Brzybohatý 2.970,-Kč

TERORISMUS

Podplukovník Mgr. Marian Brzybohatý, Ph.D.

Současný terorismus

Je to paradoxní, ale s klesající pravděpodobností klasického válečného konfliktu, v němž je nutností existence armád a masivní nasazení válečné techniky, roste nebezpečí jiných, tentokrát nekonvenčních konfliktů. Mezi těmito zvláštními formami násilí dominuje terorismus, který je možné chápat jako formu nekonvenčně vedené války.

Ještě před čtyřiceti lety byly teroristické incidenty převážně lokální záležitostí, které měly na geopolitickou situaci minimální vliv. S postupem času se však prostředky a metody terorismu rychle mění. Mění se jeho účinnost, roste jeho nebezpečnost a počty jeho obětí. Zásadním způsobem se však tvář terorismu změnila po roce 1990, kdy došlo k rozpadu socialistického bloku a k ukončení studené války.

Ke změnám došlo zejména v jeho motivaci. Ideologicky motivovaný terorismus ustoupil do pozadí a jeho místo postupně zaujímá terorismus náboženský a nacionalistický, což následně vede i ke změnám teroristických cílů, metod a prostředků.

Na základě analýzy řady teroristických incidentů a zejména útoků fundamentalistických fanatiků na cíle ve USA je možné sledovat vývojové trendy terorismu, které jednoznačně směřují k použití zbraní hromadného ničení a k obrovským lidským a materiálním ztrátám. Tyto trendy vyvracejí často frekventované tvrzení platné ještě v nedávné minulosti, že prostřednictvím terorismu nelze změnit chod dějin. Ukazuje se, že prostřednictvím terorismu lze změnit běh sociálního, ekonomického a politického vývoje minimálně ve střednědobé úrovni. Pro řadu organizací a nedemokratických chudých zemí se pak terorismus jeví jako efektivní nástroj pro prosazování vlastních zájmů ve střetu se silnějšími protivníky.

Terorismus je dnes celosvětový problém. Růst z něho vyplývajících rizik nutí instituce, organizace a státy spojovat síly a spolupracovat v boji proti tomuto zlu. Globální spolupráce v boji proti terorismu je dnes životní nutností. To platí i pro ČR, která se na protiteroristických aktivitách rovněž podílí, zejména v oblasti zahraničně politické, ve sféře policejních a zpravodajských služeb.

Pro ilustraci složitosti problému lze uvést, že i v zemi proti níž směřuje nejvíce teroristických útoků, v USA, používají různé instituce např. FBI, CIA, armáda, FEMA (Federal Emergency Management Agency) atd. vlastní definice. Velmi komplikovaná a vzrušená je rovněž diskuze o terorismu a jeho vymezení na půdě OSN. Vzhledem k různosti názorů, zájmů a potřeb různých států, které se v rámci této diskuze uplatňují, je velmi nepravděpodobné dosažení širokého konsenzu v dané oblasti. V demokratických zemích je však v současnosti nejvíce používanou definice ministerstva zahraničí USA, případně její modifikace. Z této platformy se pak následně odvíjejí i zásady protiteroristické politiky většiny demokratických států. Protiteroristická politika a z ní odvozená praktická opatření jsou založeny na následujících principech:

- Teroristům neustupovat a neuzavírat s nimi žádné dohody.

- Teroristy dopadnout a postavit před soud, kde se musí odpovídat za své zločiny.
- Státy podporující terorismus izolovat a vyvíjet na ně tlak, za účelem změny jejich chování.
- Aktivně podporovat spolupráci mezi státy v oblasti protiterorismu a boje s terorismem.

Existují desítky definic terorismu. V nejobecnější rovině je však uvedený fenomén chápán jako forma organizovaného násilí, obvykle zaměřeného proti nezúčastněným osobám, za účelem dosažení politických, kriminálních nebo jiných cílů.

Teroristické metody se vyznačují vysokou nebezpečností, bezohledností a brutalitou. Jejich výběr a použití jsou podmíněny snahou o vyvolání maximálního psychologického efektu. Násilí používané teroristy není důsledkem okolností, ale jeho použití je vykalkulováno tak, aby vyvolalo pocit strachu a ohrožení u co nejširšího okruhu lidí. Na pozadí následné hromadné společenské tenze, frustrace a deprivace jsou pak realizovány psychologické operace a manipulace, jejichž účelem je dosažení cílů, které obvykle nejsou otevřeně prezentovány.

Čím je brutalita, rozsah útoku a jeho následky větší, tím pravděpodobněji bude dosaženo soustředění pozornosti masových sdělovacích prostředků a budou vytvořeny předpoklady pro ovlivňování postojů veřejnosti, v souladu s přáními a cíli teroristů. V těchto souvislostech je terorismus považován za mimořádně ostrou formu psychologické války, jejíž účinky jsou podmíněny a znásobovány zájmem informačních médií. Činnost masmédií je pro efektivnost psychologických operací v oblasti terorismu jedním z rozhodujících faktorů.

Dalším základním rysem teroristického činu je jeho zaměření proti osobám, které v podstatě s cíli, které si teroristé kladou, nemají nic společného a nemohou jejich dosažení nijak ovlivnit. V případě napadení nebo ohrožení se však nezúčastněné osoby stávají rukojmími, jejichž prostřednictvím je vyvíjen tlak na odpovědné úřady, instituce či vládu, který je stupňován prostřednictvím sdělovacích prostředků.

Vlivní jednotlivci, instituce či vlády jsou tak vydíráni, diskreditováni a nuceni k různým ústupkům, jejichž cílem může být v konečné fázi destabilizace a změna společenského systému. Součástí teroristických aktivit jsou i zločiny, jež vytrženy z kontextu mohou být zařazeny do sféry běžné kriminality nebo organizovaného zločinu. Tyto zločiny pak často slouží jako prostředek pro získání finančních prostředků k podpoře vlastních teroristických operací, k infiltraci do vládních struktur či k vydírání.

Určení přesné hranice, zejména mezi organizovaným zločinem a terorismem, je obtížné. Vývoj ukazuje, že pro rozlišení teroristických činů od kriminálních již nestačí brát v úvahu přítomnost či nepřítomnost primární politické motivace, ale že stejně důležitým kritériem je hodnocení následků. Pokud důsledky vyplývající ze zločinu mají politický vliv a dopad, pokud ohrožují výkon státní moci a správy, pokud jsou hrozbou pro velké skupin lidí, pak lze takový skutek hodnotit jako teroristický čin.

Fenomén terorismu dorostl již do úrovně, kdy jej lze považovat za relativně novou formu ozbrojeného konfliktu, nekonvenčně vedené války. O tomto vývoji svědčí i analýzy bezpečnostní situace v uplynulém desetiletí. V jeho průběhu byla řada doposud stabilních zemí ohrožována množstvím náboženských, etnických a dalších vnitřních konfliktů, doprovázených bombovými útoky, přestřelkami, únosy, povstáními, drogovými válkami a mírovými operacemi, jejichž řešení si vyžádalo použití nových taktických postupů, vybavení, výcviku a schopností, značně odlišných od standardních postupů konvenčních bezpečnostních nebo vojenských sil.

Na základě dosavadních vývojových trendů lze odvodit, že budoucí konflikty si již nebudou vyžadovat masivní nasazení bojových jednotek operujících v pevně vymezené bojové zóně, ale bude pro ně charakteristická činnost malých skupin fanatických teroristů, používajících zbraně hromadného ničení, vysoce sofistifikovanou taktiku a technologie.

