Vitaly Tsygichko

Cyber weapons and how they transform the entire traditional paradigmof warfare

Analysts define four factors facilitating the use of cyber weapons. Theydetermine key directions of research concerning the combat use of cyberweapons.

Freedom of access to information systems. Development of informationnetworks leads to the emergence of new challenges on the part of cyber weapons.A competent swindler has a potential opportunity to gain immediate access to awide range of national strategic targets making the global informationinfrastructure. Under these circumstances, inter-connected computer networksmay become a victim of many threats initiated by skilled individuals,non-governmental structures (such as international crime groups) and statespossessing well-trained personnel for combat operation in cyberspace.

Transparency of state boundaries. One of the most significantparticularities of global information infrastructure (and nationalinfrastructures) is the elimination of traditional borders. The growinginterdependence of national and global systems inevitably undermines nationalsovereignty. One of the most serious aspects of such transparency of borders isthe lack of distinction between internal and external threats and vanishingdifference among various forms of action against the state – from regularcrime to military operations. Without clear distinction into external andinternal threats, it is difficult to identify traditional espionage, crime, orwar.

Some countries that lack sufficient military and economic power may tryto profit from this situation and attack the enemy infrastructure through thecyberspace by using individuals or international criminal community. It ispractically impossible to identify the organizer of such *strategic criminaloperations*, i.e. the person who has given the order. As a result, a victim ofcyber attack cannot understand what is going on and what actions should betaken in response.

Perception management. As a result of development of informationsystems, diminishing costs of access to the information and undermining ofnational sovereignty, there are expanding opportunities for manipulations withinformation that enable to shape the perception. For instance, the Internet maybe used for dissemination of propagandistic materials from different sources.Political groups may use the Internet to mobilize political support.

It is quite possible that facts describing certain event may bedistorted with the help of text, graphics and video techniques. This willenable a broad range of individuals and groups concerned to affect publicperception and organize large propagandistic campaigns in order to underminepeople's trust in the government. Such campaigns cause serious problemsnot only for the government, but for the mass media, which are supposed todisseminate objective information. The direct consequence of such use of cyberweapons is deception of the leadership and the society.

The lack of intelligence data. In the conditions oftransparent borders and free access to information, the intelligence serviceface serious problems in providing the government with reliable and timelystrategic information concerning current and prospective threats of cyberwarfare. It becomes more difficult to identify the objects for intelligence.The classical geo-strategic approach (focusing on specific state – asource of threat) is now nearly obsolete. The targets for intelligence aretransnational non-governmental and criminal organizations and non-state actors.The significance of information challenge will depend on the assessment ofcapabilities and intentions of potential enemies in the cyberspace andvulnerability of targets.

To identify the capabilities of the enemy employing cyber weapons, oneshould learn to resist dynamic development of telecommunication systems used byhardware and software, as well as by protection means (e.g. encoding devices).The future national information infrastructure will include the set ofdifferent components of technologically and economically developed society.Such components may be:

- general purposecommutation systems;
- electric powersupply grids;
- systems formaintaining federal reserves;
- healthcare;
- the prioritytargets for suppression or destruction are enemy information and intelligencemeans, which should be neutralized before the beginning of large-scale combatoperations;
- all available meansshould be employed to destroy the information infrastructure; one has to outdothe enemy in cyber battles;

Nowadays the most detailed concept of cyber weapons employment is the USplan of fighting against command and control systems. It was laid down in theearly 1990s and provided for the set of deliberate combat tasks to disorganize,suppress and destroy the enemy command and control structures. Higheffectiveness of such strategy has repeatedly been demonstrated in localconflicts, during the military exercise and modeling. According to the USanalysts, disorganization of the command and control system reduces the enemycombat potential by 50% and more, providing for US superiority in conflict.

The impact on communication systems is as follows:

- destruction withconventional munitions guided by radio and radio-technical intelligence means;
- destruction withnew generation high-precision weapons guided by radio and radio-technicalintelligence means to the area of the target with further self-search for thetarget and self-targeting at the most vulnerable elements of the target;
- generatingimitating jamming impeding connection, synchronization in data transferchannels, initiating functions of repeated queries and duplication of messages;
- destruction ofelectronic components with high-level electromagnetic and ionizing radiation;

The combat use of cyber weapons based on program codes depends on twofactors:

- external impact onthe system through the devices connecting it to another system with facilitatedaccess for the enemy;

It is presumed that in case of real conflict the most critical elementsof the state and military infrastructure may be isolated from accessibleinformation systems. Besides, the United States works at the possibility ofisolating its systems from the information systems of the allies. However, ifmultinational units are deployed the prospects for the use of IT to conductcyber offensive are increasing.

The sue of IT in cyber offensive is highly efficient in case of internalimpact on the system. Depending on the level of responsibility of the agent,the outcome of such impact may be total disruption of its functioning for along period of time. Such activities may involve either recruited personnel, orearlier installed software and viruses initializing at certain moment and incertain situation.

The efficiency of the use of cyber weapons is also closely connectedwith the issue of complex intelligence and counter-intelligence support. Intelligencesupport should include:

- development ofdatabases and collection of detailed information on the situation in thepotential conflict zones;
- assessment ofcapabilities and weak points of the potential targets in the system of controland communication. This information will help to identify the elements, whoseearly destruction will facilitate the accomplishment of combat missions;
- analysis of theenemy capabilities to influence control and communication systems. Collectionof precise information and classification of all sources of radio emanation inthe entire band of electromagnetic spectrum;