

Revoluční technologie jsou výzva pro armádní doktrínu: Technologie už máme, nyní je čas přemýšlet nad jejich použitím

Richard Mašek

Ve svém briefingu *Discourse on Winning and Losing* prohlásil americký stratég John Boyd, že klíčem k vítězství je použít naši sílu proti nepřítelově slabině. Nastávající éra soupeření velmocí radikálně mění poměr sil, na který jsme byli zvyklí z posledních dvaceti let války proti teroru – nepřítel bude disponovat stejně kvalitními, možná i lepšími systémy a technologiemi než my a Aliance. Tento fakt nás musí vést ke změně uvažování. Už není možné jen „nasadit“ naše technologie proti technologiím nepřítele, to znamená naši sílu proti jeho síle. Musíme přemýšlet o tom, jak nám potenciál technologií v příštích třiceti letech pomůže získat kvalitativní výhodu nad schopnostmi nepřítele.

Cílem tohoto eseje proto není pouze vyjmenovat technologie budoucího bojiště. Chceme se zamyslet nad tím, jak by technologie měly změnit způsob, jakým Armáda přemýšlí. V praxi to znamená pochopit vztah mezi současnou doktrínou a budoucí technologií – jak by technologie měla tvarovat doktrínu a jak by doktrína měla upravit použití technologií. Pokud armádní doktrína bude realisticky odrážet schopnosti technologií, pomůže nám pochopit, jak nové technologie přispějí k prosazování strategických zájmů České republiky. Pokud ČR bude schopná navrhnout způsob, jak revoluční technologie integrovat do bezpečnostního systému státu, bude to znamenat nejen obrovský přínos naší národní bezpečnosti a strategické kultury, ale také Alianci a jejím členům.

I v budoucnu bude podle konceptu *exploiting temporal advantage* (ETA) nepřítel podnikat kinetické i nekinetické údery v krátkém čase a v omezeném prostoru se skromnými operačními cíli, ale s dramatickými strategicko-politickými důsledky. Příkladem je Krym. Čím dál víc k tomu ale bude využívat proxy skupiny a soukromé společnosti, které stejně jako jeho konvenční síly budou disponovat osádkovými, bezosádkovými i zcela autonomními systémy, naváděnými střelami a ofenzivními kybernetickými schopnostmi. Těžiště operací bude často spočívat ve městech. Infrastruktura v masivní míře urbanizovaných zón bude sofistikovaná a digitalizovaná a město bude fungovat jako organismus, ve kterém bude těžké se orientovat. Můžeme si představit Coruscant z Hvězdných válek. Boj ve městě bude silně působit na obyvatele, a proto budou konflikty vysoce zaměřené na civilní populaci. Svět bude v permanentním stavu na hranici otevřeného konfliktu a studené války. Proto se psychologické a informační působení stane nenápadným, ale stále přítomným a z velké části rozhodujícím faktorem. Snahou nepřítele bude vylepšit technologii sociálních sítí, které budou díky umělé inteligenci schopné generovat obsah přizpůsobený tak, aby byl přesvědčivý pro konkrétního uživatele. Díky umělé realitě bude prožitek z užití sociálních sítí realistický a lidé se pravděpodobně budou moci „setkávat“ ve zcela virtuálním prostředí, kde bude proces sdílení propagandy dramaticky urychlen. Představme si potenciál dnešních influencerů manipulovat, kontrolovat nebo šířit emoce znásobený „instagramem budoucnosti“ s umělou realitou. Cílem použití technologií při kinetických, informačních i psychologických operacích bude spíše sledovat a ovlivňovat společnost než kontrolovat prostor. Pokud chceme najít jednu klíčovou charakteristiku budoucího bezpečnostního prostředí, je to informační přehlčení. Představme si, kolik dat by musel vyhodnotit velitel například protipovstalecké operace v superměstě budoucnosti, kde jednak působí nepřátelské neoznačené jednotky a bezosádkové pozemní a vzdušné systémy, a jednak je na sociálních sítích vedena sofistikovaná psychologická operace s použitím umělé reality a deep fake technologie, která formuje vnímání a emoce místní populace. Výsledkem je chaos, který je pro naši současnou doktrínu neuchopitelný.

