Získávání zpravodajských údajů o asymetrických ohroženích

Časopis Jane's Intelligence Review ve svých číslech 10 a 11 v roce 2000 uveřejnil článek autorů Kevina O'Briena a Josepha Nusbauma popisující změněné bezpečnostní problémy a vznik nových ohrožení po skončení studené války. Z jejich změn vyplývají nové problémy pro zpravodajské orgány. Článek byl zkrácen a redakčně upraven. Jeho obsah je po válce USA proti organizaci Al Kajda velmi aktuální. Vysvětluje povahu asymetrických ohrožení, jak se vyvinula v posledním desetiletí, a jak ovlivňují bezpečnost rozvinutého světa, problémy, které z nich vyplývají pro jeho bezpečnostní orgány a obranu, a konečně požadavky na zpravodajské orgány, jež musí na asymetrická ohrožení, včetně informačních operací a kybernetického ohrožení, reagovat, a vzhledem k nim rozšířit svou působnost.

Na mezinárodní bezpečnostní problémy a na povahu činitelů ohrožujících dnešní svět měly a mají velký vliv globalizace, liberalizace (ve dříve autokratických státech), rozšiřující se privatizace státních funkcí a – což je nejdůležitější – revoluce ve výpočetní technice, telekomunikacích a v přenosu dat, tzv. informační revoluce. Tito činitelé mají také významný vliv na vojenské zpravodajství, na požadavky, jež jsou na něj kladeny, na využívání zpravodajských údajů, protože společnost je stále více otevřená a informace se přenášejí po celém světě pouhým „kliknutím na myš".

V souvislosti s tím byl zaveden pojem „asymetrické ohrožení", který pokrývá určité typy ohrožení, vzniklých zhruba po roce 1990, jež představují zejména pro západní, tj. demokratické vlády a jejich obranné a bezpečnostní instituce značné nebezpečí. Není to jen možnost velké konvenční války proti mocnostem rozvinutého světa, nýbrž stejná nebo větší nebezpečí pro obyvatelstvo a vlády těchto států.

Svět stojí před rozšiřováním konfliktů nízké intenzity, včetně konfliktů vedených chemickými, biologickými a radiologickými zbraněmi v rukou stále většího počtu extrémistických skupin. Zvýšil se počet bezohledných útoků vedených každodenně po celém světě. Pro předvídání, analýzu a vyšetřování takových ohrožení je nutno porozumět okolnostem, za nichž se mohou asymetrická ohrožení rozvíjet. Z toho vyplývají úkoly zpravodajských orgánů.

Přeměna starých ohrožení

Asymetrické ohrožení spočívá v tom, že se jedna strana snaží využít svých relativních výhod proti slabým místům protivníka. Obecně **asymetrické ohrožení** znamená, že jedna strana není vzhledem ke své slabosti nebo vzhledem k protistojící síle schopna čelit protivníku konvenčním způsobem, s použitím prostředků nebo zbraní protivníka. Proto volí nekonvenční přístup.

Protivník bude volit zbraně a taktiku, včetně překvapení. Bude to neočekávaný způsob nebo způsob, jemuž lze obtížně čelit. Jeho smyslem je snížit nebo překonat technologickou převahu soupeře, nebo nad ním získat převahu. Asymetrické útoky zpravidla využívají zranitelných

míst. Protivník může volit strategii, která od základu změní prostor, v němž bude konflikt veden. Protivník může např. operovat v podmínkách velkých měst, čímž se sníží možnost odvety: v zastavěném terénu je obtížné zjišťovat a napadat vojensky důležité cíle.

Asymetrická ohrožení se mohou projevovat mnoha způsoby, mohou sledovat různé cíle a mohou používat mnoha způsobů a prostředků pro jejich dosažení. Mohou mít taktické a strategické důsledky.

Na strategické úrovni lze využít obavy civilního obyvatelstva, aby byla oslabena podpora demokratizačních procesů, oslabena vláda nebo ohroženo její spojenectví.

Možnost útoků na mezinárodní síly nebo na občany, majetek anebo území velkých mocností zvyšuje nutnost pružné, a někdy nekonvenční reakce (odpovědi) pro zajištění bezpečnosti zasazených sil, mírových operací anebo západních zájmů.

Na taktické úrovni může protivník nutit druhou stranu, aby změnila svou taktiku (např. využitím obavy západních vlád z vojenských ztrát), nebo vést útoky, jimž mohou západní síly nesnadno předcházet a čelit (teroristické útoky, fyzické anebo elektronické, útoky na důležité prvky infrastruktury). Asymetrický přístup ovlivnění silnějšího protivníka představují mimo ohrožení teroristickými akcemi také občanská neposlušnost a organizovaný zločin.

Skutečný problém a nebezpečí asymetrického vedení války představuje šíření levných nosičů zbraní, zvláště balistických raket, a šíření zbraní hromadného ničení, jakož i možnosti kybernetické a informační války.

Je pravděpodobné, že mnohé konflikty, jimž bude musit v blízké budoucnosti Západ čelit, budou mít asymetrickou povahu. Rovněž lze očekávat, že tato ohrožení budou založena na využití a kombinaci současných zdrojů: např. konvenční terorismus a konflikty nízké intenzity budou provázeny anebo sdruženy s kybernetickými útoky nebo útoky na infrastrukturu, čímž budou vyřazeny důležité komerční, vojenské a vládní informační a komunikační systémy. Útok, ve kterém může velká západní země utrpět značné ztráty, může vést i velmi malá, dobře vycvičená, vybavená a odhodlaná skupina méně než 50 osob. Takový útok by mohl mít účinek zcela neúměrný použitým prostředkům.

Proto je třeba vybudovat značně zdokonalené zpravodajské sítě pro varování před těmito ohroženími a pro zabezpečení odvetných operací. Tradiční zpravodajský proces neposkytuje optimální možnosti pro včasné získávání, zpracování, analýzu, hodnocení a předávání zpravodajských údajů o těchto ohroženích. Je jasné, že navyklé prostředky (stále ještě odpovídající požadavkům studené války) nepředstavují optimální možnost pro obranu proti asymetrickým ohrožením.

I když jsou technologické prostředky stále důležité pro sledování a hodnocení těchto ohrožení, optimální metodou pro získávání zpravodajských údajů o asymetrickém ohrožení je průzkum prováděný osobami *(HUMINT - human intelligence)* a využívání otevřených zdrojů *(OSINT - open source intelligence)*.

Definice asymetrických ohrožení

Asymetrická ohrožení a asymetrická střetnutí či vedení války bývají definovány mnoha způsoby. Asymetrické střetnutí je boj mezi sobě nepodobnými silami, asymetrická válka je vedena s málo a nesnadno stanovenými cíli a zpravidla zahrnuje malé počty působících aktérů anebo sil používajících nekonvenční taktiku, jež mají obvykle velký politický nebo materiální dopad – ve srovnání s úrovní zasazené síly.

Technologická úroveň rozvinutého západního světa ve vědecké a vojenské oblasti je vysoko nad úrovní třetího světa, nicméně technologie, kterou mají k dispozici státy a aktéři rozvojového světa pro použití proti mocnějším státům, lze na světovém trhu snadno zakoupit. Tito aktéři mají přístup nejen k velmi širokému spektru zbraní, přistupuje zde i snadnost cestování a přístup k poznatkům a informacím, jež také zvýšily možnosti asymetrických aktérů, což má velký vliv na vedení války na všech úrovních, od globálního konfliktu po terorismus.

