The USA and cyberwars. Part 5

Keith Alexander, head of the USA's Cyber Command, noted a few years ago: “To respond to attacks promptly, we need clear-cut areas of operations and rules of warfare”.

Indeed, the international law for conventional combat operations, described in the Geneva Conventions, does not reflect the peculiarities of cyberwars. There is a need to develop new rules.

In the background of the increasing use of cyberweapons to inflict significant damage on the adversary, many countries have been recently working intensively on the development of the legal aspects which could form the foundation for the resolution of international disputes when conflicts occur in cyberspace. Let us not dwell at this point on the diversity of these projects, where each, of course, has its positive and negative aspects. The most active work in this regard is being carried out in the United States and in NATO's specialised units dealing with planning and conducting cyberattacks.

In this context, of considerable interest may be the Manual on International Law Applicable to Cyber Warfare prepared by the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence. For the development of this document, NATO set up a special expert group under the guidance of Professor Michael N. Schmitt. The group was made up of experts from Cambridge University and a number of American and European research centres.

The document, which is the result of three years’ work, is designed to include the virtual space in the compilation of the international rules pertaining to conducting a conventional war, applying force by states and developing military operations. The authors of the Manual note in the Introduction that "there are no specific international treaty provisions today that directly deal with a war in cyberspace, but legal aspects of warfare must be applicable to cyber warfare". That is why the Manual makes an attempt to unfold the content of the existing legal instruments of a national and international nature, used in the consideration of issues of conventional wars, for their application to cyberspace and cyberwarfare. When it becomes impossible to relate the innovative capabilities of cyberweapons to existing law, the document proposes to adapt such law, where possible, to cyberwarfare.

The first fundamental legal concept considered in the document is national sovereignty. As noted by its developers, "if a State cannot claim global dominance in cyberspace, however, it still remains sovereign within its territory in cyberspace". Hence, according to the document, the sovereignty of cyberspace extends to all cyberinfrastructures within the state's territory (including, beyond its national borders). This clarification is very important since, based on threats to the state's sovereignty, it is proposed afterwards to consider the legitimacy of NATO's probable armed activities and cyberprotection measures against the initiator of such a threat.
Any attack on information infrastructure within a country's territory can, therefore, be interpreted as the violation of the national sovereignty of NATO's entity (whether major infrastructure or just a small private company). In the meantime, the experts working on the document did not manage to come to an agreement on whether possession of cyberweapons as such manifests the intention to violate a state's sovereignty... They only remind us that an "illegitimate operation (whether cyberoperation or any other normal military operation) is the one that poses a threat to the territorial integrity or political independence of a nation or is in conflict with the provisions of the United Nations".

At the same time, the authors are convinced that a cyberoperation can be aimed at the illegitimate use of force, same as in the case of a conventional armed attack, which would justify immediate military response.

The NATO Cooperative Cyber Defence Centre of Excellence intends to make this document an official instrument of international law when considering cyberconflicts.

However, it is quite obvious that the Manual is adjusted to the interests of the USA and NATO and offers them justified opportunities to launch a counter cyberattack or a conventional military attack against a certain agency or company (either private or public) or state that launched a cyberattack. Therefore, what if the Manual is going to become an instrument in Washington's hands to unleash new "retaliation" wars as we are seeing now, with the use of the information campaign - staged by the American intelligence services - "on Damascus's use of chemical weapons" in the preparation for the armed action against Syria? And what if we all are going to become hostages of the new instruments of the militant hawks who are so enthusiastically striving for global dominance, including in cyberspace?

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