CENTRE FOR SECURITY AND MILITARY STRATEGIC STUDIES
UNIVERSITY OF DEFENCE

TECHNOLOGICKÝ VÝVOJ

IMPLIKACE PRO SCHOPNOSTI OZBROJENÝCH SIL ČR 2018

JAKUB FUČÍK, FABIAN BAXA, LIBOR FRANK, JOSEF PROCHÁZKA

TECHNOLOGICKÝ VÝVOJ

IMPLIKACE PRO SCHOPNOSTI OZBROJENÝCH SIL ČR 2018

JAKUB FUČÍK A KOL.

BRNO 2019

AUTORSKÝ KOLEKTIV

Mgr. et Mgr. Jakub Fučík, Ph.D.

Ing. Fabian Baxa, Ph.D.

PhDr. Libor Frank, Ph.D.

Ing. Josef Procházka, Ph.D.

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

Studie *Technologický vývoj: Implikace pro schopnosti ozbrojených sil ČR 2018* prošla recenzním řízením ediční komise CBVSS. Recenzi v rámci recenzního řízení vypracoval pplk. gšt. Ing. Jan Farlík, Ph.D., plk. gšt. Ing. Miroslav Feix, M.S. a plk. gšt. doc. Ing. Petr Františ, Ph.D.

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).

ISBN 978-80-7582-095-2

ÚVOD

Cílem analytické studie je zhodnocení trendů technologického vývoje a jejich implikací pro ozbrojené síly České republiky. 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.[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 budou identifikovány oblasti schopností, které jsou jeho rozvojem přímo ovlivněny a mají bezprostřední význam pro dotčený subjekt (shrnutí viz závěrečná tabulka). 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 dotčených trendů. Totožný komplexní přístup je relevantní i k užitému analytickému rámci MCA a konkrétním identifikovaným schopnostem. Časově je orientována na trendy, které mohou bezprostředně ovlivňovat ozbrojené síly, se zohledněním zejména událostí za rok 2018. Verifikace výstupů byla provedena v rámci expertních jednání za účasti příslušníků MO ČR, AČR a představitelů bezpečnostní komunity.

[1] Viz FUČÍK a kol. *Technologický vývoj 2018: Implikace pro schopnosti ozbrojených sil ČR* [online]. Brno, CBVSS UO, 2018. Dostupné z: https://www.unob.cz/cbvss/Documents/publikace/TV_2018.pdf
[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 války (ozbrojeného konfliktu) – pozemní, námořní a vzdušné, pokračuje navyšování významu vesmírného prostoru a kyberprostoru, bez ohledu zda jednotlivé státy / mezinárodní organizace považují tyto domény za samostatné nebo jako součást ostatních dimenzí (např. vesmírný prostor jako součást vzdušného prostoru v rámci NATO nebo kyberprostor jako součást informační domény v rámci ruského přístupu).

VESMÍRNÝ PROSTOR

S ohledem na současnou obecnou úroveň technologického rozvoje lidstva, která neumožňuje nejen krátkodobé a ekonomické překonávání obrovských vzdáleností mezi planetami, ale též provozování permanentního osídlení např. za účelem těžby nerostných surovin, nelze v blízké budoucnosti předpokládat konflikty srovnatelné (použijeme-li určitou míru analogie) s bojem o nadvládu nad námořními trasami, popř. zámořskými koloniemi.

Na druhou stranu, již od počátků americko-sovětského soupeření si jednotlivé státy „uvědomují“ jinou implikaci charakteru vesmírného prostoru. 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. Disponování relevantními kapacitami ve vesmírném prostoru tedy sehrává poměrně zásadní roli ve schopnosti jednotlivých aktérů projektovat svoji moc, respektive vojenskou sílu, v globálním měřítku. Na tuto problematiku upozorňuje mj. nová Národní vesmírná strategie (National Security Space Strategy) USA z března 2018, která nahradila Národní vesmírnou bezpečnostní strategii (National Security Space Strategy) z roku 2011. Spojené státy pro zabezpečení národních zájmů dále připravují vytvoření samostatné složky ozbrojených sil (United States Space Force). Aktuálně byl jejich vznik autorizován nařízením prezidenta Donalda J. Trumpa.[3] Podobné směřování je patrné i u Čínské lidové republiky a Ruské federace coby hlavních „vyzyvatelů“ právě Spojených států amerických.