Metoda boje je jednoduchá. Skupina s nižší úrovní technologie použije taktiku zaměřenou na znehodnocení dokonalejších zbrojních a komunikačních technologií protivníka. Protiopatření vysoké i nízké technologické úrovně mohou využívat zranitelných míst moderních západních zbraní a jejich zabezpečovacích systémů.

Integrace informačních systémů do vojenských operací sice poskytuje značné výhody, avšak vytváří také zranitelná místa. K vyřazení důležité národní infrastruktury rozvinutého světa, včetně počítačových sítí, lze použít tzv. **informační válku**, což může ve svých důsledcích paralyzovat veškeré spojení, dopravu, energetické systémy a průmyslové podniky. Jiné informační operace, počítaje v to operace pro ovlivnění řízení a psychologické operace, mohou útočníkům umožnit využívat k ovlivnění západních politiků, jež rozhodují o odvetě, mezinárodní sdělovací prostředky.

Ve své nejhorší formě pak mohou nekonvenční útoky, vedené silami vyzbrojenými chemickými a biologickými látkami, zmařit západní vojenské operace: teroristické útoky proti civilním cílům mohou být podporovány cizími státy, s cílem podkopat podporu veřejnosti intervence v zahraničí, a také aby byly jiné státy odstrašeny od připojení se k západní koalici.

Bezpečnost Západu je ohrožována informačním vedením boje, jadernými, biologickými a chemickými zbraní. Jsou to asymetrická ohrožení, jimiž může protivník poměrně snadno a nenákladně čelit konvenční a jaderné převaze Západu.

Dalšími možnými formami asymetrické války jsou terorismus, varianty guerillových operací a ničení infrastruktury, včetně životního prostředí. Budoucí protivník může použít asymetrické metody k omezení přístupu k důležitým zdrojům a k narušení velitelských, spojovacích a zpravodajských sítí.

Západ bude vzhledem ke svému dominantnímu vojenskému postavení s velikou pravděpodobností cílem četných asymetrických strategií, protože slabší protivníci se budou snažit prosazovat své zájmy, a přitom se vyhýbat přímému střetnutí se západními ozbrojenými silami.

Názor, že asymetrické ohrožení může vycházet pouze od protivníků podle hodnocení Západu slabých, byl zpochybněn nedávnými studiemi uveřejněnými **v Čínské lidové republice, jež považují asymetrické vedení války a její taktiku za klíčové v každém budoucím konfliktu se Západem.**

Čínská armáda uvažuje o metodách jako jsou pronikání do internetových sítí a finančních institucí, terorismus, likvidace osob, využívání sdělovacích prostředků a vedení boje ve městě, což dokazuje její snahu o modernizaci možností informační války. Čínská armáda ví, že se nemůže rovnat Západu v oblasti konvenčních anebo jaderných zbraní, proto klade důraz na vývoj technologií informační a kybernetické války, včetně počítačových virů, aby neutralizovala politickou, ekonomickou a vojenskou informační síť protivníka, jeho infrastrukturu velení a řízení. Čínská lidová armáda označuje takový postup jako „neomezené vedení války". Čína prý může překonat západní *high-tech* senzory, elektronická protiopatření a výzbroj použitím metod informační války. Informační válka může uvést nepřátelský stát ve zmatek a vyvolat

politickou krizi, a to pouhým zavedením virů do jeho počítačových systémů, a tak paralyzovat zásobování elektřinou, řízení dopravy, finanční transakce, telefonní sítě a sítě sdělovacích prostředků.

Asymetrická válka je zaměřena na všechno - na strategii, taktiku, zbraně, personál, takže asymetrické bojiště bude v principu negovat výhody jedné strany. Proto lze asymetrická ohrožení definovat jako **snahu překonat převahu protivníka, a zároveň využít jeho slabých míst**, a to s použitím metod značně odlišných od jeho obvyklého způsobu vedení operací.

Prostředky asymetrického vedení války

V budoucnosti budou protivníci mít k dispozici řadu možností pro odstrašování, poškozování anebo ničení vojenské síly rozvinutého světa. Jejich metody je možno rozdělit do tří souborů:

1. Získání zbraní hromadného ničení, balistických raket nebo střel s plochou dráhou letu. Regionální protivníci mohou hrozit západním silám vojenskou eskalací. I když nebude takové možnosti operačně použito, samotná její existence může oslabit snahu spojenců o vojenský zásah proti regionální agresi.
2. Používání kybernetického vedení boje a nákup vybraných technicky dokonalých senzorů, spojovacích prostředků a zbraňových systémů. To by bylo možno nazvat „strategií skrytého hráče" (strategy of the niche player), při níž mohou být kybernetické zbraně a prostředky použity k vyřazení možností vojenské a civilní informační technologie, jakož i k útokům na informační infrastrukturu k narušení a zničení ekonomiky a infrastruktury západních států, které jsou závislé na informacích.
3. Volba prostředí konfliktu, jako jsou velká města nebo džungle, které jsou nevhodné pro konvenční síly, může znehodnotit západní vojenské možnosti pro zjišťování a ničení vojensky důležitých cílů.

Tyto kategorie – souhrnně označované jako zbraně hromadného ničení, informační operace a nekonvenční operace – existovaly v té či oné formě již dříve, avšak teprve v posledním desetiletí se jejich kombinace, a hlavně skutečnost, že potenciální protivník nemá žádné skrupule těchto zbraní použít, staly mnohem vážnější hrozbou pro celý svět.

Nesmíme ale zapomínat, že i méně složité prostředky pro vedení asymetrického boje jsou stejně účinné, zvláště na taktickém stupni. Mezi příklady **netechnologických prostředků** a metod k nimž se uchylují a jimiž disponují asymetričtí aktéři patří: maskování proti laserem řízeným zbraním, omezení komunikace pro znehodnocení elektronických senzorů, lidské štíty pro ochranu kombatantů, zdroje tepla pro oklamání infračervených senzorů a vedení boje ve městech, kde jsou těžké síly málo použitelné.

Hlavním úkolem obranných a zpravodajských institucí se tak stalo stanovení druhů a úrovní způsobu obrany zájmů a bezpečnosti státu, neboť hrozba rozsáhlé konvenční války v posledním desetiletí ustoupila do pozadí.

Metody a prostředky

Ve výše uvedených souborech existuje řada společných faktorů. Předně, každé ohrožení má několik přijatelných metod dopravy na cíl. Dosah, rychlost a přesnost dopravy se rychle

vyvíjejí, a to ve prospěch útočníka. Zatímco tradiční nosiče zahrnují letadla, řízené i neřízené rakety a speciální síly, alternativní prostředky dopravy pro asymetrickou válku zahrnují aktovky, komerční vozidla nebo kurýry, veřejné dopravní prostředky či soukromá vozidla, letadla anebo plavidla. Je nutno poznamenat, že většina ničivých asymetrických útoků byla uskutečněna nevojenskými prostředky dopravy.

Podobně tato ohrožení souvisí s nákupem technicky vyspělých senzorů, spojovacích prostředků a zbraňových systémů rizikovými státy *(rogue states)* a nestátními aktéry, jako jsou nadnárodní zločinecké organizace. Využívání civilních zdrojů – internet a komerční družicové snímky, jakož i šíření moderních zbraní – umožňují asymetrickým aktérům dokonalé operační plánování, přesnou volbu cílů a způsobení větších škod.

