Americká útočná kybernetická strategie: Rusko bylo označeno za nepřítele USA

Autor: Leonid Savin

20. září 2018 Bílý dům zveřejnil americkou Národní kybernetickou strategii, obratem podepsanou prezidentem Donaldem Trumpem.

Nadšení z dokumentu zřejmě byli jestřábi i Demokratická strana. Prvně jmenovaní proto, že strategie obsahuje nové prvky jasně naznačující expanzivní choutky. Demokraté pak mohou být potěšení obnoveným zájmem Trumpovy vlády o kyberprostor, jelikož prezident Trump bezprostředně po svém zvolení post koordinátora kyberbezpečnosti Bílého domu zrušil a zásadním způsobem omezil i výdaje určené na tuto oblast. Nyní však Trump zdá se obrátil, jak silně naznačují mnohé shody čtyřicetistránkového dokumentu se staršími podobnými dokumenty z Obamovy éry.

Ministryně vnitřní americké bezpečnosti Kirstjen Nielsenová se v prohlášení nechala slyšet, že „tato Národní kybernetická strategie, první podobný dokument za patnáct let – jasně deklaruje odhodlání vlády spolupracovat se soukromým sektorem v boji proti hrozbám naší kybernetické bezpečnosti i zajištění nepostradatelné infrastruktury.“

Ve své tiskovém prohlášení pokračovala: „Co se týče zajištění federálních sítí, plně využíváme svých pravomocí, abychom se ujistli, že orgány aktualizují své systémy, posilují bezpečnost své elektronické komunikace a odstranily ze svých systémů antivirový program

Kaspersky.“

Lze tuto zmínku o ruské společnosti odbýt jako pouhou náhodu? Samozřejmě nikoliv. I z letmého prostudování strategie je zjevné, že Rusko bylo označeno za agresivního protivníka Spojených států a Washington je připraven vůči němu zaujmout tvrdý postoj.

O lecčems svědčí i to, že jen několik dní před zveřejněním dokumentu byla vydána také aktualizovaná podoba kybernetické strategie amerického ministerstva zahraničí, podle níž by měl Pentagon do jisté míry spolupracovat s Trumpovou vládou.

Jejich sdílený zájem je zřejmý i z porovnání formulace resumé obou dokumentů. Shrnutí strategie Pentagonu zní ve stručnosti následovně:

> „Naše země dlouhodobě strategicky soupeří s Čínou a Ruskem. Tyto země rozšířily záběr tohoto soupeření vytrvalými kampaněmi ve i prostřednictvím kyberprostoru, jež představují dlouhodobé strategické riziko pro naši zemi i naše spojence a partnery. Čína postupně rozrušuje americkou vojenskou i hospodářskou převahu dlouhodobým získáváním citlivých informací z amerických institucí veřejného i soukromého sektoru. Rusko zase využívá kybernetickým prostředím umožněných kroků k ovlivňování našich obyvatel a zásahům do našich demokratických procedur. I další státy jako Severní Korea a Írán podnikají nekalé kybernetické aktivity s cílem poškodit americké občany i americké zájmy. Rozsah i tempo zlovolné kyberaktivity v celosvětovém měřítku i nadále roste. Kvůli stále se zvyšující závislosti Spojených států na kyberprostorových nástrojích pro téměř všechny základní civilní i vojenské funkce se jedná o naléhavé a pro náš národ nepřijatelné riziko.“

V úvodu k Americké národní kybernetické strategii pak stojí:

