Úpadek USA jako vojenské velmoci – kybernetická válka

(*Tomáš Rezek*)

Úvod

Spojené státy americké se během studené války staly vojenskou supervelmocí. Po rozpadu Sovětského svazu sice došlo k omezení výdajů na obranu, přesto je rozpočet ministerstva obrany USA s více než 600 miliardami USD i nadále zdaleka největším na světě.[1] Podstatnou část výdajů představují náklady na modernizaci a na zavedení moderních technologií, které umožní efektivnější řízení vojenských operací, zlepší komunikaci, ale především sníží možné ztráty na životech amerických vojáků. V současné době jsou USA jedinou zemí na světě, která je schopná provádět vojenské operace v globálním měřítku.

Poslední válečné konflikty v Afghánistánu a v Iráku jasně demonstrovaly převahu bojových jednotek USA ve všech rovinách – na zemi, ve vzduchu i na moři. Při konkrétních bojových akcích hrálo rozhodující úlohu letectvo, které zneškodnilo klíčové cíle, takže riziko pro pozemní jednotky bylo akceptovatelné. Dominance na moři umožňuje podporovat pozemní jednotky palebnou silou křižníků a zároveň poskytuje ochranu letadlovým lodím. Moderně vybaveným pozemním jednotkám se pak postaví jen značně oslabené síly protivníka. Americký způsob boje se z velké části zakládá na moderních technologiích, které umožňují přesnou navigaci, komunikaci na dlouhé vzdálenosti, a zvyšují tak účinnost konvenčních zbraní.[2]

USA jsou do určité míry vojensky dominantní i ve vesmíru. Ačkoliv původní plány představené za Reaganovy vlády jako Iniciativa strategické obrany[3] nebyly realizovány, využití satelitů pro komunikaci, průzkum a navigaci je zřejmé. Nicméně

současná pozice USA se může změnit vzhledem k nedávným úspěchům Číny ve vesmíru.[4]

Relativně novým objektem zájmu vojenských expertů je však kromě pozemních, námořních, leteckých a vesmírných sil také kybernetický prostor. Kybernetický prostor je uměle vytvořený člověkem. Je tvořen všemi počítači, systémy, stroji nebo jinými objekty, které mohou sdílet informace prostřednictvím internetu nebo jiných sítí. I v tomto prostoru je možné vést válku. Jak si stojí USA v této nové oblasti? Může případná ztráta dominance na poli kybernetického prostoru ohrozit pozici USA jako světové vojenské velmoci? A je vůbec kybernetický prostor relevantní? To jsou otázky, na které hledá odpovědi tato kapitola.

Kybernetický prostor a jeho význam

Využívání kybernetického prostoru a souvisejících technologií ovlivňuje celou společnost. Z ekonomického hlediska implementace CRM, SCM a jiných podnikových systémů umožňuje zefektivnit podnikové procesy a zvýšit tak konkurenceschopnost jednotlivým firem. Význam sociálních síti pro sdílení informací a pro virtuální kontakt s přáteli představuje zcela nový aspekt v rámci sociálních vazeb. Z politologického hlediska představuje kybernetický prostor zcela nový koncept veřejného místa, kde lidé mohou sdílet své politické názory a být občansky aktivní.

Vojenský aspekt kybernetického prostoru byl zprvu pouze informační – připojené počítače a systémy mohou obsahovat vojensky důležité informace. Další možnosti pro vojenské využití přineslo masové rozšíření uživatelů kybernetického prostoru. Vzrůstající počet uživatelů způsobil, že šíření propagandy v kybernetickém prostoru je mnohem efektivnější než třeba rozhazování letáků z letadel. Kybernetický prostor totiž lze až na výjimky jen velmi obtížně kontrolovat. V obou

zmiňovaných případech ale kybernetický prostor představuje jen další dimenzi v již existující strategii. Vojenská rozvědka používá různé metody k získávání informací, kybernetický prostor je jen novou dimenzí, ve které uplatňuje své postupy. Vojenská propaganda tak i nadále zahrnuje šíření letáků, nově však i po e-mailu. Zásadní vojenský význam kybernetického prostoru představuje rostoucí míra užívání pokročilých technologií pro vojenské účely a rostoucí míra závislosti kritických systémů na kybernetickém prostoru.