Taktéž nelze opomenout ani roli a narůstající význam nestátních aktérů (např. soukromých obchodních společností typu SpaceX), kteří fakticky privatizují vesmírný výzkum a vývoj a rozvíjejí schopnosti (např. v oblasti vesmírných nosičů – viz první let nosiče Falcon Heavy v únoru 2018)[4], které původně byly vyhrazeny státům, respektive státním organizacím. Na jednu stranu tento jev 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

[3] Text of Space Policy Directive-4: Establishment of the United State Space Force [online]. 2019. Dostupné z: https://1url.cz/zM4Ki

[4] MALIK, Tariq. *Success! Space Flight Launches Falcon Heavy Rocket on Historic Maiden Voyage* [online]. Space.com, 2018. Dostupné z: https://1url.cz/7M4Ko

k omezování státní kontroly nad systémy, které budou takto na oběžné dráze umístěny. Tato situace dále „znepřehledňuje“ níže popsaný problém „dual-use“ technologií.

V obecné rovině lze potenciál, který představuje vesmírný prostor a relevantní technologie, rozdělit do dvou skupin - civilní a vojenské -, přičemž dělícím kritériem je povaha (určení) aktivit, respektive reálných umělých těles (družice, stanice apod.) 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 bojových jednotek nebo zbraňové platformy určené k intercepci balistických střel apod. V souladu s uvedenou definicí dále nelze opomenout tzv. anti-satelitní zbraně (anti-satellite weapons, ASAT), které sice mohou být umístěny na zemském povrchu (příklad systémů USA, Ruska, Číny), ale jejich užití je přímo situováno do vesmírného prostoru.

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 přetrvávajícím fenoménem tzv. „dual-use“ (dvojího užití/určení) příslušných technologií, popř. aktivit. Satelitní navigační síť může být kupříkladu využita nejen pro určení pozice civilních subjektů, ale též koordinace postupu bojových uskupení nebo navádění řízených střel či bezpilotních letounů (odkaz na americký systém GPS nebo rozdílné druhy služeb, které budou poskytovány prostřednictvím budovaného systému Galileo). Právě navigační systém Galileo byl v roce 2018 „posílen“ o čtyři nové satelity s předpokládaným dosažením *plných operačních schopností* v roce 2020, kdy by měl být systém doplněn o poslední čtyři družice do celkového počtu 30.[5] Obdobně lze hodnotit i využitelnost budovaných satelitních sítí pro globální komunikaci a pokrytí 5G internetem (aktuálně např. OneWeb nebo LeoSat).

Vesmírný prostor nabývá na významu pro schopnost projektovat (vojenskou) moc státu a sehrává svoji roli v oblasti zajišťování národní bezpečnosti. Jeho využívání je velmi úzce provázáno s fenoménem tzv. dvojího užití, kdy dochází ke stírání hranic mezi civilním a vojenským sektorem. Současně narůstá role nestátních aktérů, kteří rozvíjejí schopnosti původně vyhrazené státům.

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. 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

[5] GALILEO GNSS. Four new Galileos join Europe’s largest constellation [online]. 2019. Dostupné z: https://galileognss.eu/four-new-galileos-join-europes-largest-constellation/#more-3542

na projekty posilující oblasti *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[6] formou mezinárodní spolupráce se Satelitním střediskem Evropské Unie (EU SatCen) nebo nákupy od soukromých poskytovatelů.

KYBERPROSTOR

Posilování strategického významu kyberprostoru je přímo navázáno na rozvoj informačních technologií a jejich využívání v současné době fakticky ve všech oblastech lidského života. Vzájemné propojení takřka veškerého zemského povrchu skrze informační sítě 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 ovlivňující fungování reálného prostředí. Z pohledu státních a nestátních aktérů je zajištění stabilního přístupu k této doméně fakticky prvotním předpokladem pro efektivní naplňování vlastních zájmů. V tomto smyslu tzv. kybernetické útoky, respektive škodlivé kybernetické aktivity (malicious cyber aktivity) - např. ve formě schopnosti odepření přístupu protivníkovi do této domény - reprezentují významné nástroje pro dosažení stanovených cílů,[7] které se obecně vyznačují velmi výhodným poměrem v hodnocení nákladů vs. zisků z diskutovaných aktivit.

Důležitým prvkem je rozvoj tzv. internetu věcí (Internet of Things, IoT), 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 fungováním tohoto prostoru. 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 (např. z roku 2016 Mirai botnet,[8] v roce 2017 Reaper botnet[9], které posloužily/slouží jako funkční rámec nově vytvářených botnetů).

