Advances in Military Technology
Vol. 16, No. 1, 2021, pp. 91-105
ISSN 1802-2308, eISSN 2533-4123
DOI 10.3849/aimt.01466

Relationships between Cyberspace Operations and Information Operations

Zs. Haig*

Department of Electronic Warfare, National University of Public Service, Budapest, Hungary

The manuscript was received on 7 December 2020 and was accepted after revision for publication as technical information on 14 April 2021.

Abstract:

Today thanks to the wireless networking technologies and social networks, the interpretation of cyberspace has expanded. According to the three-layered structure of cyberspace, not only logical effects can be induced in this domain, e.g. by malwares, but physical and cognitive effects also appear in the physical and cyber-persona layers, e.g. electronic jamming the wireless communications of network or influencing and manipulating users. This approach provides an opportunity to interpret cyberspace operations in a more complex way and to apply integrated technical and cognitive information capabilities that exploit each other's effects. Accordingly, this study presents an expanded interpretation of cyberspace, a novel and complex approach to cyberspace operations, as well as the information capabilities that can be used in these operations.

Keywords:

cyberspace, cyberspace operations, cyberspace superiority, information operations, technical and cognitive information capabilities

1 Introduction

Nowadays the rapid development of infocommunication technologies have exceeded the habitual network organizational principles, and in recent years they have brought a paradigm shift in the interpretation of networks and their operational environment, i.e. the cyberspace. Beside the conventional computer networks, the paradigm shift is mainly characterized by the significant spread of wireless networking technology, including e.g. the growing use of wireless sensor networks, 5G, M2M (Machine to Machine) communications and IoT (Internet of Things) technology. According to Statista, by the end of 2018, 22 billion IoT devices were in use around the world, which is expected to increase to 30.6 billion by 2025 and 50 billion by 2030 [1].

* *Corresponding author: Department of Electronic Warfare, Faculty of Military Sciences and Officer Training, National University of Public Service, H-1101 Hungária krt. 9-11, Budapest, Hungary. Phone: +36 1 432 9000/29343, E-mail: haig.zsolt@uni-nke.hu*

IoT can be interpreted as a worldwide network of uniquely addressable objects. IoT appears in people's daily lives, in smart homes and smart cities, as well as in the infrastructures that provide social functioning, such as healthcare, energy supply, industrial companies, transportation, public security and national defense. IoT architecture consists of the following four stages:

- networked things, typically wireless sensors and actuators, which are named as cyber-physical devices,
- sensor data aggregation and analogue-to-digital data conversion systems,
- edge IT systems to perform pre-processing of the data, as well as
- cloud computing data center systems to analyze, manage, and store data [2].

One of the critical elements of IoT technology is the communication, especially its wireless solutions. At stages 1 and 2, basically short-range and low-power communications are used, such as RFID (Radio-Frequency Identification), ZigBee, WiFi, BLE (Bluetooth Low Energy), etc. At stages 3 and 4, longer range communications are necessary, e.g. with mobile cellular systems (3G, 4G, 5G), or with long-range but low-power LPWAN (Low Power Wide Area Network) devices, such as LoraWan (Long Range Radio Wide Area Network), NB-IoT (Narrow Band IoT), etc. 5G is a major driver of IoT growth. This new mobile technology provides higher data rates (peak data rates: 20 Gbit/s and user experienced data rate: 100+ Mbit/s), extremely low latency (1 ms) and more capacity and connectivity than 4G. These qualitative features are fundamental e.g. for the large-scale proliferation of IoT and especially for autonomous vehicles. By 2024, the number of 5G mobile subscriptions is forecast to rise to around 1.9 billion worldwide [3].

