CENTRUM BEZPEČNOSTNÍCH A VOJENSKOSTRATEGICKÝCH STUDIÍ
UNIVERZITA OBRANY V BRNĚ

TECHNOLOGICKÝ VÝVOJ

IMPLIKACE PRO SCHOPNOSTI OZBROJENÝCH SIL ČR 2019

JAKUB FUČÍK A KOL.

TECHNOLOGICKÝ VÝVOJ

IMPLIKACE PRO SCHOPNOSTI OZBROJENÝCH SIL ČR 2019

JAKUB FUČÍK A KOL.

BRNO 2020

AUTORSKÝ KOLEKTIV

Mgr. et Mgr. Jakub Fučík, Ph.D.

Ing. Fabian Baxa, Ph.D.

PhDr. Libor Frank, Ph.D.

doc. Ing. Josef Procházka, Ph.D.

Tato odborná studie je dílčím výsledkem projektu *STRATAL – Strategické alternativy*, řešeného na Univerzitě obrany v Brně.

Recenzenti:
gen. Ing. Miroslav Feix, M.S. – velitel Velitelství kybernetických sil a informačních operací Armády České republiky

plk. gšt. doc. Ing. Petr Františ, Ph.D. - vedoucí Katedry informatiky a kybernetických operací, Fakulta vojenských technologií Univerzity obrany v Brně

pplk. gšt. Ing. Jan Farlík, Ph.D. - zástupce vedoucího Katedry protivzdušné obrany a proděkan pro vnější vztahy a rozvoj Fakulty vojenských technologií Univerzity obrany v Brně

Centrum bezpečnostních a vojenskostrategických studií (CBVSS)

CBVSS je součástí Univerzity obrany a je dle zákona č. 111(1998 Sb., § 22 odst. 1, písm. c), vymezeno jako jiné pracoviště pro vzdělávání a tvůrčí činnost. Jeho posláním je zejména:

- Vědeckovýzkumná činnost v oblastech bezpečnostních studií, strategického leadershipu, vojenského umění, strategického řízení a obranného plánování, která je uskutečňována pro potřeby strategické úrovně rozhodování, řízení obrany státu a výstavby ozbrojených sil ČR.
- Příprava vojenských a civilních odborníků resortu ministerstva obrany a ozbrojených sil v odborných a kariérových kurzech (KGŠ, KVD).
- Expertní, publikační a popularizační činnost (mj. garantuje vydávání časopisů *Vojenské rozhledy* a *Obrana a strategie*).

ISBN978-80-7582-344-1

ÚVOD

Cílem analytické studie je zhodnocení trendů technologického vývoje a jejich implikací pro ozbrojené síly České republiky za rok 2019. Ambicí Centra bezpečnostních a vojenskostrategických studií Univerzity obrany (CBVSS) je poskytnout alternativní příspěvek do diskuze o důsledcích technologického vývoje pro formulování a realizaci účinné obranné politiky České republiky, respektive výstavbu jejích ozbrojených sil (primárně Armády České republiky). Dokument má sloužit jako periodické zhodnocení dotčené problematiky a poskytnout tak základy pro další výzkum. V tomto smyslu studie přímo navazuje na hodnocení technologických trendů za rok 2017 a 2018.[1]

Studie vychází z analýzy a komparace otevřených zdrojů, které se vztahují k charakteru současných trendů technologického vývoje a jeho relevantních příkladů. Implikace pro OS ČR (AČR) jsou analyzovány pomocí tzv. hlavních oblastí schopností *(Main Capability Areas, MCA)* definovaných prostřednictvím metodiky NATO.[2] U každého trendu jsou identifikovány oblasti schopností, které jsou jeho rozvojem přímo ovlivněny a mají bezprostřední význam pro dotčený subjekt. Současně je nezbytné podotknout, že byť jsou jednotlivé trendy a jejich implikace analyzovány a popsány postupně, tak nelze jejich povahu vnímat odděleně.

Čtenář by měl v této problematice vždy zohledňovat „zastřešující" téma vlivu technologického vývoje na ozbrojené síly, respektive společnost obecně, a vzájemnou provázanost relevantních trendů. Totožný komplexní přístup je relevantní i k užitému analytickému rámci MCA a konkrétním identifikovaným schopnostem. Studie je časově zarámována rokem 2019 a zaměřuje se na trendy, které mohou bezprostředně ovlivňovat ozbrojené síly. Verifikace výstupů byla provedena v rámci expertních jednání a workshopu za účasti příslušníků MO ČR, AČR a představitelů bezpečnostní komunity ČR.

[1] Viz FUČÍK a kol. *Technologický vývoj: Implikace pro schopnosti ozbrojených sil ČR 2018* [online]. Brno, CBVSS UO, 2019. Dostupné z: https://bit.ly/3c7WKvE

[2] MC 400/3, MC Guidance for Military Implementation of Alliance Strategy. 2012.

NAVYŠOVÁNÍ VÝZNAMU „NOVÝCH“ STRATEGICKÝCH DOMÉN

Vedle tradičních dimenzí strategického uvažování a vedení ozbrojeného konfliktu – pozemní, námořní a vzdušné – pokračuje navyšování významu vesmírného prostoru a kyberprostoru, a to bez ohledu, zda jednotlivé státy / mezinárodní organizace považují tyto domény za samostatné nebo jako součást ostatních dimenzí (např. kyberprostor jako součást informační domény v rámci ruského přístupu).

VESMÍRNÝ PROSTOR

Podobně jako v předchozích letech narůstá zájem ze strany státních i nestátních aktérů o tuto doménu. Na úrovni států můžeme identifikovat strategické směřování rozvoje vesmírných kapacit, které by zajistily, případně podpořily, uplatňování jejich moci, respektive vojenské síly, v globálním měřítku. Vesmírné platformy v tomto kontextu zajišťují globální komunikaci, navigaci, získávání informací či využívání pokročilých (zbraňových) systémů typu přesně naváděné munice nebo dálkově ovládaných a autonomních prostředků. Tento přístup reflektuje povahu vesmírného prostoru a zejména zdůrazňuje, že kterékoliv místo na povrchu Země je přímo dosažitelné z její oběžné dráhy, přičemž nezáleží na členitosti terénu, nadmořské výšce či jeho odlehlosti (nejen od zbytku „civilizace“, ale též pevniny samotné). Obdobně není potřebné využít, popř. narušit, státní hranici, vzdušný prostor nebo teritoriální vody jiných států.

Na tento aspekt reagovalo v loňském roce NATO, když uznalo vesmír jako další samostatnou operační doménu.[3] V důsledku prozatímní absence navazujících kroků, např. v podobě tvorby strategických dokumentů zaměřených ryze na tuto doménu, nelze ovšem prozatím přesně určit, jaké bude mít toto rozhodnutí implikace pro Alianci jako celek, potažmo pro její členské státy. V USA Kongres schválil vznik Vesmírných sil Spojených států amerických coby samostatné složky Ozbrojených sil Spojených států. K jejich založení došlo 20. prosince 2019.[4] Současně byla prostřednictvím aktualizovaná verze dokumentu *Missile Defence Review*[5] v rámci systému protiraketové obrany kromě posílení vesmírné senzorové složky revitalizována myšlenka na rozvoj a rozmístění zbraňových systémů určených k intercepci balistických střel ve vzestupné fázi letu *(boost phase)*. Podobné směřování je patrné nejen u Čínské lidové republiky (v rámci Sil strategické podpory ČLOA) a Ruské federace (v rámci Vzdušně-kosmických sil Ruské federace), tj. hlavních „vyzyvatelů“ právě Spojených států amerických, ale i dalších mocností. Jako příklad lze uvést autorizaci vzniku Francouzských vesmírných sil ze strany prezidenta Macrona z července 2019.[6]

Taktéž nelze opomenout ani roli a narůstající význam nestátních aktérů (zejména v podobě soukromých obchodních společností typu SpaceX), kteří fakticky privatizují vesmírný výzkum a vývoj a rozvíjejí související schopnosti. Kromě oblasti vesmírných nosičů se postupně posouvají k letům s lidskou posádkou, které původně byly vyhrazeny

[3] NATO. *Foreign Ministers take decisions to adapt NATO, recognize space as an operational domain* [online]. 2019. Dostupné z: https://bit.ly/3ernSHB
[4] MYERS, M. The Space Force is officially the sixth military branch. Here's what that means [online]. *Air Force Times*, 2019. Dostupné z: https://bit.ly/3c3Wo95
[5] U.S. DoD. *Missile Defence Review* [online]. 2019. Dostupné z: https://bit.ly/2TL1H7j
[6] ZIHNIOGLU, K. Macron announces creation of French space force [online]. *AFP*, 2019. Dostupné z: https://bit.ly/36wp8q4

státům, respektive státním či mezinárodním organizacím. V roce 2019 Boeing i SpaceX úspěšně otestovaly svoje moduly[7] a první pilotované lety jsou naplánovány na rok 2020. Na jednu stranu tento jev s sebou mj. přináší lepší dostupnost dotčených systémů a schopností (např. prostřednictvím snížení ceny/nákladů na vynesený kg na oběžnou dráhu z důvodu konkurence mezi jednotlivými soukromými společnostmi). Na druhou stranu ale dochází k omezování státní kontroly nad systémy, které budou takto na oběžné dráze umístěny. Tato situace dále „znepřehledňuje" níže popsaný problém technologií dvojího užití *(dual-use)*.