Současně se zintenzivněním propojení lidstva v rámci tohoto prostoru dochází k nárůstu počtu sítí, které jsou vytvářeny a užívány 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

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

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

[8] ANTONAKIS, Manos et al. *Understanding the Mirai Botnet* [online]. 2017. Dostupné z: https://goo.gl/XkBp4T

[9] GOODIN, Dan. *Assesing the Threat the Reaper Botnet Poses to The Internet – What We Know Now* [online]. ArsTechnica, 2017. Dostupné z: https://goo.gl/M1HjLz

zavádění i v dalších oblastech (např. bankovnictví[10] nebo správa a sdílení dat[11]). Výslednou podobou tohoto trendu je nárůst významu tzv. „deep webu", respektive v užším pojetí s bezpečnostními konotacemi „dark webu" a „darknetu".[12] Zejména dark web/darknet je totiž přímo spojen s kriminálními 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 sebou přináší i nové formy zranitelnosti (např. problematika ovlivňování/manipulace s volebními systémy). Internet z tohoto pohledu umožňuje navýšení transparentnosti takřka všech činností v reálném prostředí. Zejména sociální média typu Facebook, Twitter, YouTube apod. 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 lze tedy chápat jako významný předpoklad pro schopnost kontrolovat a ovlivňovat veřejné mínění obecně.

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. Právě v roce 2018 pokračovalo zdokonalování jednotlivých komponentů a v lednu 2019 byl i představen první „komerční" kvantových počítač (IBM Q System One).[13]

Informační technologie jsou již v současnosti provázány se všemi oblastmi lidského života (mj. i u vazeb občan – stát). Na významu nabývá tzv. internet věcí, s čímž je spojeno i jejich zneužívání k provádění např. velkých DDoS útoků proti státním i nestátním subjektům. Současně dochází k dalšímu oslabování státní moci prostřednictvím ilegálních aktivit v rámci darwebu/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.

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

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

[12] 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

[13] 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

Implikace pro ozbrojené síly České republiky

Z pohledu nejnovější operační dimenze klade **kyberprostor** taktéž zvýšené nároky na výcvik a přípravu, a to jak pro maximalizaci jeho přínosu, tak alespoň snížení negativních dopadů závislosti na odpovídajících technologiích. Jejich význam lze pro OS ČR dále identifikovat v oblastech Project; Engage; C3; Protect; 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. Právě 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. 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 následkům/účinkům EMP či jiným způsobům narušování provozu informačních a komunikačních systémů. Současně, především v kontextu Protect by zvýšený důraz měl být kladen právě na zajišťování kybernetické obrany a bezpečnosti. Toto doručení je ovšem nezbytné vztáhnout nejen vůči dnes již tradičním platformám, ale právě i na oblast Internetu věcí 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 využívány 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 útočnými bezpilotními prostředky. Lze předpokládat, že tento obecný trend, tj. navyšování počtu států, které disponují jednotlivými kategoriemi bezpilotních prostředků, bude jen nabývat na intenzitě.

Obdobně lze zejména u hlavních velmocí mezinárodního systému identifikovat jak citelné navyšování počtu jednotlivých druhů bezpilotních prostředků, tak rozšiřování okruhu úkolů, 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.[14]

[14] 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

V současnosti je jich již minimálně jedenáct.[15] Od funkčních období Obamových administrativ lze identifikovat přetrvávající trend jejich intenzivního využívání pro údery vůči příslušníkům teroristických organizací (tzv. cílené zabíjení - targeted killings),[16] kdy jsou proti pilotovaným letadlům upřednostňovány nižší akviziční i provozní náklady a absence přímého ohrožení lidské „posádky" (operátorů). Obdobně Ruská federace velmi intenzivně rozvíjí projekty bojových bezpilotních letounů, které se momentálně nacházejí ve fázi testování jednotlivých prototypů (např. Altius-M, který by měl v roce 2019 dosáhnout počátečních operačních schopností).[17]

Bezposádkové 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 způsobujícími jak na letální, tak neletální účinek.[18] 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.[19]

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. 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.[20] 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.