This wireless networking tendency can also be observed in military systems. We can experience the gradual emergence of civilian technologies in the military networks. Several DARPA (Defense Advanced Research Projects Agency) projects focus on research into IoT, sensor networks, and artificial intelligence. They plan to monitor critical junctions, major roadways and railroads, bridges, as well as critical infrastructures and their environment with cheap, small and mass-deployable IoT sensors [4]. NATO STO (Science and Technology Organization) also began research into the military applicability of the IoT. The IST-147 (COM) research project examines the application possibilities of IoT in base operations, situational awareness, energy management, boundary surveillance including harbor etc. [5]. These research directions confirm that the IoT has many military applications. In addition to the above, IoMT (Internet of Military Things) or IoBT (Internet of Battlefield Things) applications include e.g. C4ISR, logistics, fire-control, health monitoring and other applications.

One of the important questions in creating and operating networks is the implementation of communications. Due to the requirement of mobility, the typical communication method of networks today is the wireless connection within the electromagnetic spectrum. Wireless communication in military operations, especially for maneuvering troops, is mostly the only solution in networked command and control, e.g. in the operational application of the tactical internet. However, compared to wired communications, wireless technology expands potential attack possibilities, e.g. by COMINT (Communications Intelligence) and radio jamming, GPS spoofing, etc., thereby increasing the vulnerability of networked systems.

In addition, we can see that the use of cyberspace networking technology for cognitive information and interaction purposes is increasing significantly thanks to social media. As a result, many people as users become actors of cyberspace. Because of this, people can be reached with targeted information more easily than ever before.

With targeted information, they can be informed, influenced and manipulated with greater efficiency. These information activities can also be observed in the structure of cyberspace, which will be discussed in detail in section 3.

The operating environment for each of these new, networked technologies is cyberspace. So, the cyberspace has become much more complex, due to the diversity of devices and systems used in networks, as well as wireless communications technologies. This complexity is further reinforced by the fact that people carry out their information activities largely on the Internet, especially in social media. Thus, cyberspace can be interpreted not only technologically but also in its cognitive effects. This also means that due to the complexity of cyberspace, threats are also more complex and attack surfaces are increasing and becoming more extensive.

Based on the above, the aim of this study is to interpret cyberspace operations within this new type of network environment in correlation with the information operations and their capabilities, as well as to prove the expansion of the interpretation and domains of cyberspace, and based on this, to verify the applicability of the various information activities of information operations in cyberspace.

2 The Interpretation of Cyberspace

Because of the spread of networked devices, the cyberspace nowadays is an ever increasing part of the information environment and thus of the information battlefield. Namely, today the use of modern networked infocommunication devices can be correlated with cyberspace. But what exactly is cyberspace, how can we interpret it, and what is contained within this domain?

According to the initial widely accepted definition, cyberspace has been identified as a common name of the virtual world made up of computer networks and their services and information they contain. A large group of experts and users think that cyberspace is a multidimensional, artificially created virtual reality, made up by computers and communication connections, and based on a global network.

The radical expansion of wireless networking technologies has resulted in a novel, expanded approach of cyberspace. Today the majority of users use mobile devices and mostly connect to the networks, and therefore to the internet via wireless radiofrequency connections. In addition to human-machine wireless connectivity, the growth of M2M connections (see introduction) also has a significant impact on the proliferation of wireless networks. The development of Wi-Fi technologies and mobile cellular communications, especially the 5G, as well as short- and long-range data communication solutions (e.g. ZigBee, LoraWan, NB-IoT, etc.) of other systems (e.g. IoT) enhances this tendency. This also means that in the interpretation of cyberspace, the electromagnetic spectrum appears as a new element, which can be physically and mathematically well defined.

The appearance of electromagnetic spectrum in cyberspace is shown in Sanjeev Relia's definition, who writes: *"Cyberspace is that human created digital medium used to collect, store and transmit data and information between humans using electronic devices through The EM spectrum enabling nearly instant, boundless, global connectivity without organisational, cultural, national or political borders."* [6].

It is conspicuous that according to more and more definitions, cyberspace goes beyond the world of computers. In 2008, the ITU (International Telecommunication Union) defines the cyber environment in correlation with cybersecurity as follows: *"This includes users, networks, devices, all software, processes, information in stor-*

age or transit, applications, services, and systems that can be connected directly or indirectly to networks." [7].