V obecné rovině lze potenciál, který představuje vesmírný prostor a relevantní technologie, rozdělit do dvou oblastí (civilní a vojenské), přičemž dělicím kritériem je povaha aktivit, respektive reálných umělých těles (družice, stanice aj.) ve vesmíru provozovaných nebo umístěných. Do civilní skupiny řadíme např. zřizování a využívání satelitních sítí určených k monitorování počasí nebo přenosu televizního signálu aj. Vojenská skupina zahrnuje např. špionážní satelitní sítě, satelitní navigaci vojenských jednotek nebo zbraňové platformy určené k detekci a eliminaci balistických střel apod. Podobně do této kategorie spadají tzv. antisatelitní zbraně *(anti-satellite weapons, ASAT)*, které sice mohou být umístěny na zemském povrchu nebo mořské hladině, ale jejich užití je přímo situováno do vesmírného prostoru. Ke státům, které oficiálně úspěšně otestovaly tento zbraňový systém (Čína, Rusko, USA), v loňském roce přibyla Indie[8] prostřednictvím konverze technologií užitých pro výstavbu a rozvoj vlastního protiraketového „deštníku".

Současně je nezbytné konstatovat, že hranice mezi oběma kategoriemi je velmi nejasná, respektive obě skupiny se ve svých prvcích často překrývají a jejich odlišení v praxi je poměrně problematické. Setkáváme se tak s přetrvávajícím fenoménem dvojího užití příslušných technologií, popř. aktivit. Satelitní navigační síť může být kupříkladu využita nejen pro určení pozice civilních subjektů, ale též ke koordinaci postupu operačních uskupení nebo navádění řízených střel či bezpilotních prostředků (odkaz na americký systém GPS nebo rozdílné druhy služeb, které budou poskytovány prostřednictvím budovaného evropského systému Galileo). Obdobně lze hodnotit i využitelnost budovaných satelitních sítí pro globální komunikaci a pokrytí 5G internetem (aktuálně např. OneWeb nebo LeoSat).

Využívání satelitních systému je z pohledu jak technologického vývoje (miniaturizace), tak sdílení kapacit a zmiňované úlohy vesmírných společností stále více dostupné i pro malé státy. V loňském roce tento jev demonstrovala i Česká republika prostřednictvím dostavby Satelitního centra SATCEN, které dosáhlo plné funkčnosti k 1.1.2020. Centrum je spravováno Vojenským zpravodajstvím a umožňuje zisk a analýzu elektrooptických a radarových obrazových dat z kosmického průzkumu.

Vesmírný prostor nabývá na významu pro schopnost uplatňovat (vojenskou) moc státu a sehrává svoji roli při prosazování svých národních zájmů. Tento aspekt reflektuje i NATO prostřednictvím jeho uznání jako nové samostatné operační domény. Současně narůstá role soukromých obchodních společností, které rozvíjejí schopnosti původně vyhrazené státům či mezinárodním organizacím. Využívání vesmírného prostoru je velmi úzce

[7] NASA. NASA, Partners Update Commercial Crew Launch Dates [online]. 2019. Dostupné z: https://go.nasa.gov/3c67yub; MALIK, T. Boeing's 1st Starliner Spacecraft Lands in New Mexico After Shortened Test Flight [online]. *Space.com*, 2019. Dostupné z: https://bit.ly/3caCWYh

[8] CHAUDHURY, D. R. Explained: What's Mission Shakti and how was it executed? [online]. *The Economic Times,*2019. Dostupné z: https://bit.ly/36y9oCV

provázáno s fenoménem tzv. dvojího užití, kdy dochází ke stírání hranic mezi civilním a vojenským sektorem.

Implikace pro ozbrojené síly České republiky

Narůstající vliv **vesmírného prostoru** (případně i jako samostatné operační dimenze), klade nové požadavky na oblast *Prepare/training* ozbrojených sil, které musí zohledňovat specifika této domény. Byť na první pohled může přístup k této dimenzi působit „exoticky" a vzdálený cílům a možnostem zejména Armády České republiky, tak nelze opomenout širší kontext jak Evropské unie, tak NATO. Právě členství v těchto institucích představuje potenciál pro získání přístupu k jednotlivým druhům vesmírných systémů (ať již navigačním, komunikačním či monitorovacím) a jejich využití pro rozvoj relevantních schopností. Ze strany NATO je tento aspekt dále posílen schválením vesmíru jako samostatné operační domény, což pro AČR vytváří předpoklady pro další spolupráci napříč celou organizací. Obdobně lze hodnotit i narůstající možnosti vyplývající z privatizace/komercionalizace tohoto prostoru, byť se s tímto současně pojí i hrozba závislosti na takovém aktérovi, která je spojena s potenciálně odlišnými zájmy nebo nejasnou kontrolou nad jeho aktivitami. V návaznosti na bezpečnostní zájmy a charakter České republiky, respektive jejích ozbrojených sil, by hlavní pozornost měla být zaměřena na projekty posilující hlavní oblasti schopností *Project; Consult, Command and Control* (C3); *Protect*; a *Inform*. Tyto předpoklady naplňuje mj. výše zmíněný rozvoj navigačního systému Galileo nebo zajišťování dat pro potřeby (strategického) IMINTu[9] formou mezinárodní spolupráce se Satelitním střediskem Evropské Unie (EU SatCen) nebo nákupem od soukromých poskytovatelů. Obdobné zapojení a využívání lze na vnitrostátní úrovni předpokládat od Satelitního centra. Všechny tyto projekty jsou využitelné nejen pro výstavbu/posílení komplexního systému C4ISR, ale i zajištění robustního informačního toku pro ovládání bezpilotních/bezosádkových a autonomních systémů.

KYBERPROSTOR

Posilování strategického významu kyberprostoru je přímo navázáno na rozvoj informačních technologií a jejich využívání v současné době fakticky ve všech oblastech lidského života. Informační globalizace umožňuje jakémukoliv aktérovi (státnímu i nestátnímu) takřka okamžitý a neomezený přístup k obrovskému množství dat a jejich následné zpracování a využití pro vlastní potřeby. Z informací, respektive „surových" dat, se v tomto smyslu postupně stává strategická surovina využitelná jak pro utváření pozice v této dimenzi, tak pro ovlivňování fungování reálného prostředí. Z pohledu státních a nestátních aktérů je zajištění trvalého a bezpečného přístupu k této doméně fakticky prvotním předpokladem pro efektivní naplňování vlastních zájmů. V tomto smyslu tzv. kybernetické útoky, respektive škodlivé kybernetické aktivity *(malicious cyber activities)* - např. ve formě schopnosti odepření přístupu protivníkovi do této domény – reprezentují významné nástroje pro dosažení stanovených cílů,[10] které se obecně vyznačují nejen velmi výhodným

[9] Akronym označující zpravodajskou disciplínu *Imagery intelligence*, do češtiny překládané jako „obrazové zpravodajství".

[10] Srov. např. NATO. Strategic Foresight Analyses. 2017.

poměrem v hodnocení nákladů vs. zisků z diskutovaných aktivit, ale též sníženou mírou přičitatelnosti či postižitelnosti ze strany poškozeného subjektu.

Rozvoj tzv. internetu věcí *(Internet of Things, IoT)* postupně eskaluje do podoby tzv. „internetu všeho" *(Internet of Everything, IoE)*, který nejen umožňuje mnohem efektivněji využívat výhody spojené s komplexním informačním propojením (např. zajistit monitorování a rozhodování v reálném čase), ale taktéž prohlubuje celkovou závislost na stabilním a efektivním fungování tohoto prostoru, což má za následek růst zranitelnosti uživatele. Výstavba a rozvoj 5G informačních sítí posouvá diskutovanou problematiku na kvalitativně vyšší úroveň, a to jak z pohledu příležitostí, tak možných ohrožení. Zajišťování bezpečnosti v současné době, zejména kritické informační infrastruktury, musí nezbytně tento trend zohlednit. Zvláště je-li zohledněno potenciální zneužití velkého množství diskutovaných zařízení v rámci tzv. botnetů k provádění cílených útoků proti informačním systémům jak relevantních státních, tak nestátních subjektů (v roce 2019 např. proběhly útoky na dostupnost služby Telegram v Asii[11]).

Současně se zintenzivněním propojení lidstva v rámci tohoto prostoru dochází k nárůstu počtu sítí, které jsou vytvářeny a používány na distributivním principu, tj. bez existence centrálního kontrolního či řídícího „uzlu". Jedním z takových přístupů je i technologie tzv. „blockchainu", kterou využívají současné kryptoměny, a dochází k jejímu postupnému zavádění i v dalších oblastech (např. bankovnictví[12] nebo správa a sdílení dat[13]). Výslednou podobou tohoto trendu je nárůst významu tzv. „deep webu", respektive v užším pojetí s bezpečnostními aspekty „dark webu" a „darknetu".[14] Zejména darkweb/darknet je totiž přímo spojen s nelegálními aktivitami napříč všemi oblastmi (od nelegálního získávání informací po obchod se zbraněmi, návykovými látkami nebo lidmi). Navíc kromě organizovaného zločinu jsou obdobné prostředky/možnosti využívány např. teroristickými organizacemi a v zásadě i samotnými státy. Fakticky zde dochází k dalšímu oslabování státní moci v podobě schopnosti kontrolovat a regulovat dotčené aktivity a aktéry a dle potřeby proti nim zasahovat, což je mj. spojeno se střetem mezi ochranou národních zájmů (v širokém pojetí) na jedné straně a užitnou hodnotou takových sítí na straně druhé.

Provázanost všech oblastí lidské společnosti s kyberprostorem dále rozvíjí i vzájemnou závislost ve smyslu dostupnosti samotných informací. Digitalizace státní správy a přenos vazeb mezi občanem a státem do této domény (např. formou elektronických občanských průkazů nebo voleb) přímo reflektuje tento fenomén, který ovšem s sebou přináší i nové formy zranitelnosti (např. problematika manipulace s volebními systémy). Internet z tohoto pohledu umožňuje navýšení transparentnosti takřka všech činností v reálném prostředí. Zejména sociální média typu Facebook, Instagram, Twitter, YouTube, nebo nejnovější TikTok umožňují takřka neustálý dohled a monitorování aktivit jednotlivých subjektů. Současně slouží jako ideální nástroj a platforma pro vedení informačních operací ze strany jak státních, tak nestátních aktérů. Kontrolu nad těmito sítěmi, případně jejich

---

[11] SHIEBER. J. Telegram faces DDoS attack in China…again [online]. 2019. Dostupné z: https://tcrn.ch/2ZJgfbc

[12] KELLY, Jemima. Top Banks nad R3 Build Blockchain-BasedPayments System [online]. *Reuters*, 2017. Dostupné z: https://1url.cz/vM4zs

[13] KARL, Angela. *Blockchain Technology for Cloud Storage: This Looks Like Future* [online]. Tech Genix, 2018. Dostupné z: https://1url.cz/yM4zC

[14] Podrobněji o uvedených pojmech např. SUI, Daniel – CAVERLEE, James – RUDESILL, Dakota. *The Deep Web and Darknet: A Look Inside the Internet's Massive Black Box* [online]. Wilson Center, 2015. Dostupné z: https://goo.gl/AztPdM

poskytovateli, lze tedy chápat jako významný předpoklad pro schopnost kontrolovat a ovlivňovat veřejné mínění obecně. Na druhou stranu, obdobně tento aspekt napomáhá k efektivní obraně vůči vlivovým aktivitám potenciálního protivníka. Budování samostatného ruského „internetu" RuNet, který měl být v roce 2019 úspěšně otestován[15], nebo navyšování účinnosti[16] tzv. „Velkého čínského firewallu" z tohoto pohledu v sobě spojuje obě výše diskutované charakteristiky.

Zásadní význam (nejen) pro tuto doménu bude představovat plnohodnotné zavedení kvantových (výpočetních) technologií, které ze své podstaty zásadně překonávají dosavadní výkon jednotlivých systémů. S tímto se následně pojí nové možnosti např. ve zpracovávání a ukládání velkého objemu dat (tzv. Big Data) nebo i odpovídající hrozby/příležitosti pro současné šifrovací nástroje a postupy, tj. ochranu samotných dat a informací. V lednu 2019 byl sice představen první „komerční kvantový" počítač (IBM Q System One).17 Na druhou stranu, stále se jedná o pomyslné první kroky a zajištění všeobecného využití této technologie je stále otázkou dlouhodobého výzkumu a vývoje.

Informační technologie jsou již v současnosti provázány se všemi oblastmi lidského života (mj. i u vazeb občan – stát). Postupně dochází k posunu od „internetu věcí" k „internetu všeho", s čímž je spojeno i jeho zneužívání k provádění např. velkých DDoS útoků proti státním i nestátním subjektům. Současně dochází k dalšímu oslabování státní moci prostřednictvím ilegálních aktivit v rámci darkwebu/darknetu. Velká pozornost je taktéž věnována rozvoji kvantových technologií, které mají potenciál zásadně ovlivnit současné přístupy např. v oblasti kryptografie. Z pohledu informačních operací (informačního působení včetně šíření dezinformací) mohou důležitou úlohu sehrávat sociální média / sítě a aktéři, kteří jsou schopni zpracovávat a využívat Big data.

Implikace pro ozbrojené síly České republiky

Z pohledu nejnovější operační domény klade **kyberprostor** zvýšené nároky na výcvik a přípravu, a to jak pro maximalizaci jeho přínosu, tak potlačování zranitelností, které z používání informačních technologií vyplývají. Význam výše diskutovaných trendů lze pro OS ČR dále identifikovat v oblastech *Project; Engage; C3; Protect; Sustain* a *Inform*. Rozvoj schopností v uvedených oblastech bude mj. navázán jak na systémy umožňující zpracovávání velkého objemu dat, tak systémy podporující operativní změny úrovně centralizace a decentralizace velení a řízení. Dobudování komplexního propojení C4ISR v prostředí AČR by mělo nejen zabránit v zaostávání v této oblasti vůči rozvinutějším státům, ale taktéž poskytnout důležitou kompetitivní výhodu jak v rámci „malých", tak „velkých" ozbrojených konfliktů. Podporu tomuto rozvoji mohou poskytnout prvky „cloudových" služeb upravené pro vojenské účely. Své uplatnění zde nachází i technologie „blockchain" a možnosti její implementace pro decentralizaci a zabezpečení dat (např. z průzkumných bezpilotních prostředků) nebo navýšení odolnosti *(resilience)* systémů AČR proti účinkům a následkům elektromagnetického pulsu (EMP) či jiným způsobům narušování provozu informačních a komunikačních systémů. Ve všech těchto oblastech

[15] WAKEFIELD, J. Russia 'successfully tests' its unplugged internet [online]. *BBC*, 2019. Dostupné z: https://bbc.in/2X7vyst

[16] WYCIŚLIK-WILSON, M. It is getting harder than ever for VPNs to break through the Great Firewall of China [online]. *Beta News*, 2019. Dostupné z: https://bit.ly/3gr4v32

[17] RUSSELL, John. IBM Quantum Update: Q Systém One Launch, New Collaborators, and QC Center Plans [online]. *HPC wire*, 2019. Dostupné z: https://1url.cz/kM4K2

taktéž nelze opomenout význam kyberprostoru a výše popsaných trendů pro informační působení. Pozornost je nezbytné věnovat jak možnému využití této platformy včetně „internetu všeho“, sociálních sítí, prvků umělé inteligence (podrobněji viz další kapitola) pro působení ze strany AČR vůči protivníkovi, tak obraně proti takovým aktivitám ze strany protivníka. Ústřední roli zde bezesporu sehrává zajištění jednotné a nepřetržité strategické komunikace (StratCom) vůči domácímu i zahraničnímu publiku. V rámci oblasti *Engage* se dále nabízí možnost kombinace se schopnostmi a prvky elektronického boje – např. ve formě vnášení malwarů do protivníkových informačních sítí skrze bezdrátové připojení aj. Současně, především v kontextu *Protect* a *Sustain,* by zvýšený důraz měl být kladen na zajišťování kybernetické obrany a bezpečnosti. Význam těchto aspektů byl v loňském roce podpořen zkušenostmi ČR z útoků proti nemocničnímu zařízení v Benešově a těžební společnosti OKD. Toto doporučení je ovšem nezbytné vztáhnout nejen vůči dnes již tradičním platformám, ale právě i na oblast internetu věcí / internetu všeho nebo příležitosti/hrozby spojené s rozvojem kvantové výpočetní techniky. V návaznosti na zkušenosti např. z USA lze totiž předpokládat, že tato zařízení budou v blízké budoucnosti využívána nejen jako cíle kybernetických útoků, ale i jako samotné prostředky pro jejich realizaci. I pro ozbrojené síly malého státu, jakým je ČR, je proto nezbytné zajistit v této doméně schopnosti A2/AD, které by umožnily stabilní využívání tohoto prostředí, a naopak protivníkovi přístup odepřely.