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

[15] SICARD, Sarah. 11 Military Drone Names, Ranked [online]. *Task & Purpose*, 2017. Dostupné z: https://goo.gl/Z3ExN7
[16] PURKISS, Jessica. - SERLE, Jack. Obama's covert drone war in numbers: ten times more strikes than Bush [online]. *The Bureau of Investigative Journalism*, 2017. Dostupné z: https://goo.gl/cfsqnU
[17] DEAGEL.COM. *Altius-M*. 2018. Dostupné z: https://bit.ly/2EkavJr
[18] ARMY-TECHNOLOGY.COM. *AvantGuard Unmanned Groud Combat Vehicle, Israel* [online]. 2016. Dostupné z: https://goo.gl/knZqWb
[19] 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
[20] Např. srov. TATE, Andrew. China Launches Record-breaking UAV Swarm [online]. *Jane´s 360*, 2017. Dostupné z: https://goo.gl/WCHry6

ozbrojených sil.[21] Systémy založené na prvcích AI / 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).[22] Na druhou stranu je nezbytné kriticky podotknout, že v návaznosti na historické příklady (např. kazetová munice, protipěchotní miny apod.), bude takový proces minimálně problematický.

Určité prvky těchto technologií můžeme identifikovat již v současnosti, kdy jsou např. právě vozidla Guardium schopny operovat i v plně automatizovaném (autonomním) módu.[23] 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).[24]

V systémech založených na prvcích AI / 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. Velká pozornost je věnována schopnosti simultánně nasadit a ovládat velké množství zejména UAS. Rozvoj autonomních systémů je přímo podmíněn úrovní rozvoje prvků AI 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.

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

[21] 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
[22] Např. Autonomous Weapons: An Open Letter from AI & Robotics Researchers [online]. *Future of Life Institute*, 2017. Dostupné z: https://goo.gl/X2N6CA
[23] ARMY-TECHNOLOGY.COM, ref. 18.
[24] RAYTHEON. *Phalanx Close-in Weapon System: Last Line of Defense for Air, Land and Sea* [online]. Dostupné z: https://goo.gl/Ky3RD1

kategorie mikro- a nano- UAS (viz dále kap. Aditivní výroba). Zajímavou perspektivu v této oblasti (counter-UAS) skýtá užití kombinace radaru a směrového rušiče, jež však nejsou momentálně v rámci AČR dostatečně 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 nezbytné zdůraznit v oblastech *Project; Engage; Sustain; a Inform* potenciál „rojů" bezpilotních prostředků, které by umožnily 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). Na druhou stranu je jednoznačně 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 schopností/aktivit člověka.

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 jakoby 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.[25]

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, 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 na středověké

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

válečnictví), 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/manipulovat i s větší zátěží, ale i navýšit rychlost pohybu a vzdálenosti, které je schopen zdolat.[26] 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 přichází 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" navyšování 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.

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 pracích na (letecké) technice, vč. možnosti odborného vedení, či 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.

[26] Např. ARMY-TECHNOLOGY.COM. *Raytheon XOS 2 Exoskeleton, Second-Generation Robotics Suit, United States of America* [online]. 2016. Dostupné z: https://goo.gl/p9VcB2; MARINOV, Bobby. *19 Military Exoskeletons into 5 Categories* [online]. 2016. Dostupné z: https://goo.gl/6wW1q9

BIOTECHNOLOGIE

Trendy v oblasti biotechnologií reprezentují snahu posilovat a rozvíjet kontrolu nad živými organismy a jejich biologickými procesy - v aplikaci na lidskou společnost ať již prostřednictvím zemědělství, lékařství anebo genetiky tedy utvářet a posilovat lidské jedince, jejich potomky a případně i lidskou civilizaci jako celek. Aplikace těchto trendů ve vojenství v zásadě působí jako stimulující prvek lidského faktoru ozbrojených sil a jeho významu ve vojenských operacích.

Samozřejmě podstata dotčené oblasti nepředstavuje v rámci historie lidské společnosti žádný nový aspekt (např. v odkazu na weaponizaci živých organismů a jejich využití vůči protivníkovi). Na druhou stranu právě např. rozvoj v oblastech genetiky nebo výše zmiňovaných nanotechnologií přináší nové možnosti pro realizaci uvedených předpokladů. Tyto přesahy jsou mj. viditelné na projektech komplexní výživy vojáka a jejím prostřednictvím např. limitování následků spánkové deprivace nebo stimulování růstu svalové hmoty[27] nebo využití malých živočichů a mikroorganismů jako složky senzorové sítě[28].