Velmi málo zemí disponuje v současné době potenciálem, jenž by jim umožňoval provést masivní vojenský útok na některou ze světových velmocí, například na USA, Rusko nebo Čínu. Terorismus však takovou možnost poskytuje.To je také důvod proč historicky tento sociální jev přetrvává stále se vyvíjí.

V této souvislosti lze na základě nedávných útoků ve USA a na základě analýzy teroristických incidentů v uplynulých patnácti letech přijmout názor, že současný demokratický svět je ve válce s fundamentalistickým, islámským terorismem. Tato válka je ve srovnání s jinými klasickými válečnými konflikty atypická a nekonvenční. Má globální charakter a její intenzita výrazně a často kolísá od stádií klidu až po stádia brutálního a intenzivního násilí. Bojové prostředky používané v jejím průběhu sahají od konvenčních zbraní až k zbraním hromadného ničení. Často jsou jako zbraně využívány prostředky značně neobvyklé a nekonvenční. Četnost, nebezpečnost a dopady teroristických incidentů mají stále rostoucí tendenci.

Na základě výše uvedené analýzy si dovoluji vyslovit přesvědčení, že proti demokratickým zemím je ze strany islámských fundamentalistů dlouhodobě vedena široce koncipovaná strategická operace, jejímž cílem je vytlačení vlivu demokratických zemí z oblastí, které pokládají za vlastní zájmové sféry. Týká se to zejména oblastí Eurasie, jihovýchodní Asie, Středního východu, Balkánu a části afrického kontinentu. Příznaky uvedených aktivit bylo možné již zaznamenat v souvislosti s rusko-afgánskou a později s rusko-čečenskou válkou, s balkánským konfliktem, s operacemi islámských fundamentalistů ve Francii v polovině devadesátých let, či v aktuální podobě v jihovýchodní Asii a USA. Charakteristickým operačním prvkem je v těchto případech intenzivní zpravodajská činnost a velmi sofistikované infiltrační snahy.

Důvody, které jsou oficiálně prezentovány ke zdůvodnění používání terorismu, jsou v daných případech převážně náboženské. Při jejich hodnocení lze však spíše spekulativně uvažovat o důvodech ekonomických a mocenských, které jsou do hávu náboženství zahaleny. Hlavním cílem je zřejmě strategická změna poměru sil v globálním měřítku, které má být dosaženo i za cenu vyvolání „střetu civilizací". Pokud by k něčemu takovému došlo, jednalo by se skutečně o největší vítězství terorismu v dějinách lidstva.

1. Aktuální vývojové trendy terorismu

V současné době dochází k velmi rychlým změnám kvality terorismu. Dochází k posunu od klasického (konvenčního) terorismu, který charakterizuje používání konvenčních prostředků a metod (atentáty, únosy, držení rukojmí, žhářství atd.), k novým formám, jejichž nebezpečnost je řádově vyšší. Vysoká úroveň hrozby terorismu je mimo jiné dána i možností zneužití kvalitativně nových prostředků a zbraní. V této souvislosti je proto současná nastupující etapa terorismu často nazývána stádiem superterorismu.

Superterorismus je pak v daném kontextu spojován s použitím zbraní hromadného ničení (jaderné, radiační, chemické a biologické zbraně). S postupujícím vývojem se však objevují v oblasti terorismu potenciálně nové druhy prostředků, jejichž mechanismy působení se od předcházejících kategorií liší a jsou s nimi obtížně srovnatelné. Následky (zejména sekun-

dární) jejich použití jsou však se zbraněmi hromadného ničení srovnatelné. V této souvislosti je možné podobné zbraně či metody zařadit do kategorie **„nekonvenčního terorismu"**.

Mezi nejvážnější a nejvíce sofistikované formy nekonvenčního terorismu patří **informační a psychologický terorismus** (psychologické operace).

1.1. Superterorismus

Jaderný, radiační, chemický a biologický terorismus je obvykle laickou veřejností spojován s teroristickým zneužitím zbraní hromadného ničení (ZHN), tzn. prostředků původně vyvinutých výhradně pro vojenské použití. Tato představa není zcela přesná a při hodnocení současných možností lze do dané kategorie zařadit prostředky, jejichž použití je z vojenského hlediska neopodstatněné. Termín ZHN je nutné chápat v kontextu možných rizik, vyplývajících z teroristických útoků, mnohem komplexněji. Do roku 1995 se úvahy o zneužití ZHN za účelem dosažení teroristických cílů pohybovaly pouze v rovině nezdařených pokusů, úvah a spekulací. Reálným se však toto nebezpečí stalo při útoku náboženských fanatiků v tokijském metru.

Jaderné zbraně jsou pokládány za nejničivější druh ZHN. Z konstrukčního hlediska tvoří zbraňové systémy, obvykle zahrnující jadernou náplň a prostředky dopravy na cíl. Z technologického hlediska je jejich efekt založen na využití jaderné reakce, štěpení a syntézy. Jejich výroba a skladování však vyžadují vysokou úroveň technologických teoretických znalostí i vysoké finanční náklady. Zdroje materiálů i pohyb komponent jsou v globálním měřítku sledovány a vztahuje se ně řada přísných restrikčních opatření. Z těchto důvodů je proto zneužití tohoto typu zbraní v oblasti terorismu nejméně pravděpodobné.

Radiologické zbraně jsou zbraňové systémy (často velmi primitivní), jež umožňují záměrné rozptylování radioaktivního materiálu na území protivníka. Jejich výroba a použití nejsou omezeny žádnou mezinárodní dohodou a z hlediska vojenského nasazení nemají praktický význam. V roce 1998 byl funkční radiologický zbraňový systém, postavený na kombinaci radioaktivního materiálu a klasické výbušniny, umístěn v jednom z moskevských parků čečenskými teroristy. Systém nebyl iniciován a byl použit pouze jako hrozba a prostředek politického nátlaku.

Chemické zbraně je možné vymezit jako otravné látky, které jsou schopné vyřadit živou sílu protivníka a snížit jeho akceschopnost. Nejčastěji jsou používány v plynné, kapalné, aerosolové či práškové formě. Ničivých účinků dosahují pronikáním do lidského organismu dýchacím ústrojím, pokožkou, sliznicemi a zažívacím traktem. Dnes již klasickým příkladem jejich zneužití je útok příslušníků sekty Óm šinrikjó v tokijském metru, nebo jejich nasazení proti civilnímu obyvatelstvu v průběhu iránsko - irácké války. Jejich použití však není omezeno pouze na lidské cíle. Stejně tak mohou být využity za účelem zničení vegetace, zvířat či přírodních zdrojů, které jsou pro život lidské populace v daném regionu nezbytné.

Biologické zbraně obsahují různé formy živých patogenních organismů nebo infekčních materiálů, určených pro bojové použití. Cílem jejich použití je způsobit onemocnění osobám, zvířatům nebo rostlinám. Jejich účinek je především závislý na typu použitého patogenu, na vnějších i vnitřních podmínkách a zejména na schopnosti množení patogenu v napadených organismech. Z hlediska nebezpečí zneužití ZHN jsou v současné době aktuální zejména tři níže uvedené zdroje.

- ***Existující vojenské arzenály*** ZHN, případně jejich komponent, kde je mohou získat teroristické skupiny prostřednictvím krádeží, loupeží či korupce. V této souvislosti se jako

nejpravděpodobnější jeví zneužití dnes již vyřazených ZHN, určených k likvidaci podle mezinárodních mluv a dohod. Největší zásoby ZHN určených ke zničení jsou v současné době k dispozici na území Ruska, USA, Indie a Jižní Koreje.