ROZVOJ A ŠÍŘENÍ DÁLKOVĚ OVLÁDANÝCH PROSTŘEDKŮ A AUTONOMNÍCH SYSTÉMŮ

V současné době jsou v rámci ozbrojených sil více než šedesáti států světa využívány bezpilotní systémy *(Unmanned Aerial Systems, UAS)* pro potřeby průzkumu, sledování či monitorování. Postupně taktéž dochází k rozšiřování okruhu států, které disponují bojovými (údernými) bezpilotními prostředky. Lze předpokládat, že tento obecný trend, tj. navyšování počtu států, které disponují jednotlivými kategoriemi bezpilotních prostředků, bude jen nabývat na intenzitě. Oproti pilotovaným letadlům jsou upřednostňovány nižší akviziční i provozní náklady a absence přímého ohrožení lidské „posádky“ (operátorů).

Prostřednictvím rozvoje zejména aditivní výroby a nanotechnologií (podrobněji viz kap. Aditivní výroba) jsou postupně zaváděny nové kategorie UAS – mikro a nano – které se svými rozměry mohou přiblížit až velikosti hmyzu. Právě tento aspekt jim mj. poskytuje výhodu vůči tradičním senzorům a propůjčuje schopnost nepozorovaně proniknout do zabezpečených oblastí.

Zejména u velmocí lze identifikovat jak citelné navyšování počtu jednotlivých druhů bezpilotních prostředků, tak rozšiřování okruhu úkolů (např. zásobování nebo doprava), pro které jsou využívány. Tento trend lze velmi dobře demonstrovat na příkladu Spojených států amerických, kdy ještě v roce 2000 jejich ozbrojené síly disponovaly pouze dvěma typy UAS.[18] V současnosti je jich již minimálně jedenáct[19] včetně UAS vybavených zbraňovými systémy. Obdobně Ruská federace velmi intenzivně rozvíjí projekty bojových

[18] Office of the Secretary of Defense. *Unmanned Aircraft Systems Roadmap: 2005-2030* [online], s. 3. Washington, D. C., 2005. Dostupné z: https://goo.gl/RBfrij

[19] SICARD, Sarah. 11 Military Drone Names, Ranked [online]. *Task & Purpose*, 2017. Dostupné z: https://goo.gl/Z3ExN7

bezpilotních letounů, které se momentálně nacházejí ve fázi testování jednotlivých prototypů. V srpnu 2019 byl například uskutečněn první let proudového UCAV S-70 Ochotnik-B.[20]

Bezosádkové pozemní systémy *(Unmanned Ground Systems, UGS)* jsou oproti UAS prozatím v rámci ozbrojených sil jednotlivých států zastoupeny v menším počtu i variabilitě. Jejich role je často směřována do oblasti zneškodňování nástražných zařízení a nevybuchlé munice, nakládání s nebezpečnými látkami nebo průzkumu na krátkou vzdálenost (např. v urbanizovaných oblastech). Izraelská armáda využívá tyto prostředky (projekt Guardium) i ke strážní činnosti v hraničních oblastech a ochraně základen. Vozidla disponují kromě senzorů určených k detekci protivníka (narušitele) i zbraňovými systémy jak letálního, tak neletálního charakteru.[21] Obdobně by se měla ve fázi vývoje nacházet dálkově řízená modifikace nejnovějšího ruského obrněného vozidla na platformě Armata nebo jednotlivé projekty USA pod záštitou organizace DARPA, které přímo navazují na potřeby/předpoklady zakotvené v tzv. třetí offsetové strategii.[22]

V návaznosti na ovládání jednotlivých prostředků je velká pozornost věnována rozvoji kapacit, které by umožňovaly simultánní nasazení velkého množství jednotlivých typů diskutovaných (zbraňových) systémů. Zejména u bezpilotních systémů je tento přístup spojován se schopností ovládat tzv. hejna/roje *(swarms)*, tj. vysoký počet (malých) prostředků, které umožní zahlcení protivníkovy (protivzdušné) obrany. Intenzivní testování těchto technologií probíhá např. v Číně, která je momentálně označována minimálně za jednu z vedoucích zemí.[23] Jejich využití je předpokládáno jak pro plnění samostatných úkolů (např. i zničení stanovených cílů), tak na podporu ostatních jednotek, respektive letadel s lidskou posádkou. Fakticky tak dochází i k rozvoji a posilování funkčních vazeb mezi jednotlivými prostředky navzájem pro získání synergického efektu. Prvotní potenciál takové schopnosti byl v loňském roce demonstrován při útocích na ropná zařízení v Saúdské Arábii.[24]

Obdobně se rozvíjejí projekty společného působení pilotovaných/řízených systémů a dálkově ovládaných či autonomních systémů. Prostředek s lidskou osádkou v takové kombinaci zpravidla sehrává roli vůdčího prvku, který se podpořen robotickými systémy. Výsledkem je synergické navýšení schopností takového kompletu prakticky ve všech aspektech. Například USA v souvislosti s programem *Skyborg* připravují autonomní letoun, který by doprovázel letadla F-15 a F-35.[25] Podobné projekty můžeme nalézt v zásadě pro všechny zbývající domény (kyberprostor nevyjímaje).

---

[20] ESHEL, T. Russian Okhotnik-B Combat Drone (UCAV) Makes its First Flight [online]. *Defense Update,* 2019. Dostupné z: https://bit.ly/2TLJ6rw

[21] ARMY-TECHNOLOGY.COM. *AvantGuard Unmanned Groud Combat Vehicle, Israel* [online]. 2016. Dostupné z: https://goo.gl/knZqWb

[22] LOUTH, John – MOELLING, Christian. *Technological Innovation: The US Third Offset Strategy and the Future Transatlantic Defense* [online]. Armament Industry European Research Group, 2016. Dostupné z: https://goo.gl/pvEHAc

[23] BLEEK, P.C. – KALLENBORN, Z. Drones of Mass Destruction: Drone Swarms and the Future of Nuclear, Chemical, and Biological Weapons [online]. *War On The Rocks,* 2019. Dostupné z: https://bit.ly/2TZLgEn

[24] SAFI, M. – WEARDEN, G. Everything you need to know about the Saudi Arabia oil attacks [online]. *The Guardian,* 2019. Dostupné z: https://bit.ly/3dctx3W

[25] INSINNA, Valerie. Under Skyborg program, F-35 and F-15EX jets could control drone sidekicks. *Defense News*, 2019. Dostupné z: https://bit.ly/2zq2y6t

Oproti dálkově ovládaným prostředkům autonomní systémy předpokládají buď žádné, nebo jen minimální „vměšování“ ze strany lidského operátora. Jednotlivé systémy by měly být schopny samostatně nejen získávat informace o okolním prostředí, ale i je zpracovávat (vyhodnocovat) a učinit odpovídající rozhodnutí. Motivace k etablování těchto systémů přímo vyplývá z navýšení bojové efektivity. Obdobně jako u dálkově ovládaných prostředků je zde totiž zastoupena myšlenka minimalizace lidských ztrát na straně vlastních ozbrojených sil a nezúčastněných osob.[26] Systémy založené na prvcích UI / strojového učení efektivněji potlačují a odstraňují limity vyplývající z lidské fyziologie (mj. potřeba spánku a vliv únavy, a to i u lidských operátorů, nebo vliv stresu).

