# U.S. Launching Cyber Warfare: Towards an Era of "Computer Virus Wars"?

By Svetlana Kalmykova

Global Research, September 03, 2012
Voice of Russia and Stop NATO

Theme: Intelligence, Militarization and WMD, US NATO War Agenda

The US is launching a new stage of the arms race – a race of offensive computer weapons. Namely, the US is going to arm itself with computer viruses in order to destroy the enemy's computer networks. Besides, the US Defense Department is developing a computer program which would deduce the level of information security of the enemy's strategic facilities.

Until now, the US has been denying that it had any plans of developing "computer weapons".

A website devoted to US state procurements recently announced two tenders. The first one, announced by the US Air Force, is a tender for creating computer programs which would be able to destroy the enemy's computer networks and put computer-operated devices out of order. The Air Force is planning to spend $ 10 mln on that.

The second tender was announced by the US Defense Advanced Research Projects Agency. The agency is ready to spend $110 mln on creating a program which has already received the name "Plan X" – a digital map which would reflect the enemy's military infrastructure.

"Most probably, this map will show, first of all, military bases, transport systems and electricity systems," expert in the work of intelligence services Evgeny Yuschuk said in an interview with the Voice of Russia.

"In the case of a war, it would be quite expectable for the warring sides to try to put each other's transport and electricity systems out of order. If these systems are operated by computers, they would try to use computer viruses."

"Paradoxical as it may sound, with the appearance of computers and the Web, many kinds of equipment, including military equipment, became, in some points, more vulnerable," Mr. Yuschuk continues. "Earlier, to put out of order, say, an enemy's radar, an anti-missile device or a power plant, one had to throw a bomb at it or to send a group of diversionists. At present, they may be put out of order with the help of a computer virus program."

Analysts say that wars of computer programs, in fact, have already started. For example, in May, Iran's top officials discovered regular disappearances of secret information from their computers. Later, Iranian computer experts discovered that this information was stolen by a new virus spy program called "Flame".

The abilities of this new spy program shocked computer experts. Specialists from the Kaspersky Laboratory (a Russian company which develops anti-virus programs, probably the most popular ones in Russia) say that "Flame" is currently the world's most advanced hacker program.

“Strategically important facilities in Russia have also come under US virus programs’ attacks,” another Russian expert in the work of intelligent services, Andrey Masalovich, says.

“Attacks of virus programs have already become permanent – mainly, on nuclear power plants and on objects that have to do with the trade of weapons,” Mr. Masalovich says. “There have even been attacks on computer search engines, like the Russian Yandex.”

Sometimes, after an attack of a virus on a computer-operated facility or a computer network, it is hard to say who was behind this attack – amateur hackers or a secret intelligence service of a certain country.

Russia is now insisting that the UN should introduce a ban on creating and producing computer viruses and hacker programs.

*Stop NATO e-mail list home page with archives and search engine:*
*http://groups. yahoo.com/ group/stopnato/ messages*

*Stop NATO website and articles:*
*http://rickrozoff. wordpress. com*

*To subscribe for individual e-mails or the daily digest, unsubscribe, and otherwise change subscription status:*
*stopnato-subscribe@ yahoogroups. com*

The original source of this article is Voice of Russia and Stop NATO

*Articles by:* Svetlana Kalmykova

**Disclaimer:** The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca