Hrozby a ohrožení

Podle nových principů války se ozbrojené síly již nepoužívají k tomu, aby byl nepřítel donucen podrobit se vůli druhé strany, ale spíše se používají prostředky, které mají nepřítele donutit, aby akceptoval její zájmy.

Qiao Liang, Wang Xiangsui

Dostali jsme to, co jsme vždy chtěli. Teď se tomu musíme přizpůsobit. V dnes již klasickém článku o existujících hrozbách, psaném někdy počátkem studené války, definoval J. D. Singer „hrozbu" jako potenciál spojený s ohrožením [1]. Přesně vymezil termín, který byl podle jeho mínění v debatách o bezpečnostní situaci užíván až příliš volně. Stále se jí při studiu bezpečnostní politiky užívá, bohužel, ani akademicky přesná definice nezměnila po skončení studené války zaměření americké bezpečnostní politiky. V současné době jsou jako hrozby označovány hlad, občanské nepokoje a další prvky, které tvoří bezpečnostní prostředí. Protože za „hrozbu" je označováno téměř vše, tento pojem vlastně neznamená téměř nic.

Singerova definice byla pro ty, kteří se zabývali bezpečnostní plánováním, velice užitečná v době, kdy bylo možné měřit nebezpečí v hodinách letu, množstvím pum a jejich mohutnosti megatunách. Předpokládalo se, že Sovětský svaz bude jednat podle schéma: masová odveta, odstrašení a vzájemně zaručené zničení. Klíčovým úkolem zpravodajské služby v té době bylo zjistit, zda existuje záměr, aby se daný potenciál změnil v hrozbu, a pokud ano, jak velká tato hrozba bude. Ve zpětném pohledu to bylo vlastně velmi prosté.

Mnohé se však od té doby změnilo. Avšak navzdory značnému úsilí popsat současné bezpečnostní prostředí, žádná z posledních formulací americké bezpečnostní strategie se nedá přirovnat například ke koncepci politiky zadržování Sovětského svazu, kterou zformuloval bývalý vedoucí odboru plánování zahraniční politiky na ministerstvu zahraničí George Kennan. Asi bychom chtěli příliš, kdybychom očekávali, že někdo dokáže vypracovat stejně elegantní vizi ochrany amerických zájmů v současném světě. Kennanův svět byl ovšem méně komplikovaný, než je bezpečnostní prostředí, se kterým jsme dnes konfrontováni. Pravděpodobně není možné formulovat jednoduchou a stručnou koncepci, která by v dlouhodobé perspektivě popsala všechny prostředky a cíle národní strategie. Kennanův svět sice nebyl v pořádku, ale jeho nedůvěra ve „schopnost identifikovat s využitím obecné i právní terminologie možné situace, které si nikdo nedokáže představit, natož předvídat" se hodí více na náš svět než ten jeho.

V dnešním stále více komplikovaném bezpečnostním prostředí státy již nejsou jedinými hlavními aktéry (aktivními účastníky), protože díky pokročilým technologiím jsou i malé bojové skupinky vybaveny zbraněmi, které dříve vlastnily jen velmoci. Technologie, rozšiřování znalostí, to vše zpřístupnilo biologický, radiační, chemický a elektronický potenciál i nestátním aktérům. Kennanův svět počítal se státními záměry, které jsou oznamovány hlavně prostřednictvím oficiálních vyhlášení. Základním bylo určit zbrojní potenciál protivníka, například součtem jeho jaderných raket. Takový potenciál se v dnešním bezpečnostním prostředí dá jedině odhadovat.

Vycházelo se z toho, že záměry jednotlivých aktérů v podstatě nelze poznat, což problémy jen zvyšovalo, a tak jedinou alternativou, která se nabízela, bylo sčítání sil raket či obrněných formací. Ve skutečnosti záměry jednotlivých aktérů bylo možné zjistit, ale to si vyžadovalo víc, než jen počítat raketová síla. Dnes, za situace, kdy existuje několik desítek státních i nestátních aktérů, kdy je možné provést úder na určitou důležitou americkou infrastrukturu a obyvatelstvo

zbraněmi, které nelze vysledovat z vesmíru, je jediným možným řešením tyto hrozby identifikovat.

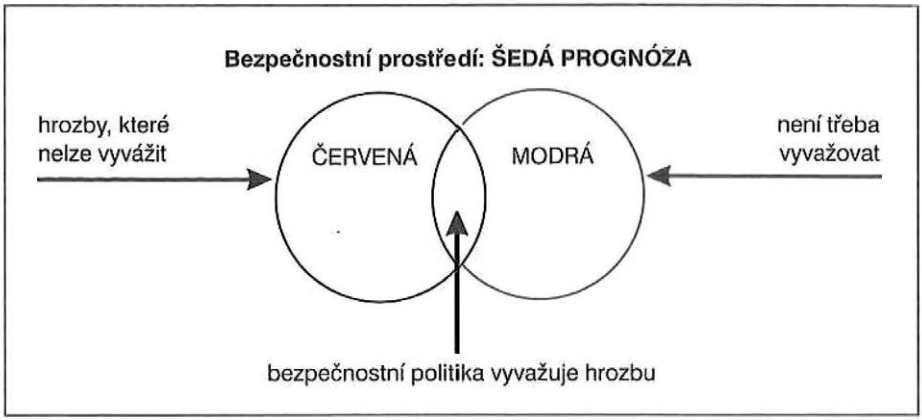
Jak vidíme sami sebe a jak vidí svět nás