Na druhou stranu zde vyvstávají závažné otázky zahrnující míru autonomie, která by měla být těmto systémům poskytnuta, a zda lze minimálně z etického hlediska přijmout rozhodnutí o zabití lidské bytosti uskutečněné ryze těmito prostředky. Právě tento aspekt je stále častěji diskutován napříč odbornou komunitou a stává se motivací pro snahy o ustanovení a prosazování kontrolního režimu na mezinárodní úrovni (např. pod záštitou OSN).[27] Na druhou stranu je nezbytné kriticky podotknout, že v návaznosti na historické příklady (např. kazetová munice, protipěchotní miny apod.) je pravděpodobnost dosažení celkového zákazu napříč všemi státy a jeho vynucování spíše nereálné.

Určité prvky těchto technologií můžeme identifikovat již v současnosti, kdy jsou např. právě vozidla Guardium schopny operovat i v plně automatizovaném (autonomním) módu.[28] Obdobně je těchto prvků využíváno u bezpilotních letounů při dlouhých přeletech, kdy lidský operátor přebírá ovládání až v prostoru stanovené mise nebo u systémů protivzdušné obrany (např. zbraňový systém blízké/objektové obrany Phalanx).[29]

V systémech založených na prvcích UI/ strojového učení lze dále identifikovat značný potenciál ve vztahu ke kyberprostoru, respektive ke sběru, vyhodnocování a nakládání s daty a informacemi obecně. Jejich rozvoj a výkonnost přináší nové možnosti např. pro oblasti podrobné analýzy velkého množství dokumentů, obrazových prvků nebo hlasových projevů. Následně s tímto souvisí schopnost jejich přesné nápodoby a vytváření kopií či naprosto nových prvků (např. virtuální televizní reportér) takřka nerozeznatelných od skutečnosti/originálů (forma tzv. *deepfakes*).

Velká pozornost je obecně věnována jak rozvoji bezpilotních, tak autonomních systémů. Ve výzbroji jednotlivých států jsou prozatím nejvíce zastoupeny průzkumné UAS, ale z jednotlivých projektů ať bojových UAS nebo UGS lze usuzovat postupné rozšiřování tohoto okruhu. Postupně jsou taktéž zaváděny nové kategorie mikro- a nano-. Výzkum a vývoj se dále zaměřuje na schopnosti simultánně nasadit a ovládat velké množství (swarm) zejména UAS. Pozornost je taktéž věnována společnému působení pilotovaných/řízených systémů a dálkově ovládaných či autonomních systémů. Rozvoj autonomních systémů je přímo podmíněn úrovní rozvoje prvků UI a ovlivňuje prostředky a aktivity ve všech doménách. Současně ale dochází k intenzivní debatě nad morálními/etickými aspekty využívání (nejen) tohoto typu technologií pro vojenské účely.

[26] Mj. i STOJAR, Richard. Bezpilotní prostředky a problematika jejich nasazení v soudobých konfliktech. *Obrana a strategie*. 2016, 16(2). Dostupné z: https://goo.gl/dYJsZ2
[27] Např. Autonomous Weapons: An Open Letter from AI & Robotics Researchers [online]. *Future of Life Institute*, 2017. Dostupné z: https://goo.gl/X2N6CA
[28] ARMY-TECHNOLOGY.COM, ref. 21.
[29] RAYTHEON. *Phalanx Close-in Weapon System: Last Line of Defense for Air, Land and Sea* [online]. Dostupné z: https://goo.gl/Ky3RD1

Implikace pro ozbrojené síly České republiky

Rozvoj dálkově ovládaných prostředků a autonomních systémů bude v prvé řadě ovlivňovat oblast *Prepare/training; a Protect* nejen ve smyslu jejich používání, ale i schopnosti reagovat na jejich nasazení ze strany protivníka (bez ohledu na jeho povahu). Rozvoj těchto prostředků ovšem nesmí jednoznačně opomenout i nově objevující se kategorie mikro- a nano- UAS (viz dále kap. Aditivní výroba). Zajímavou perspektivu v této oblasti *(counter-UAS)* skýtá užití kombinace radaru a směrového rušiče, či výkonného laseru, jež však nejsou momentálně v rámci AČR rozšířeny. Obdobně je nezbytné zajistit implementaci systémových opatření, která směřují proti zneužití našich UAS ze strany protivníka (ať se již jedná o získávání zpravodajských informací, nebo převzetí kontroly nad zasaženým systémem). Z tohoto pohledu nelze opomenout jak technologickou dimenzi ochrany a obrany, tak jejich celkové procedurální a legislativní nastavení. V návaznosti na charakter OS ČR je v oblastech *Project; Engage; Sustain;* a *Inform* nezbytné zdůraznit potenciál „hejn/rojů" dálkově ovládaných prostředků a společného působení pilotovaných/řízených systémů a dálkově ovládaných či autonomních systémů. Obě oblasti umožňují kompenzovat velikost OS (případně i nepříznivý demografický vývoj a nedostatek potřebného personálu) a obsáhnout široké spektrum úkolů (od průzkumu až po přímý střet s protivníkem). Obdobně využití autonomních systému (prvků UI / strojového učení) vytváří příležitosti pro rozvoj schopností nejen ve „fyzických" doménách, ale taktéž i v již diskutovaném kyberprostoru. Samotné efektivní využívání „hejn/rojů" UAS a UGS je závislé na nutnosti disponovat senzory, komunikační systémy a systémy zpracující obrovské množství dat o okolí působení těchto prostředků (viz problematika kyberprostoru). Současně je nezbytné zodpovědět i výše naznačené právní a etické otázky spojené s využíváním zejména autonomních systémů, a to v ideálním případě ještě před jejich potenciální akvizicí.

ROZVOJ PROPOJENÍ ČLOVĚK-STROJ

Kromě výše uvedeného trendu „robotizace bojiště" dochází k rozvoji projektů, které umožňují dosáhnout efektivnějšího propojení člověka se strojovou složkou. Tímto by obecně mělo být umožněno navýšení výkonnosti lidského potenciálu, a to ať ve vztahu k ovládání jiných systémů, nebo samostatných fyzických i mentálních schopností člověka, snížení jeho zranitelností a také eliminaci následků úrazů či nemocí.

V prvním případě lze identifikovat snahu o poskytnutí veškerých informací od senzorů lidskému operátorovi v reálném čase, odstranění prodlevy mezi reakcí člověka a ovládaného systému a současně zajistit provedení jednotlivých příkazů, jako by člověk sám byl dotčeným systémem. Právě touto cestou se ubírá vývoj a testování senzorových a ovládacích prvků amerického stíhacího letadla páté generace F-35, které by např. měly přímo do pilotovy helmy přenášet ucelený obraz z šesti infračervených kamer a poskytovat informace o celém okolním prostředí a pozici protivníka.[30]

Diskutovaná oblast je velmi úzce propojena s technologiemi umožňujícími vytvoření tzv. rozšířené, nebo přímo virtuální reality a pokud možno plného zapojení člověka do interakcí s ní. Opětovně je v tomto smyslu akcentován význam informačních technologií a kyberprostoru, které jsou využitelné nejen při výše popsaných (bojových) aktivitách,

[30] LOCKHEED MARTIN CORPORATION. *The F-35 Helmet: Unprecedented Situational Awareness* [online]. 2016. Dostupné z: https://goo.gl/MD6gDK

ale i při plánování bojových operací a výcviku a přípravě bojových jednotek. Rozvoj rozšířené a virtuální reality totiž umožňuje velmi věrně simulovat v našem případě bojové situace a prostředí, ve kterých budou jednotky operovat, a to včetně možného chování protivníka. Obdobné uplatnění lze identifikovat i pro „nebojové“ aktivity (např. oblast zdravotnictví nebo logistiky).