> „Rusko, Írán a Severní Korea podnikají bezohledné kybernetické útoky, které poškozují americké obchodní zájmy doma i za hranicemi, naše spojence a partnery… Čína se za pomoci kybernetických nástrojů dopouští hospodářské špionáže a krádeží intelektuálního vlastnictví v hodnotě bilionů dolarů… Vláda si je vědoma pokračujícího soupeření Spojených států proti strategickým konkurentům, ‚darebáckým‘ státům i teroristickým a zločineckým sítím. Rusko, Čína, Írán i Severní Korea využívají kyberprostor jako nástroj proti USA a jejich spojencům a partnerům… Tito protivníci využívají kybernetické nástroje k oslabení naší ekonomiky i demokracie, kradou naše intelektuální vlastnictví a zasévají nedůvěru v naše demokratické procesy. Jsme zranitelní vůči útokům na naši kriticky důležitou infrastrukturu v čase míru a zvyšuje se také riziko, že tyto země podniknou kybernetické útoky proti Spojeným státům v průběhu krize, jež ve válku nepřeroste. Tito protivníci neustále přicházejí s novými a účinnějšími

> zbraněmi kybernetické války.“

Rusko tak bylo nejvyššími vládními úřady označeno za nepřítele USA!

Aby účinně čelili těmto skutečným i domnělým hrozbám, plánují se američtí předáci vydat cestou rizikového managementu zavádění nových informačních technologií, stanovení priorit podnikatelských záměrů či alokace veřejných prostředků soukromým subjektům na poli kybernetické bezpečnosti.

Na stránkách 9 a 10 dokumentu narazíme dva odstavce, které hovoří o globální kyberbezpečnosti námořní přepravy a vesmírného prostoru. A protože volný a neomezovaný přístup k námořním trasám, vzdušnému prostoru i na oběžnou dráhu úzce souvisejí a americkou národní i hospodářskou bezpečností, je zachování americké kontroly nad těmito oblastmi a využití nejrůznějších technických prostředků – od lodí až k satelitním systémům budoucnosti – označeno za jednu z priorit.

Mezi vyjmenovanými cíli nalezneme mj. vylepšené elektronické sledování, jež zpravodajským agenturám umožní dohlížet na datové toky, ustavení nových pravomocí vyšetřovacích i trestněprávních orgánů, rozvoj nových metod stíhání jednotlivců mimo americké území (tj. občanů cizích zemí) i další proaktivní opatření:

> „K předcházení, reakci a zabraňování škodlivým kybernetickým aktivitám, namířeným proti Spojeným státům musejí být k dispozici všechny dostupné nástroje státní moci. Tím se myslí mj. prostředky diplomatické, informační, vojenské (kyber i kinetické), finanční, zpravodajské, veřejného označení pachatele (*public attribution*) nebo prosazování práva.“

Jinými slovy tak bude od nynějška oficiálně možné odpovídat na kybernetické útoky sankcemi, koordinovanou kampaní v kontrolovaných médiích nebo odpálením řízených střel.

Trumpův Poradce pro národní bezpečnost Spojených států amerických John Bolton na tiskové konferenci ve Washingtonu výslovně uvedl, že Bílý dům „posvětil ofenzivní kybernetické operace… ne proto, že bychom snad chtěli zvýšit jejich počty, ale abychom vytvořili odstrašující struktury, jež našim protivníkům dají jasně najevo, že cena jejich operací s cílem nám uškodit bude vyšší, než jsou ochotní snést.“

Spojené státy se však při geopolitickém (a vojenském) zastrašování velmi často uchylují k zásahům do vnitřních záležitostí cizích zemí, včetně organizace krvavých převratů a nepokrytých intervencí pod chatrnými záminkami (na mysli mi okamžitě vytanulo Haiti v roce 1993), což je typicky americký přístup k ochraně své

hegemonie.

Přenesení těchto taktických metod do kyberprostoru bude zřejmě znamenat, že se ze strany Pentagonu musíme připravit na hojné DDoS útoky, využívání spyware i malware či nejrůznější metody útoků proti zranitelným „nepřátelským“ stránkám (což může znamenat cokoliv od serverů bank či mobilních operátorů přes databáze vlastněné soukromými občany, produkční infrastrukturu až po systémy zajišťující základní sociální služby). Není vyloučeno, že některé země s dostatečnými zkušenostmi v oblasti kyberbezpečnosti se těmto útokům dokáží ubránit, mnohem pravděpodobnější se však jeví, že přinejmenším některé státy je účinně a bezbolestně odrazit nezvládnou.