Abychom dokázali zformulovat efektivní bezpečnostní politiku, musíme pochopit její tři základní prvky: sami sebe, bezpečnostní prostředí a možnou hrozbu (**obr. 1**). Pochopit sama sebe znamená znát požadované cíle, vlastní potenciál, dostupné zdroje, přijatelné způsoby reagování v různých situacích atd. Bezpečnostní prostředí ovlivňuje jak nás, tak danou hrozbu, a s využitím jeho základních charakteristik lze vytvořit jeho model. Běžný model bezpečnostního prostředí například předpokládá, že primárními aktéry jsou státy. Systém je soběstačný, neexistuje žádná autorita, která by rozhodovala spory, nejvyšším cílem je přežití, pořadí významu států v systému je určováno jejich ekonomickými, vojenskými a dalšími kapacitami [2]. Způsob, jak poznat sám sebe a bezpečnostní prostředí, se zatím změnil jen velmi málo, obtížnějším se stalo chápání hrozeb.

Je zdokumentována schopnost řady států a dalších aktérů nejrůznějšími prostředky ohrozit jak obyvatelstvo USA, tak důležitou infrastrukturu. Prostředí studené války (pro které bylo typické, že existovaly jasné záměry, ale neznámý potenciál) se změnilo na prostředí, kde známe dostupné kapacity, ale ne už záměry. Možnosti, jak zasáhnout obyvatelstvo a důležitou infrastrukturu, již nejsou omezeny na strategické jaderné nosiče, ale zahrnují laptopy, pašované chemické, biologické, jaderné a radioaktivní látky *(CBNR - chemical, biological and radiological agents)*, které mohou být libovolnými nosiči dopraveny na cíl. Způsob identifikace hrozeb, který byl založen na určení schopnosti takovou hrozbu realizovat, je nevhodný, protože potřebný potenciál má příliš mnoho aktérů. Program zjišťování zbraní hromadného ničení je jistě důležitý, ale jejich identifikace a následná verifikace je stále obtížnější .V novém bezpečnostním prostředí je to téměř nemožné, protože tyto zbraně mohou být snadno ukryty a rychle se rozšiřují. Proto se stává stále důležitějším **vyhodnocování záměrů**. Je to jako čtení myšlenek: aktéři jsou neprůhledné entity, mohou být neutrální, přátelští i nepřátelští. Ovšem „neprůhledný aktér (účastník)" je jen abstraktum, možný jen v teorii. Kdybychom přistoupili na to, že jeho záměry nelze zjistit, bylo by to, jako kdybychom na cestě potkali neznámého psa. Projde kolem nás, anebo nás kousne? Jeho potenciál známe, ale ne jeho úmysl. Výhodou je, když známe jednotlivé aktéry, zvláště státy. Až na výjimky většinou známe státní zájmy, mocenské struktury *(decision-making structures)*, jeho instituce, stav zbrojení. Státy nejsou neprůhledné, je možné je analyzovat. Jejich pravděpodobné aktivity odhadujeme díky státním úředníkům, diplomatům, vojákům, novinářům atd. Podobně můžeme analyzovat a předvídat i činnost nestátních aktérů. Na zjišťování jejich záměrů mají zpravodajské služby mnoho prostředků. Jedním nejnovějších je počítačové získávání dat a informací.

V dobách studené války byla data utajována daleko více než dnes. Změnily se dvě základní věci. Za prvé po pádu sovětského impéria vznikla možnost svobodně myslet a své myšlenky veřejně vyjadřovat, za druhé je to exploze informační technologie. Svoboda tisku zvyšuje na celém světě informační toky, např. prostřednictvím globalizované televize, nebo geometricky, prostřednictvím internetu. Bohužel **velké množství informací, které máme k dispozici, nikterak nezvyšuje úroveň jejich pochopení**. Za studené války znamenal veřejný projev vysokého sovětského činitele také vyslovení oficiální linie. Ať už byl zamýšlen jako informace či dezinformace, na sovětské straně věděli, že tento projev studujeme, a my jsme věděli, že oni ví, že my víme. Relativní vzácnost informací o jistých tématech, znamenala, že v těchto projevech bylo ukryto určité poselství, bez ohledu na přesnost vyjádření.

Každý by rád věděl, co si myslí jeho protivník. Kniha Adolfa Hitlera „Mein Kampf" ukazuje, že vyslovené hrozby někdy skutečně odhalují záměr jejich autora. Ovšem co se týče odhalování záměrů, některé zpravodajské prostředky, jako třeba satelity, mají v tomto směru jen malou použitelnost, zvláště jde-li o zjišťování stavu vývoje zbraní hromadného ničení. Také elektronický odposlech je k ničemu, užívá-li protivník komunikační síť z optických vláken. Tady jsou při získávání a třídění dat velké rezervy. Absolutní ochrana dat je nemožná, a právě jejich rozšiřování zvyšuje možnost, že se důležitá data ocitnou mimo jejich ochranný systém.



Obr. 1: Červená, šedá a modrá prognóza
(pro správné pochopení hrozby, bezpečnostního prostředí a sebe sama).

Z bezpečnostních důvodů potřebujeme vědět, kdo představuje hrozbu, jaké prostředky zamýšlí použít, jaké jsou jeho cíle a celkový záměr, který sleduje. To je celkem snadné, pokud se jedná o protivníka, kterým je stát, jde-li se o otevřený konflikt *(overt conflict)*, známý potenciál (možnosti) a vojenský záměr, která byl oznámen již při vyhlášení válečných cílů. Větším problémem je pochopení hrozeb v současném bezpečnostním prostředí, kdy aktéři používají nekonvenční prostředky na nekonvenční cíle, které se často mění, je využívána **asymetrická, potenciálně anonymní strategie**.

Ukážeme si, co vše lze zjistit z jedné knihy, i když samozřejmě žádná analýza nemůže vycházet jen z jediného pramene, ale musí se opírat stovky, ne-li tisíce zdrojů. Kniha se jmenuje „Neomezená válka" a napsali ji dva plukovníci čínské armády [3]. Podrobně se zde popisuje strategie války proti Spojeným státům. Strategie, která se vyhýbá síle a útočí na zranitelná místa. Jejím základem je konstatování, že, budoucí válka nezůstane omezena jen na vojenskou část, ale zasáhne i tradičně nevojenské a pro armádu nedůležité oblasti. Profesionální kvalifikace autorů, oficiální vydání knihy a její příznivé přijetí může znamenat, že je zde skrytě vyjádřena čínská vojenská doktrína. Kniha navíc naznačuje i možné strategické směry útoku, pokud by snad mezi Čínou a Spojenými státy propukl konflikt.

Cílem rozboru textu knihy „Neomezená válka" je strukturovaná analýza hrozeb, prostředků, cílů, která končí určením jejich vzájemných vazeb a možných změn. Tato kniha vlastně funguje jako soupis termínů a pojmů, které slouží k identifikaci všech čínských zájmových okruhů. Je doplněna slovníkem, který definuje jednotlivé termíny, a tak přiřazuje k jednotlivým pojmům jejich správný výklad. Každá část textu byla analyzována či jinak rozebrána, aby byl odhalen určitý aktér, volba jeho cílů, i záměr. V každé z těchto kategorií je text dále analyzován a k určitým typům hrozeb je přiřazen odpovídají termín, prostředky, záměry (**obr. 2**).

Zapsáním do tabulky byla odhalena skrytá osnova textu. Řada (řetězec) za sebou jdoucích pojmů, logických spojení, která sestává z: hrozby → prostředků → cílů → konečných cílů, byla rozkódována jako: pracovníci informační války → kybernetický útok → bankovnictví a finance → asymetrický konflikt/zasažení Spojených států. Rozkódování textu znamenalo také rozkódování v rámci jednotlivých kategorií, což umožnilo lepší vyjasnění záměrů. Opakující se clustery (soubory pojmů v jednotlivých kategoriích), jako kybernetický útok/ekonomický útok/infor- mační operace v rámci kategorie prostředky ukazují, že zasazení těchto prostředků by mělo být očekáváno v průběhu konfliktu s aktérem, jehož data byla analyzována.

Kvalitativní obsahová analýza *(qualitative content analysis)* poskytuje odpovědi a validní závěry z dat (jako kvantitativní obsahová analýza numerických databází), což si autoři knihy (manažeři databází) vlastně ani neuvědomují. Touto metodou lze prozkoumat velké množství dat.

Frekvence jednotlivých slov či výskyt frází pomáhá analytikům vidět „červené, modré a šedé" (tj. nepřátelské, neutrální, přátelské) perspektivy a vztahy, jak je ukázáno na **obr. 1**. Existují sice určitá omezení, což může být zjištěno při důkladném rozboru textu, ale vyvážená analýza integruje lidský úsudek s mechanickými metodami kvantitativního vyhodnocení. Při posuzování řad (řetězců), schémat, clusterů (souborů, jehož jednotky mají nějakou společnou vlastnost), častosti výskytu a dalších prvků analýzy by měl být také užíván zdravý rozum. Kvantitativní analýza je důležitou metodou, nástrojem, ale pořád je to jen určitým způsobem omezená mechanická metoda. Abychom přesně identifikovali záměr protivníka, či „viděli nebezpečí", musíme vědět, co aktéři skutečně zamýšlejí, ne jen co říkají.

Hrozby (threats), prostředky (means), cíle (targets) a konečné cíle (ends)			
hrozba	prostředek	cíl	konečný cíl
autonomní teroristické organizace	vraždy	bankovnictví a finance+	asymetrický konflikt*
náboženské sekty	biologické látky	biologický výzkum a výroba, sklady	zahrnuje Spojené státy
ekonomická válka	bomby	obchod	ekonomická výhoda
lokální/okrajová organizace	chemické látky	chemický výzkum a výroba, sklady	schopnost expanze
počítačoví hackeři	kybernetický útok	kontinuita vlády+	finanční zisk
pracovníci informační války	přímá akce	diplomatické cíle	nenávist
„osamělý vlk"	špionáž	elektrická síť+	ideologie
polovojenské skupiny	vydírání	pohotovostní krizový systém+	metafyzický cíl
špionáž	falešné informace	vodovodní systémy+	výhoda pro národní bezpečnost
státem podporovaný terorismus	informační operace	vládní zařízení a budovy	politická změna
zrádce	jaderné zbraně	vynucování zákona	politický vliv
mezinárodní organizovaný zločin	radioaktivní látky	vojenská zařízení a budovy	pomsta
stát*	ekonomický útok*	jaderný výzkum a výroba, sklady jaderných zbraní	přežití
mezinárodní aktér*	genetické látky*	ropné a plynové sítě+	vandalismus
		americké obyvatelstvo	získání ZHN
		systém veřejného zdravotnictví+	
		telekomunikační a informační systémy+	
		doprava+	