A konečně, vyspělý západní svět usnadňuje asymetrickým aktérům jejich činnost nadměrným spoléháním se na velký objem informací poskytovaných neregulovaným internetem. Ve většině případů se obyvatelstvo a vlády západních zemí téměř úplně spoléhají na národní informační infrastruktury tvořené vládními a komerčními počítačovými servery, telekomunikačními zařízeními a poskytovateli internetových služeb. Všechna tato zařízení představují vhodné cíle asymetrického útoku. Shrnuto: reakce na potenciálně zhoubný kybernetický útok se dnes stala jednou z klíčových priorit většiny vlád rozvinutého světa.

Informační operace

Zranitelnost vyspělých států kybernetickými informačními operacemi a tradičními informačními operacemi, jako je psychologická válka, se znatelně zvýšila. Je ironií, že čím více se svět „digitalizuje", je technologicky dokonalejší, tím je zranitelnější.

Zvláště ve vojenské a vládní oblasti je situace alarmující. Počítači řízené zbraňové systémy se používají k přesným úderům, e-mail slouží k vojenskému spojení a logistické procesy jsou digitalizovány. Všechna tato zařízení mohou být využita nejen odborníky, ale i hackery a cizími vojenskými narušiteli.

Používání netechnických informačních operací proti mnohem výkonnějším a technicky vyspělejším konvenčním silám bylo demonstrováno během operace v Kosovu, kdy Bělehrad v podstatě vyhrál psychologickou operaci proti NATO (PSYOP) i operace založené na znalosti situace.

Existuje nebezpečí, že během cizí intervence mohou asymetričtí protivníci používat informační operace ve strategickém měřítku, tj. v kybernetické oblasti a v psychologicko-politické oblasti, k rozsáhlému narušení občanské společnosti. Kybernetická válka může zpomalit rozhodovací proces příslušné vlády. Velké publicity se dnes dostává amatérským hackerům, ale reálným ohrožení jsou ve skutečnosti profesionálové nebo kybernetičtí bojovníci. Amatérští hackeři mají málo důvodů k přemísťování, lze je proto snadno odhalit, ale profesionálové mohou být velmi mobilní. Z tohoto důvodu jsou důležité mj. jejich vazby na nadnárodní skupiny organizovaného zločinu.

Informační operace jsou akce vedené pro ovlivňování rozhodovacích činitelů působením na informace a informační systémy „druhých", při současné ochraně vlastních informací a informačních systémů. Cíle obecně zahrnují: velké prvky národního hospodářství - veřejné komunikační sítě, finanční a bankovní systém, rozvod elektřiny, ropovody a plynovody, národní dopravní systém včetně letecké dopravy.

Vedení ofenzivních informačních operací je jasnou asymetrickou hrozbou pro Západ, který se stále více spoléhá na informace a informační systémy jako důležitou složku rozho-

dování. To pro organizace anebo jednotlivce s nepřátelskými úmysly vytváří řadu vhodných možností jak narušovat nebo likvidovat infrastrukturu západní společnosti, což by mohlo mít – zejména v kombinaci s použitím zbraní hromadného ničení nebo teroristickými akcemi – zhoubné následky. Například vyřazení městského tísňového telefonního systému kybernetickým útokem by se současným roznětem teroristických bomb a narušením sdělovacích prostředků mohlo vytvořit asymetrickou synergii, takže by jednotlivé útoky byly mnohem a mnohem účinnější, než kdyby byly provedeny jednotlivě.

Informační operace se tradičně užívají k infiltraci do vojenských anebo civilních informačních systémů, včetně systémů používaných pro velení, řízení, spojení a logistiku, a to ke změně dat, nebo k útoku na národní strategickou infrastrukturu, např. narušením důležitých systémů, jako je mezinárodní systém řízení letového provozu.

Ofenzivní informační operace je možné rozdělit do tří hlavních kategorií:

1. Útoky na infrastrukturu způsobí poškození, znehodnocení informací, anebo informačních systémů, případně naruší jejich provoz. Zahrnují široké spektrum operací, včetně útoků na počítačové sítě, elektronický boj a fyzické ničení, a to od řádění hackerů ve veřejném internetu až po koordinované zpravodajství, infiltraci, manipulaci dat, nebo znemožnění přístupu k vládním informačním systémům.
2. Klamání je určeno k uvedení nepřítele v omyl manipulací, zkreslením nebo falšováním důkazů, aby byl přinucen reagovat způsobem škodícím svým zájmům. To může zahrnovat cílené manipulace sdělovacích prostředků, jako jsou propagandistické operace ve veřejných komunikačních kanálech (televize, rozhlas, internet), jakož i klamné informace a podvody, někdy využívající výhod, jež poskytuje vyspělá technologie pro manipulaci s informacemi, video i audio a počítačové animace.
3. Psychologické operace jako schopnost ovlivňovat vůli jiné společnosti. To zahrnuje politická anebo diplomatická pracoviště, prohlášení nebo komuniké, jakož i šíření letáků, rádiové nebo televizní vysílání a jiné prostředky šíření informací, vyvolávající strach anebo rozkol, přičemž jsou takové zprávy podporovány akcemi, jako je např. braní rukojmích anebo hrozba hromadných ztrát.

Je zajímavé, že kybernetický terorismus je zaměřen nejen na poškozování systémů, ale také na získávání zpravodajských údajů. Přílišné soustředění se na ničivé strategie ignoruje jiné, potenciálně účinnější používání informačních technologií pro teroristický boj, a to získávání zpravodajských údajů, kontrašpionáž a dezinformace. Konflikt ve formě kybernetické války, který by setřel konvenční hranice mezi zločinem a válkou, je přitažlivý pro protivníka, který nevidí žádnou strategickou výhodu v přímém vojenském střetnutí se Západem.

Nekonvenční operace

Konvenční organizovaná válka je – alespoň v technologicky vyspělém světě – mezi konvenčními mocnostmi rychle nahrazována konflikty nízké intenzity. Jaderná výzbroj téměř vyloučila možnost konfliktu mezi velmocemi, vzhledem k obavám z eskalace, a pokrok v konvenční palebné síle států vyspělého světa proti státům rozvojového světa ponechává velmi málo prostoru pro koncepci tradiční konvenční války mezi státy. Když se konflikt nízké intenzity stává dominantním rysem války ve 21. století, povaha vedení války se rovněž mění.

Západní mocnosti jsou nuceny čelit tomuto novému ohrožení regionální stability. Vzájemné působení a vazby mezi takovými konflikty a nadnárodním obchodem s narkotiky, zbraněmi, jaderným materiálem a lidmi na jedné straně, a terorismem na straně druhé, jsou téměř nerozpoznatelné.

Terorismus je ve své povaze asymetrický a dosahuje výsledky podobné vojenským proti síle, která má převahu, relativně levně a s malými vlastními ztrátami na životech. Aktéři mohou používat terorismus na strategické i taktické úrovni. Nedávné teroristické útoky dokazují zranitelnost moderních společností právě takovými formami asymetrického útoku.

Nekonvenční operace mohou zahrnovat: používání složitého terénu, nové taktiky a technologie (taktika „udeř a uteč"), boj v rozsáhlých městských oblastech (kde je identifikace útočníků ztěžována velkými počty civilních diváků a kde může být protiútok spojen s rizikem dalších civilních ztrát), moderní trhavou munici (jež může usnadnit přímé útoky na západní vojenské síly, maximalizovat fyzický a psychologický účinek útoku a zabránit vojenské a policejní odvetě).

Ekonomické poruchy jsou další taktikou, včetně útoků na výrobní prostředky, na konečné produkty a na komerční infrastrukturu. Tím může být snížena národní produktivita, což může vést k vážnému materiálnímu nedostatku, a tak přímo negativně ovlivnit obyvatelstvo. Používá se také taktiky občanské neposlušnosti: demonstrace, ilegální okupace závodů, bojkot, nepokoje pro destabilizaci nebo diskreditaci vlády anebo jejích bezpečnostních sil.

Teror je též primárním nástrojem asymetrického vedení války: působení proti nekombatantům v místech, kde se o útocích dříve nikdy ani neuvažovalo, nebo braní rukojmí vyvolají mezi obyvatelstvem strach neúměrný riziku nebo výdajům útočníků. Tím jsou opět eliminovány výhody západních vojenských a bezpečnostních sil. Bojové prostředky používané za podobných operací vedou od dýky, přes podomácku vyrobené pumy, až po široké spektrum vojenských zbraní a munice.

Zbraně hromadného ničení

Zbraně hromadného ničení, jejich šíření a prostředky dopravy, představují velmi nebezpečné asymetrické ohrožení. Způsobují hromadné ztráty, vyvolávají strach a mohou ohrozit morálku obyvatelstva i armády. Je možné, že některé z těchto zbraní budou vyrábět jednotlivci, a tento faktor jen zvětší rozsah potenciálního ohrožení. Již to nejsou jen „odstrašující zbraně", jako tomu bylo v dobách studené války, nýbrž jsou to zbraně, jejichž pravděpodobnost použití vojenskými mocnostmi „druhého řádu" a nestátními skupinami se stále zvyšuje.

Nákup zbraní hromadného ničení potenciálními protivníky vybavenými nebo nevybavenými nosiči dalekého dosahu, jako jsou balistické rakety anebo střely s plochou dráhou letu, může ohrožovat západní státy anebo rozvinuté spojenecké síly formou vojenské eskalace. Disponibilita a přítomnost těchto zbraňových systémů jsou také důležitým faktorem, protože už jen pouhá samotná hrozba, i bez přímého operačního použití, může působit jako odstrašující činitel pro zasazení a operace jednotek a dokonce pro akce k udržování míru. Hrozba použitím zbraní hromadného ničení může vytvářet strategické a politické účinky, které převáží jejich vojenskou užitečnost. Odtud i snaha Spojených států zabránit, aby se tyto zbraně staly součástí vojenského arzenálu Iráku.

Chemické zbraně jsou levné, snadno se vyrábějí a jsou vždy pohotově k použití. Jejich šíření je snadné. Informace o jejich výrobě je k dispozici na internetu a tyto výrobní techno-

logie jsou často dvojího použití (komerčního i vojenského). Suroviny pro výrobu chemických zbraní jsou k dispozici všude.

Výroba **biologických látek** je snazší a levnější než jaderných nebo chemických zbraní. Jistou nevýhodou je jejich nestabilita. Biologické látky mohou způsobit ztráty v rozsahu podobném ztrátám způsobeným jadernými zbraněmi, nebo mohou ohrozit zásobování potravinami. Biologické zbraně je nutno považovat za atraktivní pro potenciální protivníky.

Rizikové státy a nestátní aktéři budou pravděpodobně v programech výzkumu a výroby těchto zbraní pokračovat. Důležitým novým faktorem je, že rizikové státy vlastně ani nemusí mít velké zásoby např. chemických zbraní, jež byly vyráběny během studené války, protože pro teroristickou činnost postačují malá množství těchto látek.

Také **jaderné zbraně** přicházejí v úvahu pro asymetrické útoky. Existuje sedm známých jaderných států, ale je pravděpodobné, že v blízké budoucnosti získají tyto zbraně i další státy, jež chtějí zvýšit svůj bojový potenciál. V dohledné perspektivě západní státy ohroženy jaderným útokem zřejmě nebudou, avšak vzhledem k ničivým účinkům jaderného útoku nelze tuto možnost přehlížet, zvláště když spojenecké síly působící v zámoří mohou být vystaveny účinkům jaderných zbraní použitých při jaderné „výměně" mezi zeměmi, v nichž se jaderné zbraně šíří. Zde je možné jako příklad uvést Indii a Pákistán.

Bojové prostředky založené na **radioaktivních látkách** mohou být vyráběny poměrně snadno a levně. Vždyť řada zemí, včetně těch nestabilních, má k dispozici jadernou technologii. Z toho vyplývá nebezpečí, že radioaktivní látky nebo prostředky vytvářející radiaci mohou být použity k vyvolání ztrát nebo k zabránění v používání terénu nebo objektů.

Zbraně hromadného ničení mohou být zasazeny i méně ničivým způsobem. Např. jaderná zbraň může být použita k vytvoření tzv. **elektromagnetického impulzu**, který v rozhodující fázi vojenské operace v rozsáhlém prostoru naruší, respektive zcela vyřadí, soustavu prostředků velení, řízení, spojení, pozorování a průzkumu možného protivníka.

Neschopnost řešit problém

Zatímco byla nezbytnost zpravodajských údajů o šíření zbraní hromadného ničení, o nadnárodním organizovaném zločinu a nekonvenčních operacích v odborné literatuře rozsáhle popsána, málo pozornosti bylo zatím věnováno úloze zpravodajství při obraně proti ofenzivním informačním operacím, zvláště proti kybernetickým útokům.

Na operační úrovni se vlády tradičně staví k terorismu (za který je kybernetické ohrožení většinou považováno) jako k problému v podstatě taktickému, nikoli strategickému. Takový přístup je zastaralý. Operační úroveň je zaměřena na konvenční metody získávání zpravodajských údajů, které používají omezených pracovních postupů, vyjadřujících potřebu reagovat na teroristická ohrožení na taktické úrovni. Avšak jakmile je společnost stále více odkázána na informační technologii a telekomunikace, objevilo se vedení informační války jako prostředek použitelný v budoucím konfliktu.

Kybernetický terorismus je logickou aplikací informačního vedení války. V souvislosti se šířením počítačových sítí a komunikačních systémů jsou fyzické útoky na Západ méně pravděpodobné než kybernetické útoky. Velká pozornost byla věnována kybernetickým teroristickým útokům na důležité informační infrastruktury, jako hlavnímu způsobu budoucí asymetrické války. Nedávné útoky hackerů a virů to nejen potvrdily, ale zároveň ukázaly na zranitelná místa elektronických sítí a systémů. V obraně proti nim bylo dosaženo

bohužel relativně málo. Při daném rozptýleném a redundantním uspořádání takových sítí a při znalosti rizika, které tyto útoky přinesly, je možné, že toto ohrožení bylo přeceněno. Nikomu se dosud nepodařilo (nic nevylučuje, že se to může podařit v budoucnu) zcela narušit nebo zničit důležité infrastruktury státu.

