The USA and cyberwars. Part 1

The last decade, cyberweapons have been actively used in the confrontation between ideologies, nations and states. The term "cyberwar" has been increasingly used not only in journalism and in the rhetoric of political figures, but also in the actions of many states, the USA in particular. In this connection, readers are provided with a selection of articles here looking into such issues as "the US cyberwarfare against the countries of the East", "the use of Syria's social networks by the US intelligence services", "the enhancement of control over social networks on the part of the US intelligence services", "the tools and means of the USA for conducting cyberwars", "international law and the cyberwar".

The US cyberwarfare against the countries of the East

In spite of the international community's efforts to reduce the military risk when solving interstate disputes, the war was in the past and, unfortunately, still remains a quite actively used means in the fight between countries, nations and social groups. During a war, the armed forces are used as the main means of fight along with political, economic, ideological and other means.

In the current military conflicts and wars, the range of these tools depends primarily on the financial and economic capacities of the parties participating in the wars. The more economically powerful is this or that state, the more sophisticated and large-scale are the means that it uses in military operations (latest-generation aircraft, ships, aircraft carriers, missiles, nuclear tactical weapons or even nuclear bombs as it happened in 1945 when they were used against the Japanese cities of Hiroshima and Nagasaki). There are ample examples of that: just look what is happening right now around the Syrian conflict and what resources and forces have already been concentrated by Washington to put in place a "military action of intimidation of Damascus" in the Mediterranean and the Red Sea, in the countries which are so-called "Syria's friends".

The weaker are the countries or opposition forces, the less selective they get in terms of the means used in military activities, even resorting to the use of chemical weapons or terrorist actions. Very often, of course, this does not happen without the involvement of the powers pumping the conflict regions and states with more weapons, in the hope of gaining dominance over the countries and areas which are, first of all, rich in natural resources. I think that there is no need for examples here since we all remember very well the developments around Iraq, Libya, Syria and a number of other countries and what role was played, say, by the USA in those events.

In spite of the public calls made by the heads of the world's leading countries on the international stage to stop the war and in spite of the fact that some of them have even been awarded the "peace prize" (it is, obviously, clear that we talk here of Nobel Prize laureate B.Obama, in particular), it is these countries that are carrying out research and development in the field of new and more sophisticated means of war. It is them who are now, on the basis of "humane considerations", conducting wars using bloodless, technological means by transferring military activities to the information space and waging information wars, cyberwars and cyberterrorist actions.

The USA and its most loyal allies are in the permanent status of a real cyberwar, whilst Russia, China, Iran and a host of countries of the East, which have considerable reserves of natural wealth and human resources, are their...
Thus, in spite of Washington's formidable campaign to raise international awareness of the alleged threat on the part of China in cyberspace, the website of China's Ministry of Defence alone was subjected to about 144 thousand cyberattacks each month in 2012. And it is remarkable that more than 60% of the IP addresses from which these attacks were launched were registered in the USA.

The confrontation between the USA and China has a decades-long history reflected in the Pentagon's various secret plans, including even the USA's "preventive strikes" on China under the code name AirSeaBattle1. You could say that the cyberwar between these two countries was given a certain impetus by the events that took place in Yugoslavia in 1999, when a NATO aircraft opened fire at the PRC embassy in Belgrade. Back then, in response to this military action, China's Red Hacker Alliance launched a number of powerful hacker attacks against the US government websites.

The cyberwar waged by Washington in the Middle East is, first of all, associated with the dissemination in the region of the computer virus Stuxnet: there are numerous sources and experts pointing to the fact that the United States (in particular, the American company Symantec) and Israel took active part in the development of Stuxnet. It is known that Stuxnet was primarily aimed at industrial facilities, including Iranian factories and nuclear plants. As a result of this cyberattack, the Iranian nuclear industry nearly ended up under the control of Stuxnet's developers, who could have easily and very quickly arranged large-scale industrial sabotage, including possible radioactive contamination of not only Iran's territory but also of the whole region.

In 2012, the new computer virus Flame was identified; it was capable to delete information from the computers of the Iranian Ministry of Petroleum and affect the country's entire infrastructure. Flame was a very aggressive virus, and its creation was associated with "experts" of the American intelligence services and Symantec.

The active use of the capabilities of cyberspace by the US CIA's "experts" to launch cyberattacks, with some of them turning into real cyberwars, is broadly known. However, some of the aspects are worth looking at in more detail.

(To be continued...)

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