4

Kybernetická síla Ruska

Invaze informačních a komunikačních technologií vyžaduje informační převahu. Dlouhá tradice podvodných kampaní poskytla zkušenosti.

Ruský a americký přístup k chápání kybernetické síly se od sebe zásadně liší.[16] Podle mnoha ruských akademiků a vojenských expertů zahrnuje kyberválka nejen aspekty informačnětechnologické, ale také informačně-psychologické.[17] Podle názoru ruských akademiků a vojenských expertů Rusko zažívá neustálý útok v nepřátelském kyberprostředí prostřednictvím obsahu zaměřeného na podkopávání ruských strategických zájmů. Pochopit rozdíl mezi pojetím kybernetické síly mezi Spojenými státy a Evropou na jedné straně a Ruskem na straně druhé je základem pro klasifikaci aktivit probíhajících v kyberprostoru. Rozdíly spočívají v chápání

16 Medvedev, S. A., 2015. *Offense-Defense Theory Analysis of Russian Cyber Capability.* Dizertační práce. Naval Postgraduate School.

17 Thomas, L. T., 2010. „Russian information warfare theory: The consequences of August 2008". In: *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*, ed. Blank, J. S. – Weitz, R. Carlisle: PA: Strategic Studies Institute, s. 265–301.

samotné kybernetické moci a z jejich rozporu nakonec vyplývá, že konkurenční strany využívají odlišné nástroje a soubory aktivit. Rusko chápe kybernetickou sílu a informační válku jako holistický koncept.[18]

Souhrnně řečeno, z ruského hlediska zahrnuje informační válka – „informacijnaja vojna" – operace zaměřené na sítě, elektronický boj, psychologické operace a informační operace.[19] Existuje rozdíl mezi nepřátelským kódem a škodlivým obsahem,[20] což jsou dvě odlišná opatření, která Západ často nechápe jako součást jedné kampaně. Informačnětechnologické operace slouží k distribuci nepřátelského kódu a obsahu. Sahají od vlivových operací až po fyzické poškozování infrastruktury, jakož zahrnují i informačně-psychologické operace s cílem zaútočit na vnímání a morálku entit či celých sociálních skupin, jak to popsal generálmajor Šeremeť.[21]

Cílem je dosáhnout digitálního narušení, jakož i psychologické subverze. Kromě narušení komunikačních schopností je další kritickou součástí úspěšné válečné informační kampaně například dezorientovat, delegitimizovat a diskreditovat protivníka a demoralizovat jeho vůli použitím nepřátelského obsahu a kódu.

Existují tři zdroje ruského celostního přístupu k informační válce. Prvním je vojensko-technická revoluce, resp. informačnětechnologická revoluce ve vojenských záležitostech. Během éry studené války čelily obě supervelmoci výzvám, jež se týkaly nasazení informačních technologií. Tento koncept je však stále hnacím motorem vojenských inovací, protože se technologie vyvíjí. Můžeme s jistotou konstatovat, že armády v dnešním multipolárním světě nejsou ušetřeny výzev spojených se zaváděním nových technologií a koncepcí.

Proces zavádění technologického pokroku do našich vojsk ani zdaleka neskončil. Úkol je téměř stejný jako v případě závodů ve zbrojení: překonat protivníka osvojením si nové technologie nebo přizpůsobením starých konceptů a nástrojů nové realitě. V kyberprostoru jsme svědky

18 Tamtéž.

19 Giles, K., 2011. „‚Information Troops' – A Russian Cyber Command?", in: *Cyber Conflict (ICCC)*, 2011, třetí mezinárodní konference v Tallinu: IEEE, s. 43–59.

20 Medvedev, S. A., 2015. *Offense-Defense Theory Analysis of Russian Cyber Capability*. Dizertační práce. Naval Postgraduate School.

21 Tamtéž.

začleňování prvků nových i adaptace starých, zejména v oblasti informačních operací; přizpůsobování analogových konceptů pro digitální éru je více než volba – zdá se, že je to nutnost.

