GlobalResearch
Center for Research on Globalization

Cyber Warfare: US Military Hackers and Internet Spies

US gets ready to knock the world offline

By Leonid Savin
Global Research, September 06, 2010
Strategic Culture Foundation 6 September 2010

Theme: Intelligence, Police State & Civil Rights

After October 1 thousands of US military hackers and spies will get down to their cyber war activities.

The declarations for taking cyber defense measures can be heard more and more often in the US. US analysts state that information and communication networks, on which the national infrastructure depends on, are becoming vulnerable for cyber criminals.

Cyberspace defense issue is urgent not only for the US. “The statistics revealed that cybercriminals have upped the ante and are becoming more sophisticated and creative, distributing more aggressive forms of malware” -Defence IQ website states.

“Our statistics show that Trojans and rogueware (‘fake’ antivirus programs) amounted to almost 85 per cent of all malware activity in 2009. 2009 was also the year of Conficker, though this belies the fact that worms ranked at just 3.42 per cent of last year’s malware creation”, the magazine read.

“The Conficker worm has caused serious problems in both domestic and corporate environments, with more than 7 million computers infected worldwide, and it is still spreading rapidly”. (1)

However it seems that the US is too concerned with the problem of cyber defense in comparison with other countries. On April 26, the CIA unveiled its plans to new initiatives in the fight against Web-based attacks. The document outlines the plans for the next five years and director of the CIA Leon Pannetta said that it was “vital for the CIA to be one step ahead of the game when it comes to challenges like cyber space security” (2).

In May 2009, the White House approved Cyberspace Policy Review (3), submitted to the US president by the members of a special commission. The document summed up the state of things in the US cyberspace and national information security. It was proposed to a appoint cyber security policy official responsible for coordinating the US cyber security policies and activities.

The report outlined a new comprehensive framework to facilitate coordinated responses by government, the private sector, and allies to a significant cyber incident. The new system of coordination would enable Federal, State, local, and tribal governments to work with industry to improve the plans and resources they have in place in advance to detect,

prevent, and respond to significant cyber security incidents. The initiative also implies providing US counter intelligence with more technical and functional options and training of new cyber defense specialists.

The last but not least – in mid 2010, on the territory of the Lackland air base in Texas the construction of the first specialized cyber intelligence center for a 400 personnel began. The 68th Network Warfare Squadron and 710th Information Operations Flight were moved to San Antonio. This place was chosen because of it is close to other cyber military facilities – Air Force Intelligence, Surveillance, and Reconnaissance Agency, Texas Cryptology Center of the USNational Security Agency, united information operations command and the US Air forces cryptology support. It will function in the interests of the US Space command, US Air Forces command and US Air Forces'reserve.

Numerous publications in the US mass media show that the reform of the national cyber defense forces as well as the introduction of the doctrine and strategy of the cyber war are soon to be completed. As for the US cyber strategy we can assume that it is in line with the general concept of the US global leadership.

William Lynn III in his article "ThePentagon's Cyberstrategy", published in Foreign Affairs journal (September/October 2010), outlined five basic principles of the future strategy:

– Cyber must be recognized as a warfare domain equal to land, sea, and air;

– Any defensive posture must go beyond "good hygiene" to include sophisticated and accurate operations that allow rapid response;

– Cyber defenses must reach beyond the department's dot-mil world into commercial networks, as governed by Homeland Security;

– Cyber defenses must be pursued with international allies for an effective "shared warning" of threats; and

– The Defense Department must help to maintain and leverage U.S. technological dominance and improve the acquisitions process to keep up with the speed and agility of the information technology industry (4).

When commenting this article analysts point out that "The capabilities being sought would allow U.S. cyber-warriors to "deceive, deny, disrupt, degrade and destroy" information and computers around the globe". (5)

Gen. Keith Alexander, the head of the Pentagon's new Cyber Command(ARFORCYBER) said: "We have to have offensive capabilities, to, in real time, shut down somebody trying to attack us," Earlier Keith Alexander compared cyber attacks with weapons of mass destruction and according to his recent statements the US is planning offensive application of the new warfare.

While Washington is accusing other countries of aiding and sponsoring cyber terrorism (Statistic shows that most of cyber attacks against US informational systems were made from China), the US special forces are training new personnel for cyber wars.

The command – made up of 1,000 elite military hackers and spies under one four-star

general – is the linchpin of the Pentagon's new strategy and is slated to become fully operational Oct. 1.- Washington Post reports (6). The Defense Department has "15,000 networks and 7 million computing devices in use in dozens of countries, with 90,000 people working to maintain them and it depends heavily on commercial industry for its network operations" (7). Attracting allies and private companies working in the sphere of IT and security the US plans to establish the new order in the global cyber space.

Considering all this what may we expect? It is quite likely that we may expect spying by means of tabs and backdoors in software sold by well-known companies such as Microsoft, as well as an informational blockade, limiting access to alternative sources of information. Thus from October 1, all the achievements of the informational age can be challenged.

Notes

(1) http://www.defenceiq.com/article.cfm?externalID=2718
(2) http://www.defenceiq.com/article.cfm?externalID=2460
(3) http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
(4) William J. Lynn III W. Defending a New Domain: The Pentagon's Cyberstrategy.// Foreign Affairs. September/October 2010.
http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain(29.08.2010)
(5) Webster S. Pentagon may apply preemptive warfare policy to the Internet. August 29, 2010.
http://www.rawstory.com/rs/2010/0829/pentagon-weighs-applying-preemptive-warfare-tactics-internet/ (30.08.2010).
(6) Nakashima E. Pentagon considers preemptive strikes as part of cyber-defense strategy. Washington Post. August 28, 2010.
http://www.washingtonpost.com/wp-dyn/content/article/2010/08/28/AR2010082803849_pf.html
(7) Daniel L. Lynn Outlines Cyber Threats, Defensive Measures. American Forces Press Service.
http://www.defense.gov/news/newsarticle.aspx?id=60600