Obr. 2

Poznámky:

* Jako stát můžeme chápat i pojem „státem podporovaný terorismus". Termín mezinárodní aktér v této souvislosti chápeme buď jako známou mezinárodní instituci, např. Mezinárodní měnový fond, nebo soukromou společnost, která působí po celém světě, např. Private Military Company, Sandline, Inc. Termíny ekonomický útok a genetické látky jsou převzaty z oficiálních dokumentů. Ekonomický útok zahrnuje celou řadu metod, od obchodních sankcí až po dumpingové zboží. Genetická látka je patogen, který mění genetické vybavení obilovin, dobytka i lidí.

+ Tyto složky vytvářejí americkou kritickou infrastrukturu a jsou definovány v dokumentu Presidential Decision Directive 63, 22 May 1998.

• Asymetrický konflikt sám o sobě není konečným cílem, ale je s tímto cílem spjat, protože tento pojem specifikuje hlavní cíl hrozby.

Vidět nebezpečí

Ve světě existuje celá řada různých nebezpečí. Především by měly být studovány již známé hrozby, které jsou představovány státními i nestátními aktéry. Vedle nich bychom se měli zabývat i hypotetickými aktéry, jakými jsou mezinárodní zločinecké organizace, a určit, jaké prostředky by mohly užívat a jaké by mohly mít cíle. Tímto způsobem vzniká určitá holistická (celostní)

typologie hrozeb bezpečnostního prostředí. Nabízí se zde analogie s vědeckou klasifikací živočišné a rostlinné říše. Hrozby můžeme rozdělit do různých kategorií (říše, řád, čeleď, kmen atd.), což nám umožní lépe pochopit důvody (motivy) různých hrozeb, prostředky, metody a cíle. „Říše hrozeb" by tak zahrnovala veškerý možný vojenský potenciál a záměry obsažené v bezpečnostním prostředí.

Různá nebezpečí se mohou překrývat, podle typu hrozeb, podle dostupných prostředků, priorit a konečného cíle, jiná mohou být zcela samostatná. Aktéři se mohou blížit jednomu čistému typu, jako třeba autonomní teroristická organizace, zatímco jiní aktéři, jako Čína, mohou mít jak potenciál, tak úmysl v možném konfliktu obsadit celé spektrum hrozeb a skutečně je využít.

Autoři knihy „Neomezená válka" se domnívají, že otevřený konflikt mezi dvěma konvenčními armádami, postavenými proti sobě, je zastaralý. Konflikt se Spojenými státy, v současné době jediné dominující vojenské síly, nebude probíhat tradičním způsobem, jako třeba válka v Perském zálivu. Jejich uvažování je založeno na staré vojenské poučce, že: inteligentní aktér se vyhýbá síle a útočí na slabá místa. Autoři tvrdí, že právě ohromný úspěch koalice v Perském zálivu, vedené Spojenými státy, a použití nových zbraňových systémů, paradoxně takovému typu střetnutí odzvonily. „Zasazení všech prostředků, včetně ozbrojených i neozbrojených sil, vojenských i nevojenských prostředků, letálních i neletálních zbraní, aby byl protivník donucen přijmout naše podmínky," představuje novou tvář války. Autoři dále dokazují, že vojenská konfrontace se Spojenými státy by byla nejen neplodná, a navíc není ani nezbytná, protože nové prostředky útoku rozšiřují spektrum možných cílů.

Nové technologie daly vzniknout „zbraním nové generace". Tyto zbraně jsou daleko ničivější (letální) než zbraně, které byly dosud užívány. Ale jejich vývoj je v současném bezpečnostním prostředí zbytečný, a navíc i drahý. Jednak je zde vedoucí mocností Amerika, kterou je nemožné v tomto směru dostihnout, jednak tyto zbraně nemohou uniknout omezením, která se ukázala již ve válce v Perském zálivu. Na úspěšné vedení války - zejména se Spojenými státy - je zapotřebí zcela nové strategie, s novými zbraněmi, které by na jedné straně „překračovaly čistě vojenské použití, na druhé straně by bylo možné jejich zasazení ve vojenských operacích. ... Vše, co prospívá, může také škodit ... a na světě není nic, co by se nemohlo proměnit ve zbraň .... průlom v našem myšlení nám rázem otevře království zbraní: jediný člověk dokáže zničit trh s akciemi, jediný počítač může zahájit virovou invazi, jediný skandál může v zemi protivníka změnit kurzy akcií nebo vystavit její politické představitele pomluvám na internetu, to vše lze zařadit do koncepce nových zbraní".