Pravděpodobně nejvíce diskutována je v tomto problematika tzv. genetických manipulací a možnosti jejich prostřednictvím ovlivňovat vlastnosti a schopnosti živých organismů, nebo konkrétně lidského jedince (až v podobě určitého ideálu „super-člověka"). Podobně jako u robotických technologií (propojení člověk-stroj) zde jednoznačně vyvstává možnost kompenzování újmy způsobené např. „bojovým zraněním", ovšem ne prostřednictvím protetické náhrady, ale třeba i stimulací růstu nové končetiny apod. Obdobně nelze opomenout širokou problematiku tzv. biologických zbraní, co by jedné z kategorie zbraní hromadného ničení, které 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 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 inkorporace např. výživových doplňků do nutričního a výživového zabezpečení personálu, a to ať již během výcviku/přípravy, nebo 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

[27] Např. SCHARRE, Paul – FISH, Lauren. *Human Performance Enhancement* [online]. Centre for a New American Security, 2018. Dostupné z: https://1url.cz/gM4z8

[28] SOUTH, Todd. From Shellfish to Plankton [online]. *Navytimes,* 2018. Dostupné z: https://1url.cz/LM4zA

problematika ochrany proti biologickým zbraním a postupně se objevující potřeba zohlednit právě i možnost využití modifikovaných mikroorganismů ze strany protivníka (statní i nestátní aktér) nejen proti ozbrojeným silám, ale i civilnímu obyvatelstvu.

ROZVOJ ENERGETICKÝCH TECHNOLOGIÍ

Zásadním trendem se postupně stává i rozvoj energetických technologií, které by umožnily nejen získání stabilního a efektivního zdroje energie jako alternativy zejména pro fosilní paliva, ale též samotnou weaponizaci a využití v dedikovaných zbraňových systémech. První kategorie je přímo navázána na nároky např. výše uvedených robotických exoskeletů, jejichž využití je momentálně tímto aspektem citelně limitováno (co do výkonu nebo doby provozu). Právě 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.[29] Mj. je zde přítomna i logika snižování závislosti na externích aktérech a navyšování soběstačnosti.

Weaponizaci energetických technologií lze rozdělit do tří hlavních kategorií v návaznosti na podobu jejich využití, a to jak s letálním, tak neletálním účinkem. Jedná se o zbraně využívající směrovanou energii (Directed Energy Weapons, DEW), zbraně využívající energetické pulzy (oblast elektromagnetického záření) a elektromagnetické zbraně. Obecně je rozvoj orientován na všechny tyto kategorie, přičemž u první a třetí je identifikován potenciál nahradit „tradiční" palné zbraně. Druhá kategorie – EMP – oproti tomu směřuje vůči elektronickým systémům protivníka a dosažení jejich vyřazení/zničení. Ústřední pozornost je věnována rozvoji nejaderných prostředků, které by byly nasaditelné bez potřeby eskalace konfliktu nebo právě disponováním jadernou zbraní.

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[30] nebo završení pozemních testů elektromagnetického děla ze strany USA, byť umístění a testování na dedikovaném plavidle bylo prozatím oddáleno.[31] Na druhou stranu, námořnictvo ČLR se dle dostupných zdrojů[32] do této fáze již posunulo. Tato orientace je dána faktickými limity souvisejícími se získáním efektivního zdroje energie a jeho využitím k plnění požadovaných úkolů (zničení plavidla, přilétající střely apod.). Z tohoto důvodu je citelně omezena využitelnosti v oblasti ručních palných

[29] Srov. FUTURE ASSESMENT DIVISION. *Notes from the Edge: Insights into Evolving Future*, s. 1–2. 2017.
[30] RAFAEL. *Iron Beam* [online]. Dostupné z: https://goo.gl/NGYa6N
[31] Srov. např. ECKSTEIN, Megan. Navy Making Room For Railguns In Next Warship, But No Extra Investments [online]. *USNI News*, 2018. Dostupné z: https://1url.cz/mM4z7
[32] Srov. např. AXE, David. China's Navy Railgun Is Out for Sea Trials. Here's Why It's a Threat to the U.S. Navy [online]. *National Interest*, 2019. Dostupné z: https://1url.cz/zM4KM; KELLER, Jared. China Just Blew The US Navy's Electromagnetic Railgun Out Of The Water [online]. *Task & Purpose*, 2018. Dostupné z: https://taskandpurpose.com/china-electromagnetic-railgun-deployment

zbraní, kde právě energetické nároky neumožňují oproti „tradičním“ zbraním dosažení vyšší efektivity (např. z důvodu hmotnosti, mobility či destrukčního účinku).