- ***Vlastní výroba komponent*** ZHN je dalším potencionálním zdrojem nebezpečí. Aktuální je zejména v těchto případech výroba chemických zbraní, tj. otravných látek s důrazem na supertoxické nervové jedy a zneužití běžně průmyslově vyráběných toxických chemikálií, odcizených radioaktivních nebo vysoce infekčních patogenních materiálů.
- ***Úmyslné vyvolání sekundárních účinků havarijních dějů*** je pravděpodobně nejreálnějším a velmi účinným možným zdrojem teroristického zneužití ZHN. Jedná se o násilné vyvolání sekundárních účinků havarijních dějů, obdobně jako v průběhu válečných konfliktů prostřednictvím sabotáží, nebo údery konvenčními zbraněmi na kritické body průmyslové infrastruktury, jakými jsou například vodohospodářská, chemická, energetická a jaderná zařízení. Podobné typy teroristických útoků se z hlediska svých charakteristik podobají mírovým haváriím, ale vzhledem k jejich spouštěcímu mechanismu se od nich liší rozsahem a rychlostí nástupu ničivých faktorů.

Vzhledem k tomu, že úspěšně čelit teroristickým činům na taktické úrovni je prakticky nemožné, jsou z hlediska obrany proti teroristickému zneužití ZHN nejúčinnější preventivní opatření. Z tohoto hlediska lze za nejdůležitější považovat zabezpečení následujících oblastí:

- legislativa,
- systematická příprava odborníků v oblasti krizového managementu,
- výkonnost a spolupráce zpravodajských služeb na bilaterální i multilaterální mezinárodní úrovni,
- systematická příprava specialistů (speciálních jednotek) pro oblasti protiterorismu a boje s terorismem,
- informovanost a příprava obyvatelstva,
- funkční integrovaný záchranný systém,
- finance a logistika.

Zabezpečení uvedených preventivních opatření nemůže v žádném případě zcela eliminovat možnosti teroristických útoků s použitím ZHN. Funkční preventivní systém však může odrazovat před teroristickým útokem a může sehrát významnou roli při snižování ztrát lidských životů i materiálu.

1.2. Nekonvenční terorismus

Pro oblast nekonvenčního terorismu je typické použití specifických prostředků, které se z hlediska mechanismu působení a účinků od klasických zbraní nebo ZHN liší. Obvykle primárně nevyvolávají ničivé účinky, nicméně jejich sekundární devastační efekt může být srovnatelný se ZHN. V posledním období zaznamenávají prudký rozvoj zejména dvě formy nekonvenčního terorismu - informační a psychologický terorismus.

1.2.1. Informační terorismus je relativně nová forma „nekonvenčního terorismu". Jeho princip ovšem nový není. Krádeže, změny a ničení informací u oponentů nebo politických

protivníků jsou stejně staré jako lidstvo samo. Hrozba informačního terorismu však strmě stoupá se stále rostoucí globalizací a s rozvojem informačních technologií. Z vojensko-politického hlediska je možné informační terorismus pokládat za důležitou odnož informační války. Klasický (konvenční) politický terorismus se snaží prostřednictvím použití fyzického násilí, případně jeho hrozbou, vytvořit klima strachu a nejistoty, cílevědomě zaměřené k ovlivnění chování populace a následně vládní politiky. Na rozdíl od něho, informační terorismus využívá ke stejnému účelu podstatně sofistikovanější prostředky - digitální informační systémy, sdělovací prostředky, či jejich jednotlivé komponenty, jejichž prostřednictvím jsou podporovány teroristické kampaně či akce. V takových případech pak nemusí být nutně k vyvolání strachu použito násilí proti lidským cílům. Z kriminalistického úhlu pohledu je možné považovat informační terorismus za kombinaci kriminálního zneužití informačních technologií a teroristického fyzického násilí.

Informační technologie nabízejí teroristům mnoho nových příležitostí. Umožňují jim napadnout a zneužít s nízkou úrovní rizika a před zraky široké veřejnosti informační zdroje a informační systémy. V úsilí o upoutání pozornosti rozsáhlého publika plánují a realizují informační teroristé útoky tak, aby byly zajímavé pro **informační média**.

Uvedený princip vychází z předpokladu, že masmédia jsou úzce spojena s mocí. Z toho vyplývá, že prostřednictvím sofistikovaného útoku na informační systémy mohou být následně dosahovány politické cíle. Jako příklad lze uvést krádeže informací a jejich kriminální zneužití k vydírání nebo k osobnímu prospěchu pachatelů, změny informací a dokumentů v tištěné, vizuální či fonetické formě, za účelem vedení dezinformačních kampaní či ničení informací s cílem fyzické či funkční destrukce technologických a informačních systémů atd.

Útok na informační systémy se jeví pro teroristy jako efektivní i z hlediska nákladů a vybavení. S technologií za několik tisíc korun či dolarů mohou napáchat mnohamilionové, případně mnohamiliardové škody a způsobit kolaps průmyslových, finančních, dopravních či mocenských struktur. V této souvislosti jsou za nejvíce ohrožené cíle pokládány letiště, plynovody a elektrické sítě, komunikační systémy, banky, vodní rezervoáry, velké průmyslové aglomerace, armádní řídící systémy atd.

S růstem globalizace a centralizace informačních systémů a technologií roste i jejich zranitelnost. Právě z tohoto důvodu je v popředí zájmu teroristů i pracovníků bezpečnostních sborů specifická oblast informačního terorismu - kyberterorismus (cyberterrorism).

Kyberterorismus je možné definovat jako zneužití počítačových technologií proti osobám či majetku, za účelem vyvolání strachu nebo vydírání a vymáhání ústupků, zaměřené proti vládním institucím nebo civilní populaci, případně proti jejich segmentům, pro podporu politických, sociálních, ekonomických, případně jiných cílů, zaměřené na informační systémy používané cílovým objektem.

Aplikací definice terorismu vlády USA je možné kyberterorismus rovněž vymezit jako prokalkulovaný, politicky motivovaný útok proti informačním, počítačovým systémům, počítačovým programům a datům, vedený subnárodními skupinami nebo tajnými agenty, jehož výsledkem je násilí proti nezúčastněným a nebojujícím osobám.

Přímým důsledkem teroristického útoku, který může být proveden z kteréhokoliv místa na Zemi, mohou být způsobeny primárně rozsáhlé škody a poškozeny miliony lidí. Následné sekundární efekty je však zpravidla svými účinky převyšují a umocňují.

V několika uplynulých letech byly zaznamenány tisíce víceméně úspěšných útoků na informační systémy, převážně subverzivně či kriminálně motivovaných, jejichž cíle jsou rozloženy

v širokém spektru. Sahají od krádeže osobních informací za účelem vydírání až po proniknutí do digitálních sítí a následné fyzické či elektronické destrukce informačních systémů.

Jako příklad lze uvést případ, kdy sympatizanti irské teroristické organizace Sinn Féin (My sami) na texaské univerzitě v Austinu získali prostřednictvím internetu tajné informace o britských armádních a policejních operacích v Irsku a předali je Irské republikánské armádě. Dalšími známými případy jsou útoky teroristů proti systému řízení vlakové dopravy v Japonsku, jehož výsledkem byla mnohahodinová paralýza dopravního systému, nebo útoky italských Rudých brigád na vládní informační systémy, či modifikace webových stránek MV ČR.

Obecně jsou používány dvě základní metody teroristických útoků. V prvním případě jsou informační technologie cílem útoku, jenž je zaměřen na zničení vlastního informačního systému a systémů, které jsou na něm závislé. Druhá metoda využívá informační technologie jako nástroj k manipulaci a k zneužívání cizích informačních systémů, ke změně nebo krádeži dat, případně k přetížení a zahlcení informačních systémů.

Zcela výjimečné možnosti k uplatnění teroristických metod poskytuje prostředí internetu. Umožňuje teroristickým skupinám i jednotlivcům rychlou a utajenou výměnu informací, poskytuje prostor pro šíření jejich ideologií a názorů, umožňuje získávání nových aktivistů i sympatizantů. V jiných případech se internet stává bránou k průniku do počítačových sítí a poskytuje tak příležitosti k vedení kyberteroristických operací. Je však faktem, že teroristické skupiny využívají zatím internet více k propagandě a ke vzájemné komunikaci než ke kybernetickým útokům.

V současnosti má podle údajů ministerstva zahraničí USA dvanáct z přibližně třiceti nejaktivnějších teroristických organizací na internetu vlastní webové stránky. V této souvislosti je zajímavá i zpráva amerického Úřadu pro alkohol, tabák a zbraně, publikovaná v roce 1997, v níž je uvedeno, že v období 1985 až 1996 bylo vyšetřováno třicet čtyři případů bombových útoků, pro něž byla výbušná zařízení zkonstruována podle návodů uveřejněných na internetu.

Klasickým nástrojem používaným ke kyberteroristickým útokům jsou viry. **Viry** jsou speciální programy, které mají schopnost vlastní reprodukce. Mohou být připojeny k jiným programům a mohou tvořit vlastní kopie nebo další modifikované viry. Mohou poškodit nebo zničit data, měnit je, případně degradovat funkce operačního systému. Podle mechanismu jejich působení je lze rozdělit do několika základních skupin:

- **Logical bombs** (logické bomby) jsou programy, které se tajně vkládají do aplikací nebo operačního systému kde provádějí destruktivní aktivity, když nastanou předem specifikované podmínky. Předem specifikovanou podmínkou startující logickou bombu může být v těchto případech například konkrétní datum.
- **Trojan horses** (trojští koně) jsou škodolibé programy, které obvykle nepůsobí velké škody. Narušují však bezpečnost počítačových systémů a sítí a zneklidňují jejich uživatele. Často jsou maskovány jako hry nebo antivirové programy.
- **Worms** (červi) je označení pro typy virů, které se šíří v počítačových sítích. Velmi často jsou šířeny prostřednictvím e-mailů. V současné době se jejich autoři zaměřují zejména na hledání „bezpečnostních děr" systémech nebo v poštovních programech.
- **Mocking-bird** (druh ptáka napodobující zpěv jiných ptáků) je software umožňující monitorovat komunikaci mezi uživatelem a serverem, případně mezi uživatelem a dalším počítačem. Umožňuje odhalit jeho identifikační jméno i přístupové heslo.

- **Back door** (zadní vrátka) jsou synonymem software pro „hledání „díry" v zabezpečení systému, jež byla záměrně vytvořena jeho tvůrci nebo správci. Jejím cílem je obvykle umožnění rychlého přístupu do systému v problematických případech či v kolizních situacích. V případě jejího odhalení či prozrazení je však ideálním místem průniku pro neoprávněné osoby.

Jedním z příkladů zneužití virů je virus „Code Red", který se objevil na přelomu července a srpna 2001 v počítačových sítích. Z technického hlediska je považován za jeden z nejpozoruhodnějších wormů (červů) historie. Během jediného dne se jeho obětí staly desítky tisíc webových serverů a jejich prostřednictvím se šířil dál po celém světě. Jeho primárním cílem byl server Bílého domu, který se však podařilo díky včasnému zásahu administrátorů zachránit. Postupně následovalo několik dalších, méně masivních útoků, jež byly odraženy a obešly se bez velkých následků.

Po krátkém období klidu se však objevil zdokonalený Code Red II. a III., jehož tvůrci se z nedostatků původního viru poučily. Druhá verze viru napáchala škody, které výrazně převyšovaly škody dosažené při prvním útoku. Jejich celková částka je zatím odhadována přibližně na dvě miliardy dolarů.

Federální úřad vyšetřování (FBI) zveřejnil verzi v níž prezentuje názor, že použití uvedeného viru bylo součástí důmyslného plánu kyberteroristů. Podle názorů řady dalších odborníků je pravděpodobné, že útoky byly pouze „kouřovou clonou" pro operaci, jejímž primárním cílem bylo napadení velkých finančních institucí. V současné době se většina předních bezpečnostních agentur snaží najít osoby, které jsou za útok odpovědné.

Mimo virů je další používanou metodou „zahlcení" cílového systému (serveru), vedoucí k jeho zhroucení. Vyvolání uvedeného stavu (DoS - Denial of Services) předpokládá široce koncipovanou akci stovek, případně tisíců počítačů, při níž mají pachatelé nainstalovaný software, který jim umožňuje koordinovat útok na webové stránky oběti.

Stále aktuálnějším nebezpečím pro ochranu dat v kyberprostoru se stává tzv. **spyware.** Jedná se o malé utility které se na cílový počítač nainstalují s jiným programem, s jehož funkcí však nesouvisí. Jejich posláním je průběžné zasílání informací o uživateli programu, obsahu a aktivitách jeho počítače firmě, která program vytvořila. V současné době je známo více než čtyři sta standardně používaných programů, které spyware obsahují. Spyware nejčastěji zjišťuje následující údaje:

- systémové jméno uvedené v systémovém registru,
- IP adresu (adresu počítače pro připojení na internetu),
- záznam DNS adresy (informuje o poskytovateli připojení, lokalitě - státu kde se počítač nachází),
- seznam všech nainstalovaných programů,
- údaje o souborech uložených na počítači,
- záznamy o aktivitách na síti (datum, čas, připojená adresa atd.),
- informace o telefonickém připojení (telefonní čísla kam se počítač připojuje),
- hesla pro připojení k síti atd.

Spyware je využíváno zejména ze zištných, případně z kriminálních důvodů. Možnosti jeho využití např. v oblasti zpravodajství nebo ve sféře terorismu jsou však evidentní, stejně jako u výše uvedených nástrojů a technik.

Původci podobných aktivit jsou obecně označováni jako hackeři (průnikáři), což je poněkud zkreslující termín. Pro upřesnění je možné početnou komunitu jedinců, kteří se snaží systematicky pronikat do počítačových sítí, z hlediska jejich motivace rozdělit do dvou základních skupin:

Hackeři jsou osoby, které pronikají do chráněných systémů, za účelem prokázání vlastních schopností. Jejich cílem není získání citlivých informací, získání osobního prospěchu nebo poškození systému. Hlavním motivem jejich jednání je překonávání ochranných bariér za účelem zábavy, pocitu dobrodružství a intelektuální převahy. Řídí se nepsaným „morálním kodexem", který jim mimo jiné ukládá informovat o nalezených nedostatcích v zabezpečení bez nároků na osobní veřejné uznání.

Crackeři používají z technického hlediska stejné nebo podobné metody jako hackeři, ale na rozdíl od nich pronikají do systémů za účelem krádeže nebo porušení dat. Podle jejich specializace je možné je dále dělit do řady dalších podskupin. Jako příklad lze uvést následující:

- Phrackeři se snaží napadat programy a zneužívat databáze telefonních společností za účelem získání telefonních služeb zdarma.
- Preakeři používají ukradené telekomunikační informace (čísla telefonních karet, telefonní čísla, atd.) pro přístup k dalším počítačům.
- Knackeři odstraňují ochranný kód programů za účelem jeho volného používání.

Z uvedených poznatků vyplývá, že demokratické státy musí v boji s terorismem stále řešit dilema vztahu osobní svobody a společenské bezpečnosti a s ní úzce související bezpečnosti informačních technologií. Výše uvedené aktivity jsou vždy ze společenského hlediska nebezpečné a hranice mezi jejich „sportovním", kriminálním či čistě teroristickým zneužitím je velmi nezřetelná. Z tohoto důvodu pokládá již dnes řada států jakýkoliv pokus o zneužití informačních technologií, bez ohledu na jeho prvotní motivaci, za teroristický čin. Takový postoj je pochopitelný v souvislosti s faktem, že prakticky všechny významné kriminální a teroristické organizace i zpravodajské služby disponují skupinami kvalifikovaných odborníků, jejichž úkolem je pronikání do informačních systémů protivníka.

Při koncipování zásad informační bezpečnosti je proto nutné odpovědět na řadu otázek, které jsou z tohoto hlediska zásadní a mají i svůj etický podtext. Jedná se především o následující problémové okruhy:

- Jaké jsou možnosti vlády, státní správy, bezpečnostních agentur a dalších institucí reagovat na informační teroristický útok?
- V jaké míře ohrožuje informační terorismus chráněné údaje a jaké legislativní možnosti k jeho postihu existují?
- Na základě jakých principů je možné rozlišit politicky motivovaný informační terorismus od běžné (ekonomické) kriminality?
- Jakým způsobem může policie přispět k ochraně státní, veřejné a soukromé informační struktury?
- Jakým způsobem může policie a odpovědné instituce efektivněji reagovat na hrozbu mezinárodního informačního terorismu?

Odpovědi na uvedené otázky je možné chápat jako východiska pro budování účinného preventivního systému v oblasti ochrany informací.

1.2.2. Psychologický terorismus

Pod termínem „terorismus" si laická veřejnost obvykle představuje použití nejhrubších forem násilí, jakými jsou např. bombové útoky, vraždy a únosy. Z hlediska teroristů jsou však takové akce pouze prostředkem k pronikání do sdělovacích prostředků, k dosažení potřebné publicity a k zajištění pozornosti širokých skupin obyvatelstva. Dosažení takového stavu jim pak následně umožňuje psychologicky působit na veřejnost a cíleně a sofistikovaně měnit její postoje. V této souvislosti lze pak chápat terorismus jako specifickou formu psychologické války.

Psychologická válka je na rozdíl od psychologického terorismu vedena ve válečném období a je směřována proti nepřátelskému lidskému potenciálu, za účelem změny jeho názorů, postojů a následně chování. V průběhu válečného konfliktu je hlavním cílem vedení psychologické války paralyzovat vůli protivníka a civilního obyvatelstva k odporu a k boji. Psychologický terorismus je však na rozdíl od psychologické války využíván i v mírové době. V jeho rámci je používána řada nástrojů a metod shodných s principy psychologické války a cíleně vědomě ovlivňujících rozhodování a chování cílových skupin. Stejně tak jako je nezbytným předpokladem úspěchu psychologické války vedení informační války, je z hlediska vedení teroristických psychologických operací nutností využívání informačního terorismu. Tyto dvě formy terorismu jsou na sobě existenčně závislé a jedna bez druhé nemůže v delším časovém horizontu existovat. V daném kontextu pak můžeme psychologický terorismus vymezit následovně:

Psychologický terorismus je plánované použití propagandy a dalších psychologických prostředků v době míru, za účelem ovlivnění názorů, emocí, postojů a chování jednotlivců či cílových skupin populace tak, aby přímo nebo svými důsledky ohrožovaly bezpečnost a ústavní principy státu.

Psychologický terorismus, stejně jako psychologická válka, je zaměřen na vědomí lidí a snaží se ovlivnit jejich chování a rozhodování prostřednictvím psychologických operací. **Psychologickou operaci** je tedy možné považovat za základní prvek vedení psychologické války. Psychologické operace mohou mít mnoho forem a jsou obvykle namířeny proti konkrétní cílové skupině, za účelem jejího zmanipulování a vyvolání požadované reakce (formy chování) jejích členů. K tomuto účelu používají organizátoři psychologických operací celou řadu prostředků. Mezi něž patří např. propaganda, dezinformace, podvrhy a falšování dokumentů, atd. Cílem působení komplexu vlivů odvíjejících se z použitých prostředků je vyvinout na protivníka (vládu, instituci, zájmovou skupinu, jednotlivce,atd.) takový psychologický tlak, který ho nutí k jednání, oslabující jeho materiální, mocenskou i morální pozici. Aplikovaně, v souladu s definicí NATO, je pak možné termín „psychologické operace" blíže vymezit. **Jedná se o plánované aktivity v míru i ve válce, zaměřené proti nepřátelské, neutrální i přátelské veřejnosti, za účelem ovlivnění jejích postojů a chování a následném dosažení politických a vojenských (aplikovaně ekonomických, náboženských, sociálních atd.) cílů.**

Vedení psychologické operace je náročnou činností, která vyžaduje relativně hluboké speciální znalosti či zkušenosti a náročné plánování. Samotné plánování probíhá v několika fázích:

V první fázi plánování operace jsou stanoveny cíle operace a analyzovány podmínky a vztahy cílové skupiny (skupin). Pro tyto účely je třeba důkladně prostudovat její historii, geografické podmínky, hodnotovou strukturu, hierarchii, sociální klima, ideologii, ekonomické vztahy, vztah k náboženství, atd. Primárním cílem je v tomto případě najít přitažlivá a neuralgická témata, na něž bude cílová skupina reagovat.

Dalšími objekty zájmu jsou při plánování lidé, kteří mají ve skupině význačnou formální či neformální pozici. Podpora prezentace jejich názorů, posilování vlivu, či naopak jejich diskreditace, může výrazně ovlivnit formování postojů u ostatních členů skupiny k určitému problému.

Třetí etapa plánování je zaměřena na formulace konkrétního „sdělení" které bude cílové skupině předneseno a bude ji ovlivňovat. Základním předpokladem jeho úspěšnosti je, aby bylo v souladu s výsledky předcházející analýzy a jeho skutečná či zdánlivá věrohodnost. Rozhodující pro jeho úspěšnost jsou zejména následující faktory:

- Forma sdělení (musí být v souladu s historickým, kulturním prostředím a zvyklostmi).
- Racionální informace (musí být ověřitelné).
- Iracionální informace (jsou voleny tak aby vyvolávaly silné emoce a byly obtížně ověřitelné).
- Zjevný obsah sdělení (obvykle se odvolává na morálku, právo, veřejné mínění či obecně známá fakta).
- Četnost a frekvence opakování.
- Skrytý obsah sdělení (nabízí skrytou formou řešení problémů obsažených ve sdělení v souladu s cíli psychologické operace).
- Výběr vhodných sdělovacích prostředků (letáky, noviny, rozhlas, televize, atd.)
- Zpětná vazba, umožňující hodnocení aktuálních výsledků psychologické operace a její následné korekce (obvykle jsou využívány psychologické a sociologické metody a prostředky).