Jednoznačně se zvyšuje množství cílů. Klasická válka byla zaměřena na ozbrojené síly. Liang a Xiangsui tvrdí, že hlavní zátěž příští války ponese především civilní obyvatelstvo, protože útoky budou z větší části zaměřeny proti hodnotám *(countervalue targeting)*. „Co musí být jasné, je to, že nové pojetí zbraní je těsně spjato s životy obyčejných lidí. ... Jsme přesvědčeni, že se jednoho dne lidé probudí a s úžasem shledají, že zcela běžné, příjemné věci získávají útočný a smrtící charakter."

Předzvěstí války budou útoky na důležitou infrastrukturu. Elektrická energie, voda, národní finanční systém, doprava, veřejné zdravotnictví, havarijní služba, telekomunikace, to jsou příklady cílů, které mohou být zasaženy. Tato strategie se vyhýbá síle USA, jejím cílem jsou naopak americké slabiny. Jsou překračovány tradiční vojenské hranice. Ovšem cíle nejsou omezeny jen na fyzická zařízení. Kvalitativní obsahová analýza odhaluje, že mezi tyto zbraně autoři řadí i tzv. „genové zbraně" *(gene weapons)*. Genetické zbraně působí na živé organismy, na obilí, dobytek i lidskou populaci. Vzhledem k tomu, že skutečný genetický výzkum je ještě ve svých začátcích a vzhledem k neúspěchům genetického lékařství, o kterých se občas píše v tisku, může mít výzkum a vývoj těchto zbraní v budoucnu pro člověka velmi nepříznivé důsledky [4].

Říše hrozeb

Čistě teoretický aktér, který představuje hrozbu, není tak složitý, co se týče potenciálu a záměrů, jako smíšený typ. Nejkomplexnější aktér by měl mít „nejvyšší a všezahrnující" zbrojní potenciál i strategii. Nejnebezpečnějším potenciálním protivníkem je potom ten, který je

schopný působit v celém spektru konfliktu, v čase, prostoru, intenzitě, má a používá všechny dostupné prostředky, včetně strategické asymetrie a anonymity.

„Říše hrozeb" *(threat kingdom)* není synonymem či nálepkou pro supervelmoc nebo velmoc. Supervelmoci a velmoci mohou být omezovány různými faktory, včetně vlastních právních norem a politických institucí. Ve Spojených státech, jako supervelmoci, se nepokládá vražda za legitimní užití síly. Británie, jako velmoc, nepoužívá geneticky pozměněné biologické zbraně. A tak při vyhodnocování hrozby zde opět vystupuje důležitost rozlišení mezi možnostmi a záměrem. Mnoho aktérů má technologické znalosti a schopnost vyvinout a použít celý svůj potenciál, ale nemá v úmyslu to udělat. Z čehož plyne, že **tím nejnebezpečnějším protivníkem a aktérem v současném mezinárodním bezpečnostním prostředí, kterému musíme čelit, není supervelmoc, ale aktér, který má schopnosti i odhodlání tyto schopnosti použít.**

Cesta („červená" perspektiva), která vede k neomezené válce, závisí na dvou předpokladech: za prvé je to vojenský potenciál, za druhé existence záměru použít jej, bude-li to ospravedlnitelné konečnými cíli. „Tento druh války znamená, že všechny prostředky budou v pohotovosti, že informace budou všudypřítomné a že bojiště bude všude. Znamená to, že všechny zbraně a technologie mohou být zasazeny podle potřeby, znamená to, že **hranice, které leží mezi světem války a ne-války, mezi vojenským a nevojenským, budou naprosto zrušeny.**"

Při vedení ozbrojeného zápasu musíme mít na paměti, že naše konečné cíle omezují používané prostředky. Konečné cíle jsou primární, což tento model nechápe. To ale neznamená, že vztah mezi prostředky a cíli, jak jej analyzovali Liang a Xiangsui, je méně důležitý. V bezpečnostním prostředí proběhlo nesmírné množství změn. Potenciál pro neomezenou válku existuje, a ve svém rozsahu a obsahu se podstatně liší od typu války v Perském zálivu, jejímiž charakteristickými rysy bylo zasazení americké techniky, zpravodajská a technologická převaha. Rozdíl je způsoben různými faktory: zvláště vznikem nových technologií, ale také změnou systémové struktury, nástupem nových aktérů, s netradičními motivacemi, útoky na neutrální cíle („modrá" místa zranitelnosti). Tato formulovaná koncepce neomezené války velmi pomáhá při analýze možných hrozeb, prostředků, cílů a konečných cílů příští války.

Pěti nejčastěji citovanými aktéry hrozeb *(threat actors)* podle čínských strategických vizí neomezené války jsou: (1) autonomní teroristické organizace, (2) pracovníci informační války, (3) státy, (4) hackeři a (5) státy podporované teroristické organizace. Nezávislá teroristická organizace *(autonomous terrorist organization)* je definována jako skupina, která má politické cíle i motivy, je násilná, nebo násilím hrozí, provádí operace, které mají dalekosáhlý psychologický efekt, přesahující bezprostřední oběti nebo cíl, má neidentifikovatelnou organizační strukturu, respektive konspirační buňky (členové nenosí uniformu nebo rozlišovací odznaky), je to subnárodní organizace či nestátní entita [5]. Pracovníci informační války *(information warfare team)* jsou definováni jako skupina utvořená buď státními, nebo nestátními aktéry za účelem vedení informačních operací, jako jejich hlavního úkolu. Nemusí to být stálá skupina, může být tvořena *ad hoc*, jen pro určitý úkol. Státem podporované teroristické organizace *(state-sponsored terrorist organizations)* jsou skupiny, které mají podobné rysy jako autonomní teroristické organizace, ale navíc dostávají logistickou, výcvikovou, zpravodajskou a jinou pomoc od určitého státu. Útoky jsou prováděny za operačního vedení podporujícího státu.