Military science was amongst the firsts to realize this comprehensive and expanded definition of cyberspace, and declared that it is considered as one of the important areas of military operation environment and information battlefield. According to the military terminology dictionary issued by the USA DoD in 2017, the cyberspace is *"A 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."* [8].

By analyzing the referenced cyberspace definitions, we can draw the following conclusions: Cyberspace is a manmade domain that provides interpersonal relationships for people. A very good example of this is the social media, where people can establish new kind of connections, create connection networks by using the latest network technologies. However, we have to highlight the fact that the new type of connection space provided by cyberspace is not solely for people. With the appearance of IoT and the M2M communication, connecting physical devices into networks and accessing various smart services (self-driving cars, smart homes, smart cities etc.) becomes available. In this case, in cyberspace we are not talking about interpersonal relationship, even if there are indirect services provided for people.

Besides this, cyberspace is a dynamic domain, which points at its ever changing and expanding nature. This change and expansion are indicated by the quantity and variety of devices that can be used in this space (e.g. cyber-physical devices, sensor technology, IoT), by the improvement of communication methods (e.g. M2M connections), and by the shifting emphasis from wired to wireless. It is also important that, in addition to traditional computer networks, any device or system that is connected to networks via wired or wireless communication methods, and collects, stores, processes and transmits information is part of the cyberspace.

Ke Xu and co-authors highlight such nature of cyberspace where humans, computers, and smart objects are pervasively interconnected. This interconnection can be observed in the integration of IoT and existing network systems, including the Internet, cloud computing, cellular network, social and industrial networks. They point out that the integration of heterogeneous network technologies is the major driver of network innovation. In consequence, they offer novel interdisciplinary concepts such as the Cloud of Things (CoT), the Web of Things (WoT), and the Social Internet of Things (SIoT) [9].

Based on the analysis and synthesis of the presented definitions we can compose a novel, comprehensive definition of cyberspace as follows. *The cyberspace is an artificially created, dynamically changing domain, where the infocommunication devices and systems – connected to each other via networks, and using also the electromagnetic spectrum – operate to collect, store, process, forward and utilize information, enabling continuous and global connection between people and various devices.*

This definition supports the structure of cyberspace – presented in the next chapter – and provide an opportunity to interpret cyberspace operations more broadly than before. In addition to the typical malware threats, these operations include electronic attack modes against the network and its components (e.g. electronic interception, electronic jamming and spoofing, etc.) and protective measures (e.g. electronic defense, TEMPEST, shielding, etc.) that can be used in the electromagnetic spectrum, as

well as cognitive influencing techniques (e.g. propaganda, fake news, misinformation, etc.). This definition also points out that cyberspace is now becoming not only an arena for interpersonal relationships, but also for human-machine and machine-machine connections. This also means that attack and defense surfaces further expand for cyberspace operations. These will be discussed in more details in the following sections.

It is important to emphasize that the military interpretation of cyberspace can also be applied to networked electronic systems. At the present, however, not every device is networked in the military operations. There are several electronic devices which operate independently on the battlefield, e.g. stand-alone unattended sensors, expendable jammers, RC-IED-s (Radio Controlled Improvised Explosion Devices), etc. These devices also manage information. The sensors collect data and transmit them into data processing centers, which are used in decision-making, or expendable jammers interfere e.g. communication. However, these devices do not do this in a networked operating environment such as e.g. the IoMT systems. As the most important element in the interpretation of cyberspace is networked operation, so these military electronic devices (systems) are not part of cyberspace, their operating environment is not the cyberspace.

At the same time, the networking can also be observed in military applications. In this case, we can discover the formation of both loose and firm heterogeneous networks, similarly to the civilian sphere. These are also the main sources of military network development in military operational applications. Good examples for these heterogeneous networks are the military cloud, the IoMT, or IoBT, the tactical internet, as well as the ad hoc networked unattended ground sensor systems.

Therefore, it can be seen that there is a convergence between the cyberspace and the electromagnetic spectrum. This means that these two domains have a common set, based on the operation of networked infocommunication systems. However, the full convergence has not yet taken place, but for instance the U.S. Army's Cyberspace and Electronic Warfare Operations doctrine published in 2017, already shows a closer connection between electronic warfare in the electromagnetic spectrum and cyberspace operations [10].

The appearance of the electromagnetic spectrum in the cyberspace is important because communication by radiofrequency increases the possibility of threats against networks. Due to the growing prevalence of wireless networking technologies and their widespread use in military operations, electronic warfare (EW) as one of the capabilities of information operations, is also becoming an increasingly important part of cyberspace operations. This military activity, which is over nearly 120 years old, has always played an important role in restricting enemy's command and control capabilities. The possibility of using it in cyberspace further enhances the importance of this capability.

EW is similar to computer network operations (CNO) in many ways. Main tasks of both are intelligence, attack and protection of command and control systems, but the CNO does all these with logical methods, e.g. with malwares, while EW carries them out in the electromagnetic spectrum by causing physical effects. EW in the cyberspace is manifested in the electronic surveillance (electronic support measures), electronic attack (electronic jamming, deception and neutralization) and electronic defense of network devices and network communications. In addition, during CNO, malwares are injected into the network in the radio frequency spectrum through wireless access. So, this may also be considered as a specific and novel EW technique, i.e.

transmitting malwares to the network instead of signals interference. Based on these, the appearance of EW in cyberspace indicates a serious challenge to network protection and cybersecurity for both system designers and users.

3 The Structure of Cyberspace

The cyberspace is part of the information environment; it can be interpreted in all three of its dimensions, i.e. the physical, informational and cognitive dimension. The various literatures on cyberspace mostly refer to these dimensions as layers. They interpret various components with different names within the layers that also define the relationship with each other. [6, 11-13]. Using these, we can include the following among the layers and components of cyberspace:

- physical layer:
  - geographic component,
  - network component,
- logical layer,
- cyber-persona layer:
  - interface component,
  - user component,
  - social component (Fig. 1).

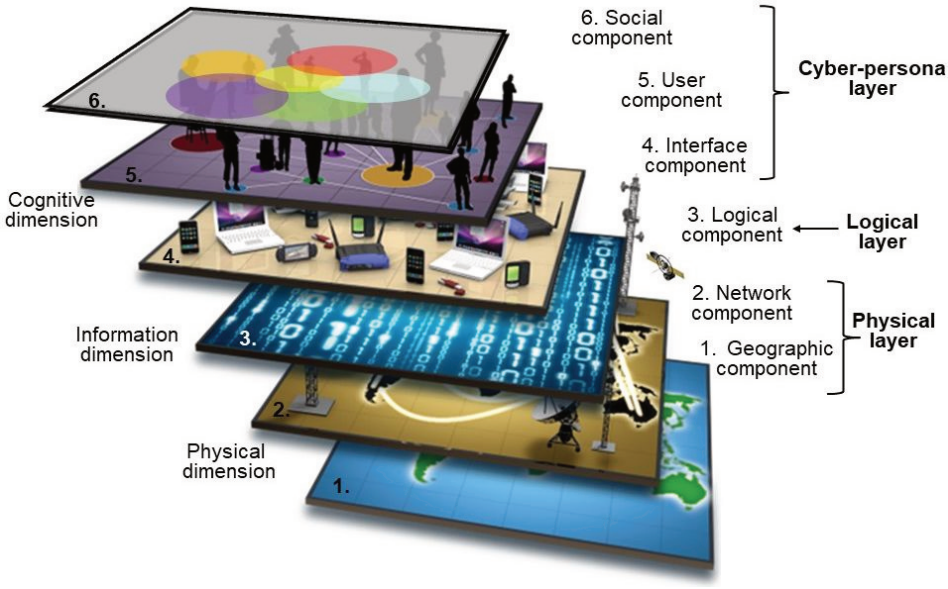

Fig. 1 Structure of cyberspace (edited by the author based on [13-14]*)*

The physical layer consists of geographic and network components. The geographic component refers to the geographical/physical location of the infrastructures and the hardware elements of the networks. The network component shows the types and kinds of the infrastructure and the hardware elements of the networks. These include among others the sensors, data storage centers, servers, routers, cables, optical cables, radiofrequency data transmitting devices, mobile cellular base stations, satellite

devices, etc. The physical layer also includes the electromagnetic spectrum, as the physically definable domain of the wireless network communications.