Psychologická operace je tedy založena na cílevědomém využití již existující nebo uměle vytvořené situace, ve které je cílová skupina (veřejnost) účelově informována prostřednictvím sdělovacích prostředků, s cílem vyvolat u ní požadovaný typ reakcí (chování). K tomuto účelu jsou používány **psychologické manipulace**, jejichž podstatou je vložení cílevědomě vybraných či upravených informací do vědomí (do podvědomí) člověka či skupiny lidí, s cílem docílit jejich **indoktrinaci** (změny postojů). Nástroje používané k tomuto účelu mohou být založeny na využití logické nebo emocionální argumentace, na psychologických, sociálních či fyziologických principech.

Základním předpokladem úspěšné indoktrinace je vytvoření emočně vypjaté situace - ve sféře terorismu obvykle na základě rozvinuté frustrace nebo deprivace, většinou související s použitím různých forem násilí. V tomto typu situací dochází k potlačení kognitivních mechanismů a lidé v nich mají zvýšenou tendenci k nekritickému přijímání vnějších informací a následné změně chování, která je často iracionální.

Psychologické manipulace mohou mít různou úroveň a intenzitu a v žádném případě nejsou spojeny pouze s negativními jevy. S jejich sociálně, morálně a právně přijatelnými formami se setkáváme prakticky denně v různých reklamních kampaních i v osobním kontaktu s druhými lidmi. Mohou však mít i podstatně tvrdší a nebezpečnější formy, založené na tzv. vymý-

vání mozků *(brain-washing)*, což je souhrnný název pro speciální postupy, které k dosažení indoktrinace používají mimo jiné i psychické či fyzické násilí a mohou vést až k nevratnému fyzickému a psychickému poškození osob, proti nimž byly použity. Jako příklad lze uvést postupy používané náboženskými sektami nebo zpravodajskými službami.

Základním nástrojem psychologické války a psychologického terorismu je **propaganda.** Pro vymezení obsahu tohoto termínu existuje řada definic různých autorů. Touto problematikou s např. zabýval Jowet, G. S., Hachten, W., Bittman, L., a další. Přes různé odlišnosti názorů lze na jejich základě odvodit, že uvedený termín vyjadřuje záměrnou a sofistikovanou činnost, jejímž cílem je s pomocí účelově vybraných informací vyvolat u cílové skupiny takové formy chování, které jsou v souladu se zájmy propagandisty.

Na základě znalosti zdrojů, ověřitelnosti a pravdivosti informací lze propagandu rozlišit na **bílou** (selektivně použité pravdivé informace z ověřitelných zdrojů), **šedou** (částečně pravdivé či upravené informace z problematicky ověřitelných zdrojů) a **černou** (lživé, účelově používané informace - dezinformace, z falešných či neexistujících zdrojů).

Je zajímavé, že většina odborníků zdůrazňuje nutnost udržení odstupu propagandisty od obsahu propagandy. Jinými slovy, identifikace propagandisty s obsahem propagandistické kampaně znemožňuje objektivní hodnocení jejího průběhu a výslednosti. Dotaženo *ad absurdum*, propagandista by neměl bezmezně věřit vlastním argumentům a měl by je používat pouze jako racionální účelový prostředek, umožňující cílenou manipulaci osob nebo skupin.

Pro moderní vedení propagandy je typické využití široké palety různých masových médií, např. plakátů, filmů, televizních programů, inzerátů, fotografických snímků, novinářských tiskových forem a počítačové techniky. Propaganda není ideologie, ale nástroj ovlivňování, který je k dispozici politickým, náboženským či jiným organizacím. Její sílu a možnosti je možné demonstrovat na příkladech z nedávné minulosti, kdy např. záběry televizních kamer a novinové články dokázaly svým působením na veřejné mínění ve velmi krátké době donutit západoevropské země a USA ke stažení vojenských sil z Libanonu či ze somálského hl. města Mogadišo (Muqdisho) a k přehodnocení jejich diplomatických, politických i vojenských aktivit v krizových regionech. Stejné mechanismy působení je možné zaznamenat v současnosti např. v průběhu mírových operací na území bývalé Jugoslávie.

Terorismus propagandu využívá, je s ní bezprostředně spojen a je na ní existenčně závislý. Samotné konvenční teroristické akty lze v souladu s L. Bittmanem zařadit do propagandistické kategorie **„propagandy činem"**. Uvedený termín, který historicky pochází z anarchistického slovníku, v sobě zahrnuje fyzické akty násilí nebo hrozby násilím, případně jiné typy demonstrace síly, za účelem upoutání pozornosti, vytvoření emociálně vypjatého klimatu v cílové skupině, případně v celé společnosti, zastrašení protivníka a docílení politických ústupků. Propaganda spojená s teroristickým činem nemusí mít nutně slovní podobu. Teroristický čin v závislosti na společenských podmínkách, na aktuálních okolnostech, na způsobu provedení, na výběru cíle a načasování, atd., obsahuje prakticky vždy určité poselství (hrozbu), které má symbolickou, nonverbální formu.

Teroristické operace nemají fakticky z vojenského či z mocenského hlediska žádný význam. Jejich hlavním smyslem je manipulace a změna veřejného mínění.

Jak z předcházejícího textu vyplývá, psychologické operace jsou nedílnou součástí terorismu. Současně je potřebné zdůraznit, že mohou být využity jako protizbraň proti uvedenému jevu, formou *public relations*, jejichž cílem může být například eliminace teroristické

(nepřátelské) propagandy, snížení účinků posttraumatického šoku, nebo příprava veřejnosti na možnost teroristických útoků a na optimalizaci jejího chování v krizových situacích.

Public relations (vztahy s veřejností) jsou v tomto kontextu chápány jako psychologické operace vedené oficiálními institucemi vůči přátelské veřejnosti, s použitím zákonných a morálně přípustných prostředků a metod, za účelem dosažení pozitivních cílů.

V jejich rámci může být veřejnost seznamována s mechanismy působení terorismu, mohou být odhalovány jeho skryté cíle, kompenzovány psychologické dopady a poskytovány návody k optimálnímu chování v krizových situacích. Mohou být využity i ofenzivně, například v rámci zpravodajských aktivit.

Public relations není možné pokládat za samospasitelný nástroj v boji s terorismem. Ve sféře protiterorismu může plnit tento typ bezpečnostních operací úlohu důležitého podpůrného mechanismu. Z hlediska budoucnosti lze pak přijmout tvrzení, že vzhledem k rychlému rozvoji globalizace a informačních technologií význam psychologických operací a protioperací poroste.

2. Možnosti terorismu v České republice

Při hodnocení aktuální situace v evropském regionu se prozatím Česká republika jeví jako region, v němž terorismus nepředstavuje vážnější bezpečnostní problém. Od roku 1990 do současnosti zde došlo pouze k několika incidentům, které lze z hlediska charakteristik do kategorie terorismu zahrnout. U většiny z nich nebyla politická motivace jejich pachatelů jednoznačně prokázána. Pokud však budeme brát v úvahu jejich důsledky, je jejich dopad na veřejnost a následně na politickou sféru zřejmý. Situace se však může kdykoliv změnit, zejména na základě rostoucí angažovanosti naší země v rámci NATO a po vstupu do EU.

Důležitým podnětem v tomto směru se staly útoky islámských fundamentalistických radikálů na cíle ve USA, při nichž byla použita jako smrtící zbraně unesená letadla. Útok, jehož následky nemají doposud obdoby, přinesl zásadní změny v geopolitické a bezpečnostní situaci a pravděpodobně nastartoval změny, které se plně projeví v průběhu příštích měsíců a let.