Pěti nejběžnějšími prostředky jsou kybernetické útoky, informační operace, ekonomické útoky, pumové atentáty a přímá akce. Kybernetický útok je definován jako koordinovaný útok na počítačovou síť *(CNA - computer network attack)*, proti systémům, které má omezit, poškodit, zničit, případně změnit schopnost cílového systému fungovat tak, jak bylo plánováno. Následky jsou dalekosáhlé. Nejčastějším cílem kybernetického útoku bude nejdůležitější (kritická) infrastruktura. Informační operace „zahrnují akce, které mají ovlivňovat informace a informační systémy protivníka, a současně své vlastní informační systémy chránit. Mají za cíl ovlivnit procesy založené na informacích, ať již prováděné lidmi, nebo automatizované".

Tento způsob analýzy informací využívá metod informačních operací americké vojenské doktríny minus složka CNA. Převládá zde kybernetický útok, který se odlišuje od všech ostatních informačních operací, jako je např. klamání, a proto musí mít svoje zvláštní označení. Dalším taxonomickým pojmem je „ekonomický útok" **(obr. 3)**, který je definován jako útok na

ekonomické zájmy protivníka, prostřednictvím ekonomických sankcí, zmrazením finančních a dalších položek, měnová destabilizace či nepřátelské obchodní praktiky, např. dumping zboží. „Pumové útoky" *(bombing)* budou prováděny nekonvenčními náložemi. Nejsou to letecké nálety jako při otevřeném konfliktu. „Přímá akce" je přímý fyzický útok na cíl, ať již jej provedou uniformované složky, ozbrojené síly nebo gerilové či teroristické oddíly. Vzhledem k těmto skutečnostem, příští válka nezůstane omezena na fyzickou vojenskou konfrontaci mezi uniformovanými ozbrojenými silami. Analýzy spíše ukazují, že vzájemně se doplňující fyzické a nefyzické prostředky budou okamžitě zasazeny do konfliktu.

Počet cílů, o kterých se zmiňují činští autoři, je relativně malý. Nejvíce zdůrazňovaným cílem je americký bankovní a finanční systém. Druhým je obchod, velké korporace, které tvoří jádro americké ekonomiky, ať již skutečné, nebo symbolické. Že se jedná o skutečné ohrožení potvrzuje fakt, že zahraniční zpravodajské služby určují za možný vojenský cíl americké korporace, aby poskytly svým vlastním národním společnostem konkurenční výhodu. Třetím cílem je americká populace a čtvrtým systémy, které společně vytvářejí tu nejdůležitější (kritickou) americkou infrastrukturu, jak je popsána v prezidentské směrnici č. 63 [6]. Bankovní a finanční systém je jednou z mnoha složek kritické infrastruktury, ale jejich význam vyžaduje, aby byly vedeny jako samostatný cíl. Tyto vybrané cíle naznačují strategii, která obchází a současně útočí na důležité prvky infrastruktury a obyvatelstvo. Spolu s asymetrickými a anonymními metodami může tento způsob vedení války způsobit značné škody. Bez možnosti identifikace nepřítele je totiž odveta nesmírně obtížná. Schopnost ohrozit tímto způsobem americké území dává protivníkovi potenciál strategického odstrašení. A vliv amerických zbraní a diplomacie z pozice síly se snižuje, pokud může protivník zasáhnout americkou infrastrukturu a obyvatelstvo.

Pět nejvíce citovaných konečných cílů v případě konfliktu je získání národní bezpečnostní výhody, ekonomické výhody, finanční zisk, politický vliv a politická změna. Národní bezpečnostní výhoda je definována jako cíl získání převahy nad protivníkem k zajištění bezpečnosti státního či nestátního aktéra. Tato výhoda může být hmatatelná či nehmatatelná, v jakékoli podobě. Ekonomická výhoda je definována jako získání konkurenční převahy v ekonomické oblasti díky státnímu nebo nestátnímu aktérovi. Finanční zisk je definován jako získání bohatství ve formě měny, zboží či dalších předmětů, se kterými se obchoduje. Politický vliv je definován jako získání vlivu v politickém systému na podporu zájmů aktéra sledujícího určitou strategii. Politická změna je definována jako způsobení podstatné změny v politické struktuře druhého aktéra, díky promyšlené strategii, používající jakékoli mocenské nástroje.

Konečný cíl překračuje všechny čtyři skupiny mocenských prostředků: vojenské (národní bezpečnostní výhoda), ekonomické (ekonomická převaha/zisk), diplomatické/politické (politická změna) a informační (politický vliv). Z hlediska možné konfrontace (červená perspektiva), stojí každý cíl za to, abychom se pokusili jej dosáhnout. Bez ohledu na demonstrovaná ohrožení, použité prostředky nebo zvolené cíle, tato prognóza popisuje racionálního aktéra usilujícího o **maximalizaci své moci.** Jsou-li jeho operace odhaleny, tato charakteristika relativně usnadňuje odhad jeho záměrů, ať již sleduje jakoukoli strategii. Na **obr. 3** je tento vztah, mezi: hrozbami → prostředky → cíli → konečnými cíli, vysvětlen.