V rámci druhého tématu (navýšení výkonnosti schopností/aktivit člověka) nelze především opomenout projekty, které směřují k vytvoření robotických bojových obleků (tzv. exoskeletů). Přínos lze spatřovat nejen v navýšení síly, výdrže či rychlosti osoby (vojáka), která je tímto prostředkem vybavena, ale i další posun v ochraně např. před nepřátelskou palbou. Hydraulické systémy totiž mj. navyšují nosnost a výrazně zjednodušují manipulaci s „brněním“ (pokud použijeme analogii se středověkým válečnictvím), které by jinak člověk samotný nebyl schopen unést, pohybovat se v něm apod. Současné stádium vývoje lze demonstrovat na prvotních zkouškách exoskeletů společnosti Lockheed Martin nebo Raytheon, které mají nejen přebrat za bojovníka hmotnost nesené výzbroje a výstroje a umožnit případně nést větší zátěž (a manipulovat s ní), ale i navýšit rychlost pohybu a vzdálenosti, které je schopen zdolat.[31] V loňském roce taktéž Velitelství speciálních operací Spojených států uzavřelo smlouvu na dodávku robotických exoskeletů Guardian XO se společností Sarcos Robotics.[32] Oproti tomu funkční model „brnění“ prozatím představen nebyl, byť lze očekávat, že v průběhu nadcházejících let se tato situace změní.

Kromě projektů exoskeletů ovšem taktéž nelze opomenout technologie, které se přímo propojují s lidským organismem a stávají se tak jeho (nedílnou) součástí. V úvahu zejména přicházejí robotické náhrady končetin, které mají/mohly by umožnit až dokonale kompenzovat takovéto druhy (bojových) zranění nebo třeba i náhrady zraku či sluchu. Na druhou stranu ovšem nelze potenciál těchto technologií omezit pouze na tyto situace a lze velmi dobře předpokládat, že s pokrokem v oblasti kybernetiky, neurobiologie aj. bude stále „lukrativnější“ zvyšování schopností člověka prostřednictvím nejrůznějších svalových, senzorových aj. implantátů nebo možnost náhrady zdravého orgánu či končetiny s cílem dosáhnout výše popsaných výhod. Aktuálně ovšem nejsou v zásadě řešeny etické a ani právní aspekty spojené s ponecháním nebo odebráním těchto implantátů po ukončení jejich aktivní služby např. v ozbrojených silách.

Rozvoj propojení člověk-stroj je velmi úzce navázán na aspekty informačních technologií. V prvé řadě se jedná o zefektivnění ovládání jiných systémů – např. UAS – a rozvoj prvků rozšířené a virtuální reality. Druhým tématem je samotné navýšení lidského potenciálu skrze jeho samotné „posílení“. Kromě rozvoje exoskeletů se jedná i o možnost náhrad jednotlivých částí lidského těla, a to nejen v případě potřeby kompenzovat následky (devastujících) zranění.

[31] Např. HUSSEINI, T. US Army trials exoskeletons for military use [online]. *Army Technology*, 2019. Dostupné z: https://bit.ly/2XCXZ0n

[32] Sarcos wins USSOCOM contract to supply XO robotic exoskeleton [online]. *Navy Technology*, 2019. Dostupné z: https://bit.ly/2X4kcFM

Implikace pro ozbrojené síly České republiky

Trendy v **rozvoji propojení člověk-stroj** umožňují v oblasti *Prepare/training* prostřednictvím rozšířené a virtuální reality navýšit efektivitu výcvikových programů a vytvořit pro potřeby přípravy příslušníků OS ČR podmínky, které se např. velmi přibližují reálnému bojovému nasazení. Aktuálně lze vyzdvihnout kladné zkušenosti mj. z výcviku pilotů, leteckých návodčích či servisních prací na (letecké) technice, vč. možnosti odborného vedení nebo přímého převzetí prací výrobcem. Zejména ve výcvikovém využití je také možné uvažovat o propojení se systémy strojového učení, které by mohly umožnit lépe přizpůsobovat tréninkovou zátěž danému jedinci. Obdobné implikace vyplývají i pro oblast *C3* a *Inform* mj. prostřednictvím vytvoření komplexního obrazu o bojišti a jeho zprostředkování relevantním subjektům. Zefektivnění ovládání jiných systémů – např. UAS – a zlepšování vlastností člověka jak prostřednictvím exoskeletů, tak samotné náhrady lidských končetin a orgánů reprezentují významný potenciál pro oblasti *Project; Engage; Protect*, přičemž zejména první zmíněné téma (ovládání jiných systémů) dále podporuje rozvoj předchozího trendu.

BIOTECHNOLOGIE

Trendy v oblasti biotechnologií reprezentují snahu posilovat a rozvíjet kontrolu nad živými organismy a jejich biologickými procesy. Ve vztahu k lidské společnost je toto zejména vyjádřeno prostřednictvím zemědělství, lékařství a genetiky a jejich směřováním k utváření a posilování lidského jedince, jeho potomků a případně i lidské civilizace jako celku. Aplikace těchto trendů ve vojenství v zásadě působí jako stimulující prvek lidského faktoru ozbrojených sil a jeho významu ve vojenských operacích.

Podstata dotčené oblasti sice nepředstavuje v rámci historie lidské společnosti žádný nový trend (např. v odkazu na užití mikroorganismů ve formě biologických zbraní). Na druhou stranu právě rozvoj v oblastech genetiky nebo výše zmiňovaných nanotechnologií přináší nové možnosti pro realizaci uvedených ambicí. Tyto přesahy jsou mj. viditelné na projektech komplexní výživy vojáka, jejímž prostřednictvím dochází k limitování následků spánkové deprivace nebo stimulování růstu svalové hmoty.[33] Obdobně lze interpretovat i využití malých živočichů a mikroorganismů jako složek senzorové sítě.[34]

Pravděpodobně nejvíce diskutovaným tématem je problematika tzv. genetických manipulací. Ty umožňují přímo ovlivňovat vlastnosti a schopnosti živých organismů, nebo konkrétně lidského jedince (až do podoby určitého ideálu „superčlověka“). Podobně jako u robotických technologií (propojení člověk-stroj) zde jednoznačně vyvstává možnost kompenzování újmy způsobené např. „bojovým zraněním“. Kompenzace ovšem neprobíhá prostřednictvím protetické náhrady, ale např. prostřednictvím stimulací růstu nové končetiny. Obdobně nelze opomenout širokou problematiku tzv. biologických zbraní, coby jedné z kategorie zbraní hromadného ničení. Prostřednictvím této oblasti mohou mj. získat „potřebné“ atributy zaměřitelnosti nebo kontroly nad jejich účinky. Na druhou stranu právě tyto implikace odráží ve srovnání s ostatními diskutovanými oblastmi trendů

[33] Např. SCHARRE, Paul – FISH, Lauren. *Human Performance Enhancement* [online]. Centre for a New American Security, 2018. Dostupné z: https://1url.cz/gM4z8
[34] SOUTH, Todd. From Shellfish to Plankton [online]. *Navy Times,* 2018. Dostupné z: https://1url.cz/LM4zA

technologického vývoje pravděpodobně největší míru kontroverze a etických/morálních výzev pro celou lidskou společnost.

Biotechnologie reprezentují schopnost utvářet a ovlivňovat povahu a podstatu živých organismů vč. lidského jedince. Z pohledu vojenství jsou v zásadě spojeny s akcentací lidského faktoru ozbrojených sil. Obecně zahrnují široké spektrum aspektů sahajících od úpravy výživového režimu až po tzv. genetické manipulace. Současně právě tato oblast se vyznačuje pravděpodobně největší mírou kontroverze a výskytem morálních/etických výzev.

Implikace pro ozbrojené síly České republiky

Implikace **biotechnologií** pro OS ČR momentálně primárně vyplývají pro oblasti *Prepare/training; Engage; Sustain.* Zde lze identifikovat možná využití prostřednictvím zahrnutí výživových doplňků do nutričního a výživového zabezpečení personálu, a to ať již během výcviku/přípravy, tak i při nasazení ve vojenských operacích. Obdobně přichází v úvahu i permanentní evaluace a monitorování efektivity cvičebních procesů a jejich vlivu na rozvoj lidského organismu. Do oblasti *Protect* následně spadá problematika ochrany proti biologickým zbraním a postupně se objevující potřeba zohlednit možnost využití geneticky modifikovaných mikroorganismů ze strany protivníka (statní i nestátní aktér) nejen proti ozbrojeným silám, ale i civilnímu obyvatelstvu.

ROZVOJ ENERGETICKÝCH TECHNOLOGIÍ

Zásadním trendem se stává i rozvoj energetických technologií. Obecně se jedná o dva provázané směry: 1) získání stabilního a efektivního zdroje energie jako alternativy zejména pro fosilní paliva; 2) využití v dedikovaných zbraňových systémech.

První směr je přímo navázán na energetické nároky např. výše uvedených robotických exoskeletů, jejichž využití je momentálně tímto aspektem citelně limitováno (co do výkonu nebo doby provozu). Snaha o nalezení efektivní náhrady za fosilní paliva je v tomto smyslu motivována (kromě obecného přístupu státních a nestátních aktérů k problematice klimatických změn) potřebou disponovat mobilními či jednoduše přepravitelnými zdroji energie a decentralizací samotné produkce.[35] Současně je zde přítomna i logika snižování závislosti na externích aktérech, místních zdrojích a navyšování soběstačnosti.

Druhý směr lze rozdělit do tří hlavních kategorií zbraňových systémů. Rozdělení reflektuje podobu využití energetických technologií, a to jak pro dosažení letálního, tak neletálního účinku. Jedná se o zbraně využívající směrovanou energii *(Directed Energy Weapons, DEW),* zbraně využívající energetické pulzy (oblast elektromagnetického záření, EMP) a elektromagnetické zbraně. Obecně je rozvoj orientován na všechny tyto kategorie. U první a třetí je identifikován potenciál nahradit „tradiční" palné zbraně. Oproti tomu má druhá kategorie – EMP – specifičtější zaměření. Zejména je určena vůči elektronickým systémům protivníka a dosažení jejich vyřazení či zničení. Ústřední pozornost je věnována rozvoji nejaderných prostředků, které by byly nasaditelné bez potřeby eskalace konfliktu nebo disponováním jadernou zbraní. Postupně je ale taktéž rozvíjeno možné použití mikrovlnného záření proti personálu protivníka.

[35] Srov. FUTURE ASSESMENT DIVISION. *Notes from the Edge: Insights into Evolving Future*, s. 1–2. 2017.

U DEW a elektromagnetických zbraní dochází v současnosti zejména k rozvoji projektů zaměřených na využití těchto prostředků v rámci vzdušného a námořního boje, případně jako alternativy k prvkům protiraketové obrany. Příkladem je rozmísťování izraelského protiraketového systému Iron Beam[36] nebo obnovení pozemních testů elektromagnetického děla ze strany USA[37], byť umístění a testování na dedikovaném plavidle bylo prozatím oddáleno.[38] Na druhou stranu, námořnictvo ČLR se dle dostupných zdrojů[39] do této fáze již posunulo a v loňském roce uskutečnilo palebné námořní zkoušky. Tato orientace je dána faktickými limity souvisejícími se získáním efektivního zdroje energie a jeho využitím k plnění požadovaných úkolů (např. dočasné či trvalé oslepení senzorů, zničení plavidla nebo přilétající střely). Z tohoto důvodu je citelně omezena využitelnost v oblasti ručních palných zbraní, kde právě energetické nároky prozatím neumožňují oproti „tradičním" zbraním dosažení vyšší efektivity (např. z důvodu hmotnosti, mobility či destrukčního účinku).

Současně nelze opomenout využitelnost těchto technologií ve formě neletálních zbraní, tj. prostředků, které mají za úkol protivníka „pouze" dočasně paralyzovat či zneškodnit. Výhodou je obecná minimalizace ztrát na životech civilního obyvatelstva, což nabývá na relevanci zejména v případě bojů v zastavěných oblastech nebo i při plnění úkolů, které přímo s bojovou činností nesouvisejí (např. v případě zajišťování veřejného pořádku).[40]

Rozvoj energetických technologií se zaměřuje jak na hledání/získání alternativního zdroje energie, tak na jejich využití ve zbraňových systémech. U zbraňových systémů lze identifikovat tři základní kategorie - zbraně využívající přímo směrovanou energii, zbraně využívající energetické pulzy (zejména problematika elektromagnetického záření) a elektromagnetické zbraně. U DEW a elektromagnetických zbraní dochází v současnosti k rozvoji zejména projektů v rámci vzdušného a námořního boje, případně protiraketové obrany. Zásadním limitem je získání stabilního a efektivního zdroje energie, který by současně splňoval nároky na výkon či mobilitu.

Implikace pro ozbrojené síly České republiky

Z pohledu **energetických technologií** lze pro OS ČR v současnosti za relevantní považovat především rozvoj (nových) alternativních zdrojů energie. V oblastech *Project; Engage; Sustain; Protect* totiž přímo naplňují obecné snahy o zabezpečení soběstačnosti a nezávislosti ozbrojených sil nejen během jejich nasazení. Současně dochází i ke snižování tzv. stopy na bojišti, tj. zátěže např. pro logistiku OS a odvislého zefektivnění využití vynaložených (finančních aj.) zdrojů. V rámci oblasti *Protect* je taktéž nezbytné poukázat na hrozbu použití elektromagnetického pulzu ze strany protivníka. V tomto smyslu je potřebné zajistit odolnost jednotlivých systémů a podobně jako pro reakci na rozsáhlé kybernetické útoky připravit alternativy (zálohy) pro případ jejich vyřazení.

[36] RAFAEL. *Iron Beam* [online]. Dostupné z: https://goo.gl/NGYa6N
[37] TREVITHICK, J. Navy's Railgun Now Undergoing Tests In New Mexico, Could Deploy On Ship In Northwest [online]. *The Drive*, 2019. Dostupné z: https://bit.ly/3glXccS
[38] Srov. např. ECKSTEIN, M. Navy Making Room For Railguns In Next Warship, But No Extra Investments [online]. *USNI News*, 2018. Dostupné z: https://1url.cz/mM4z7
[39] VAVASSEUR, X. Chinese Navy Railgun: What We Know Thus Far [online]. *Naval News*, 2019. Dostupné z: https://bit.ly/2AZVEFc
[40] Podrobněji např. ARTICLE36. *Directed Energy Weapons* [online]. Discussion paper for the Convention on Certain Conventional Weapons, 2017. Dostupné z: https://goo.gl/fiV7AW

ADITIVNÍ VÝROBA

Aditivní výroba (zejména „3D tisk“) představuje velmi rychle rozvíjející se průmyslovou oblast. Například v USA přibližně dvě třetiny výrobců využívá 3D tisk v některé z fází vývoje a produkce.[41] Obdobně je tato technologie stále častěji využívána i pro „výstavbu“ budov/objektů[42], což z pohledu ozbrojených sil představuje potenciální ulehčení a zlevnění budování základen nebo stanovišť např. na vzdálených nebo obtížně přístupných místech.

Na druhou stranu, celospolečenské rozšíření a využívání této metody výroby se předpokládá až v následujících deseti letech. Již nyní ale lze jeho prostřednictvím velmi flexibilně a ve srovnání s tradičním způsobem výroby i poměrně jednoduše vytvořit např. náhradní díly zbraňových systémů a snížit nároky na skladovací a transportní kapacity. Byť uvedený příklad poukazuje na význam pro logistiku, tak samotná využitelnost zasahuje do mnohem širší oblasti projekce ozbrojené síly nebo výroby požadovaných (zbraňových) systémů.[43] Obdobně dochází k rychlému rozvoji této oblasti ve zdravotnictví. Aditivní výroba (3D tisk) zde představuje možnost pro vytváření (tisk) lidských orgánů pro transplantaci, náhrad kostí, tkání a dalších částí lidského těla.[44]

Nanotechnologie v tomto kontextu reprezentují kvalitativní posun v možnostech aditivní výroby. Jedná se o oblast, která zásadně ovlivňuje rozvoj nejen energetických technologií, ale i např. technologií robotických. Schopnost vytvářet a ovlivňovat strukturu jednotlivých materiálů a objektů na úrovni miliardtiny metru s sebou přináší nové možnosti jak pro odolnost a ochranu ozbrojených sil (např. i ve formě aktivního maskování), tak prostředků neutralizace protivníka.[45] Využití těchto aspektů je viditelné mj. na testování a akvizici tzv. mikro- a nano- bezpilotních systémů (např. nano-UAS Black Hornet 3 aj.)[46] ve všech typech bojové činnosti.

Aditivní výroba umožňuje velmi flexibilní produkci takřka libovolného objektu, což souvisí se značným potenciálem zefektivnění nejen oblasti logistiky, ale například i širšího pojetí projekce ozbrojených sil. Nanotechnologie v tomto smyslu představují kvalitativní posun, který je dán schopností vytvářet a ovlivňovat strukturu jednotlivých materiálů a objektů na úrovni miliardtiny metru. Význam pro ostatní oblasti mj. reprezentuje miniaturizace např. UAS a jejich postupná akvizice.

---

[41] NATO STO Sensors & Electronics Technology (SET) Panel. *Flexible Displays Technology Watch Card*. 2016.