Mary C. FitzGeraldová v roce 1997 správně uvedla:

> Podle ruské armády pramení převaha v nové revoluci ve vojenských záležitostech (RMA) z převahy v systémech C4ISR, těmi jsou: 1) systémy průzkumu, pozorování a zaměřování cílů; 2) „inteligentní" systémy velení a řízení. Tvrdí se, že informační systémy jsou dnes „nejmocnějšími zbraněmi 21. století", svými účinky srovnatelné se zbraněmi hromadného ničení. Jsou skutečně základem nové, čtvrté revoluce ve vojenských záležitostech. Politicko-vojenské vedení Ruska proto provádí ostrý posun od materiálně intenzivních systémů průmyslového věku k systémům *informačního* věku: od balistických raket, ponorek, těžkých bombardérů, tanků a dělostřelectva k pokročilých systémům C4ISR a EW. Vedení boje se vskutku přeměnilo ze střetu útočných systémů v konflikt informačních systémů.[22]

V minulosti se armády průmyslového věku zakládaly na masových odvodech. Základem válečného úsilí byl tudíž koncept „totální války", definovaný Erichem Ludendorffem.[23] Znamenalo to, že vše ve státě je podřízeno válečnému úsilí. Dnes jsme zcela závislí na moderních technologiích. Veškerý proces velení a řízení – od získávání zpravodajských informací po analýzu – je prostřednictvím rozhodovacího řetězce založen na nepřerušeném toku informací. Jsme svědky takzvaných průzkumných úderných systémů. Technologie, jež nám zajišťuje schopnost shromažďovat a analyzovat velká množství dat a předávat je dříve nepředstavitelnou rychlostí, rovněž způsobila vnitřní zranitelnost v rámci rozhodovacího systému.

[22] FitzGerald, M. C., 1999. *Russian Views on IW, EW, and Command and Control: Implications for the 21st Century.* Online. Dostupné na: http://www.dodccrp.org/events/1999_CCRTS/pdf_files/track_5/089fitzg.pdf [Přístup 28. ledna 2017].

[23] *Ludendorff: Strategist.* Online. In: 1992. Dostupné na: http://www.dtic.mil/dtic/tr/fulltext/u2/a250915.pdf [Přístup 20. ledna 2017].

Vedení boje se vskutku přeměnilo ze střetu útočných systémů v konflikt informačních systémů.[24]

V dnešní době je možné porazit průzkumný útočný komplex prostřednictvím informačního úderu. Takový úder může být velmi jednoduchý. Díky technologii a kanálům k šíření informací existují způsoby, jak skrýt skutečné záměry, zajistit hodnověrné popření [*plausible deniability, pozn. překladatele*], využít doručovací platformy a rychlost šíření. Můžete tak ovlivnit celé společnosti.

Informační úder, jejž Andrew Marshall z Office of Net Assessment [*interní vládní think tank založený Richardem Nixonem, prezidentem USA, pozn. překl.*][25] označuje za informační válku, je silně závislý na posunu od armád průmyslového věku, sestávajících z obrovských počtů vojáků a zaměřených na zničení protivníka, k rostoucí závislosti na informacích a kognitivnímu pojímání rozhodovacích procesů. Tento přístup, dodání uměle vytvořené falešné zpravodajské informace nebo manipulace se senzorickým povědomím nepřátelských rozhodovacích činitelů na bojišti není nic nového. Je součástí vojenské strategie a operačního umění od prvních válek, které proti sobě lidé vedli. Novým faktorem je technologická podpora dnešních informačních bojových aktivit, jež nepříteli poskytuje efektivitu a technické nástroje, které byly do konce osmdesátých let nepředstavitelné.

Druhým zdrojem ruského celostního přístupu k informační válce je koncept aktivních opatření. Tento pojem zahrnuje několik technik popsaných ve Zprávě sovětského ministerstva zahraničí z roku 1987–1988 s názvem „Sovětské vlivové aktivity, zpráva o aktivních opatřeních a propagandě".[26] Má tyto čtyři části:

[24] FitzGerald, M. C., 1999. *Russian Views on IW, EW, and Command and Control: Implications for the 21st Century.* Online. Dostupné na: http://www.dodccrp.org/events/1999_CCRTS/pdf_files/track_5/089fitzg.pdf [Přístup 28. ledna 2017].