Jaká technologie nám umožní získat kvalitativní výhodu? Potřebujeme vést rychlé, široce distribuované a vysoce flexibilní operace, při kterých dosáhneme dokonalé orientace na bojišti a maximálně využijeme schopnosti jednotek, osádkových i bezosádkových systémů a kybernetických a psychologických nástrojů. Klíčem je systém velení a řízení. Vycházejme z představy, že člověk zůstane *in the loop*, to znamená člověk v poslední instanci rozhodne o provedení útoku. V tom případě velitel a jeho štáb potřebují společný operační obraz s grafickým výstupem. V přehledném uživatelském rozhraní by měla být dostupná zjednodušená data o veškerém pohybu a o veškeré činnosti v prostoru operace nebo regionu. Prezence údajů o všech jednotkách a osádkových i bezosádkových platformách by měla být maximálně plastická a rozhraní by mělo v co největší míře využívat virtuální reality, kde jsou data sdílena v reálném čase. Výhodou takového rozhraní je, že umožňuje graficky zobrazit i netradiční prostředky vedení války, hlavně kybernetické, informační a psychologické operace. Kybernetické operace by tak měly v myšlení velitelů přestat být „magickou kartou“ zahrnou v poslední fázi wargamingu hráčem, který už neví kudy kam. Naopak by se měly stát nástrojem využitým na operační a taktické úrovni. ČR by mohla využít například zkušenosti z amerických námořních válečných her, které mají umožnit pochopit taktické využití kybernetického útoku třeba tím, že na lodi protivníka vypnul a zapnul světla. Stejně tak by grafický výstup společného operačního obrazu měl umožnit veliteli sledovat a kontrolovat psychologické a informační operace. Podmínkou pro vytvoření takové architektury velení a řízení je, že operační obraz bude zobrazovat pouze data relevantní pro rozhodování velitele. K tomu je potřeba, aby všechny komunikační toky byly sjednoceny, fúzovány a data sdílená v reálném čase platformami a senzory v poli byla podrobena jedné datové analýze. Pokud se v příštích letech podaří vybudovat dostatečně velkou databázi, poskytující data o geografii, nepřátelských schopnostech a systémech, umělá inteligence by měla datovou analýzu urychlit a sdílet do operačního obrazu pouze data relevantní pro velitele. Flexibilní velení a řízení, které by se mělo opírat o z velké části bezosádkovou a automatizovanou logistiku, navíc umožní reagovat na široké spektrum hrozeb – třeba na živelné pohromy způsobené pokračujícím globálním oteplováním nebo šíření vysoce nakažlivé nemoci. Příkladem vývoje takového systému může být *Advanced Battle Management System* amerického letectva, kterým by se měla Česká republika inspirovat a usilovat o vytvoření vlastních operačních nástrojů, které budou dokonale kompatibilní se strukturou velení a řízení NATO. Největší doktrinární výzvou bude změnit výcvik, vzdělání a myšlení velitelů na všech úrovních, jejichž úkolem bude maximálně využívat informační nástroje a výsledky datové analýzy a rozhodovat o širokém spektru činností. Daleko menší roli v přemýšlení velitelů by tak měly hrát standardizované operační procedury (SOPs). K pochopení operačního obrazu, který sjednocuje celou paletu nástrojů od kinetických po kybernetické a psychologické, by mělo sloužit experimentování a wargaming (hlavně stolní hry), kterému především by se Armáda měla v následujících letech intenzivně věnovat.

