční mocnost přitom pomocí své propagandy uvedené pocity dále prohlubuje a navíc se často pokouší prezentovat jako spojenec či zachránce zmíněné skupiny, čímž nejen oslabuje její loajalitu ke společenskému konsenzu, ale zároveň vytváří a posiluje její vazby k sobě samé.

VYBRANÉ VLIVY UMOŽŇUJÍCÍ ŠÍŘENÍ PROPAGANDY

V současnosti se západní společnosti nachází ve značně specifické situaci, kdy zde působí hned několik zásadních vlivů, jež oslabují její soudržnost a usnadňují šíření zahraniční propagandy. Z těch nejdůležitějších je třeba zmínit:

1) Krize důvěry ve stát a jeho instituce. V posledních desetiletích dochází k poklesu důvěry v část veřejných institucí, jež často začínají být chápány jakožto implicitně nepřátelské k některým vrstvám obyvatelstva.[15] Rovněž extrémní polarizace společnosti vede k tomu, že stoupenci těch politických uskupení, jež jsou aktuálně v opozici, radikálně odmítají veškerá vládní opatření jen proto, že je zavádějí jejich ideoví protivníci, a to bez toho, zda jsou sama o sobě prospěšná či nikoliv. Tato nedůvěra vede ke snížení vnitrospolečenské loajality a snadnějšímu přijímání zahraničních propagandistických narativů.

2) Zdůrazňování individuality. Poslední dekády se rovněž nesou ve znamení oslabovaní a mizení tradičních kolektivních identit (národní či třídní vědomí, stranická příslušnost), jež sice dílčím způsobem nahrazují kolektivní identity nově konstruované, avšak v mnohem větším rozsahu identity individuální. Jedinec je chápán jako formálně zcela autonomní subjekt, jenž není podřízen žádné širší identitě, nicméně

[15] Tento posun našel své umělecké vyjádření již v 90. letech, kdy na široké oblibě získávala díla naznačující, že „vládní místa skrývají pravdu" a že „vše je jinak". Do této skupiny lze přitom řadit nejen díla o korupci, klientelismu a vlivu velkého kapitálu (např. vliv zbrojařsko-průmyslového komplexu na zahraniční politiku USA), ale i celou řadu zábavně-fantastických děl, jež s tímto motivem pracují (Akta X, Matrix a fakticky i epizody I až III Hvězdných válek).

tato jeho autonomie jej zároveň činí mnohem zranitelnějším vůči informačnímu působení, které jeho individualismu formálně vychází vstříc.[16]

3) Demokratizace informačního prostoru. Masivní rozšíření výpočetních technologií, internetu a sociálních sítí vedlo k nejvýraznější proměně mediálního prostoru od dob vynálezu knihtisku. Tyto faktory umožnily nebývale masivní šíření informací a zároveň vedly k pádu faktického monopolu, jež na tuto činnost doposud měla tradiční média a profesionální novináři či komentátoři.[17] Došlo tak k výrazné demokratizaci veřejného prostoru, kde místo několika málo médií ovlivňují debatu tisíce entit, jejichž úspěch je založen nikoliv na profesionalitě, ale na schopnosti zaujmout a přitáhnout pozornost. Vzhledem k tomu, že k tomuto účelu nejlépe slouží informace vyvolávající emoce, otevírá zmíněný posun široké pole nejen pro bulvarizaci médií, ale i pro šíření propagandy, která je právě na šíření emočně zabarvených informací ve většině případů založena.

4) Souběh krizí. Přibližně posledních patnáct let lze považovat za období, kdy na západní společnosti v rychlém sledu dopadlo několik zásadních krizí (hospodářská, finanční, ekologická, migrační, identitární, zdravotnická, válečná), přičemž jen menší část z nich se podařilo uspokojivě vyřešit. Rovněž vzhledem k výše zmíněné bulvarizaci mediálního prostoru přitom dochází k tomu, že ve veřejné debatě převládá radikální interpretace těchto krizových jevů, která spočívá buď v jejich označování za extrémní existenční rizika, nebo naopak v bagatelizaci a popírání, přičemž stoupenci obou táborů se obviňují z nečestných pohnutek (včetně vědomého či mimovolného jednání ve prospěch cizí moci), což dále podporuje rozklad společnosti. V tomto prostředí je pak pro zahraniční propagandu snadné se etablovat a takto vyhrocenou debatu využívat k tomu, aby jeden ze zmíněných táborů oslovila a minimálně částečně jej začala ovlivňovat.

SITUACE V ČESKÉ REPUBLICE

Z výše uvedených důvodů je zřejmé, že česká společnost patří v tomto ohledu mezi ty, jež jsou zranitelné propagandistickým působením. Přestože není možné jednoznačné určit, do jaké míry zahraniční propaganda ovlivňuje zdejší veřejnou debatu a do jaké míry k jejímu vyostření přispívají jiné procesy (včetně výše nastíněných), lze mít za jisté, že část české společnosti slouží jako terč zahraničních propagandistických aktivit, kdy jsou některé sociální a politické skupiny vzhledem ke svému rozčarování ze společensko-politického vývoje náchylnější k přebírání a následnému šíření zahraniční propagandy.