Tím není řečeno, že tradiční teroristické útoky pomocí trhavin zaniknou, zvláště když se objevil jiný objekt útoku. Tímto objektem je **národní informační infrastruktura**, definovaná jako soustava moderních počítačových systémů, bází dat a telekomunikačních sítí, která činí elektronickou informaci rozsáhle disponibilní a přístupnou. Zahrnuje internet, veřejnou přepínanou síť a kabely, bezdrátové a družicové spojení. Protože se moderní společnost spoléhá na svou informační infrastrukturu, její každé větší narušení může mít vliv na národní hospodářství, jakož i na jednotlivá ministerstva anebo podniky. Národní informační infrastruktury ale nebývají budovány se zřetelem k jejich bezpečnosti, takže zatímco některé jejich části jsou velmi bezpečné, celkově jsou informační infrastruktury velmi zranitelné: narušením buď fyzickým, anebo kybernetickým útokem vedeným hackery, teroristy nebo cizími vládami.

Hackeři soustavně dokazují, že domněle bezpečné vládní a komerční systémy nejsou zas tak chráněné, jak se oficiálně tvrdí. Ovšem zde je nutno připomenout, že většina hackerů pochází z právě té organizace, ve které se jim podařilo obejít bezpečnostní opatření, jsou uvnitř organizace. A příklad jejich využití během konfliktu? V Kosovu v roce 1999 byla v Srbsku z profesionálů z Evropy a Severní Ameriky vytvořena síť hackerů pro útoky na webové stránky a počítačové sítě NATO a spojeneckých vlád.

Před několika léty vypracovalo Mezinárodní středisko pro analýzu bezpečnosti (ICSA) výcvikovou metodu pro zpravodajství v oblasti kybernetického zločinu a informační války. Tato metoda je obsažena v „systému hodnocení informačních útoků" (IWAAS) a tvoří rámec pro hodnocení ohrožení a systém včasného varování pro defenzivní informační válku. Systém hodnocení informačních útoků má tři úkoly:

- hodnotit ohrožení informační válkou (vytvářené různými aktéry),
- oznamovat příznaky a poskytovat výstrahu o informačním útoku,
- předpovídat způsoby jednání nepřítele.

Tento systém definuje zpravodajství o informační válce jako schopnost shromažďovat, hodnotit a předávat data pro dosažení určitých vojenských a politických výsledků týkajících se informační války. Hlavním účelem zpravodajství je **vyloučit strategické překvapení**. Takové překvapení lze dosáhnout (zvláště v asymetrickém smyslu, kdy je dosažení výhody velmi důležité) na třech úrovních:

- diplomatické překvapení neočekávanou nebo zásadní změnou politiky,
- vojenské překvapení neočekávanou taktickou nebo strategickou ofenzivou,
- technologické překvapení, kde neočekávané zavedení nových zbraní nebo jiné technologie od základu změní rovnováhu (toto překvapení je největším rizikem pro zpravodajství v oblasti informační války).

Většina analytiků posuzovala asymetrické kybernetické ohrožení stejným způsobem jako terorismus. Tato krátkozrakost vedla ke standardním požadavkům na zdokonalení opatření pro obranu proti této nové „teroristické" hrozbě a k volání po „dokonalejším zpravodajství". Jen málokteří pochopili, že je třeba provést další krok a popsat, jak různé možnosti zpravodajských orgánů řeší asymetrické ohrožení a kde jsou jejich mezery.

Všeobecně se uznává, že současné zpravodajské procesy jsou neadekvátní pro předpovídání a pro prevenci narůstajícího ohrožení kybernetickým terorismem. Zpravodajské orgány sice zavádějí „zlepšené možnosti" pro řešení kybernetického ohrožení, ale kapacity pro kybernetické útoky se zvyšují rychleji než tyto možnosti. Důvod, proč se těmto „zlepšeným možnostem" nedaří odstrašovat kybernetické útoky, je jasný: od jejich výzkumu a zavádění odrazuje nepříliš velká návratnost investic do složitých protiopatření, což je stav, jež bude zřejmě pokračovat i nadále.

Obrana proti asymetrickým útokům je nesnadná, protože často existuje jen málo zjistitelných příznaků vedeného útoku a účinný útok může realizovat i malá skupina.

Zpravodajská řešení

Odpověď na obranu proti novému ohrožení kybernetickým terorismem nelze hledat v tom, že se takovému ohrožení bude čelit stále rozsáhlejšími technologickými opatřeními. Nejen že jsou tato opatření stále méně účinná, avšak také počet jednotlivců schopných překonávat tato bezpečnostní opatření se zvyšuje alarmující rychlostí. Z toho vyplývá, že zpravodajství se v budoucnu musí zaměřit více na zpravodajství typu HUMINT (z lidských zdrojů) než na technologie. Pokusy čelit technologii útoku obrannou technologií jsou jen *taktickou* odpovědí různých zpravodajských institucí, jiné snahy neměly v úsilí zastavit stálé zvyšování počtu kybernetických útoků příliš velký úspěch.

Tradiční zpravodajské metody získávání zpráv se řídily postupy uzavřených a účinných struktur. Při hodnocení a potírání terorismu spoléhaly na operační postupy, jež vymezují cíle a metody teroristických skupin a působí na základě „případ od případu". V minulosti tyto metody snad mohly mít příznivé výsledky proti mezinárodnímu a nadnárodnímu terorismu, avšak neřeší novou povahu kybernetického terorismu. Takový přístup k hrozbě informační války je starý, statický, dnes pro řešení tohoto problému zcela nevhodný.

Statický přístup je nevhodný pro oblast zpravodajství právě svou neochotu upustit od tradičního ulpívání na uzavřených a konvenčních metodách zpravodajského procesu. Je jasné, že optimální informace týkající se kybernetického terorismu nebudou většinou nalezeny ve zdrojích vysoce hodnocených v minulosti. Jsou nezbytné odlišné zdroje. A podobně se budou metody získávání informací lišit i ve snaze získávat stále hodnotnější informace.

Technický průzkum a elektronický průzkum

Automatickou reakcí při řešení problémů asymetrických a kybernetických ohrožení – protože ohrožení jsou založena na internetu a jeho použití (jakož i na jiných elektronických prostředcích jako modemy, místní a dálkové sítě) pro vedení útoků – je použít technologicky podložené odpovědi, včetně získávání zpravodajských údajů pomocí technických prostředků.

I když netechnické prostředky, jako zpravodajství prováděné z **lidských zdrojů** *(HUMINT - human intelligence)*, budou v této oblasti hrát velmi důležitou úlohu, existuje i potřeba technického zpravodajství o těchto ohrožení, včetně **rádiového průzkumu** *(SIGINT - signals intelligence)* a **elektronického průzkumu** *(ELINT - electronic intelligence)*. Takové průzkumové údaje mohou být získávány z otevřených i utajených zdrojů, podobně jako jsou dnes snímky z komerčních družic používány k doplnění utajovaných technických prostředků.

Zpravodajské údaje o hrozbách informační války mohou být odvozeny ze změny přístupu asymetrického aktéra k použití hrozby, podle něhož se zjistí zranitelná místa a příležitosti, přístupy, možnosti a nakonec rizika a ohrožení. Proto jsou zjištění zranitelných míst, a tím i možných rizik, a analýza uzlových bodů, důležitých pro informační infrastrukturu, prvým důležitým krokem zahrnutým do hodnocení důležitosti, zranitelnosti a závislosti různých uzlů informačního systému. Jakmile je zjištěno riziko, je možné hodnotit ohrožení jako kombinaci důležitosti, zranitelnosti, záměru a možnosti.

