• RECENZIE A ANOTÁCIE – REVIEWS AND ANNOTATIONS •

CC BY

JOSEF SMOLÍK
Fakulta bezpečnostního managementu, Policejní akademie České republiky v Praze, Praha, Česká republika
0000-0001-5841-8598

Daniel P. Bagge. Demaskování maskirovky: ruské vlivové kyberoperace. Praha: Academia, 2025. 183 s. ISBN 978-80-200-3661-2.

Daniel P. Bagge. Unmasking Maskirovka: Russia's Cyber Influence Operations. Prague: Academia, 2025. 183 pp. ISBN 978-80-200-3661-2.

Kybernetická a informační bezpečnost se v posledních letech proměnila z úzce odborného tématu v jednu z klíčových oblastí současné bezpečnostní politiky. Digitalizace společnosti, rostoucí závislost států i jednotlivců na informačních systémech a globalizace online prostoru vytvořily prostředí, v němž se kyberprostor stal plnohodnotným bojištěm. Státní i nestátní aktéři jej využívají nejen k technickým útokům na infrastrukturu, ale stále častěji také k informačním a psychologickým operacím, jejichž cílem je ovlivňovat veřejné mínění, oslabovat důvěru ve státní instituce a narušovat demokratické procesy.

Právě o těchto trendech pojednává kniha Demaskování maskirovky: Ruské vlivové kyberoperace, kterou v roce 2025 vydalo nakladatelství Academia v Praze. Jejím autorem je Daniel P. Bagge, odborník na kybernetickou bezpečnost, který se dlouhodobě pohybuje na pomezí akademické a praktické sféry (mj. působil v Národním úřadu pro kybernetickou a informační bezpečnost). Publikace vychází z autorova původního anglického textu vydaného v roce 2019 u nakladatelství Defense Press v New Yorku a přináší systematický pohled na ruské vlivové operace v kyberprostoru, zasazený do širšího bezpečnostního a politického rámce.[1]

Studie se zaměřuje na ruské postupy v informační válce, přičemž „rozhodující arénou se stal kyberprostor", který umožňuje „psychologický dopad s nízkými náklady" (s. 19).

Kyberprostor je dnes široce chápán jako nová operační doména (vhodná k provádění škodlivých aktivit), srovnatelná s tradičními oblastmi vedení konfliktů, jakými jsou země, moře, vzduch či vesmír. Stal se prostředím, v němž jsou systematicky vedeny operace namířené proti jednotlivým státům, jejich institucím, kritické infrastruktuře i obyvatelstvu. Tyto aktivity často zůstávají pod prahem otevřeného ozbrojeného konfliktu, přesto však mohou mít zásadní politické, ekonomické i bezpečnostní dopady. Význam kyberprostoru v tomto ohledu reflektovalo již v minulosti také NATO, které jej oficiálně uznalo jako samostatnou doménu vojenských operací

[1] Daniel P. Bagge: *Unmasking Maskirovka: Russia's Cyber Influence Operations*, New York: Defense Press 2019, 252 p.

a postupně jej začlenilo do svého strategického a obranného plánování. Tento krok podtrhuje skutečnost, že kybernetické a informační operace nejsou okrajovým fenoménem, ale integrální součástí současných i budoucích konfliktů.

Bagge se zaměřuje na popis postupů, které jsou známé jako dezinformace, klamání a popírání (maskirovka), které mají dlouho historii, přičemž se zaměřuje na využívání v SSSR a Ruské federaci. Cílem těchto postupů je ovlivnit protivníka tak, aby činil rozhodnutí, které jsou výhodné pro toho, kdo ovlivňuje, tj. klame. V tomto kontextu jsou podstatné informace (jejich kvalita, rychlost, důvěryhodnost atp.), kterými se působí na psychiku a rozhodovací procesy manipulovatelné osoby.

