The USA and cyberwars. Part 4

Understanding better than its allies the potential of cyberattacks and the size of the possible damage that can be caused by their application, Washington has focused in recent years on strengthening its "fighting efficiency" in cyberspace. The CIA, the NSA and the Pentagon were oriented towards these goals and were annually allocated significant funds to develop and build cyberweapons. Thus, in the year 2013, just for conducting "offensive cyberoperations", developing special cyber spyware such as Flame and Duqu and cyberweapons like Stuxnet that was aimed at the "non-friendly" countries of the Middle East and Southeastern Asia (Iran, Syria, China and North Korea), Washington allocated 1 billion dollars for the NSA and 685.4 million dollars for the CIA.

Apart from involving the CIA, the NSA and the Pentagon in this activity, in 2009 Washington also established the specialised division called United States Cyber Command, with the headquarters located at the military base Fort Meade (Maryland). This specialised division was led by head of the National Security Agency General Keith Alexander. The task of Cyber Command is planning, coordination and conducting a broad range of operations in cyberspace. In accordance with Presidential policy directive Directive/PPD-20, recently signed by the US President, the main focus of Cyber Command are offensive operations and the total control over cyberspace and means of communication (such as mobile networks). In mid-2012, the state procurement website announced two tenders jointly worth 120 million dollars to develop virus programmes and the so-called “electronic map” of the location of the potential enemy. In January 2013, the US Ministry of Defense announced its intention to establish, by the year 2015, more than one hundred special cyber units at Cyber Command. The cyberunits will be engaged in both protecting domestic networks and implementing their own "offensive" scenarios.

For the 2013 fiscal year, the budget of Cyber Command has been defined as 3.94 billion dollars, and for the year 2014 – 4.65 billion dollars, with the total budget allocated for this division for the coming five years standing at 23 billion dollars. In the near future, according to the Bloomberg News agency, the number of staff of this division is going to increase to 5,000 people.

According to American open sources, the US NSA intends to make a qualitative leap, within a short time space, in the field of processing information gathered in cyberspace. The NSA is actively working on the development of modern high-performance information technology tools and on the improvement of the activities of the NSA numerous operational centres located not only within the country’s territory, but also beyond.
In particular, at the beginning of January 2012, the construction of the new complex of the Hawaii Regional Operations Security Center 'Joseph J. Rochefort Building' was completed on the island of Oahu (Hawaii). The Centre's area of operations covers the countries of the Pacific and the Middle East.

In March 2012, another new NSA facility was opened at Fort Gordon, Georgia – the John Whitelaw Regional Security Operations Center – fitted with the most cutting-edge high-performance computer equipment, which significantly enhanced its operational capabilities. This regional centre's area of operations covers the countries of Africa and the Middle East.

In addition to that, in Fort Meade (Maryland), the construction of Cyber Command's modern complex and the NSA's High Performance Computing Center (HPCC) are also approaching completion. Over 2 billion dollars was allocated by the US Congress for the construction of this facility.

As noted by foreign experts, the US Congress has been allocating substantial funds for a number of years and completely meeting the NSA's needs even though the Defense Ministry's budget cuts have been formally endorsed in legislation. Thanks to such support, the USA intends, in the short term, to place under its intelligence services' total control cyberspace and the huge information flows, including the interstate exchange channels not on the Middle East and in South Eastern Asia alone but in Western Europe as well. So should one be surprised that the media has recently discovered that Angela Merkel's phone was tapped along with a number of high profile European authorities. All these "breaking news" is nothing more than a tip of an iceberg, while the better part of the U.S. doings in their attempt to get a total control of the cyberspace remains hidden.

A natural question arises: If the US citizens look leniently at all actions of the US intelligence services in regard to these citizens and keep funding, year after year, the insatiable appetites of the CIA, the NSA, the Pentagon and Cyber Command, then how do these actions comply with international law?

(To be continued...)

Vladimir Platov, Middle East expert, exclusively for the online magazine "New Eastern Outlook".