Chapter 7
The Fifth Space of Military Action and Confrontation

Nika Chitadze
International Black Sea University, Georgia

ABSTRACT

The concept of fifth dimension operations is conceptually based on adding the five-dimensional, holistic approach to warfare that uses the three dimensions of land, sea, and aerospace but also incorporates the temporal and cyber dimensions of warfare. In more recent times, the concept of fifth dimensional operations, as a concept under military operations, has taken a wider scope than its original information operations background, focusing on the advanced space-time manipulating capabilities cyberspace offers. This development was begun as early as 1996 in regards to advanced battlespace and cybermaneuver concepts.

INTRODUCTION: TECHNOLOGY DEVELOPMENT AND THE ISSUE OF USING TERMS IN THE INFORMATION (CYBER) SPACE

In the information age, one of the main factors in the development of the socio-political system has become the production and use of information. It plays a decisive role not only in public and state institutions but also in the life of each person and is the only reality of communication with the world. Computers and digital information and telecommunication systems are used in everyday life, in all spheres of human, society, and state activity - ensuring national security and state governance as a whole (health care, education, housing and communal services, air and railway communications, trade, etc.).

Comprehensive internet technologies have changed the political, economic, and social reality. Along with the emergence of the World Wide Web, the state gradually loses certain functions, its role and influence on human relations decreases, and the state border changes its original purpose. For example, cyber terrorists can "invade" another state, conduct criminal operations and cause great damage to the country. The nature of war and the standards of its understanding have also changed.

Thus, from the second half of the 20th century, the classic forms of military armed wars and conflicts are gradually being replaced by new forms of conflict, among them cyberterrorism, and cyberwar. The

DOI: 10.4018/978-1-6684-8846-1.ch007

area of military action and conflict has become cyberspace - a complex interconnection of information and telecommunication technological infrastructure, which includes the global Internet network, computer systems, telecommunication networks, and processors. Cyberspace does not exist in any physical form, it is a complex virtual environment that is created as a result of the interaction between people, software, Internet services, technological devices, networks, and network connections.

The fifth form of war, cyber war (besides land, sea, air, and space dimensions), attempts to gain informational-technological superiority in the information age have given rise to new dangers, where no one obeys the imposed restrictions and prohibitions.

The urgency of the problem of cyberspace protection is due to the unprecedented development of information communication and cyber technologies, the irreversible processes of cyber-attacks of an indefinite scale, which present to the whole world the need to strengthen security measures.

The Growing Danger and the Expansion of the Scientific-Research Area

Back in the industrial era, the technical term "security" (computer, information, cyber) is used to protect the computer from threats arising after the emergence of computer viruses, which refers to the protection of computer and information-telecommunications components (networks, computers, programs, data, devices) from cyber-attacks (Digital attacks, damage, unauthorized access, etc.) A set of technical protection technologies, methods, and processes.

Since the end of the last century, viruses have become not only a narrow target of computers but also an unpredictably damaging weapon and have become a huge problem with catastrophic consequences for the world. For the creators of viruses, on the battlefield of cyberspace, the computer becomes not a goal, but a means, and a multi-step combined target - national security mechanisms, and state and defense military infrastructures.

Both, states and the provision of national security of individual countries, moreover, humanity as a whole, faced danger. It is a fact that in the information age, following the unprecedented development of digital technologies that damage computer components, extremely diverse and unpredictable threats arising from computer viruses have gone beyond the narrow scope of the computer and have created a threat to all spheres of state and public life, threatening the fundamental values of national security: personal safety, social security, and state security, national security assurance system.

Coping with the emerging danger in itself required serious socio-political decisions at the national and international levels (as well as academic research, development of new political theories, new normative requirements, regulation systems, social norms, etc.).

To solve the problem, if technical measures taken by informatics specialists were sufficient before, today it is necessary to take political, legal, economic, military-defense, and social measures.

Dr. Robert Dewar, a Swiss specialist in cyber security and cyber defense, notes that there is an increasing focus on cyberspace from politicians and the military, as cyber security is already a legal, military, and economic challenge. No state can cope with this global problem alone, only with its forces and resources (Dewar, 2022).

It is welcome that in the last decade, a whole plethora of researchers working on cyber security problems who develop this point of view have appeared in Western scientific circles (Collier, 2018). For example, Professor Miriam Dan Cavelty of the Zurich Center for Security Research and Professor Andreas Wenger, a recognized researcher on the "threat politics" of cyberspace, points out that "as