Autor se v první kapitole zaměřuje na vlivové operace a kampaně, jejichž cílem je ovlivnit komunikaci (např. prostřednictvím DDoS útoků), demoralizovat nepřítele a narušit či paralyzovat jeho velitelskou a řídicí strukturu. DDoS (Distributed Denial of Service) útoky vedou především k dočasnému nebo dlouhodobějšímu znefunkčnění informačních systémů a komunikačních kanálů, a to zahlcením serverů či sítí nadměrným množstvím požadavků. V důsledku toho dochází k omezení dostupnosti klíčových služeb, zpomalení či přerušení komunikace mezi institucemi a ztrátě schopnosti efektivně reagovat na vzniklou situaci. V širším kontextu mohou tyto útoky vyvolávat chaos, snižovat důvěru veřejnosti ve státní instituce a podporovat pocit nejistoty, čímž se stávají účinným nástrojem psychologického a informačního působení, nikoli pouze technickým problémem. S těmito typy útoků má navíc praktické zkušenosti i Česká republika, která byla v minulosti opakovaně cílem kybernetických útoků. Tyto útoky byly namířené proti státním úřadům, nemocnicím a dalším prvkům kritické infrastruktury, což názorně ukazuje jejich potenciál reálně ohrozit fungování státu i každodenní život obyvatel.

Druhá kapitola konstatuje, že právě kyberprostor „umožnil státům vést vlivové operace účinněji a využívat při ofenzivě výhody kyberprostoru“ (s. 25). Autor správně zdůrazňuje, že je nezbytné studovat charakter vlivových operací z minulosti, protože tradiční koncepty a strategie, které formovaly dosavadní konflikty, stále ovlivňují a strukturalizují novou rozhodující arénu budoucích střetů. Porozumění těmto historickým precedentům je klíčové pro analýzu současných metod působení ve sféře kybernetické a informační bezpečnosti a pro předvídání evoluce moderních konfliktů.

Třetí kapitola má název „Všeobecný úvod ke klamání“ a představuje klamání jako nástroj vojenského a politického konfliktu. Autor předkládá historické příklady klamání na úrovni strategické, operační i taktické a částečně využívá i psychologických jevů, například kognitivní disonance, kterou lze definovat jako stav vnitřního napětí vznikajícího, když jsou jedinci předkládány informace, které jsou v rozporu s jejich předchozími přesvědčeními či očekáváními. Tento psychologický fenomén (systematicky zkoumaný Leonem Festingerem) může být cíleně využíván k manipulaci vnímání a rozhodování protivníka, neboť vyvolává zmatek, nejistotu a zvýšenou pravděpodobnost chybného hodnocení situace. Autor tak ukazuje, že klamání není jen otázkou dezinformačních kampaní, ale hluboce souvisí s lidskou psychikou a principy vnímání reality, což z něj činí účinný nástroj v moderních konfliktech.

Následující kapitola se věnuje kybernetické síle Ruské federace. Bagge konstatuje, že „kyberválka nezahrnuje pouze aspekty informačně-technologické, ale také informačně-psychologické“ (s. 31). Kapitola dále popisuje proměny vedení bojových operací, kdy konflikt již nezahrnuje jen

střet útočných systémů, ale také střet informačních systémů. Součástí textu je i přehled nástrojů dezinformačních kampaní, mezi které patří například blogy, vlogy, on-line média a působení na sociálních sítích. Diskutován je pojem „maskirovka“, který je obtížně uchopitelný, protože zahrnuje široké spektrum klamavých metod – od kamufláže a popírání přes klamání až po cílené šíření dezinformací (s. 36).

Další součástí textu je vysvětlení termínu „reflexivní kontrola“, který Bagge charakterizuje jako „mnohem širší pojem než psychologická válka, informační válka a informační operace“ (s. 43). Reflexivní kontrola označuje strategii, jejímž cílem je ovlivnit rozhodování protivníka tak, aby sám jednal v souladu s cíli útočníka, často aniž by si byl vědom manipulace. Tento přístup zahrnuje cílené zasévání určitých představ, očekávání či dezinformací do vnímání protivníka, aby jeho reakce byly předvídatelné a řízené. Psychologický rozměr hraje v reflexivní kontrole klíčovou roli, protože úspěch strategie závisí na hlubokém porozumění lidskému myšlení, emocím a rozhodovacím mechanismům cílových osob. Reflexivní kontrola kombinuje psychologické principy, informační působení a taktickou manipulaci, čímž vytváří situaci, kdy protivník „dobrovolně“ činí kroky, které pro něj nejsou výhodné, ale odpovídají záměrům útočníka. V kybernetickém a informačním prostředí se tento princip uplatňuje prostřednictvím kombinace dezinformačních kampaní, sociálních sítí, médií a dalších nástrojů, což výrazně zvyšuje jeho účinnost a komplexnost.

