Ohrožuje nás kybernetická válka?

Kybernetický boj není v zásadě odlišný od konvenčního, fyzického boje. Pokud jej vede národní stát, je integrován do definované strategie a doktríny, stává se součástí vojenského plánování a je uskutečňován v rámci specifických parametrů.

Válka, která používá jako jeden ze svých prostředků Internet, je již dnešní realitou. Počet vojáků nemusí být rozhodujícím kritériem a jednotlivé, dobře zamaskované výpady mohou být stále častější. Půjde jen o to, aby zpravodajské služby nezjistily zdroj útoku nebo aby zde alespoň zůstal stín pochybnosti. Internet musíme vnímat jako velmi nebezpečné bojiště. Internet zpravidla vnímáme jako studnici informací nebo jako zdroj zábavy. Jenže, v současné době je už na něm naše současná civilizace do značné míry závislá. Toho si jsou vědomi generální štáby i kyberteroristé.

Výrazně vzroste množství útoků na mobilní bankovnictví. Útočníci v tomto případě budou častěji zkoušet obejít samotné PC a cílit přímo na bankovní aplikaci v mobilním zařízení.

Během rusko-gruzínské války byly napadeny i stránky tbiliských vládních institucí. Gruzínské ministerstvo zahraničí dokonce na nějaký čas přestěhovalo své stránky na aplikaci blogger.com.

A aby toho nebylo málo, kanadští badatelé nedávno přišli s tvrzením, že jistá počítačová síť se sídlem v Číně ukradla vojenská tajemství Indii, nabourala se do kanceláří dalajlámy a zaútočila na některé počítače na různých místech světa. Jak se dalo čekat, Peking vše popřel.

V roce 2012 dojde k ukázkovým akcím v oblasti „kybernetické války". Hlavním cílem zatím bude spíše testovat možnosti těchto útoků. Až dosud vlády vyspělých zemí chránily především své vládní a vojenské sítě. Nyní si bude třeba uvědomit i míru škod, které mohou způsobit akce proti další kritické infrastruktuře.

Řada zemí nevyvíjí pouze obranné, ale také útočné zbraně, které mohou ohrozit cizí infrastrukturu, například elektrorozvodné sítě, vodovodní systémy, finanční sektor, dopravu či telekomunikace.

Tímto způsobem lze poměrně jednoduše a levně způsobit rozsáhlé škody. CIA potvrdila, že výpadky elektřiny v několika městech byly zřejmě důsledkem kybernetických útoků. V důsledku toho je možno je analyzovat a varovat před způsobem, jenž je velmi podobný tomu, který se používá v případech ostatních vojenských operací. Existuje fakticky několik způsobů, jak snižovat zranitelnost vůči kybernetickému boji. Patří k nim předvídání a vyhodnocování, preventivní či odstrašující opatření, obranná opatření a opatření ke zmírnění škod a k obnovení původního stavu.

Kybernetický arzenál: Zbraně použitelné v kybernetické válce má nyní k dispozici především pět států: USA, Rusko, Francie, Izrael a Čína.

Scénář kybernetické války: Představme si situaci, kdy mezi dvěma státy narůstá napětí, které vyvrcholí totální roztržkou směřující k válce. Ještě než dojde ke střetu armád, jsou plně mobilizováni IT specialisté. Nejprve dojde ke skrytému útoku na vládní servery, které jsou postupně paralyzovány. Následuje atak na bankovní systémy, čímž se zastaví fungování ekonomiky daného státu. Krátce na to se agresor zaměří na informační systémy. Základ je hotov. Útočník poté ochromí energetickou soustavu.

V tu chvíli je již v napadené zemi vyvolán chaos. Je narušena doprava i komunikace, mobilní sítě jsou postupně likvidovány. Napadený stát je pak snadnou kořistí. Taková kybernetická válka by ve svém konečném důsledku pravděpodobně vedla k významným ztrátám na životech i k výraznému zhoršení ekonomické a sociální situace.

Ruský kybernetický útok na Estonsko začínal přesně takto, ruští hackeři nejdříve vyřadili vládní a poté bankovní systémy. Zemi trvalo více než týden, než se ze všeho vzpamatovala.

V kybernetických válkách se zatím nepočítají ranění ani mrtví, po útocích nezůstávají rozbořená a vypleněná města — v nich jde o něco jiného:

Ochromit hlavní obchodní tepny, získat či zničit důležitá vládní data, narušit bezpečnost státu, poškodit síťovou infrastrukturu země. V Estonsku šlo o vyústění napjatých vztahů mezi Tallinnem a Moskvou. Útoky se odehrály krátce poté, kdy z Tallinnu, hlavního města Estonska, byl odstraněn kontroverzní památník věnovaný Rudé armádě. Reakcí byly mohutné protesty, demonstrace etnických Rusů, během kterých bylo zatčeno kolem 1300 osob, 100 zraněno a jedna usmrcena.

Památník symbolizuje v očích Estonců půlstoletí sovětské okupace, ale jeho přenesení na válečný hřbitov Rusové vnímají jako urážku padlých v boji proti nacismu. Kybernetické útoky měly podobu zahlcení serveru, ke kterému dochází například tehdy, když je přetěžován provoz.

Atakovány byly:

- stránky prezidentského úřadu a parlamentu
- téměř všechny vládní ministerstva země
- politické strany
- tři ze šesti největších zpravodajských organizací
- dvě největší banky a firmy specializující se na komunikace.

Estonci reagovali velice pružně, především zamezením zahraničnímu přístupu za účelem zachování provozu pro domácí uživatele. Rusko samozřejmě obvinění odmítalo a prohlašovalo, že třebaže tyto útoky zdánlivě pocházely i z IP adres ruských vládních úřadů, byly naopak něčí snahou poškodit Rusko. Do vyšetřování případu se vložilo i NATO, které vyslalo do Tallinnu několik svých nejlepších odborníků na kybernetický terorismus.

Skutečnost, že „počítačově-obranné" centrum NATO stojí od roku 2008 na kopci nad hlavním městem Estonska, není náhoda. V roce 2007 byl na nejsevernější ze tří pobaltských států veden první komplexní kybernetický útok na světě. Mimo provoz byly nejen banky, ale i ministerstva. Nyní je Estonsko také centrem vojenské služby pro počítačové vědce.

Pplk. Miloš Bílý