Při hlubší analýze bezpečnostních rizik jsou proto názory zlehčující nebezpečí terorismu obtížně obhajitelné. Do jisté míry se na jejich existenci podílí i absence oficiální, mezinárodně kompatibilní definice terorismu, která by nemusela nutně mít existenci zákonné normy. Její hlavní smysl je nutné hledat především ve sjednocení přístupu odpovědných představitelů a institucí k problematice terorismu. Stejným způsobem by její existence pravděpodobně přispěla ke zkvalitnění práce masmédií a následně k objektivnějšímu informování široké veřejnosti. Nicméně do konce roku 2001 předloží odborná komise EU návrh legislativních úprav, který bude osahovat evropskou definici terorismu, jež se po pravděpodobném přijetí stane závaznou i pro Českou republiku.

Za nejvážnější možné zdroje terorismu v České republice lze v současné době pokládat především následující oblasti: (1) mezinárodní vztahy, (2) extremismus, (3) kriminální scénu, (4) patologické jedince a skupiny.

Oblast mezinárodních vztahů v České republice je charakterizována stále se prohlubující integrací s demokratickými zeměmi a sdílením jejich hodnot. Tento proces však přináší rizika, vyplývající z účasti České republiky v akcích a operacích, které s ním úzce souvisí. Jako příklad lze uvést činnost rádia Svobodná Evropa a jeho vysílání do Iráku a Íránu, případně účast české

armády v řadě mírotvorných misí, zejména na území bývalé Jugoslávie. Možnými cíli je však i celá řada objektů souvisejících s činností zahraničních institucí, jakými mohou být například budovy a personál ambasád či zahraničních firem.

Na základě dosavadního vývoje lze konstatovat, že vážný teroristický útok na území České republiky relativně dlouhou dobu nehrozil. Do 11. září 2001 nebyly k dispozici žádné indicie, svědčící o otevřených aktivitách příslušníků mezinárodních teroristických organizací na území ČR. Po tomto datu se však situace výrazně změnila a na základě informací zpravodajských služeb lze usuzovat, že mezinárodní terorismus se zcela jistě stává hrozbou i v tomto, doposud relativně klidném regionu.

Extremismus v České republice expanduje a je závažným společenským problémem. Pro extremistickou krajně levicovou (anarchistickou) i krajně pravicovou (převážně prezentovanou příslušníky neonacistických skinheads) scénu je zřetelný silný trend k radikalizaci postojů a projevů, což do jisté míry souvisí i s jejich vazbami na zahraniční subjekty. Pro obě křídla extremistických organizací je typická snaha o zdokonalování struktury, organizace, koordinace akcí, konspirace, spojení a operačního plánování. V některých případech (např. v souvislosti se sjezdem MMF v Praze) bylo zaznamenáno i použití prostředků typických pro informační terorismus nebo pro vedení informační války.

Zvláště u extremistických pravicových organizací je zřejmá snaha o legalizaci a jejich přeměnu na občanská sdružení či politické strany, což by výrazně rozšířilo jejich sféru působnosti a společenský vliv. V souhrnu je možné hodnotit vývojové trendy a současný stav extremismu jako velmi znepokojující.

Většina oblastí **kriminality** je v České republice od roku 1990 na vzestupu. Z hlediska nebezpečí terorismu je možné hodnotit formy kriminality spojené s organizovaným zločinem jakými jsou např. zneužívání informací, korupce, ekonomická, počítačová a násilná kriminalita. Přestože v uvedených oblastech není politická motivace primární, může jejich rozvoj sekundárně politické klima ovlivnit. Kriminální sféra může sehrát v případech teroristických aktivit podstatnou logistickou úlohu, například při zajišťování financí, informací a zbraní. Znepokojující jsou z tohoto hlediska i kriminální aktivity příslušníků národnostních menšin (vietnamská, čínská, bulharská, arabská, ruskojazyčná, „jugoslávská", atd.) žijících na území České republiky. Závažný je rovněž dlouhodobý trend růstu (s výjimkou roku 2000) použití výbušných systémů a stálý růst násilných forem kriminality.

Patologičtí jedinci (skupiny) jsou možnými, i když nejméně pravděpodobnými pachateli teroristických incidentů. V průběhu posledních let bylo zaznamenáno na území našeho státu několik případů spojených s použitím nástražných výbušných systémů, jejichž pachatele lze do této kategorie zahrnout. Politická motivace však nebyla v uvedených případech prokázána.

Pokud hodnotíme současnou bezpečnostní situaci z hlediska hrozby terorismu v České republice, lze náš stát považovat za relativně bezpečný. Současně s tímto tvrzením je však nutné upozornit na existenci latentního potenciálu a podmínek k jeho existenci a rozvoji, tak jak byly výše stručně popsány. Z bezpečnostního hlediska tedy nemá smysl se ptát zda se „to" stane. Účelnější je v tomto případě kladení otázek typu: kdy, kde a jak se „to" pravděpodobně stane? a jak jsme připraveni? Odpověď na poslední otázku není v žádném případě jednoduchá. Při formulaci odpovědi na ni je třeba brát v úvahu stav zejména níže uvedených oblastí:

- Zpravodajství (strategické, taktické, operační)
- Legislativa

- Vyšetřování
- Speciální jednotky
- Integrovaný záchranný systém (IZS)
- Spolupráce (mezinárodní, vnitrostátní)
- Public Relations (vztahy s veřejností)
- PSYOP (psychologické operace)
- Věda a výzkum

Zpravodajství je považováno za základní prostředek boje s terorismem. V České republice má dominantní roli v této oblasti BIS. Nicméně problematice věnují pozornost i další zpravodajské služby a instituce. Důležitá je tato činnost i v jiných oblastech, např. v činnosti SPOK (Služba pro odhalování korupce a závažné trestné činnosti) atd. V souhrnu je možné konstatovat, že ze zpravodajského hlediska je oblast terorismu zabezpečena na relativně dobré úrovni, v souladu s potřebami a možnostmi naší země. To se prokázalo i v průběhu krize související s útoky teroristů v USA dne 11.9. 2001, kdy české zpravodajské organizace velmi dobře kooperovaly se spřátelenými zpravodajskými službami a byly v tomto smyslu pozitivně hodnoceny.

Trestní zákon (zákon č.140/1961 Sb.) České republiky skutkovou podstatu „terorismus" neobsahuje a samotný obsah termínu „terorismus" není vymezen v žádné obecně závazné právní normě. Trestní zákon však umožňuje stíhat trestní činy spadající do uvedené kategorie na základě jiných skutkových podstat. Zásadním způsobem bude tento problém pravděpodobně vyřešen až po vstupu ČR do EU a po provedení s tím souvisejících legislativních úprav.

Vyšetřování je činnost která je považována za základní nástroj při objasňování teroristických incidentů. Obecně je vyšetřování založeno na použití kriminalistických metod, prostředků a postupů, případně na aplikacích z dalších vědních oborů. Výslednost vyšetřování v České republice je zejména v tradičních oblastech kriminality plně srovnatelná s vyspělými státy. Toto hodnocení bezesporu platí i v případech doposud vyšetřovaných potencionálních teroristických konvenčních incidentů. V oblasti nekonvenčního terorismu však zatím bezpečnostní aparát nedisponuje potřebnými zkušenostmi a specialisty, jež bylo možné k vyšetřování použít.