Hrozby (threats), prostředky (means), cíle (targets) a konečné cíle (ends)			
hrozba	prostředek	cíl	konečný cíl
anonymní teroristické organizace	kybernetický útok	bankovnictví a finance	bezpečnostní výhoda
pracovníci informační války	informační operace	obchod	ekonomická výhoda
stát	ekonomické útoky	obyvatelstvo	finanční zisk
počítačoví hackeři	pumový útok	kritická infrastruktura	politický vliv
státem sponzorovaný terorismus	přímá akce	kritická infrastruktura	politická změna

Obr. 3

Po provedené analýze textu nám zpracovaná data ukáží jejich vzájemné vztahy. Například pro analytika, zajímajícího se o vztahy mezi prostředky, sloužícími k dosažení daného cíle, by bylo vhodné zaměřit se na četnost termínů spjatých s prostředky. Tyto vazby by ukázaly, které prostředky jsou pro získání určitého cíle preferovány. Existuje nekonečné množství permutací a kombinací, které mohou být analyzovány, ale je třeba dbát, aby nebyly analyzovány bez ohledu na pochopení aktéra, jejich původní zdroj a zásady pro shromažďování údajů týkajících se bezpečnostní politiky. Další manipulace s vybraným daty *(extracted data)* může znamenat konec relevantní zpravodajské analýzy. Opětně zpracovávaná a probraná data, mohou snižovat hodnotu kvalitativní analýzy. V určitém okamžiku další manipulace s daty sice může poskytovat přesvědčivou statistiku o tom, co bylo řečeno, ale neprospívá pochopení toho, co bylo zamýšleno. Kdy tento okamžik nastane závisí na zdroji, ze kterého analytik vychází. Kvalitativní analýza je účinnou pomůckou, ale získávání zpravodajských informací vyžaduje také zdravý rozum a úsudek.

Čínští stratégové nejčastěji uvádějí řadu (řetězec) ve formě: hrozby → prostředek → cíl → konečný cíl, čemuž odpovídá řada: stát → ekonomický útok → bankovnictví a finance/obchod → ekonomická výhoda. To svědčí jen o tom, že ekonomické otázky jsou pokládány za natolik důležité, že mohou zažehnou i určitou formu konfliktu, jehož cílem by byla změna relativní ekonomické síly jednotlivých aktérů. Klíčovými cíli jsou zde bankovnictví, finance a obchod. Pro Ameriku by byl efektivní útok na její finanční infrastrukturu katastrofou. Naproti tomu obchod v Americe nepředstavuje klíčový cíl, protože není přímo spjat se státem. Čínští vojenští stratégové se dívají na podobné systémy, jako je ten americký, jako na vysoce centralizované, ale křehké. Co se týče některých vybraných systémů, pak mají pravdu. Ale celková infrastruktura je tak rozsáhlá, až nadbytečně velká, navíc je flexibilní a schopná regenerace. Systémová analýza jednotlivých cílových infrastruktur by mohla odhalit jejich charakter a zranitelná místa.

Interpretace této řady (jako ostatně všech řad, které vznikly z kvalitativní analýzy) by neměla být nepružná. V textu, který tvoří její podklad, jsou odkazy na ekonomickou špionáž, na pomoc, kterou poskytují soukromé korporace státním zpravodajským agenturám, na ekonomický potenciál jako nástroj regionální politické kontroly, ekonomické ohrožení atd. Podstata je v tom, že při vedení neomezené války je hlavním cílem **fungování ekonomiky státu** - ne jeho ozbrojené síly.

Na druhém místě je řada (řetězec): informační válka → pracovníci informační války/stát → kybernetický úder → kritická infrastruktura → národní bezpečnostní výhoda. Tato řada zvyšuje intenzitu konfliktu, tím, že se dotýká širokého spektra, které má fyzické důsledky. Jejím konečným cílem je také národní bezpečnostní výhoda, protože jednotlivými vojenskými a diplomatickými opatřeními zlepšuje relativní mocenský poměr. Zaměření se na kritickou infrastrukturu odpovídá strategii vyhýbání se síle a útočení na slabá místa.

Vzhledem k uvedeným faktům by nás nemělo překvapit, že tato prognóza je zaměřena hlavně na stát, jak svými závěry, tak shromážděnými daty. Je to tím, že v této řadě (řetězci) je konflikt iniciován státem, který působí jen jako skrytý aktér, ale navenek vystupuje jiný aktér, takže cílový stát povede „šedou" válku s neznámými aktéry. Žádný z výše uvedených příkladů netvrdí, že stát musí zůstat skrytý, ale analýza obou uvedených řad (řetězců) ukazuje, že počáteční fází konfliktu bude překvapivý útok, který provede skrytý aktér.

