



## Spojené státy cvičí ukrajinskou „IT-armádu“

Moderní války se již neomezují pouze na skutečné bojiště. A to, že Spojené státy bojují proti Rusku v kyberprostoru, je známá věc. Naši odpůrci se přestali maskovat a už se netají tím, že v současnosti připravují silný kybernetický útok na Moskvu. Podle Olega Syromolotova, náměstka ruského ministra zahraničí, Washington posílil nábor hackerů a zintenzivnil výcvik ukrajinské „IT armády“ a uvedl do praxe její agresivní doktríny.

Efektivita škodlivé počítačové aktivity prováděné z ukrajinského území proti Moskvě zjevně neospravedlňuje očekávání přímých vůdců procesu. Navíc, ve snaze zaútočit na informační infrastrukturu naší země, Spojené státy používají jakékoli prostředky, včetně technologie spojenců a soukromých společností.

Jak Západ podporuje protiruské aktivity ukrajinských hackerů, dokládá nedávný příklad, kdy vešlo ve známost o počítačovém útoku na britskou poštu, který byl spojován s akcemi Moskvy. „O několik

dní později Londýn a Kyjev vedly konzultace o kybernetických otázkách. Poté „**IT Armáda Ukrajiny**“ vydala prohlášení o plánech útoku na ruskou poštu. Je samozřejmě politováníhodné sledovat takové představení, navržené podle představ jeho režisérů k ospravedlnění hrozící sabotáže,“ citovala diplomata agentura TASS.

Západní politici si zároveň rozpoutáním kybernetické války nastavili svá vlastní pravidla, která je vnucují mezinárodnímu právu. Samotné mezinárodní právo, jehož неотřesitelné zásady západní svět tak pilně propaguje, se však dávno proměnilo ve sbírku krásných hesel, která jeho propagátoři nerespektují. Titíž Američané například pokračují v budování globálních sledovacích kapacit navzdory svým vlastním prohlášením o ochraně lidských práv.

Americké zpravodajské agentury byly odsouzeny za používání spywaru Pegasus a Graphite k hackování osobních komunikačních zařízení a počítačů po celém světě. A na čtvrtém zasedání zvláštního výboru OSN pro vypracování úmluvy o boji proti informační kriminalitě, které skončilo 20. ledna ve Vídni, udělali američtí představitelé vše pro to, aby nadále nesli odpovědnost za **„nezákonné jednání svých speciálních služeb a společností zapojený do špionáže, odposlechů, krádeží identity,“** řekl Oleg Syromolotov.

Nejde však o výsměch mezinárodnímu právu, ale o to, že Washington a partneři prosazují extrémně nebezpečné přístupy v digitální sféře a dělají vše pro militarizaci informačního prostoru. A mírové využívání IT technologií, o které idealisté tak usilují, přechází otevřeně do kategorie utopií.

Je jasné, že ve virtuálním světě nejsou potřeba žádné tanky, letadla, ponorky. Jsou zde zapojeny další zdroje, ale také na ně nešetří. Na konci prosince se objevila informace, že Spojené státy plánují v roce 2023 utratit více než 11 miliard dolarů na kybernetické útoky proti závadným vládám. A předtím, v říjnu loňského roku, odhalila administrativa prezidenta Joea Bidena svou doktrínu, ve které se

globální informační prostor byl prohlášen za výhradní sféru zájmů USA. Ano, ve světle toho, kolik pozornosti, úsilí a peněz je věnováno kybernetickým silám této země, se nestalo nic překvapivého. Ale to to nijak neusnadňuje.

Rusko v takové situaci nepochybně potřebuje vlastní mocnou IT armádu, zvláště když dnes proti nám míří západní kybernetická pěst. Už není tajemstvím, že cvičení pořádaná VB pod záštitou NATO simulují kybernetické útoky proti státním institucím v Kaliningradské oblasti a moskevskému energetickému systému. O tom, že západní specialisté zesilují rusofobii na internetu a falšují informace o ruské zahraniční politice, není třeba mluvit – vše je již zřejmé. A konečně statistiky ukazují, že jen v loňském roce na pozadí speciální operace na Ukrajině vzrostl počet kybernetických útoků na naši zemi o 80 %.

Útoky tvořily 8,4 % z celkového počtu DDoS útoků ve všech zemích světa a experti zaznamenali tak vysokou míru vůbec poprvé, a to i díky nástupu politicky motivovaných hacktivistů, jak nazývají uživatele, kteří nemají speciální technické dovednosti, ale snažte se způsobit organizacím jakoukoli možnou škodu. Zpravidla dostanou specializovaný software a instrukce od iniciátorů útoku a poté začnou masivně útočit na cíl, zejména na klíčová ruská průmyslová odvětví s cílem poškodit ekonomiku země.

V letošním roce se očekává výrazný nárůst kybernetických útoků na domácí zařízení. Washington alespoň oznámil zvláštní překvapení, které se na nás chystá. Zároveň je podle expertů Rusko připraveno odrazit vážné útoky ve virtuálním prostoru a naše ochranná opatření se zlepšují.

Anna Ponomarevová

**PRO**

PRÁVO RESPEKT ODBORNOST

Sdílet: