Cyberspace: Key Properties and Traits

V Kh Fedorov¹, E G Balenko¹, Yu I Starodubtsev², P V Zakalkin²

¹Federal State Budgetary Educational Institution of Higher Education DON STATE AGRARIAN UNIVERSITY
pos. Persianovsky, 346493, Russian Federation
²FGKVOU VPO "Military Academy of communications named after Marshal of the Soviet Union S. M. Budyonny», St. Petersburg, 143900, Russian Federation

E-mail: balenko2008@mail.ru, Yelena.Vershennik@mail.ru

Abstract. Backbone telecom networks have become one, which created an artificially global space known as cyberspace. The very emergence of such a complex space calls for detailed investigation and making a thesaurus. This paper is an attempt to create a terminology base applicable to the concept.

1. Introduction
Globalization creates regional centers of power that wield substantial political, economic, and military resources. There are ever more international corporations that have ever greater financial capacities; in fact, we have come to a single labor, finance, and technology market; further exacerbating the conundrum are the dwindling non-renewables, the inexorable increase in population (~75 million every year), the actual collapse of supranational organizations such as the UN, OSCE, etc., and the existence of billions of individuals with diverse goals and approaches to them. All the factors have inevitably resulted in a multitude conflicts that the existing legal frameworks can still resolve; yet, the backlog of issues civilized resolution cannot address is piling up [1-2].

2. Statement of problem
Analysis shows the known optional solutions do not fully apply to the situations that arise from globalization.

Firstly, newly developed, tested, and proven economic methods for seizing any resources are not limited by nationality or geographical location.

Secondly, total eradication of the enemy’s manpower is irrelevant in the context of how nearly any country’s population is heterogeneous in terms of race, ethnicity, religion, economic status, etc.

Thirdly, taking physical possession of the enemy’s weapons is far less significant now thanks to the international arms market. This factor is somewhat mitigated by the fact that many specifications of the i-th specimen of armaments only fully apply to the j-th environment that cannot be reproduced in reasonable time.

Fourthly, actual annexation of more territory only creates more problems, as the annexing party has to ensure some minimum living standard, and only a limited portion of that area will actually generate profits—profits, that could be made alternatively, e.g., by economic exploitation.
Fifthly, total destruction of the opposing party’s economic potential is virtually of no value today, as substantial, and often critical elements of any national economy are owned by other states or international corporations.

Sixthly, all fields of any state’s or nation’s activity are now deeply integrated into cyberspace. This research is mainly an attempt to create a terminology base for the area.

3. Theory

Cyberspace is a concept that has many interpretations; the key definitions are listed in Table 1.

Table 1. Interpretations of the concept of cyberspace.

| Source | Interpretation |
|--------|----------------|
| Russia – U.S. Bilateral on Cybersecurity “Critical Terminology Foundations 2” – EastWest Institute, 2013. – 82 p. “Dictionary of Military and Associated Terms” Department of Defense, 2013. – 482 p. | Is an electronic medium through which information is created, transmitted, received, stored, processed and deleted. Global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. |
| Cybersecurity Strategy Concept of the Russian Federation (draft) | A field of information space activity that arises from the combination of (i) communication channels backed by the Internet and other telecom networks and infrastructures, and (ii) any human activity carried by such channels, whether on individual, organizational, or national level. |
| ISO/IEC 27032:2012 | The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form. |
| Order of the Russian Railways No. 3192r dd. December 30, 2014 | An environment created by computer and communication networks where information and data exchange takes place. Cyberspace elements include servers, computers, telecom equipment, communication channels, information and telecommunication networks. |
| ITU-T X.1205 (04/2008) SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Telecommunication security. Overview of cybersecurity. | Software that runs on computing devices, the stored (also transmitted) information on these devices or information that are generated by these devices. Installations and buildings that house the devices are also part of the cyber environment. |

However, the existing definitions rely on terminology that is not clearly defined or does not have a clear physical meaning, ignores causal relations, and is not based on the principle of constructiveness, which effectively compromises any attempt to formulate research problems to solve [3].
The authors hereof came up with the following definition: **Cyberspace** is an artificial heterogeneous technological space with many supervision and process control agents at different tiers, the process of creating and operating which is not predetermined by the requirements of one control system, but functions in the interests of many heterogeneous control systems, some of which can be antagonistic, whereby its properties depend both on those of the cyberspace elements and on the scope and properties of the processes being run in the interests of internal and external consumers.

In the process of research, the authors isolated the following key features of cyberspace:

- cyberspace does not have a single design idea behind it, nor does it have a single control system or a single architectural toolset.
- cyberspace is heterogeneous. It refers to any means that create cyberspace, communication channels, the density of their placement in an area, the connectedness between them, the bandwidth of communication lines, the number of subscribers, etc. To give an example of such heterogeneity: fiber optic lines, satellite communication networks, 3G/4G/5G networks use different equipment and different media to carry data, and yet their users can freely exchange data. The density of cellular base stations is another example of cyberspace heterogeneity. Megacities like Moscow or St. Petersburg have as many stations per unit area as possible, whilst they are few and far in between in sparsely populated areas;
- each telecom carrier controls its own segment of cyberspace and develops it exclusively in its own interests. Therefore, cyberspace is controlled by multiple agents at different tiers. It is safe to say the cyberspace is controlled by everyone and no-one at the same time;
- technological processes are integrated using cyberspace resources. Cyberspace controls or serves as the means to control processes run within or by critical national infrastructures, their facilities and actors, including the banking system, logistics, energy, water supply, health sector, education, etc. Notably, whereas cyberspace controls the energy sector, the latter actually powers up cyberspace, i.e., cyberspace somewhat independently controls its own critical resource.
- the advancement and buildup of cyberspace capacities has complicated its algorithms. Cyberspace elements exchange service data; balancing, loading, self-testing, integrated security, and power control systems enable cyberspace to function for extended periods of time with virtually no intervention from the maintenance staff. It is safe to say that in the near future, cyberspace will dictate the quality and the very feasibility of its own vital processes;
- cyberspace functions by running various foreign-made protocols and equipment that supranational structures create to serve their own interests. For instance, telecom protocols, standards, and control interfaces are in line with the recommendations of the International Telecommunication Union (ITU-T);
- data exchange in cyberspace serves the interests of many non-biological objects (automatic control systems, critical infrastructure monitoring systems, IoT, communication equipment, etc.), and there are many times more of them than people.

The properties of any space per classical definition of the term apply to cyberspace as well:

- **Objectivity.** Cyberspace is created by humanity but exists regardless of the needs of an individual. Cyberspace will exist, function, and provide its resources to an unlimited number of users, whether biological or electronic, regardless of the needs of an individual or group of persons at or around the moment. Often, people do not realize that they might be using cyberspace resources at the moment. Examples include car navigation, GPS-enabled smartwatch, cell phone, etc.
- **Physical changeability.** Cyberspace has three dimensions, and thus the location of each of its elements can be described in coordinates. Besides, each cyberspace elements has such dimensions as length, height, and width. The virtual part of cyberspace can use such coordinates as IP addresses, unique networks IDs, etc.
- **Physicality.** Cyberspace has energy, time, and information parameters.
In addition to the classical properties of any space, cyberspace features *indestructibility*. Given that cyberspace covers the entire planet and near space, destroying it physically is not an option in the current context for both technical and political reasons.

4. Conclusions
Thus, this paper discusses the key features and traits of cyberspace that allow viewing it as an actual space, as we would consider land, air, or water space. Besides, the terminology base proposed herein enables further cyberspace research.

5. References
[1] Starodubtsev Y I, Balenko E G, Zakalkin P V, Fedorov V H 2020 Change dynamics for forms and opportunities of centers of power under globalization In the collection: 2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon) p 9271172
[2] Starodubtsev Yu I, Zakalkin P V, Ivanov S A 2020 Technosphere war as the main way of resolving conflicts in the context of globalization *Military Thought* 10 pp 16-21
[3] Starodubtsev Y I, Vershennik E V, Balenko E G, Fedorov V H 2020 Cyberspace: terminology, properties, problems of operation In the collection: 2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon) p 9271282