Následující kapitola se zaměřuje na předpoklady realizace reflexivní kontroly a rozpracovává je do uceleného analytického rámce. Identifikovány jsou čtyři klíčové podmínky této účinnosti: 1) manipulace se smyslovým vnímáním, která ovlivňuje to, jak protivník interpretuje realitu; 2) systematické skrývání skutečných úmyslů, jež ztěžuje správné vyhodnocení situace; 3) cílené působení na protivníkovy zdroje informací, ať už jejich narušením, zkreslením či zaplavením; a 4) kombinaci manipulace s tzv. filtry, tedy mechanismy zpracování dat a informací, se smyslovým vnímáním. Právě tato kombinace umožňuje útočníkovi zasahovat jak do vstupních informací, tak do způsobu, jakým jsou následně vyhodnocovány.

V návaznosti na tento rámec jsou představeny také tři základní způsoby, jimiž sovětská škola vojenského myšlení usilovala o ovlivnění protivníka. Prvním z nich je demonstrace síly, která má vyvolat odstrašení nebo přehnanou reakci. Druhým je záměrné šíření velkého množství dvojznačných a nejistých informací, jež zvyšují míru chaosu a nejistoty v rozhodovacím procesu protistrany. Třetím postupem je realizace hrozby, která nutí protivníka soustředit se především na obranu, čímž omezuje jeho schopnost iniciativního jednání (s. 52). Bagge tímto způsobem ukazuje, že reflexivní kontrola není nahodilým souborem technik, ale promyšlenou strategií, jejímž cílem je dlouhodobé ovládání rozhodovacích procesů protivníka spíše než jeho přímá porážka.

Sedmá kapitola se zaměřuje na základní předpoklady úspěšného klamání. Autor zde rozpracovává zejména význam jasně definovaného cíle, promyšleného plánování klamavých aktivit a vhodné volby jedné či více metod klamání. Důraz je kladen rovněž na koherenci celého klamného působení, jeho věrohodnost a na technologické aspekty, které nabývají zásadního významu především v prostředí kyberprostoru.

Následující kapitola stručně uvádí příklady reflexivní kontroly, například vytvoření cílem pro protivníka, formování cíle přenosem obrazu o situaci, transfer obranu vlastní představy o situaci atp.

Následující části knihy se věnují analýze jednotlivých ruských doktrín v kontextu informačního a kybernetického válčení. Bagge se zabývá zejména Informačně-bezpečnostní doktrínou Ruské federace z roku 2000, Doktrínou informační bezpečnosti Ruské federace z roku 2016 a Národní bezpečnostní strategií Ruské federace z roku 2015 (s. 62). V těchto dokumentech autor systematicky identifikuje potenciální hrozby, například vysokou závislost státu na informačních a komunikačních technologiích, analyzuje cíle, jako je omezení šíření nepravdivých informací z pohledu Ruské federace, a zkoumá navrhované reakce, mezi něž patří například posílení státní kontroly nad informační scénou. Text tak poskytuje ucelený pohled na strategické rámce, které formují ruský přístup k informační a kybernetické bezpečnosti.

Podobným způsobem jsou rozebrány i klíčové vojenské dokumenty Ruské federace, mezi něž patří Vojenská doktrína Ruské federace (2010), Koncepční náhledy na činnost ozbrojených sil Ruské federace v informačním prostoru (2010), studie Hodnota vědy v tvorbě výhledu: nové výzvy vyžadují přehodnocení forem a metod vedení bojových operací (2013) a Vojenská doktrína Ruské federace (2013). Autor v nich sleduje proměnu ruského vojenského myšlení, v níž informační a kybernetická dimenze konfliktu nabývá stále většího významu a je chápána jako integrální součást moderních bojových operací.

