The USA and cyberwars. Part 3

The enhancement of control over social networks on the part of the US intelligence services

One of the main areas of the US intelligence services' activity has recently been the enhanced control of the electronic information space, social networks, in particular. Initially, this control was mainly carried out in the form of detecting the so-called "domestic" threats coming from mentally unstable or extremist-minded individuals as well as from such organisations as the Anonymous group or the terrorist organisation Al-Qaida, which are considered by the US intelligence services' officials a national security threat. However, another important area of such activity has been, in the last period, the probing of social networks in order to determine and control the public opinion and the reaction of various segments of the population to the internal and external policy of the US administration.

For example, according to the information published in November 2011 by The Associated Press, the CIA alone daily monitors 5 million users of social networks, in particular, Twitter, Facebook and Internet blogs. A team of one hundred CIA staff referred to internally as "vengeful librarians" are constantly analysing information from social networks in various languages in order to form a real-time vision of the public opinion in various regions around the world and to gather intelligence information of their interest. According to Doug Naquin, Director of the CIA Open Source Center, such daily analysis "is evaluated most positively at the highest level in the White House".

Following the developments of the Green Revolution of 2009, in which Twitter and Facebook played an important role, the CIA Open Source Center, established in 2005 in accordance with the recommendations of the US Congress 9/11 Commission with the priority task of countering terrorism, was also assigned to monitor through social networking the developments in Egypt, Bangkok and Iran. Although the majority of the Center's staff are based in Virginia, a significant number of them also work in various countries around the world under the diplomatic cover of the US embassies by supplying the information of Washington's interest "directly from the regions which present interest for the USA".

Apart from the CIA, a considerable amount of work on controlling social network websites is also carried out by the US Ministry of Defence, in particular, through the programme "Social Media in Strategic Communication" of the Pentagon's Defence Advanced Research Projects Agency (DARPA), which is engaged in the development of special software tools and means of monitoring the Internet networks and exerting influence on users' behaviour. In particular, for the year 2011, it was planned to allocate 41 million dollars for the funding of DARPA's research programmes in three major areas:

- developing the tools and methods enabling the Pentagon to analyse the processes taking place in social networks with a view to identifying the "organisers of persuasion campaign structures";
- "exerting effective influence on the "operations" of possible potential adversaries in social networks;
- taking measures for the "counter messaging of detected adversary influence operations".

The technical aspect of DARPA's programme implies the development of automatic or semi-automatic software tools and means to ensure systematic obtaining of information from social networks and its analysis. With their help, it is possible to "identify, classify and monitor the shaping and dissemination of ideas and concepts as well as targeted
and misleading disinformation, to determine the organisers of advocacy campaigns, identify participants and their intentions, develop and implement measures to counter adversary influence operations. The programmes that are being developed DARPA also provide for automatic content generation in social networks by using the so-called "sock puppet" or "bots" (false accounts) which conceal the real installation data of concrete individuals advocating "special points of view" and, by creating false propaganda websites, they attract those social network users who sympathise with the opposition or extremists.

One of the high-profile denunciations of the US intelligence services' activity related to the monitoring of social networks was the article published by the newspaper Le Monde on 30 November 2011, in which 25-year-old American Android developer Trevor Eckhart reported that he had spotted spyware CarrierIQ on 140 million American Android phones BlackBerry and Nokia, and that, when you press the phone keys, the spyware sends the information on the users and their SMS-messages to the US intelligence services.

The fact that the United States has been implementing, in the computer information space, secret programmes of monitoring their own citizens as well as those abroad has also been confirmed by the revelations of the recent months made by former CIA contractor Edward Snowden.

Given the billions of dollars in annual costs of the American intelligence services for the implementation of these secret programmes in cyberspace, this kind of activity could now be rightfully described as not just cyberattacks or cyberoperations, but a proper cyberwar conducted by the USA both against its own people and foreign states.

What is remarkable here is that considerable funds for monitoring and secret cyberprogrammes directed against US residents are coming from this country's citizens themselves! – But maybe they have no other way to spend their own money? Have all the problems related to unemployment, education, healthcare and other social fields been solved in the USA? – It would be nice to hear their own opinion on this!

(To be continued...)

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