Vitaly Tsygichko

Cyber Weapons as New Means of Combat.

Classification of Cyber Weapons

Abstract

The development of the universalclassification and a system of identification attributes of informationalweapons is a foundation for launching meaningful international negotiations onproblems of its development, application and proliferation. A functionalapproach to informational weapon classification and a subjective classification exercised on its basisare suggested.

The definition of the subject area of international information security and its conceptual tools is the most pressing task for drafting an international legal framework securing control over the development, limitation and proliferation of informational weapons (IW). The key concept for defining the subject area of information security is the one of "**informational weapons**". Yet, despite an intensive research into the problem conducted in variouscountries, no uniform concept has been developed thus far, Russia included. Webelieve that the definition and classification of IW should be based on afunctional approach, i.e. with regard to the forms, ways and consequences ofits utilization. Key to the suggested approach is the concept of"information war" for this form of armed confrontation suggests theuse of the entire variety of IW. In all other areas of IW potential application(informational confrontation, informational terrorism, and informational crime)only individual types of IW can be used.

The definition of "**information war**" concept sparked heated debates. The majority of analysts believe, however, that since the concept of "war" is clearly defined in international legal documents as an open armed struggle between states or groups thereof, hence "information war" is a part of combat operations along with traditional forms thereof. In outlining a wide range of issues linked to concepts of combat operations in "information age", international security experts and the military more and more frequently use the term "information war". The new concepts of warfare are closely linked to the fact that a rapid evolution of cyberspacetime. the global information infrastructure on national and international levels can not only open up extra opportunities for upgrading weaponry and military equipment, but also give rise to new problems of warring parties 'vulnerability. More vulnerable at present is the warring party, which has less information on the battlefield, is slower in data processing and decision making. While an essential shortage of tactical information could, in past wars, be offset by putting in additional forces, then now informational superiority does, in effect, unambiguosly determine the outcome of modern transient military conflict. Hence, information war can be defined as **actions taken for securing information superiority by damaging information, information-based processes, and information systems of the enemy along with protecting one's own information, information-based processes, and information systems.**

The results of informational weapons application manifest themselves in a destructive impact on civilian and military information infrastructure of the enemy and in disorganization of political and military control systems, in damaging or disturbing information systems, obtaining or distorting data contained in them, as well as in a purposeful dissemination of beneficial information.

Proceeding from the above definition, **it would be logical to refer to the non-traditional means of armed struggle, helping to effectively achieve the information war objectives, as to informational weapons. The latter should assist in gaining informational superiority, preventing heavy fire strikes and orienting at high-precision, selective and possibly maximum latent non-lethal ways of action.** Naturally, these attributes of IW identification are rather general and can, with time, be specified and expanded. Yet, they are conducive to a primary IW classification useful for further research in this area.

All types of IW, falling under thesuggested identification attributes, can be classified by objects and means ofinfluence. IW can be classified into:

- Means for highly accurate spotting of electromagnetic equipment and its destruction by way of rapid identification of separate components of control, recognition, guidance and fire information systems.
- Means for hitting components of electronic equipment and power supply thereof with a view to putting individual components of electronic systems out of action for short-term or irreversibly.
- Means of affecting software of electronic control modules for putting the latter out of action or for altering the functioning algorithm thereof with special software.
- Means for affecting data transmission process with a view to terminating or disorganizing operations of data exchange subsystems by affecting signal propagation environments and functioning algorithms.
- Propaganda and disinformation facilities for modifying control system data, creating virtual picture of the situation different from real one, changing human value system, damaging morale of the adversary’s population.

It would be wrong to say that this classification encompasses all possible types of informational weapons, which can emerge in future. However, it fully covers all of the known current developments.

The informational weapons of each type can, in its turn, be classified by a number of attributes:

- Single- and multisession or universal.
- Short- and long-range of operation.
- Individual, group and mass destruction.
- Type of carrier.
- Destruction effect.

Informational weapons can be divided into two categories: information technology-based weapons and weapons having energy or chemical effect. Examples of informational weapons based on energy action are given below:

- High precision homing ammunition, cruise missiles or strike unmanned flying vehicles.
- Facilities for power electronic suppression, superpower ultra-high frequency generators, facilities for power action via electrical networks.
- Ground and airborne electronic struggle facilities, disposable jamming transmitters.
- Special oscillators affecting human psyche.

The following means are examples of informational weapons based on chemical effect: ammunition filled out with gases, aerosols or biological cultures destroying components of electronic facilities.

Most promising is utilization of information technologies as information weaponry. Information technologies are an integral component of high-precision ammunitions as they are guided by systems of position finding and reconnaissance by visual, electronic and other give-away factors. It would therefore be reasonable to treat these functional subsystems as informational weapons too.

Also, under intensive development is soft-code-based informational weapons. The latter's delivery to the target is exercised in different ways:

- Through self-dissemination of virus-like envelopes, the most sophisticated viruses break security systems and travel along information networks (so called "worms").
- Through the transfer by other frequently used software, whose initialization launches informational weapons.
- Through various long-term data storage facilities, including reprogrammable chips.
- Through bookmarks, known as "Trojan horse", embedded in advance.
- Through remote embedding of program code through input ports.

These types of information weaponry allow the following actions:

- Putting electronic systems out of operation by tuning hard disk heads to resonance or by "burning out" displays.
- Erasing writeable store.
- Switching continuous power supply sources to a dangerous power setting or turning off their protective functions.
- Breaking information security systems.
- Penetrating into the enemy's information systems.
- Masquerading sources of information.
- Disabling all or concrete IS software, possibly at precisely fixed instant in time or upon a certain event within the system.
- Secret partial modification of software functioning algorithm.
- Collecting data circulating in the enemy's information system.
- Delivery and embedding certain algorithms in a specific place within the information system.
- Affecting data transmission protocols of communications and data transmission systems.
- Affecting addressing and routing algorithms in communications and data transmission systems.
- Intercepting data and disturbing flow thereof through transmission channels.
- Overloading the system with faked queries.
- Creation of or altering virtual reality.
- Imitating the voices of control system operators (e.g., systems of internal affairs department) and creating virtual video images of concrete individuals with their own voices (leaders of parties and countries).
- Modification of data stored in databases of the enemy's information systems.
- Input of false information and data (e.g., target designation or freight destinations) in the enemy's information systems.
- Security system disinformation.
- Altering data in navigation systems, meteorological systems, precise time systems, etc.

The above informational weapons classification is far from being universal and complete. We hope, however, that it can serve as a basis for international negotiations on information security problems. We believe also that our suggestions may trigger wide discussions of the problem. It is quite possible that, following the future joint activities, the above classification could be expanded, modified or replaced with some other set of attributes and terms of IW identification, reflecting the common approach of scientific community to the problem.