Současně ale 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 nesouvisí (např. v případě zajišťování veřejného pořádku).[33]

Rozvoj energetických technologií se zaměřuje jak na hledání/získání alternativního zdroje energie, tak na jejich weaponizaci a využití ve zbraňových systémech. U weaponizace lze identifikovat tři základní oblasti - 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 právě získaní 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. na logistiku OS, což dále umožní zefektivnit vynakládané (finanční aj.) zdroje. V rámci oblasti *Protect* je ovšem taktéž nezbytné poukázat na hrozbu využití elektromagnetického pulzu ze strany protivníka. V tomto smyslu je potřebné zajistit odolnost jednotlivých systémů a podobně jako pro reakci na rozsáhlé kybernetické útoky připravit jejich alternativy (zálohy) pro případ jejich vyřazení.

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.[34] Obdobně je tato technologie stále častěji využívána i pro „výstavbu“ budov/objektů[35], 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

[33] Podrobněji např. ARTICLE36. *Directed Energy Weapons* [online]. Discussion paper for the Convention on Certain Conventional Weapons, 2017. Dostupné z: https://goo.gl/fiV7AW
[34] NATO STO Sensors & Electronics Technology (SET) Panel. *Flexible Displays Technology Watch Card*. 2016.
[35] Např. LANSARD, Martin. *The 15 Best Construction 3D Printers In 2019* [online]. Aniwaa, 2019. Dostupné z: https://www.aniwaa.com/house-3d-printer-construction/

příklad poukazuje na význam pro logistiku, tak samotná využitelnost do mnohem širší oblasti projekce ozbrojené síly nebo výroby požadovaných (zbraňových) systémů.[36]

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.[37] Využití těchto aspektů je viditelné mj. na testování a akvizici tzv. mikro- a nano- bezpilotních systémů (např. nano-UAS Black Hornet 3 aj.)[38] 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.*

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. Z dlouhodobějšího hlediska je následně patrný význam miniaturizace prostřednictvím nanotechnologií, které z popsaných ovlivňují zejména další rozvoj trendů dálkově ovládaných/autonomních systémů; propojení člověk-stroj; a energetické technologie (navazující oblasti *Engage; Protect*).

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

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

[38] KIRVE, Patrik. Small Drones Take Flight for Military Applications [online]. *RBR*, 2018. Dostupné z: https://www.roboticsbusinessreview.com/unmanned/small-drones-military-surveillance/

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 o zapojení do projektů mezinárodní spolupráce, nebo zahájení výstavby Velitelství kybernetických sil a informačních operací 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, co by nástroje k naplňování národních zájmů.

Souhrnně nelze opomenout potřebu zajistit vzájemnou kompatibilitu 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, redundance) a navyšuje efektivitu jednotlivých prvků.

Stíráním hranice mezi vojenskou a civilní dimenzí lze předpokládat, že i AČR (zejména z titulu zahraničních operací) bude konfrontována s použitím např. bezpilotního letounu i ze strany nestátního aktéra. Z tohoto titulu 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 např. 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 nedostupností 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 sebou přináší i nové výzvy pro režimy kontroly zbrojení, respektive proliferace, jednotlivých systémů, a to ať již na vnitrostátní, tak mezinárodní úrovni. Zvýšená pozornost by měla být věnována zejména problematice dostatečnosti současný (právních) norem, způsobům jejich naplnění a jejich případnému doplnění.

Dopady technologických trendů na hlavní oblasti schopností OS ČR

TRENDY/MCA	Vesmírný prostor	Kyberprostor	Rozvoj dálkově ovládaných prostředků a autonomních systémů	Propojení člověk-stroj	Biotechnologie	Energetické technologie	Aditivní výroba
PREPARE-TRAINING	X	X	X	X	X		
PROJECT	X	X	X	X		X	X
ENGAGE		X	X	X	X	X	X
C3	X	X		X			
SUSTAIN			X		X	X	X
PROTECT	X	X	X	X	X	X	X
INFORM	X	X	X	X			

Název: Technologický vývoj: Implikace pro schopnosti ozbrojených sil ČR 2018
Autoři: Mgr. et Mgr. Jakub Fučík, Ph.D., Ing. Fabian Baxa, Ph.D., PhDr. Libor Frank, Ph.D., Ing. Josef Procházka, Ph.D.
Grafická a ediční úprava: Mgr. Martin Doleček
Vydavatel: Univerzita obrany
Tisk: Oddělení vydavatelství a správy studijních fondů UO, Brno
Náklad: 50 ks
Rok vydání: 2019

Vydání: první