The logical layer is the virtual space of the network, which contains the physically not tangible elements of cyberspace. The elements of the logical layer could be the information managed in the networks, transmission control- and address protocols {like e.g. TCP/IP (Transmission Control Protocol/Internet Protocol)}, software applications, the data of network providers and users, internet domain names, information security solutions, etc.

The cyber-persona layer consists of interface, user and social components. This layer personalizes the cyberspace. This means the digital representation of network users in the cyberspace. The identities of the cyberspace actors appear in this layer that e.g. can be used to obtain information and to influence users, while their real identities and affiliations remain hidden [15].

In the cyber-persona layer, the interface component connects people to the logical and physical layers of cyberspace and through them to each other, applying the users' hardware and software tools. This contains the user's own personal infocommunication devices, like personal computers, laptops, tablets, smartphones, navigation devices etc.

The user component refers to the people on the network, who have unique addresses, ID-s, e.g. IP address, e-mail address. A person can even have multiple personalities in the network, e.g. one can be a registered user on multiple social media platforms, can have multiple e-mail accounts, or can connect to the network using various devices, like PC-s, tablets, smartphones.

The third and highest level of the cyber-persona layer is the social component which means the relations and interactions of the people on the networks. Because of the intensifying of usage of social media, the significance of this component is increasingly important. Thanks to the social component, the individuals are now not merely passive users of the cyberspace, but also its active participants.

The properties of these layers and components show in which layers and what devices, techniques and procedures can be applied to realize information operations taking place in the cyberspace, It shows who or what could be their targets and what effects can be achieved by certain information operations capabilities.

Accordingly, the following information operation activities can be conducted in the three layers:

- in the physical layer e.g. physical destruction of network infrastructures, electronic based intelligence, interception and jamming of network communication devices, or protection against these methods,
- in the logical layer e.g. applying Malwares, deleting or compromising databases, limiting network access by DDoS (Distributed Denial of Service) attacks etc., or protection activities using firewalls, antivirus software, access control, etc.,
- in the cyber-persona layer e.g. influencing the users by targeted messages, news, hoaxes, fake news, or enhancing the protection by security awareness training.

4 A Brief Overview of Information Operations

The information environment is the operational domain of the information operations, in which physical, informational and cognitive dimensions can be interpreted. Cyber-

space makes up an increasingly important and significant part of this environment, and it touches all three dimensions of information environment.

The general purpose of information operations is to support military operations in the information environment. Creating information superiority and/or influencing effects, depending on the nature, and environment or target audience of the operations, can achieve this general purpose. In traditional military operations, the information superiority is basically a technical question. Weakening the enemy's information capabilities and protecting one's own capabilities can usually gain it. In 4th generation operations, the information operations are often not carried out against enemies, instead the target audience contains neutral actors, civilians. The purpose of these operations is not the weakening of capabilities, but convincing or influencing civilian actors. It can be achieved by the influence-based adaptive informational superiority [16].

Information operations are a set of activities aimed at the integrated, synchronized and coordinated application of information capabilities in the information environment, which create desired effects on the will, understanding and capability of the target audience directly with cognitive capabilities and/or indirectly with technical capabilities to achieve the objectives of the operations [17].

These information capabilities can be divided into the following two major groups, depending on dimensions which they affect:

- technical capabilities,
- cognitive capabilities.

The technical capabilities focus on information management processes, namely information gathering, storing, processing and transmitting. In contrast, the cognitive capabilities focus on the content of the information, using various mediating tools and methods and they directly target the conscious activities of people with pre-designed messages.

