GlobalResearch
Center for Research on Globalization

# Cyber Warfare, Massive "Hacker-like Penetration": The U.S. in Search of an Absolute Weapon

By Boris Volkhonsky
Global Research, October 18, 2011
Voice of Russia 18 October 2011
Region: USA
Theme: Militarization and WMD

On Tuesday, U.S. Secretary of State Hillary Clinton arrived in Tripoli bringing with her millions of dollars of U.S. aid to the interim government and a message of peace and encouragement to the Libyan people. As reported by The Washington Post, her talks focus on "how we set the table for a long-term, completely different partnership between the United States and Libya that is deep and broad."

Be it a coincidence or a pre-planned move, the day before Ms. Clinton's trip to Libya, several American newspapers published a story disclosing that the Pentagon had planned to use cyber-attacks against Muammar Gaddafi's air defense systems. The exact manner in which the U.S. military had planned to disrupt the country's air defense system and thus secure U.S. and NATO aircrafts, still remains classified, but the general picture looks as such: massive hacker-like penetration would have disrupted all computer networks of the Libyan military and prevented early-warning radars from gathering information and relaying it to missile batteries.

Why the U.S. decided not to use these techniques is also not entirely clear. One reason might have been that they just ran short of time since such operations need a lot of preparation. On the other hand, it is possible that they did not want to provoke and set an example for other countries possessing advanced computer technologies.

In any case, if such techniques had been used it would have set a precedent of a completely new type of warfare, presently known only from Hollywood blockbusters. The advantages of such warfare are obvious – the party being more advanced than the adversary, can feel 100 percent safe and operate deadly weapons inflicting strikes on enemy targets, even while comfortably sitting in their own bedrooms.

What is even more dangerous for the adversary is that sometimes it is not so easy to detect where exactly the attack had originated.

In recent times, cyber attacks have already happened several times, hitting vital facilities of the countries listed as foes of the U.S. For example, last year a Stuxnet computer worm affected Iran's computers, wiping out a part of the nuclear centrifuges and delayed the country's ability to produce nuclear fuel. Until now, it remains unclear what the source of the virus was, although there is ground to believe that the virus was of Israeli-American origin.

But what remains not so obvious is the fact that no party, even the most advanced one, can feel safe forever. Technology is advancing everywhere, and sometimes it is hard to predict

who and may strike back and when.

In August of this year, the former director of the CIA's Counterterrorist Center Cofer Black said that cyber attacks constitute the next biggest threat to the U.S. security and that the attitude of the U.S. administration to such threats is similar to the attitude towards terrorism before 9/11.

Also, this year there have been several hacker attacks on some American commercial organizations allegedly originating in China. They may not amount to cyber-terrorism or cyber-warfare, but what makes them even more dangerous is that such attacks can be launched by non-state actors and thus are virtually impossible to be detected at early stages and prevented completely.

Many years ago, a famous American science fiction writer Harry Harrison wrote a story picturing a world where no wars are possible because one community has invented an absolute weapon forcing all others to acknowledge its leading role. "Now that any war is impossible," the father says to his children, "we can use the weapon for peaceful means."

*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*



---



*Articles by:* Boris Volkhonsky