O skutečné velikosti těchto skupin lze však pouze spekulovat,[18] a stejně tak i o tom, do jaké míry jejich názory a aktivity formuje pouze zahraniční propaganda a do jaké ji ovlivňují jiné zdroje včetně například radikálů z vlastních řad.

Ke koncepci boje se zahraniční propagandou v rámci České republiky pak lze podotknout, že ač bezpečnostní složky státu včetně zpravodajských služeb mají v těchto snahách nezastupitelnou úlohu (především při rozkrývání způsobů, jakým je zahraniční propaganda šířena, a při identifikaci osob, jež při šíření propagandistických poselství spolupracují s cizí mocí za účelem poškození zájmů České republiky či rozvratu zdejšího ústavního zřízení), musí se vzhledem ke své působnosti zaměřovat pouze na řešení následků a nikoliv příčin působení zahraniční propagandy. Podobně jako v celé řadě jiných oblastí přitom platí, že bez dostatečné prevence a zásadních změn v celé řadě státních politik bude pro bezpečnostní orgány stále obtížnější řešit byť jen nejkřiklavější projevy těchto fenoménů.

[16] Toho využívají jak obchodní řetězce, jež své standardizované produkty nabízejí ke koupi se sloganem „měj svůj styl“, tak i propagandisté apelující na „rozum“ a „inteligenci“ příjemců propagandistických sdělení, jejichž schopnost pochopit svět kladou do protikladu k většinové společnosti „zmanipulovaných ovcí“.

[17] Za první volby, v nichž se internet plně projevil jako síla srovnatelná s tradičními médii, je považován souboj o pozici guvernéra amerického státu Minnesota v roce 1998, kde zvítězil bývalý wrestlingový zápasník a protisystémový kandidát Jesse Ventura, jehož kampaň se vzhledem k nedostatku finančních prostředků zaměřila právě na on-line prostor.

[18] Podle poznatků Vojenského zpravodajství se počet čtenářů webových stránek, jimž je veřejné debatě často přisuzován přívlastek „dezinformační“ či „prokremelské“, pohybuje v řádu vyšších desítek tisíc. Tvrzení, že tyto projekty šíří výhradně zahraniční propagandu, lze však úspěšně zpochybnit.

Jakékoli úspěchy zahraniční propagandy totiž představují především průvodní jev celkového odcizení panujícího mezi institucemi a jednotlivými vrstvami společnosti. Bez obnovení celospolečenské důvěry a konsenzu tak bude část obyvatelstva Česká republiky zřejmě i nadále vysoce náchylná k jejímu přebírání a šíření.

DŮLEŽITÉ UDÁLOSTI MIMO HLAVNÍ ČINNOST

Představitelé Vojenského zpravodajství se účastnili řady konferencí a odborných diskuzí pořádaných bezpečnostní a akademickou sférou.

Již tradičně se Vojenské zpravodajství zapojilo do osvětových a vzdělávacích aktivit, mimo jiné záštitou ředitele a poskytnutím cen pro vítěze podpořilo 6. ročník studentské Národní soutěže v kybernetické bezpečnosti.

Aktivní byla služba i na mezinárodním poli. Česká republika prostřednictvím Vojenského zpravodajství v roce 2022 předsedala Vojenskému zpravodajskému výboru NATO (MIC).

MIC
CHAIRMANSHIP
CZECH REPUBLIC
2022

PŘEDSEDNICTVÍ VOJENSKÉMU ZPRAVODAJSKÉMU VÝBORU NATO

Tuto prestižní roli zastávalo Vojenské zpravodajství poprvé a ve velmi složitém období. Prioritami českého předsednictví byly zavádění nových technologií do zpravodajských činností, problematika umělé inteligence a posílení spolupráce mezi vojenskými a civilními službami v rámci Severoatlantické aliance včetně tvorby společných výstupů.

Aktivní český přístup byl oceněn na různých jednáních NATO, včetně jednání Severoatlantické rady a Vojenského výboru.

PŘEVOZ OSTATKŮ GENERÁLA FRANTIŠKA MORAVCE DO ČESKÉ REPUBLIKY

Po několikaletém úsilí se podařilo uskutečnit převoz ostatků generála Františka Moravce, který je historicky nejvýznamnější osobností čs. vojenského zpravodajství, do rodné Čáslavi. Urnu s ostatky převzala v dubnu 2022 ve Washingtonu od zástupců rodiny a americké administrativy delegace vedená ministryní obrany Janou Černochovou.

SLAVNOSTNÍ NÁSTUP K 104. VÝROČÍ VZNIKU VOJENSKÉHO ZPRAVODAJSTVÍ

Při příležitosti 104. výročí vzniku Vojenského zpravodajství se 14. listopadu 2022 uskutečnil v Národním památníku na Vítkově slavnostní nástup.

Na něm převzalo 47 příslušníků služby z rukou ministryně obrany, ředitele Vojenského zpravodajství a náčelníka Generálního štábu Armády ČR resortní vyznamenání a čestné či pamětní odznaky. Během nástupu byl také bojový prapor VZ dekorován stuhou Československé obce legionářské.

VOJENSKÉ ZPRAVODAJSTVÍ OBDRŽELO MEDAILI ZA ZÁSLUHY O DEMOKRACII

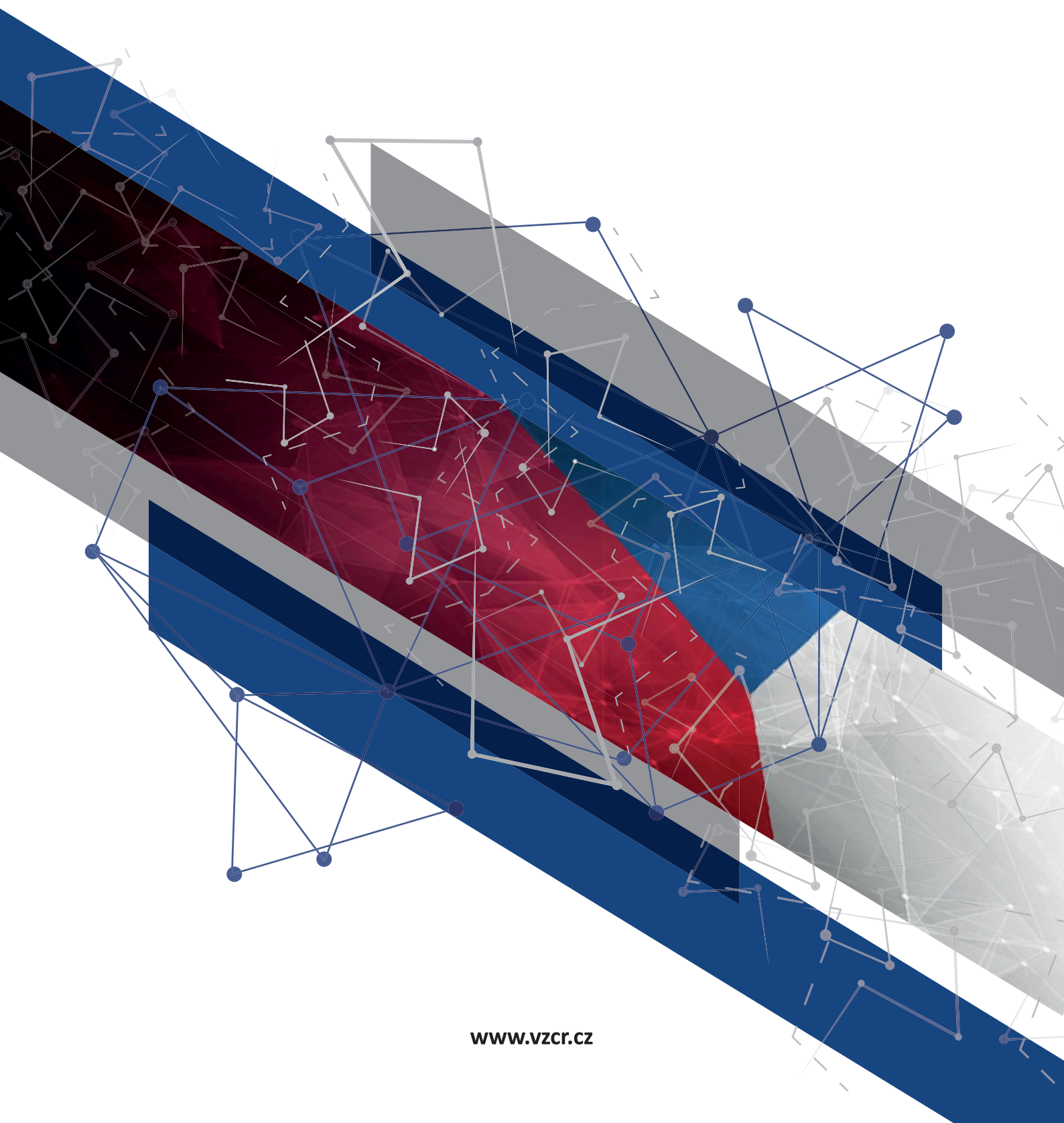
Vojenské zpravodajství obdrželo 17. listopadu 2022 Medaili Za zásluhy o diplomacii. Ta je udělována od roku 2019 jako jedno ze dvou rezortních vyznamenání Ministerstva zahraničních věcí. Ministři zahraničí ji udělují za mimořádný přínos pro českou diplomacii, českou zahraniční politiku, rozvoj zahraničních vztahů České republiky a upevňování míru ve světě.

SBÍRKA PRO VOJENSKÝ FOND SOLIDARITY

V tradiční listopadové sbírce ke Dni válečných veteránů ve prospěch Vojenského fondu solidarity příslušníci Vojenského zpravodajství přispěli částkou téměř 140 tisíc Kč.

Vojenské zpravodajství se stejně jako v minulosti zařadilo výší svého příspěvku mezi největší podporovatele fondu v rámci rezortu Ministerstva obrany.

VOJENSKÝ FOND SOLIDARITY



www.vzcr.cz