Systém velení a řízení, který je založen na sdílení dat v reálném čase, se musí opírat o sofistikovanou informační strukturu na taktické úrovni. Každá dostupná jednotka a každý dostupný systém se proto musí proměnit ve všestranný senzor sdílející data v reálném čase. Vzorem může být třeba letoun F-35, který funguje jako informační uzel. Klíčová je přitom schopnost strojů komunikovat mezi sebou bez nutnosti zapojení člověka. Senzory s umělou inteligencí na taktické úrovni (například ve formě senzorů tanku) budou mít dvě hlavní schopnosti. Jednak dojde ke zkrácení kill chainu na úrovni samotné platformy – na základě informací ze senzoru bude možné v řádu sekund rozhodnout o ničení nebo dalším postupu buď velitelem platformy přímo z místa, nebo operátorem na dálku. Druhým projevem by však bylo sdílení informací – pokud možno v reálném čase – v síti všech dalších propojených platform, a hlavně do společného operačního obrazu. Znalost prostoru bojové činnosti se dostane na bezprecedentní úroveň. Už teď jsou vyvíjeni roboti asistující posádce (hlavně letounů) podobně jako fiktivní R2D2. Takový robot může asistovat jednak s řízením činnosti samotné platformy, jednak

s tříděním a sdílením dat. Do této architektury zapadá i *manned-unmanned teaming* (MUM-T), které představuje budoucnost pozemních i vzdušných sil. Jedna mateřská platforma může ovládat větší počet bezosádkových platforem, používat je jako multiplikátor a průzkum. Vzhledem k ambivalentní povaze moderních konfliktů by mělo být integrováno také co nejvíce neletálních bojových prostředků, například akustické zbraně, které umožní našim silám efektivně se pohybovat na hranici a pod hranicí konfliktu vysoké intenzity. Optimálním sdílením dat mohou naše platformy získat převahu nad nejmodernějšími systémy. Po posledním konfliktu v Náhorním Karabachu spousta analytiků zpochybňovala roli tanku na budoucím bojišti. Přitom během cvičení prvků systému ABMS dokázala americká houfnice Paladin, jejíž první kus byl nasazen v roce 1963, sestřelit moderní bojový dron, a to právě díky bezchybnému sdílení dat z bojiště. Česká republika by proto měla přemýšlet, jak se postavit k projektům, jako je německo-francouzský evropský tank, který staví na informačním propojení jednotlivých platforem.

Realitou je, že budoucí konflikt se bude pohybovat na nebo pod hranicí konfliktu vysoké intenzity. Flexibilní pokročilý systém vedení boje bude jednak působit jako efektivní deterent, jednak jako kvalitativní výhoda v boji. Armáda ale nikdy nebude úspěšná, pokud její doktrína nepochopí význam, jaký současné technologie mají pro sdílení informací mezi lidmi. Tím nemyslíme technickou rovinu, ale psychologické působení na recipienta – uživatele sociálních sítí a komunikačních nástrojů, kterým může být místní populace, politik nebo voják. Jak navrhuje americký Modern War Institute, doktrína by měla chápat psychologické působení jako tzv. *shaping operations*. Sociální sítě budou stále dokonalejší – při použití umělé reality mohou vytvořit zcela paralelní universum, ve kterém se bude uživatel setkávat jen s tím, s kým chce, a přijímat informace, které chce. V rámci *whole-of-government approach* by Armáda měla definovat, jaké pokročilé komunikační technologie (často zcela veřejně dostupné) může využít, při protipůsobení jednak na naši populaci, a jednak na populaci státu nepřítele při vytváření naší vlastní ofenzivní *soft-power* doktríny. Protože informace je zbraň, měly by být psychologické informace zastoupeny v operačním obrazu, aby velitel v daném prostoru operací mohl rozhodnout o jejich použití.

Pokročilý systém velení a řízení posune současný koncept *joint command* na novou úroveň. Integruje přitom všechny dostupné technologie do jednoho systému a umožní nám pochopit bojiště. Tím získáme kvalitativní výhodu nad protivníkem. Revoluční změna doktríny, kterou přinese, umožní velitelům rozhodovat rychle a pokrýt širší spektrum činností. Propojenost kinetických, informačních a psychologických nástrojů bude od vojáků a civilistů v resortu obrany vyžadovat jak znalosti, tak schopnosti analyzovat a pochopit komplexní situace. Slovy Paula Giarry proto čím dál víc budeme potřebovat *warriors-scholars*, kteří se budou orientovat nejen v technických parametrech systémů, ale také v doktríně jejich použití a ve strategických důsledcích jejich nasazení. Technologie už máme, teď je čas naučit se je správně používat.