Pro hodnocení ohrožení a získávání zpravodajských údajů o takových ohroženích je důležité společné *(combined)* úsilí všech zemí. Západní vlády musejí neustále udržovat krok s technologickým vývojem v soukromém sektoru. Výsledky tohoto vývoje jsou často k dispozici skutečně každému, jako komerční zboží, což aktérům asymetrických ohrožení umožňuje provádět „technicky pokročilé útoky" na informační infrastrukturu.

Je důležité, aby existovala spolupráce mezi dodavateli komerčního zboží a vládou. Tato spolupráce musí kombinovat zkušenost politologů a strategických analytiků, komerčních analytiků a odborníků pro informační a počítačové systémy pro zjišťování možností nutných k odražení asymetrického aktéra. Připomeňme, že asymetrický útočník pravděpodobně již předem vypracoval všechny varianty vedení útoku – v tomto smyslu nemusí být vždy utajován druh zpravodajských informací nutných pro získání příznaků a výstrahy před útokem, a jež na konec vedou k jeho zmaření.

Asymetričtí aktéři

Velké státy v přechodném stadiu. V roce 2010 mohou pro Západ představovat značný problém velké státy nacházejících se v tzv. přechodném stadiu, se schopností dopravy jaderných zbraní přes oceány, s rozsáhlou technologickou a vojensko-průmyslovou základnou, rozsáhlými regionálními vojenskými možnostmi a s kosmickými programy, majícími přístup ke globálnímu leteckému a kosmickému průmyslu prostřednictvím komerčních zdrojů. V současnosti je podobný vývoj nejpravděpodobnější v Číně, Rusku a Indii. V přechodovém období budou tyto státy jak spolupracovat, tak soutěžit se Západem v širokém spektru strategických a geoekonomických oborů. Zatímco Čína a Rusko budou na jedné straně klást značný důraz na úlohu jaderných zbraní pro odstrašování a možná i vedení války, aby čelily převaze technicky vyspělých konvenčních sil Západu, na druhé straně mohou rozvíjet vztahy s některými rizikovými státy (Írán, Irák, Sýrie, Libye), což Západ považuje za znepokojující, jakož i do těchto států vyvážet vojenskou techniku. Kromě toho, všechny tyto země mohou investovat do nejnovějších technologií, včetně investic do výzkumu a vývoje usměrněné energie, elektromagnetického impulzu, mikrovln velkého výkonu a kybernetických zbraní, určených ke zmaření západních koncepcí pro vedení války, s využitím převahy ve znalosti bojiště.

Rizikové státy. Od poloviny devadesátých let většina rizikových států (zvláště Sýrie a Libye, přičemž se k ním pomalu přibližují Severní Korea, Írán a Indonésie) více méně zlepšila své vztahy se Západem. Avšak v jiných státech autokraté držící se u moci (Zimbabwe, Libérie, Barma) oponují mezinárodnímu společenství těmi nejrůznějšími způsoby, někdy v otevřeném konfliktu (Somálsko, Jugoslávie, Čečensko), někdy jinými prostředky. Mnohé z nich se snaží vytvořit geostrategické a geoekonomické aliance buď s Ruskem, nebo s Čínou, nebo nejlépe oběma, což by mohlo mít dalekosáhlé důsledky pro budoucí regionální krize a intervence. Rizikové státy se budou všeobecně snažit do konce tohoto desetiletí dosáhnout možností, jaké

mají státy v přechodném stadiu. Získání zbraní hromadného ničení je pro ně z asymetrického hlediska velmi přitažlivé, neboť vyvažují vojenský potenciál Západu. Tyto státy se budou snažit v rovině psychologických operací zpochybnit anebo dokonce přímo znemožnit možnou západní intervenci.

Neúspěšné státy symbolizují jednak mezeru mezi rozvinutým a rozvojovým světem, jednak nelegitimitu vlády vojenských diktátorů a despotů. V těchto státech bojují o moc různé soupeřící frakce, často jsou střídány síly dosazené ještě za studené války. Soupeřící frakce i vlády se legitimizují ochranou organizovaného zločinu, obchodem se zbraněmi, narkotiky, kradeným zbožím a lidmi. Využívají ochranu, již jim někdy poskytují velmoci: USA, Čína, Izrael, Velká Británie a Francie. Na rozdíl od svých předchůdců mají tito noví povstalci a vojenští diktátoři přístup k moderním technologiím a moderním zbraním dodávanými některými státy NATO i státy bývalé Varšavské smlouvy. Pro své operace budou schopny využívat kosmických prostředků (pro navigaci, pozorování a spojení), jakož i mobilních telefonů s šifrováním přenosu.

Nadnárodní organizovaný zločin. Jakmile organizovaný zločin začíná využívat výhod informační revoluce (zvláště internetu), stává se nejen rafinovanějším, ale také nadnárodním – tj. existujícím všude ve světě – tím, že využívá pokročilé technologie a rozšiřující se globalizace. Začíná se zapojovat do konfliktů způsobem podobným rizikovým státům anebo teroristickým organizacím. V mnoha případech by mohly být některé státy ovládnuty politicky a finančně nadnárodním organizovaným zločinem. Tento globální fenomén představuje zvětšující se problém, protože se je možnost, že některé země využijí domácího nadnárodního organizovaného zločinu způsobem, jakým je využíván terorismus, podporovaný státem. V určitém smyslu může být tato aktivita nazvána „ekonomickým terorismem", kde se skupiny ideologických anebo náboženských fanatiků, aktérů nadnárodního organizovaného zločinu, žoldnéřů, dokonce nepřátelských států, sdružují s národními teroristickými sítěmi. Rozsáhlé útoky na infrastrukturu nebo na ekonomické cíle mohou vést až k celkovému zhroucení společnosti, což usnadňují občanské nepokoje. Existují jasné důkazy, že tyto skupiny mají na svědomí útoky na ekonomické cíle (banky, obchodní domy, prodejny vozidel, ropovody a soudní budovy) v místech jako je Korsika, Řecko, Kolumbie, Indie a Srí Lanka.

Nadnárodní terorismus (včetně extremistických, náboženských, anarchistických nebo vlasteneckých sil). Během devadesátých let mezinárodní terorismus ustoupil tzv. nadnárodnímu terorismu. Teroristická skupina je považována za nadnárodní, jestliže **politické hranice nejsou pro cíle skupiny důležité a nepůsobí ve prospěch žádného určitého státu, jestliže členové a zdroje pocházejí od podporovatelů ve více než jednom státě, a jestliže prostor působení, včetně volby cílů, přesahuje státní hranice.** Zatímco mnohé mezinárodní teroristické organizace, které existovaly ve dvou minulých desetiletích, uskutečňovaly jednoduchou nadnárodní migraci, dnes se do popředí dostaly jiné velké skupiny, včetně islámských fundamentalistických frakcí. Jsou aktivní a schopné těžit ze zásoby tisíců mudžahedínů po celém světě. Většina jejich úsilí zřejmě sleduje dva směry: předně poskytovat bojovníky pro nábožensky motivované války na celém světě (Balkán, Čečensko), a za druhé působit rozsáhle proti cílům v USA, Velké Británii a Izraeli.