Je možné zjistit i další vztahy a vazby, ale i tento malý příklad ukazuje, jak může být kvalitativní analýza užitečná. Může poskytovat analytikovi řadu cenných informací a zvyšovat jeho pochopení problému. Jednou z interpretací by mohl být závěr, že v případě války s Čínou bude proveden útok na americké soukromé i státní ekonomické cíle, pravděpodobně současně s tímto útokem bude proveden úder na počítačovou síť a kritickou infrastrukturu. To je už zcela jiný scénář, než jaký mají ozbrojené síly rozmístěné po obou stranách tchajwanské úžiny. Představuje daleko větší balancování na pokraji války, než během raketové kubánské krize v r. 1962.

V dnešním, zcela změněném bezpečnostním prostředí je textová analýza nutná i pro chápání mírových i válečných prognóz („modré" a „červené" perspektivy). Je nezbytným předpokladem pro tvorbu efektivní národní bezpečnostní politiky. Také v průběhu konfliktu může být kvalitativní analýza hodnotným zdrojem informací, která dokáže zdůvodnit ofenzivní nebo defenzivní užití ozbrojených sil. Rozbor textů a údajů je také jedním z důležitých prvků zpravodajské práce při vypracovávání charakteristik cílů.

Pomocí kvalitativní analýzy můžeme vytvořit model jakéhokoli aktéra, ať již jde o státní organizaci nebo teroristickou skupinu. Zdrojem dat může být třeba programový manifest nebo webbová stránka. Mohou být vytvořeny mírové, neutrální nebo válečné (modré, šedé nebo červené) prognózy, které nám tak či onak pomohou zvýšit bezpečnost. Kvalitativní analýza může sloužit i jako zrcadlo, které ukazuje jak nás vnímají jiní.

„Neomezená válka" zde byla použita jako názorný příklad. Není to oficiální čínská doktrína příští války, jsou to jen úvahy čínských vojenských teoretiků. Kniha se zabývá povahou možné války mezi Čínou a Spojenými státy a odráží se v ní postoje dvou čínských důstojníků. Rozbor takových dokumentů nám ale umožňuje pohlédnout na problémy zevnitř, očima protivníků. Metodou, technikou jak toho dosáhnout, je kvalitativní analýza hrozeb.

Pokud nemáme jasný a spolehlivý popis budoucí politiky určitého aktéra, dalším zdrojem informací jsou otevřené, běžně přístupné zdroje *(open sources)*, jako jsou projevy, články v časopisech, knihy, rozhory a politické dokumenty. Kvalitativní analýza se neomezuje jen na text, ale může zahrnovat nejrozličnější prameny, od video přenosů k zachyceným telefonním rozhovorům. Při určování záměrů protivníka se nelze řídit hodnotou jednoho jediného informačního zdroje. Text a jeho analýza mohou prověřit všechny dostupné informační zdroje, v reálném čase, nebo archivované, vybrané klíčové informace z informačních shluků a utřídit schémata a vazby, které nejsou přístupné běžným analytickým technikám.

Určování záměru je velmi obtížné. V současném bezpečnostním prostředí, kde je značný objem zbraní nejrůznějšího druhu rozšiřován bez jakékoli kontroly, musí být odhady potenciálu protivníka velmi opatrné. A klíčovým prvkem při identifikaci možných hrozeb je určení záměru.

Poznámky:

1. **David Singer:** Threat-Perception and the Armament Tension Dilemma. Journal of Conflict Resolution, March 1958.
2. Tyto principy obecně popisují to, čemu se říká realistické perspektivy mezinárodního systému. Existují ale i další perspektivy. Viz Classic Readings of International Relations, 2nd Editon, Harcourt Brace College Publishers, New York 1999.
3. **Qiao Linag, Wang Xiangsui:** Unrestricted Warfare (trans. Foreign Broadcast Information Service). Beijing, China, February 1999. Texty v uvozovkách jsou citace z této knihy.
4. Dokonce i genetický výzkum zaměřený na léčbu ve vyspělých zemích může dopadnout špatně, jak ukazuje smrt 18leté Jesse Gelsinger, která byla podrobena genové léčbě, která měla odstranit její zdravotní obtíže na Institutu pro genovou terapii při Pennsylvánské univerzitě. Přitom „genové zbraně" nemají pomáhat léčit, ale způsobit škody ve velkém měřítku, což může mít katastrofální následky. Např. v dubnu 1979 byl zaznamenán únik antracitu v tajné sovětské laboratoři sloužící vývoji biologických zbraní poblíž Sverdlovska. Přesný rozsah není znám, ale měl za následek stovky, možná tisíce úmrtí. (P. J. Jackson, PCR Analysis of Tissue Samples from the 1979 Sverdlovsk Anthrax Victims, Proceedings of the National Academy of Sciences, February 1998.)
5. **Bruce Hoffman:** Inside Terrorism. Columbia University Press, New York 1998.
6. Americká kritická infrastruktura se skládá z klíčových sektorů, nezbytných pro minimální fungování ekonomiky a vládního aparátu, která mají bezprostřední dopad na americké obyvatelstvo. Tato infrastruktura je tvořena informačními a komunikačními prostředky, funkčními vládními, bankovními a finančními službami, jsou zde zařízení na zásobování vodou, elektrickou energii, ropou a zemním plynem, doprava, orgány pro řešení přírodních katastrof, průmyslových havárií ap., veřejná zdravotní služba. Presidental Decision Directive 63. Washington, D.C., 22 May 1998.

Threat Kingdom, Lt.Col. Bill Flynt
Military Revue, July-August 2000
red. zkráceno, upraveno