[25] Khalilzad, Zalmay – White, John P. – Marshall, Andy W., eds., 1999. *Strategic Appraisal: The Changing Role of Information in Warfare.* Online. Dostupné na: https://www.rand.org/pubs/monograph_reports/MR1016.html [Přístup 28. ledna 2018].

[26] United States. Department of State, 1989. *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1987–1988.* U.S. Dept of State, Washington.

Dezinformace a podvrhy

Dezinformace, záměrný pokus oklamat veřejné mínění či vládu, může být ústní a/nebo písemná.[27] Padělané dokumenty se často používají při pokusech diskreditovat jednotlivce, instituce nebo politiku tak, aby to poškodilo zahraničněpolitické zájmy USA.[28]

Krycí společnosti a spolky přátelství

Fronty se zpravidla prezentují jako nevládní nepolitické organizace, zapojené do podpory pozitivních cílů, jako je světový mír.[29]

Nevládnoucí komunistické a levicové strany

Kontakty s těmito stranami jsou zpravidla otevřené a často jsou využívány k přesvědčování těchto stran, aby prováděly specifickou politiku nebo propagandistickou kampaň v zájmu SSSR.[30]

[27] V současné době to mohou být blogy, vlogy, online mediální kanály, padělané digitální dokumenty, audio- a videosoubory, účty na sociálních sítích a avataři. Role médií a platforem pro šíření dezinformací je dnes posílena online obsahem a kanály. Avšak novináři byli cílem dlouho předtím, než kybernetická sféra usnadnila tvorbu a šíření obsahu, nebo dokonce zacílení na mediální kanály. Podle svědectví Stanislava Levčenka, agenta KGB přímo zapojeného do vlivových kampaní ve prospěch Sovětského svazu: „Sovětské vedení si dobře uvědomovalo, že novináři jsou lidé, kteří vytvářejí veřejné mínění na Západě, a mohou být použiti jako agenti vlivu – ne přímo, ale nějakým nepřímým způsobem, protože existují dva typy agentů vlivu. Prvním je, když je novinář, podnikatel nebo nějaká politická osobnost naverbována. Druhým je, když je použit nevědomě, když mu dodají materiál nebo informace příznivé pro Sovětský svaz. Mluvím zcela zodpovědně, protože jsem sám předával takové informace americkým, francouzským nebo německým novinářům a oni je úspěšně využili ve prospěch sovětské propagandy. Nebyla to lež. Byla to dobře připravená dezinformace." Spojené státy. Ministerstvo zahraničí (1989). „Sovětské vlivové aktivity: zpráva o aktivních opatřeních a propagandě, 1987–1988". Ministerstvo zahraničí USA, Washington.

[28] Dnes se zaměřují také na domácí politiku a domácí zájmy, jako je národní bezpečnost, demokratické instituce či občanská společnost.

[29] V současnosti vědomě i nevědomě lákají také významná mezinárodní fóra úředníky a hodnostáře, aby projevovali mezinárodní podporu cílům krycích akcí.

[30] Dnešní Ruská federace používá krycí akce rovněž tajně, k podpoře politiky vyhovující

Politické vlivové operace

Agenti vlivu maskují své vazby na KGB tím, že aktivně působí ve vládních, politických, tiskových, hospodářských, odborových či akademických sférách svých zemí. Jejich cílem je vytěžit ze svého vlivu v těchto oblastech reálné politické zisky pro Sovětský svaz. Někdy Sověti využívají k dosažení podobných výsledků i náhodných kontaktů.