[42] Např. LANSARD, Martin. *The 15 Best Construction 3D Printers In 2019* [online]. Aniwaa, 2019. Dostupné z: https://bit.ly/2Xyma01

[43] AKER, Berenice. Made to Measure: The Next Generation of Military 3D Printing [online]. *Army-Technology.com*, 2018. Dostupné z: https://goo.gl/jFKaRY

[44] HOOIJDONK, R. Exciting New Advances in 3D Printing Could Help Solve Cut Organ Transplant Waiting Lists [online]. *The Journal of mHealth*, 2019. Dostupné z: https://bit.ly/2zABJwj

[45] Podrobněji např. WONG, Wilson W. S. Emerging Military Technologies: A Guide to the Issues. Oxford: Praeger, 2013.

[46] KIRVE, Patrik. Small Drones Take Flight for Military Applications [online]. *RBR*, 2018. Dostupné z: https://bit.ly/2yHOZ1S

Implikace pro ozbrojené síly České republiky

Rozvoj **aditivní výroby** podobně jako předchozí trendy v oblasti alternativních zdrojů energie reflektuje snahy o zabezpečení soběstačnosti a nezávislosti ozbrojených sil nejen během jejich nasazení. AČR může profitovat ze snížení nároků kladených na logistiku nebo projekci sil prostřednictvím využívání „3D tisku" (oblasti schopností *Project; Sustain*). Právě možnosti výstavby budov/objektů nebo výroba náhradních dílů představují bezprostřední podnět pro rozvoj relevantních schopností. Současně rozvoj „biotisku" představuje pro vojenskou medicínu unikátní prostředek, jak zajistit vyléčení mj. i amputačních či ztrátových poranění. Z dlouhodobějšího hlediska je následně patrný význam miniaturizace prostřednictvím nanotechnologií, které z popsaných trendů ovlivňují zejména další rozvoj dálkově ovládaných/autonomních systémů, propojení člověk-stroj a energetických technologií (navazující oblasti *Engage; Protect*).

HYPERSONICKÉ TECHNOLOGIE

Hypersonické technologie reprezentují další z oblastí strategického soupeření mezi hlavními velmocemi.[47] Tyto zbraňové systémy operují při rychlostech vyšších než Mach 5 (6125 km/h), což je spolu s vysokou manévrovatelností činí téměř nezastavitelnými současnými prostředky protiraketové obrany. Hypersonická fáze letu obecně nastává během návratu z vesmíru nebo jeho těsné blízkosti do atmosféry nebo během atmosférického letu poháněného raketovým nebo náporovým *(scramjet)* pohonem. Příkladem těchto technologií jsou hypersonické kluzáky *(hypersonic glide vehicles, HGV)* nebo hypersonické řízené střely *(hypersonic cruise missile, HCM)*. V návaznosti na vyvinuté rychlosti se tyto systémy mohou spoléhat především na kinetické destrukční účinky. Na druhou stranu, mohou být taktéž využívány jako nosiče konvenčních či jaderných hlavic. Pro tyto potřeby má být mj. určena ruská střela Ch-47M2 Kinžal, která byla i v průběhu loňského roku testována v arktických oblastech.[48] Obdobná pozornost je věnována protilodním střelám, které jsou v čínském strategickém myšlení považovány za ideální prostředek pro zajištění schopnosti A2/AD vůči americkému námořnictvu (svazům letadlových lodí) minimálně pro oblasti Jihočínského, Východočínského a Žlutého moře. V roce 2019 ČLOA veřejně představila nový typ hypersonických střel s plochou dráhou letu – DF-100.[49]

Implikace pro ozbrojené síly České republiky

Z pohledu úrovně rozvoje **hypersonických technologií** a zejména ekonomických nákladů nepředstavují tyto zbraňové systémy bezprostřední možnosti pro navyšování schopností AČR. Na druhou stranu, v návaznosti na členství České republiky v NATO nelze opomenout předpoklad, že tyto systémy představují jasnou výzvu pro efektivní zajištění obrany proti nim, tj. protiraketové ochrany (oblast schopností *Protect*). I AČR by tak měla postupně zohledňovat narůstající schopnosti na straně možných protivníků, a to jak na praktické, tak koncepční úrovní.

[47] WILSON, J. R. The emerging world of hypersonic weapons technology [online]. *Military & Aerospace Electronics*, 2019. Dostupné z: https://bit.ly/36Ao9VE
[48] NILSEN, T. Russia's top General indirectly confirms Arctic deployment of the unstoppable Kinzhal missile [online]. *The Barents Observer*, 2019. Dostupné z: https://bit.ly/2ZJg6Ez
[49] DF-100 [online]. *Military-Today.com*, 2020. Dostupné z: https://bit.ly/3gsk3U6

OBECNÉ IMPLIKACE PRO OZBROJENÉ SÍLY ČESKÉ REPUBLIKY

Tempo rozvoje jednotlivých výše uvedených i dalších technologických oblastí lze předvídat jen velmi obtížně. Na druhou stranu minimálně již známé projekty disponují poměrně značnými vojenskými implikacemi, které by ani ozbrojené síly České republiky neměly přehlížet. Jednoznačně kladně lze hodnotit aktivity/iniciativy, které tyto aspekty reflektují (ať již se jedná zahájení výstavby 533. praporu bezpilotních systémů AČR nebo pokračující budování schopností Velitelství kybernetických sil a informačních operací AČR). Obdobný přínos mohou poskytnout i projekty mezinárodní spolupráce, byť je vždy nezbytné posuzovat jejich výstupy v kontextu posilování schopností AČR.

Samozřejmě nelze předpokládat, že by se bylo možné zaměřit na komplexní sadu schopností, tak jak jsme toho svědky u hlavních světových mocností - zejména USA. Přesto je nezbytné, aby nedocházelo k opomíjení ani těch oblastí, které mohou na první pohled vypadat jako irelevantní a vzdálené cílům a možnostem zejména Armády České republiky coby nástroje k naplňování národních zájmů.

Souhrnně nelze opomenout potřebu zajistit vzájemnou kompatibilitu a výslednou interoperabilitu zaváděných systémů (nejen v rámci kyberprostoru) nejen se spojenci zejména v rámci NATO/EU, ale taktéž napříč jejich jednotlivými generacemi. Výhody, které jsou spojeny se schopností flexibilně centralizovat a decentralizovat strukturu velení a řízení a vytvořit vzájemné propojení mezi jednotlivými složkami ozbrojených sil, lze v tomto smyslu získat pouze při naplnění výše uvedeného požadavku. Současně vzájemná kompatibilita posiluje i odolnost celé struktury (robustnost a redundance – zastupitelnost) a navyšuje efektivitu jednotlivých prvků.

Stíráním hranice mezi vojenskou a civilní dimenzí lze předpokládat, že i AČR bude jak v zahraničí, tak případně ve vnitrostátním prostředí konfrontována s použitím např. bezpilotního letounu ze strany nestátního aktéra. Z tohoto hlediska je jednoznačně žádoucí alokace prostředků na projekty, které se zaměřují na komplexní obranu proti takovým systémům a případně zhodnocení, zda např. současný výcvik zohledňuje i takovou eventualitu.

Obdobně lze předpokládat, že tento vývoj bude ovlivňovat povahu dodavatelů, a to nejen domácích, ale i zahraničních. Samozřejmě tak ale dochází k vytváření určité závislosti na těchto subjektech, což se může projevit negativními jevy, jako je hrozba špionáže nebo nedostupnosti služeb v případě vzniku rozporu mezi zájmy ozbrojených sil, respektive ČR obecně, a těmito subjekty.

Současně nelze opomenout, že rozvoj jednotlivých technologických trendů a oblastí s sebou přináší i nové výzvy pro režimy kontroly zbrojení, respektive proliferace jednotlivých systémů, a to ať již na vnitrostátní, tak i na mezinárodní úrovni. Zvýšená pozornost by měla být věnována zejména problematice dostatečnosti současných (právních) norem, způsobům jejich naplnění a jejich případnému doplnění.

Název: Technologický vývoj: Implikace pro schopnosti ozbrojených sil ČR 2019
Autoři:
Mgr. et Mgr. Jakub Fučík, Ph.D.
Ing. Fabian Baxa, Ph.D.
PhDr. Libor Frank, Ph.D.
doc. Ing. Josef Procházka, Ph.D.
Grafická a ediční úprava: Mgr. Martin Doleček
Vydavatel: Univerzita obrany v Brně
Rok vydání: 2020
Vydání: první