Speciální jednotky jsou mocenským nástrojem, který v průběhu uplynulých třiceti let prokázal svoji účinnost při potlačování projevů terorismu. V současné době fungují ve většině zemí jako nezbytná součást bezpečnostního aparátu. Výjimkou není ani Česká republika. Útvar rychlého nasazení PČR a policejní zásahové jednotky jsou relativně dobře připraveny a z hlediska výkonnosti srovnatelné s podobnými jednotkami v zahraničí. Jejich příprava je však především zaměřena na řešení konvenčních teroristických incidentů. V incidentech typu nekonvenčního terorismu, případně superterorismu, se proto jeví možnosti jejich nasazení jako omezené.

Integrovaný záchranný systém (IZS) je důležitým předpokladem úspěšného řešení krize nebo tísňové situace, související s hrozbou teroristických incidentů. IZS zahrnuje aktivní účast všech záchranných organizací (policie, hasiči, záchranáři,atd.) při plánování, výcviku a řešení krizí. Za jeho řízení odpovídá ministr vnitra.

Současný IZS je v České republice funkční relativně krátkou dobu a trpí mnoha dětskými nemocemi, souvisejícími např. s novými legislativními normami, s finančním zabezpečením

a s potřebou zajištění vysoce kvalifikovaných odborníků. Problémy související s jeho funkčností a výkonností jsou však postupně řešeny a koordinace i schopnosti systému mají trvale rostoucí tendenci.

Spolupráce v oblasti antiterorismu (defenzivní opatření) i v boji s terorismem (ofenzivní opatření) je v České republice zajišťována a realizována na základě řady bilaterálních smluv a mezinárodních konvencí na různých úrovních. Ve vnitrostátní oblasti je tato spolupráce realizována např. v rámci IZS, bezpečnostních složek, či státní správy. Velmi aktuální jsou však formy mezinárodní spolupráce. Ta je realizována především v oblasti legislativní, diplomatické, zpravodajské, atd.

Psychologické operace (PSYOP) a **public relations**, jejichž podstata byla stručně vysvětlena v předchozím textu, jsou v České republice v bezpečnostní praxi prakticky neznámým fenoménem. Pro jejich efektivní využití zatím chybí především fundované teoretické a legislativní zázemí. Zahraniční zkušenosti ukazují, že mohou být velmi účinnou zbraní i podpůrným prostředkem ve sféře protiterorismu a boje s terorismem.

Věda a výzkum patří bezesporu mezi nejúčinnější, i když nejméně viditelné nástroje k potlačování terorismu. Aplikace teoretických i praktických výsledků výzkumu hraje obecně stále větší roli v oblasti prevence, potlačování a redukce následků teroristických operací. Racionalizace bezpečnostních postupů založená na nových a aktuálních vědeckých poznatcích je nezbytná při potlačování konvenčního terorismu, ale její význam je přímo životně důležitý v boji s nekonvenčním terorismem, nebo v případech hrozby či zneužití zbraní hromadného ničení. Česká republika má bohužel v dané oblasti relativně velké rezervy. Výzkumné programy s bezpečnostním zaměřením jsou realizovány ve velmi úzkém spektru problémů a chybí jim potřebná koordinace i materiální zázemí. Jedním z negativních důsledků je pak následně i nedostatek potřebných, vysoce kvalifikovaných odborníků.

Z obsahu výše uvedeného textu lze následně vyvodit obecné závěry, na jejichž základě je možné dále navrhnout vhodná opatření ke zvyšování připravenosti České republiky v oblasti protiterorismu a boje s terorismem:

- Zvážit možnosti novelizace právních norem vztahujících se k oblasti protiterorismu a boje s terorismem.
- Zkvalitňovat podmínky a vytvářet předpoklady pro systematický monitoring a analýzu teroristických hrozeb. V rámci této činnosti přehodnotit a zkvalitnit funkci protiteroristického systému (CTS), jehož hlavním cílem je výměna a efektivní využívání informací zaměřených na problematiku terorismu.
- Prohlubovat mezinárodní spolupráci.
- Zdokonalovat integrovaný záchranný systém.
- Vytvářet finanční a materiální zdroje.
- Vytvořit výzkumný program a v jeho rámci řešit tématické úkoly zaměřené např. na psychologické a sociální aspekty terorismu, krizový management, problematiku výcviku, nové technologie atd.
- Zpracovat a realizovat plány systému přípravy potřebných specialistů.

Představa, že se podaří terorismus zcela vymýtit se ve světle uvedených faktů jeví jako velmi nepravděpodobná a nereálná. Nicméně s terorismem je nutné a možné bojovat. Na základě možných protiopatření je možné jeho projevy a ohniska potlačovat, kontrolovat a omezovat. Uvedená nutnost však přesahuje možnosti jednotlivých složek státní moci i možnosti jednot-

livých států. Právě z tohoto důvodu musí být boj s terorismem veden komplexně, na základě široké mezinárodní spolupráce. Bez splněných uvedených podmínek, pak nemůže být nikdy dlouhodobě úspěšný.

Použitá literatura:

Brzybohatý, M.: Terorismus I. a II. Police History, Praha 1999.

Matoušek, J., Mika, O.: Chemický, biologický, radiologický a jaderný terorismus. Sborník přednášek z pátého ročníku. Mezinárodní konference medicíny katastrof, EGO Zlín, s.r.o., Zlín 2001.

Devost M., Houghtton B., Pollard N.: Information Terrorism. http://www.geocities.com/CapitolHill/2468/itpaper.html.

Volkognov, D.: Psychologická válka. Novosti, Praha 1986.

Propaganda and psychological warfare studies. Joint Chiefs of Staff Department of Defense, JCS Pub 1, USA, 1987.

Bittman, L.: Mezinárodní dezinformace. Mladá fronta, Praha 2000.

Danics, Š.: Politické a bezpečnostní aspekty transformace naší společnosti. Sborník Vojenské akademie v Brně. Řada C-D. 1998/2.

Danics, Š.: Terorismus jako součást nekooperativní politiky. Bezpečnostní teorie a praxe, Sborník Policejní akademie ČR, 2001/2.

Němec, M.: Organizovaný zločin. Naše vojsko, Praha 1995.

Straus, J.,Tureček, J.: Význam přírodních a technických věd pro činnost policie: In: Problémy rozvoje teorie policejně-bezpečnostní činnosti a policejních věd. Sborník Policejní akademie ČR k problematice vědecko-výzkumného úkolu: Bezpečnostní teorie a praxe. Zvláštní číslo. Policejní akademie ČR, Praha 2000.

Straus, J.: Forensic Application of Biomechanics. Second European Academy of Forensic Science Meeting. Institute of Forensic Research Publisher, Krakow 2000.

Má-li být zvládán rostoucí počet bezpečnostních úkolů v novém tisíciletí, nestačí jen pokračovat v dřívější politice a zavedených zvyklostech. Tyto problémy jsou prostě příliš obtížně politicky zvladatelné, příliš tematicky provázané a příliš ekonomicky nákladné. Dobré úmysly vycházející z užší spolupráce a sdílení – zejména tváří v tvář velké tragédii – nebudou v dlouhodobé perspektivě postačující ani udržitelné. Toho, čeho je zapotřebí, je neomezená, ucelená a nadnárodní strategie, jejíž pozornost bude zaměřena nad rámec bezprostředního okamžiku a směrem k horizontu. Předvídání budoucnosti bude vždy spojeno s úskalími, ale to není důvod k tomu, abychom ignorovali rozlišitelné trendy a vývoj v rychle se měnícím světě, natož abychom se snažili přijímat izolované plány v naději, že události projdou mimo nás.

Robert Hall a Carl Fox
Přehodnocení pohledu na bezpečnost
NATO review zima 2001/2002