Součástí této kapitoly jsou rovněž poznatky o vedení informačních operací vycházející z textů Valerije Gerasimova, jehož přístup je často uváděn v souvislosti s debatami o tzv. hybridním válčení. Bagge upozorňuje na nutnost nahlížet Gerasimovovy úvahy spíše jako analytickou reflexi charakteru moderních konfliktů než jako jednoznačný operační manuál. Text zdůrazňuje, že ruské pojetí hybridních operací zahrnuje propojení tradičních vojenských aktivit s kybernetickými, informačními a psychologickými prostředky, které mají vytvářet tlak na protivníka pod prahem otevřeného konfliktu. Gerasimovovy principy jsou zasazeny do širšího kontextu ruské vojenské doktrinální tradice, kde jsou dlouhodobě kombinovány strategie klamání, reflexivní kontroly a informační převahy. Současný vývoj ukazuje, že tyto koncepty nadále ovlivňují praxi ruských operací, přičemž jejich aplikace je sofistikovanější díky rychlému rozvoji digitálních technologií, sociálních sítí a analytických nástrojů, které umožňují cíleně modulovat informace a veřejné mínění jak v domácím prostředí, tak v zahraničí.

Za klíčovou část knihy lze považovat především příklady využívané při informačních operacích, které vychází z poznatků Sergeje A. Komova. Jedná se o tyto postupy či prvky informační války: odvedení pozornosti, přetížení, paralýza, vyčerpání, klamání, rozdělení, pacifikace, odstrašení, provokace a tlak. Všechny tyto postupy Bagge blíže představuje, analyzuje jejich využívání při ruských operacích, přičemž je v následující kapitole představuje v rámci obsáhlého schématu, které se týká kyberútoků a informačních operací na Krymu a východní Ukrajině (blíže s. 140-157).

V následujících pasážích lze očenit především doporučení, která by bylo vhodné aplikovat v případě nepřátelského užití dezinformací a informačním opatřením. Tyto prvky lze vnímat jako obecné prvky, které mají za cíl snížit efektivitu informačních a kybernetických útoků. Jedná se o vzdělávání v oblasti kritického myšlení, převzetí iniciativy a opuštění pouze reaktivního přístupů, určení červené linie, kterou protivník nesmí překročit, šíření pozitivních narativů, zvyšování vnímavosti politiků a politických stratégů v kontextu kybernetického boje, cvičení rozhodovacích činitelů v této oblasti atp.

Autor poukazuje na to, že vlivové operace, které kombinují informačně-technologická a informačně-psychologická opatření, umožňují aktérům působit efektivně bez nutnosti přímého vojenského střetu s protivníkem, a přitom mají značný dopad na formování mezinárodní politiky. Tyto strategie umožňují cíleně zasahovat do rozhodovacích procesů, veřejného mínění i fungování institucí, čímž se stávají mocným nástrojem prosazování zájmů v prostředí moderních hybridních konfliktů. Jak Bagge výstižně konstatuje: „Informační údery mohou způsobit škodu a zasáhnout klíčové jednotlivce, běžnou populaci a zranitelné společenské skupiny, a tím ochromit společenské funkce, rozvrátit instituce a nakonec vyvolat zhroucení celého státu“ (s. 171).

Závěrečná část knihy rovněž akcentuje potřebu systematicky posilovat kybernetickou a informační bezpečnost nejen mezi odborníky, ale i v rámci široké veřejnosti. Na tomto místě je zmiňována zásadní role kritického myšlení a kognitivních i psychologických předpokladů, které ovlivňují schopnost jednotlivců analyzovat informace a realisticky vnímat okolní svět. Zvláštní pozornost je věnována tzv. rozhodovacím činitelům, tedy politikům a expertům, kteří však v některých případech sami přispívali k šíření neověřených informací, spekulací či otevřeně nepravdivých zpráv prostřednictvím médií. Tyto příklady zároveň ukazují obecně platný princip informační gramotnosti: každou zprávu je nezbytné ověřovat z relevantních a ideálně více nezávislých zdrojů.

Závěrem lze konstatovat, že knihu Daniela P. Baggeho lze doporučit nejen bezpečnostním expertům, ale i politikům, novinářům, akademikům a všem čtenářům se zájmem o současné bezpečnostní hrozby a fungování informačního prostoru. Publikace nabízí srozumitelný, analyticky ukotvený a zároveň empiricky podložený pohled na problematiku ruských vlivových operací v kyberprostoru, čímž přispívá k lepšímu porozumění mechanismům moderních konfliktů. Její přínos spočívá nejen v popisu konkrétních případů a strategií, ale také v širším kontextualizování kybernetických a informačních operací jako dlouhodobého a systematického nástroje státní moci. V tomto smyslu kniha představuje hodnotný zdroj poznání i praktickou oporu pro orientaci v čím dál komplexnějším bezpečnostním prostředí současného světa.