CYBERSPACE AS A SPHERE OF WARFARE

Yaroshchuk V.D., *vadim2003ya@gmail.com*
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

Development of information and cyber technologies and global informatization have led to the fact that the information and cyber sphere have become areas in which and through which various destructive influences are carried out on all spheres of activity of society. Cyberspace supplemented the existing ones and became a new and first artificially formed sphere of conflicts and possible military operations. Moreover, the future war may be provoked in cyberspace.

The concept of "cyberspace" was first used in 1984 by the American writer William Gibson to refer to the entire set of information contained in computer networks. In the doctrine of information operations of the US Armed Forces of 2006, it was defined: "cyberspace is a virtual environment, in which digital information circulates in computer networks" [2].

The first official definition of cyberspace was given by US military experts in the 2006 Information Operations Guide: "Cyberspace is an area that uses various radio-electronic means that use a wide range of frequencies of the electromagnetic spectrum for receiving, transmitting, processing, storing, converting, and sharing information, as well as the related information infrastructure of the US Armed Forces" [2].

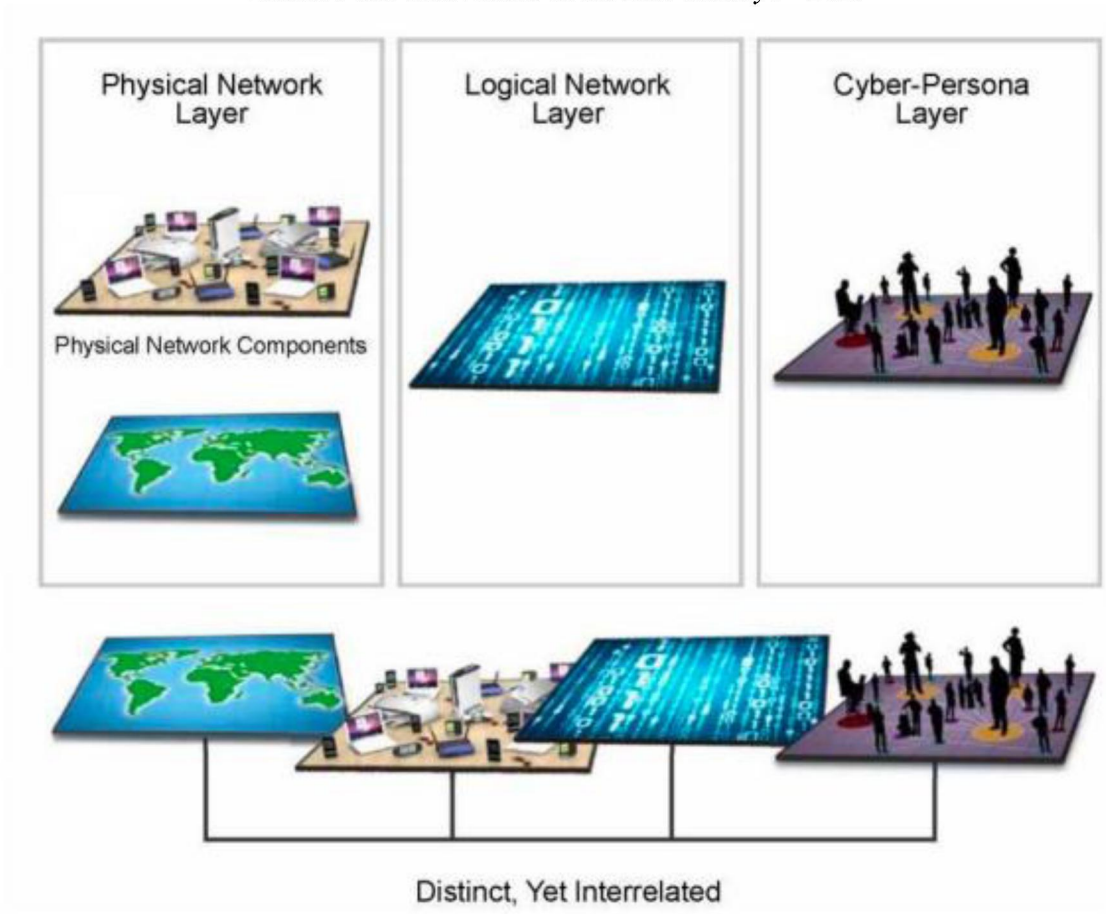
Cyberspace consists of three layers: a physical network, a logical network and cyber-persona.

Physical network layer includes IT devices and infrastructure in the physical dimension that provides storage, transmission, and information processing in cyberspace, including data warehouses and communications, which transmit data between network components [1].

The logical network layer consists of network elements that are combined with each other in a way based on logical programming that controls network components [1].

The cyber-persona layer consists of a network or it's user accounts, both real human and automatic, and their relationships with each other [1].

The cyberspace level model is shown in the figure below.



According to individual US military experts, the dominance of the cyberspace should go beyond telecommunications and information technology and needs advantages in all its components: social, technical, telecommunications, information, network computer, etc. and over the entire electromagnetic spectrum – "from direct current to daylight, including radio waves, infrared and X-ray radiation, directed energy, and areas about which we haven't even started thinking about ensuring a global command and control, global access and global power" [3]. Therefore, the following components of cyberspace should be considered: a part of the information space directly related to cyberspace, the space of communication systems, the virtual computer-network space, and the sociotechnical one space.

Currently, cyberspace is considered as a combination of society, which forms the social component of cyberspace, and a set of technical and software features funds that are the technological basis for the formation of a technical component cyberspace and their intersection and unification of the sociotechnical system that forms the ideas about its sociotechnical nature.

Before the advent of active artificial intelligence, a person is an integral part of the phenomenon of cyberspace, which is a participant in all processes, forms cyberspace and supports its existence, functioning and development. It can become self-organized and self-managed only in the presence of artificial intelligence. People in cyberspace are represented in their activities, in their interactions in and through cyberspace.

Therefore, we can conclude that, in most countries of the world, the defense sector of states includes two main components: the deterrent potential, consisting of traditional types of Armed Forces, and the potential for waging wars of a new type, which is based on the forces and means of special operations, cybersecurity and Cyber Defense, Information and psychological operations, electronic warfare, intelligence, information and analytical support. Therefore, among the threats to national security in the military sphere, many countries have already today, they see not only a lag in the development and adoption of the arming new high-tech weapons and military equipment.

This topic is and will continue to be relevant throughout the 21st century, because it is not for nothing that it is considered the century of the information boom.

References

1. JP 3-13 Information 51 Operations Doctrine. URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf (Last accessed 04.03.2021)

2. Cyberspace Operations Concept Capability Plan 2016-2028. URL: https://fas.org/irp/doddir/army/pam525-7-8.pdf (Last accessed 04.03.2021)

3. Govorukha V.V., Danik Yu. G., Klevets V. V. (2009). Directions for improving the mechanisms of functioning of Public Administration bodies in the conditions of transformation of technologies of external information and psychological influence on them / / actual problems of Public Administration. (1). 9-16. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/apdy_2009_1_3.pdf (Last accessed 04.03.2021)

Language adviser: *Sokyrska O.S., PhD in Philology, senior lecturer, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"*