Aktivní opatření se přizpůsobila plnění operačních a strategických cílů v digitálním věku, a to s podporou možností dostupných prostřednictvím moderní technologie. Aktivní opatření zahrnují širokou škálu aktivit, ale abychom jim porozuměli v původním kontextu, je nutno znát pojem *maskirovka* ve smyslu „něco zamaskovat". Pojem maskirovka není do češtiny přímo přeložitelný, nicméně zahrnuje takové činnosti, jako je využití nastrčených osob, vějiček, provádění demonstračních manévrů, kamufláže, skrývání, popírání, klamání a dezinformací. Maskirovka není v žádném případě novým konceptem, jenž by se zrodil teprve v kyberprostoru. Je naopak součástí operačního umění a zpravodajského arzenálu po staletí; byla systematicky vyučována na vojenské škole, kterou založil car Mikuláš II. Pro Rusy je maskirovka klíčovou komponentou informační války, a to primárně v závislosti na úrovni pronikání technologie do vojenských aktivit.[31]

Kyberdoména, se svými problémy v oblasti atribuce a mlhavými hranicemi, je ideálním prostředím pro vedení informačních operací. Díky své specifické povaze je kyberprostor považován za mohutný multiplikátor. Ve strategickém kontextu poskytuje menším a středním entitám, státům a nestátním aktérům výrazně vyšší výhody, o nichž si do té doby mohly nechat jenom zdát. Vzdálenost, nasazení sil, riziko odhalení a atribuce odpovědnosti vyrovnávají podmínky pro všechny aktéry v kyberprostoru bez ohledu na jejich velikost, geografickou polohu nebo úroveň konvenční vojenské vyspělosti.

ruským zájmům, jako jsou ony politické síly v evropských zemích, které provádějí rozvratnou politiku.

31 Heickerö, R., 2010. *Emerging Cyberthreats and Russian Views on Information Warfare and Information Operations*. Analýza obrany, Swedish Defence Research Agency (FOI). Online. Dostupné na: https://foi.se/en/foi/reports/report-summary.html?reportNo=FOI-R--2970--SE [Přístup 28. ledna 2018].

Každému stratégovi či vojevůdci se tak plní jeho sen. Vždyť nyní je schopen rychle zasáhnout proti vzdáleným entitám bez nasazení bojových sil, dokáže jednat v utajení při minimalizaci nebezpečí prozrazení, jež by vedlo k atribuci a riziku protiútoku. Má rovněž možnost vést téměř bez omezení informačnětechnologické a informačně-psychologické operace jako prostředky narušení, odepření, destrukce či subverze kriticky důležité státní infrastruktury, aniž by nutně překročil práh, za nímž jej čeká ozbrojený konflikt. Aktivní opatření, jež byla v analogové éře omezena na fyzickou sféru, se stala přirozenou volbou, „sadou nástrojů adaptace" za účelem využití v kyberprostoru.

Expanze kyberprostoru podstatnou měrou zesílila aktivní opatření. Koncept strategické maskirovky je přímočarý. Usiluje o zmanipulování rozhodovacího procesu protivníka tak, aby se jeho strategické chování ubíralo žádoucím směrem. Tento koncept je jedním z kritických zdrojů ruské inspirace pro kognitivněpsychologické aktivity týkající se kyberprostoru.

Třetím zdrojem je kybernetika, podobor aplikované matematiky. Na rozdíl od pojmu „kyber" je kybernetika oborem, jenž propojuje oblast exaktní matematiky a sociálních věd. Kybernetika zkoumá zákony či charakter rozhodovacích procesů v komplexních systémech či systémech systémů. Odtud plyne skutečnost, že kybernetika sestává z technologických/digitálních a kognitivních komponentů, což má opět značnou důležitost v dnešním digitálním věku, v němž „konzumujeme" obsahy poskytované technickými prostředky.

Tyto tři zdroje ruského operačního umění v kyberprostoru splývají v informačním zápase, který je mnohem obsáhlejší než americko- či eurocentrické chápání kyberválky či kyberoperací.

Abychom doložili, jak hluboko je koncept maskirovky zakotven v ruském strategickém myšlení a nakolik rozsáhlé jsou jeho historické kořeny, musíme se ponořit do historie. Car Mikuláš II. v armádní uniformě (viz obr. 2) má s informačními operacemi více společného, než by se dalo předpokládat. Vyšší škola maskirovky, založená v roce 1904 za Mikulášovy vlády, poskytla rámec této dodnes používané strategie.[32]

[32] Thomas, L. T., 2004. „Russia's reflexive control theory and the military". *Journal of Slavic Military Studies*, 17. 2., s. 237–256.