Moderní vojenská technika je prakticky závislá na počítačích. Ať už mluvíme o radarových systémech, o tancích nebo o stíhacích letounech, všude jsou využívány počítače, které hrají podstatnou roli. Například identifikace neznámého objektu na obrazovce radaru již není realizována operátorem, ale počítačem. Zaměřovací systém v tanku, noční vidění, to vše částečně nebo úplně řídí počítače. Moderní stíhací letouny jsou plné různých počítačových systémů, které udržují letadlo ve vzduchu.[5] Další kategorii představují zbraně, které jsou zcela pod kontrolou počítačových systémů. Jde třeba o bezpilotní letouny nebo starší, ale stále využívané rakety s plochou dráhou letu. Možnost vyřadit z provozu nepřátelské systémy, které například řídí bezpilotní letouny, jsou odpovědné za navigaci raket nebo za detekci nepřátelských letadel, může znamenat klíčovou výhodu při případném konfliktu. Jakékoliv přerušení spojení s operačním střediskem má za následek přechod na předprogramované jednání, které se často liší od původního úkolu.[6]

Závislost společnosti na kybernetickém prostoru není příliš často zmiňována, ať už z obav možného zneužití nebo čistě z nepochopení podstaty problému.[7] S rostoucí mírou využívání ICT a kybernetického prostoru se ale tato závislost zvyšuje. Může být zneužita v případě teroristického útoku nebo kybernetického konfliktu. V rámci soukromého sektoru můžeme mluvit například o bankovnictví. Velká většina transakcí probíhá přes internet. Bankovní výpisy jsou zasílá-

ny e-mailem, informace o stavech jednotlivých účtů jsou udržovány v bankovních databázích. Obdobně tomu je v případě obchodů s cennými papíry. Ačkoliv by výpadek některého z těchto systémů nemusel znamenat nutně ztrátu veškerých informací, určitě by naboural důvěru veřejnosti. Například potíže newyorské burzy při úpisu akcií Facebooku způsobily škodu v hodnotě stovek miliónů dolarů.[8] V případě státu můžeme hovořit o využití ICT při volbách nebo při interakci s občanem (například daňové přiznání). Na pomezí mezi státním a soukromým sektorem je kritická infrastruktura. Můžeme hovořit například o distribuční síti vody, elektrické energie, o řízení letového provozu a o dalších systémech, které jsou kritické pro chod dané země. Závislost na kybernetickém prostoru může být využita nepřítelem k získání strategické výhody při případném konfliktu.

Vážnost situace si uvědomuje i prezident USA Barack Obama, který prohlásil: „Dnes můžeme vidět kybernetickou hrozbu pro naše sítě, na kterých závisí náš moderní způsob života. Máme příležitost a odpovědnost být aktivní a o krok napřed před našimi protivníky. […] Je na čase zesílit naši obranu proti tomuto rostoucímu nebezpečí.“[9]

Vzhledem k americké tradici nemůžeme očekávat dramatický přesun strategie a financí směrem k informačním systémům, serverům a jinému vybavení pro kybernetickou válku. Konvenční zbraně a bojové systémy budou i nadále dominovat v armádních složkách USA, nicméně alespoň z hlediska obrany tento projev naznačuje alespoň zvýšený zájem o kybernetickou bezpečnost na té nejvyšší úrovni.

Metodologie

Předmětem této kapitoly je posoudit aktuální stav USA ve vztahu k možnému nebezpečí, které s sebou přináší kybernetický prostor a jeho využívání. Klíčovou otázkou je, zda

si USA udrží dominantní pozici vojenské velmoci i na kybernetickém poli ve vztahu k dalším mezinárodním hráčům. Případná ztráta dominance na kybernetickém poli by mohla představovat první krok na cestě k úpadku USA jako světové vojenské velmoci.

Z metodologického pohledu se pro porovnání a pro měření síly v kybernetickém prostoru nabízí komparativní analýza. Nicméně přesné stanovení síly na pomyslné stupnici je velmi obtížné, a to z několika důvodů.

V případě kybernetické vojenské síly není možné stanovit vojenský potenciál na základě počtu vojáků v dedikovaných jednotkách. V případě kybernetického prostoru nerozhoduje množství, ale kvalita. Stovka speciálně vycvičených vojenských pracovníků může selhat tváří v tvář jednomu nadanému protivníkovi. Můžeme sice hovořit o početní převaze, ale ta nemusí být v kybernetickém prostoru rozhodující. Objektivně je třeba konstatovat, že ani v případě „konvenčních" armád není přímé porovnávání možné vzhledem k rozdílné technologické úrovni výzbroje.[10] Pro přímé srovnání je navíc nezbytné mít k dispozici dostatečně přesné údaje. V případě jednotek určených pro kybernetické konflikty nemusí být uveřejněná čísla přesná, v některých případech nemusí být vůbec dostupná.