Zpravodajství z otevřených zdrojů (OSINT) jako plod informační revoluce

S tím, jak se možnosti informační technologie neustále rozšiřují, spojováním pokroku ve výpočetní technologii a v telekomunikacích, stává se objem informací a typy informací získaných z otevřených zdrojů rozsáhlejší než kdykoli dříve. Proto je ironií, že ačkoli se hodně teoretizuje o potenciálu teroristických skupin k využívání informační války, existuje pouze omezený výzkum otevřených zdrojů. Zpravodajství využívající otevřené zdroje je rozhodně klíčovým prostředkem pro sledování potenciálních ohrožení kybernetickými teroristy, zvláště proto, že informace týkající se západních programů v oboru informační technologie a jejích slabých, zranitelných míst mohou být snadno zjišťovány z otevřených zdrojů.

Z tradičního přístupu k získávání zpravodajských údajů vyplývá jistá neochota využívat otevřené zdroje pro zpravodajské účely. Tato neochota může být vysvětlena nedostatkem podpory ze strany zpravodajských orgánů. Úzké zaměření a omezená „produkce" utajovaných zpravodajských možností sice napomohly k vytvoření účinnějších orgánů, ale tato účinnost může vést ke vzniku dalších zranitelných míst. Utajované zdroje, na které se zpravodajské instituce musely spoléhat, svou výlučností značně ztěžovaly pochopení toho, jaká ohrožení s sebou kybernetický terorismus přináší. Zdá, že zpravodajské instituce – na utajované úrovni – v současné době usilují o zpracování metodologie pro hodnocení kybernetického ohrožení.

Zpravodajství využívající otevřené zdroje poskytuje prostředek pro souhrnnou analýzu kybernetického teroristického ohrožení. Je však třeba poznamenat, že tyto rozšířené zdroje značně vyostřily problém tzv. informačního přetížení. Povaha zpravodajství využívajícího otevřené zdroje jako poměrně neúčinného zpravodajského zdroje je přesně tím, co ji znehodnocuje coby zdroj získávání údajů vzhledem ke kybernetickému terorismu.

Kybernetický terorismus je svou povahou zaměřen proti vysoce výkonným systémům informačních technologií, jež jsou vytvářeny širokou základnou velmi složitých proměnných. To umožňuje, aby kybernetické útoky nabývaly mnoha forem, při svém zacílení na rozsáhlou soustavu zranitelných míst nebo klíčových uzlů nějakého informačního systému. Kromě toho, tyto útoky mohou rychle změnit svou povahu a zdroj. Proto, jestliže se zpravodajství příliš spoléhá na jednu oblast, nebude schopno se přizpůsobit novým metodám kybernetického útoku a tyto metody rozpoznat.

Neexistují žádné vzory pro neoprávněné pronikání do počítačových sítí. Metody se neustále mění a každá nová zjištěná metoda může změnit celkový způsob posuzování kybernetické zločinnosti. V tomto smyslu široká základna zdrojů, z nichž těží zpravodajství využívající otevřené zdroje, napomáhá získávat hodnotnější zpravodajské údaje, vzhledem k problémům své účinnosti při působení v prostředí bohatém na informace.

Internet poskytuje nejnovější pokrytí současných asymetrických ohrožení se zdroji, které podávají zevrubné vysvětlení určené pro „počítačově vyspělé" osoby. V praxi je největším omezením internetu jeho náchylnost k informačnímu přetížení. Získávání zpravodajských údajů z internetu je pak téměř nemožným úkolem.

Schůdnou cestou pro vyřešení přetížení zpravodajskými údaji z otevřených zdrojů je **zařízení pro internetový rozhovor.** Na rozdíl od všeobecného získávání zpráv z internetu je internetový rozhovor prostředkem pro získávání zpravodajských údajů rozhovorem s jednotlivci v reálném čase ve stanovené oblasti týkající se kybernetické bezpečnosti. Takto

mohou být určité otázky týkající se potenciálních asymetrických ohrožení kladeny přímo počítačovým odborníkům.

Také netechnické zpravodajské zdroje mohou být využívány pomocí internetového rozhovoru. Sociologickým prvkem převládajícím u většiny subverzivních počítačových hackerů je velká míra jejich sebevědomí, týkajícího se jejich schopnosti „pronikat". Tito „mazaní" uživatelé se mohou zaměřit na zranitelná místa zjištěná na internetu, jakož i na vychloubání se s vlastními schopnostmi.

Nové aplikace zpravodajství prostřednictvím osob

Ve většině situací – zvláště v kybernetické oblasti – jsou konvenční prostředky odvety (řízené střely s plochou dráhou letu, taktické jaderné zbraně a jiné taktické zbraně) účelné jako odstrašující prostředek proti mnoha novým ohrožením. Pro obranu proti asymetrickým ohrožením jsou ale prakticky neužitečné. Obrana proti těmto ohrožením je spíše věcí skupin dobře vycvičených, vybavených a motivovaných zpravodajských profesionálů, kteří mohou sledovat a infiltrovat takové aktéry, čelit jim a zničit je.

Zpravodajství vedené osobami lze považovat jak za všeobecně uznávanou, tak i za tu nejkontroverznější formu zpravodajství. Avšak přes svou proslulost je zpravodajským zdrojem, jenž byl ve vztahu ke kybernetickému terorismu velmi přehlížen. Zatímco spojovací a elektronický průzkum, jakož i průzkum vedený jinými technickými prostředky, může mít omezenou hodnotu pro zpravodajství o kybernetických ohrožení, je zpravodajství prostřednictvím osob velmi užitečné při zjišťování záměrů a akcí asymetrických aktérů. V jiných asymetrických oblastech, jako je šíření zbraní hromadného ničení a podpora mírových operací, mohou technické prostředky hrát významnější úlohu.

Zpravodajství vedené osobami je zdrojem, který poskytl prostředky pro nesčetné kybernetické útoky. Kevin Mitnick, údajně nejznámější hacker na světě, se vyjádřil o nejslabším článku počítačové bezpečnosti takto: „Největší úsilí vlády o zastavení rozšiřující se záplavy počítačového zločinu bude převážně neúčinné, pokud nebude zaměřeno na lidské chyby, které umožňují většinu pronikání do počítačových sítí. Peníze vydané na hodnocení zranitelných míst počítačů a na bezpečnostní opatření jsou vyhozeny, protože žádné z nich neřeší tento nejslabší článek v řetězci bezpečnosti počítačů." Je účelné používat osoby k rozpoznání např. triků ke zjištění hesel, jež by mohly prozrazovat hrozící útok.

Stejně jako u zpravodajství využívajícího otevřené zdroje, existuje neochota využívat ve zpravodajské práci osob mimo jejich tradiční úlohu, při níž se zpravodajské údaje získávají pod oficiálním krytím diplomatického personálu. Zpravodajcům to poskytovalo mnohem lepší ochranu a snazší přístup k utajovanému spojení, ale také značně omezovalo jejich schopnost spolupracovat s jinými důležitými zájmovými objekty, což je důležité zvláště ve věci terorismu.