Zmíněna je dokonce i „kinetická“ reakce, tedy výlučné hájemství armády. Proto citujeme výňatek ze strategie amerického ministerstva obrany.

Dokument z dílny Pentagonu jasně popisuje zavádění této strategie do praxe.

> „Náš strategický přístup spočívá ve vzájemně se podporujících postupech k vytvoření efektivnější síly: bojovat a odstrašovat v kyberprostoru; budovat spojenectví a partnerství; reformovat ministerstvo; a pečovat o své talenty“.

Už první položka jasně svědčí o těchto agresivních vojenských záměrech:

> „Hodláme se soustředit na vytváření kapacit, jež velitelům Společných sil (*Joint Forces*) poskytnou co největší škálovatelnost, přizpůsobitelnost a rozmanitost pro maximální flexibilitu. Společné síly budou při ochraně a prosazování amerických zájmů schopny využívat kyberoperací na všech úrovních konfliktu, od každodenních operací až po válečné střetnutí.“

Zjednodušíme-li to, tak americká branná moc doslova dává zelenou kyberútokům a podobným operacím po celém světě. Klidně zapomeňte na jakékoliv formální vyhlášení války, což je v americkém systému velice složitý počin. Už dlouhá léta ostatně platí, že američtí vojáci se do konfliktů v cizích zemích zapojují v rámci operací, jež oficiální kritéria války ani stabilizační operace rozhodně nesplňují. Amerika si ale mnohdy s právními omezeními hlavu příliš neláme, a jelikož žádná obecně uznávaná definice „zlovolných aktů v kyberprostoru“ neexistuje, a uvedené označení tak snadno lze „přilípnout“ na cokoliv a kohokoliv, může tento krok vytvořit v kruzích amerického vojenského a politického establishmentu stát dost znepokojivý precedent.

Co víc, ze strany Washingtonu se jedná o jasný signál záměru uplatňovat nátlak i prostřednictvím mezinárodních organizací, v prvé řadě OSN. Protože OSN tradičně slouží jako platforma pro diskuse o regulacích kyberprostoru a Spojené státy zjevně tahají za kratší

konec celé řady jednání o národní jurisdikci, suverenitě a zodpovědnosti na vrcholné úrovni, snaží se teď Washington podle všeho pomstít. Proto se uchyluje k nařčením a metodám preventivní diplomacie (tj. výhrůžky a vydírání – osvědčené to metody americké zahraniční politiky).

Není tak náhoda, že web Global Security se zaměřil na jeden z bodů strategie, kde stojí: **„Prosazování amerického vlivu: Národní kyberstrategie dlouhodobě zachová otevřenost internetu** [*sic*]**, která posiluje a podporuje americké zájmy“.**

Jak by ale otevřenost internetu mohla americkým zájmům prospívat? Samozřejmě jen v případě, že Američané určují pravidla hry v kyberprostoru, podobně jako tomu je u regulace mezinárodního obchodu s americkou kontrolou bankovních transakcí, burz a dalších nástrojů globalizované ekonomiky. Pokud si snad některá země troufne vzpěčovat se pokynům z Washingtonu, rychle se stává černou ovcí globální obce a terčem nařčení ze záludného chování. Neochota přijmout americké standardy se de facto bude chápat jako akt války proti americkým občanům prostředky, vedené jinými prostředky. Takové prohlášení má proto podobnou váhu jako slova prezidenta Bushe po útocích 11. září, kdy jasně řekl, že „kdo není s námi, je proti nám“.

A tak mohou nepodložená obvinění o vměšování ruských hackerů do amerických prezidentských voleb nebo čínské průmyslové špionáži v amerických společnostech v blízké budoucnosti působit v porovnání s tím, do čeho se Washington dnes zřejmě vrhá, jako selanka a mnoho povyku pro nic.

Analýza Leonida Savina America’s Offensive Cyber Strategy vyšla na stránkách Geopolitica.ru. Původně byla publikována na stránkách Oriental Review 2. října 2018.