Jeden z možných způsobů hodnocení síly je přes finanční prostředky dedikované na danou formu boje, tedy přes rozpočet. Jakkoliv mají USA nejvyšší rozpočet na obranu ve světě, neznamená to, že jsou automaticky nejsilnější na poli kybernetické války. Absolutní i relativní výši rozpočtu můžeme porovnat, ale již bude obtížnější získat přesné informace o tom, jaká část je určena přímo na kybernetické jednotky. I v tomto případě bude obtížné získat konkrétní údaje. Dalším faktorem v neprospěch této metody je organizační zajištění těchto jednotek. Financování kybernetických válečníků může být realizováno napříč několika útvary nebo ministerstvy. Bez detailních znalostí organizační struktury,

která nemusí být veřejná, je tento způsob porovnání velmi nepřesný.

S rozpočtem souvisí i dostupné technické vybavení, které jednotky využívají. I tento způsob srovnání je velmi nepřesný, protože vybavení je bez znalosti technické specifikace neporovnatelné, a navíc hraje spíše podpůrnou roli. Zničující virus nebo útok je možné připravit na běžném osobním počítači.

Stejně tak je nemožné porovnávat destruktivní potenciál jednotlivých kybernetických jednotek. Nejde o raketové hlavice, kde můžeme porovnávat ničivou sílu na základě hmotnosti a síly výbušniny. V případě kybernetického boje hovoříme spíše o potenciálních možnostech, konkrétní informace většinou nejsou dostupné. Důvodem je skutečnost, že jakékoliv vyjádření může protivníka na potenciální slabiny připravit, může vyprovokovat zkušební akci nebo může narušit důvěru veřejnosti. Pokud například USA prohlásí, že jejich jednotky jsou schopné získat přístup do jakéhokoliv počítače na síti, bude následovat rozsáhlá kontrola systémů v ostatních státech, případně přechod na zcela jiný systém nebo způsob připojení s cílem eliminovat toto riziko. Prohlášení o dokonalém zabezpečení vlastní sítě zase může vyprovokovat zkušební akce s cílem odhalit možné slabiny, a to i ze strany nestátních aktérů v kybernetickém prostoru, například hackerů. Stejně tak objektivní zhodnocení možných rizik nemusí veřejnost přijmout kladně. Například konstatování, že bankovní systém je vlastně nedostatečně chráněn a že se může kdykoliv zcela zhroutit, neprospěje domácí situaci. Proto je třeba brát jakákoliv prohlášení týkající se vojenského potenciálu v kybernetickém prostoru s rezervou a s ohledem na cíl, kterému slouží (jako například výše citovaný projev Baracka Obamy).

Vzhledem k povaze kybernetického prostoru a kybernetických jednotek není možné provádět komparaci na základě přesných dat. Navíc absolutní čísla nebo zpřesňující infor-

mace týkající se kybernetických jednotek nejsou určující. Je 1 000 speciálně vycvičených vojáků hodně, nebo málo? Pouze relativní vyjádření vztažené k jinému státu umožní stanovit alespoň relativní sílu. Z těchto důvodů je komparace založena na přímém porovnávání jednotlivých zemí na základě objektivně ověřitelných faktů, ale i subjektivních analytických úvah, které z nich vyplývají. Oblasti, na které se analýza soustředí, vycházejí z podstaty kybernetického prostředí. Pro účely této analýzy byly použity tři hlavní, po vzoru analýzy v knize *Cyber War*.[11] Tato publikace je jednou z mála, která se zabývá mimo jiné i politickým aspektem kybernetické války v USA a vnitřními procesy, které stojí za formováním národní kybernetické strategie. Hlavním cílem této knihy je upozornit na skutečnost, že USA mají nedostatečně organizovanou obranu klíčových systémů a kritické infrastruktury. Tato publikace je velmi hodnotná především díky tomu, že autor dlouhou dobu působil v úzkém kruhu poradců prezidenta pro jednotlivé bezpečnostní otázky, a má tak jedinečné informace o vnitřních procesech a konfliktech mezi jednotlivými odděleními. Zmiňované tři oblasti pro analýzu jsou: schopnost podniknout útok v kybernetickém prostoru (útočný potenciál), schopnost útok odvrátit (obranný potenciál) a závislost na kybernetickém prostředí (závislost). Za další aspekty pro širší analýzu můžeme považovat schopnost obnovit klíčové systémy, existenci náhradních/záložních systémů, krizové plány a další. Pro každý aspekt jsou porovnávány vždy dvě země a za použití dedukce jsou formulovány konečné závěry. Výčet zemí pro porovnání vychází z výše zmiňované publikace, což umožní srovnání výsledků na konci analýzy. Vybrané země zahrnují především možné politicko-vojenské konkurenty USA a země, které mají značnou motivaci využít případných výhod, které by jim převaha v kybernetickém prostoru přinesla. Vybrané země jsou: USA, Rusko, Čína, Írán a Severní Korea.