Při této alternativě se využívají neoficiální, skrytí agenti, jež představují rozsáhlý potenciál pro zpravodajství týkající se kybernetických útoků. Používání neoficiálního krytí se zřetelem ke kybernetickému terorismu může nabýt formu snahy o infiltraci do společenství hackerů nebo do jiných skupin schopných vést kybernetické útoky, a to jako prostředku pro rozpoznání a prevenci možných akcí kybernetického terorismu.

Na základě porozumění jednotlivcům podílejících se na takových útocích, jejich metodám, náboru, organizaci a motivaci, lze odvodit nové klíče pro prevenci, které leží mimo běžně pou-

žívané modely technické anebo technologické prevence a odstrašování. Další důkazy naznačují účelnost používání zpravodajství prostřednictvím osob v neoficiální krycí úloze v rozvíjející se kultuře společenství hackerů. Někteří hackeři vyprávějí o rozkolu ve společenství hackerů: jednotliví hackeři motivovaní přáním zachovat bezpečné a otevřené „počítačové prostředí" působí tak, aby zastavili škodlivé hackery páchající destruktivní akce v tzv. kyberprostoru. Možné výhody využití pomoci takových „slušných" hackerů jsou zřejmé. Metody získávání zpravodajských údajů pomocí osob působících mimo oficiální krytí mohou využívat potřeby otevřené výměny myšlenek podvratných uživatelů počítačů a legitimních odborníků na informační technologie.

Potenciální výhody zpravodajských operací pomocí osob v těchto oblastech jsou vyšší než výhody operací využívajících technickou obranu. Nicméně navzdory jejich efektivitě, tato varianta zpravodajské práce byla obecně opuštěna ve prospěch technického pozorování. I když jsou potenciální asymetrická ohrožení převážně realizována „off-line", je cena za neuznávání osobních zpravodajských zdrojů pravděpodobně značná.

Kooperativní zpravodajství

Kybernetický terorismus je v oblasti terorismu jedinečný tím, že aktéři mohou z velké vzdálenosti od cíle způsobit rozsáhlé škody na technologické infrastruktuře. Počítače používané k vedení kybernetického útoku se často nacházejí mimo zemi, v níž je cíl jejich útoku. Takto se kybernetický terorismus stává skutečně globálním problémem, bez ohledu na zemi, v nichž se nacházejí aktéři a jejich cíle.

Proto se musí změnit přístup k obraně proti terorismu, a zejména proti kybernetickému terorismu. Je nutno spolupracovat a vzájemně si předávat informace bezprecedentními způsoby. V tomto kontextu nejdůležitější ohrožení a úkoly získávání údajů a jejich analýza pro obranu proti kybernetickému terorismu leží mimo tradiční oblast zpravodajství a jeho možností. Pro boj proti němu je nutno koordinovat působení policejních, zpravodajských a bezpečnostních služeb, včetně jejich včasného rozpoznání a sledování možných ohrožení, a pro vyšetřování útoků, k nimž již došlo.

Kybernetický zločin vyžaduje rozvoj zcela nových vyšetřovacích dovedností, metod a technologií, které lze nazvat „kybernetickou kontrašpionáží". Na tom se musí podílet i soukromé firmy, protože v soukromém sektoru a jeho vysokých školách existuje mnoho lidí s odbornými zkušenostmi.

Boj proti kybernetickému ohrožení bude také vyžadovat sloučení analýz, příznaků a výstrahy týkajících se elektronického boje a informační války v rámci ozbrojených sil, a to s využitím zdrojů a poznatků orgánů spojovacího a elektronického průzkumu, jakož i spolupráci s jejich protějšky v civilních bezpečnostních a zpravodajských agenturách a u policie.

Ačkoli mezinárodní dohody a spolupráce jsou stále důležitějšími nástroji pro boj proti terorismu, je nesnadné je definovat. Z politického hlediska totiž existuje rozdílnost názorů na to, zda je v mezinárodním společenství mezinárodní dohoda omezující kybernetický terorismus dosažitelná, anebo vůbec žádoucí. Omezující činitelé ve vytváření mezinárodní zpravodajské spolupráce mohou být spatřováni zvláště v neochotě jednotlivých států uvolnit kontrolu své vlastní zpravodajské oblasti.

Ve snaze potlačit mezinárodní organizovaný zločin nejnovější analýzy doporučily jako nejúčinnější metodu vzájemné předávání informací, včetně sdílení tajných informací a zpra-

vodajských údajů o mezinárodních zločineckých skupinách. Protože terorismus je zločineckou aktivitou, musí být do tohoto úsilí začleněno i zpravodajství týkající se kybernetického terorismu a jeho organizací.

Závěr: spojené úsilí

Neochota zpravodajských služeb navázat širokou mezinárodní spolupráci může mít své kořeny ve zjištění, že sdílené zpravodajské údaje jsou, respektive bývají, málo hodnotné, což je dalším omezením vyplývajícím z institucionální mentality uzavřených a důvěrných zpravodajských zdrojů. Přestože zpravodajství využívající otevřené zdroje a osoby nabývá hodnotu především pro svou otevřenou a vzájemně sdílenou povahu, účinnost jednotlivých institucí musí ustoupit před bezpečností mezinárodní spolupráce. Při získávání zpravodajských údajů o kybernetickém terorismu se bude rozšířené používání zpravodajství využívající otevřené zdroje nutně překrývat se zpravodajstvím využívajícím osob v několika dalších oblastech a bude poskytovat i jiné prostředky pro účinné zpravodajství.

Aby se neopakovaly dřívější chyby, je důležité upustit od zpravodajských metod, jež mají omezený účel a patřičně neřeší problém kybernetického terorismu. Kombinované metody získávání zpravodajských údajů technickými prostředky z otevřených zdrojů, osobami, kooperativní zpravodajství, poskytují hlavní alternativu k tradičnímu zpravodajskému procesu používanému proti terorismu v minulosti.

Zásadní rozdíl mezi těmito dvěma základními řídicími metodami spočívá v tom, jak působí. Jedna používá uzavřeného, centralizovaného a v podstatě velmi účinného komplexního přístupu; druhá používá otevřeného, rozmanitého a kooperativního získávání zpravodajských údajů. Zatímco prvá metoda využívá pro vyřešení komplexních problémů komplexní řešení, druhá metoda získávání údajů se snaží dokázat, že účinné bezpečnosti proti velmi složitým ohrožením – jako je kybernetický terorismus – lze dosáhnout jen rozsáhlým a trvalým získáváním zpravodajských údajů.

V nejbližší budoucnosti bude nutné, aby se instituce zabývající se pasivní i aktivní obranou proti kybernetickému cílenými spojenými akcemi – od ozbrojených sil, civilního a policejního zpravodajství, až po soukromý sektor – sdružovaly a vzájemně spolupracovaly. Žádná z nich nemá všechny možnosti ani znalosti nezbytné k tomu, aby proti tomuto ohrožení bojovala sama. Jsou na sobě vzájemně závislé, jejich operační úspěch bude vyžadovat symbiotický vztah pro dosažení synergického úsilí v oblasti získávání, analýzy a využití zpravodajských údajů. Institucionální a právní překážky, neexistence společných postupů a odlišné organizační kultury snad mohou spolupráci bránit, nicméně zkušenost dokazuje, že spolupráci navázat lze, zvláště vzhledem k rychle se rozšiřujícím elektronickým informačním sítím, které tyto překážky snadno překonávají.

- nas -