Based on the above, the technical and cognitive capabilities of information operations include:

- technical capabilities:
    - electronic warfare (EW),
    - computer network operations (CNO),
    - physical destruction of information targets,
    - technical capabilities of operation security (OPSEC),
    - technical capabilities of deception.
- cognitive capabilities:
    - psychological operations (PSYOPS),
    - public affairs,
    - civil-military cooperation (CIMIC),
    - cognitive capabilities of operation security,
    - cognitive capabilities of deception.

The synchronized and integrated application of the technical and cognitive capabilities appropriate to the target audience ensures the achievement of the objectives of information operations and thus the successful support of military operations.

5 Cyberspace Operations

5.1 Cyberspace Superiority and Cyberspace Influencing Effects

In parallel with the recognition of the significance of cyberspace, the interpretation of cyberspace superiority also appeared in military doctrines. The US Army's doctrine FM 3-12 Cyberspace and Electronic Warfare Operations issued in 2017 defines cyberspace superiority. According to the definition: *"Cyberspace superiority is the degree of dominance in cyberspace by one force that permits The secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an enemy or adversary. Cyberspace superiority enables, supports, provides, and facilitates warfighting capabilities that affect, support, and enable every warfighting function and daily activity."* [10]. Cyberspace superiority is the part of information superiority that can be achieved by the utilization of networked infocommunication technologies, and as a result of this, one's own capabilities increase significantly.

Similarly to information superiority, we can distinguish three equal and closely related elements of achieving and maintaining cyberspace superiority:

- information gathering about the other parties' capabilities, about own possibilities and environment by using various electronic and IT data collection devices, sensors and communication tools,
- obstructing the operation of the other parties' networked infocommunication systems, restricting and encumbering the procession and transmission of information, as well as influencing the decision makers and personnel through infocommunication networks,
- protection of one's own networked information capabilities, decision makers and personnel against the other parties' various logical and physical (electronic) attacks and influencing attempts implemented via networks.

In non-traditional, 4th generation hybrid operations, where the enemy is not obviously identified, similarly to the traditional informational superiority, the traditional cyberspace superiority cannot be completely interpreted. The use of cyber countermeasures and negative influencing effects is not appropriate against civilian actors. Instead, the goal is to create adaptive cyberspace superiority caused by influencing and information effects.

5.2 Interpretation of Cyberspace Operations

The traditional and adaptive cyberspace superiority is related to the information superiority and part of that, which can be achieved in cyberspace. Since the cyberspace superiority is interpreted as part of the information superiority, it can be achieved through cyberspace operations that can be interpreted as a part of information operations.

Based on the definition of information operations, we can define cyberspace operations. Cyberspace operations are a set of activities aimed at the integrated, synchronized and coordinated application of information capabilities in the cyberspace, which uses cyberspace networked infocommunication systems to create desired effects on the will, understanding and capability of the target audience directly with

cognitive capabilities and/or indirectly with technical capabilities, to achieve the objectives of the operations.

In consideration of the expanded interpretation of cyberspace, activities within the scope of technical capabilities include:

- accessing the computer networks and exploitation them,
- accessing, modifying, and destroying databases,
- disrupting services by DDoS attacks,
- interception of telecommunication networks,
- jamming of data collection and communication devices and systems,
- various forms of electronic attacks against navigation systems, as well as
- protection against the similar activities of the opposing parties.

The cognitive capabilities taking place in the cyberspace can be accomplished by real and false messages delivered to the target audience through networked infocommunication systems. These may include messages and news disseminated via internet news portals, social media, and partly through the traditional electronic media (TV, radio), which are able to influence and inform the public opinion of the chosen target group or target individuals. The listed activities introduce just a few examples from the wide range that can be used for offensive purposes against the other parties' networked infocommunication systems and user, or for defensive purposes, in the interest of protecting our own similar systems, as well as preparing people and enhancing their security awareness.

Activities in cyberspace contribute to achieving military purposes more and more frequently. This is supported by the events that have already taken place, in which opposing parties carried out cyberattack activities synchronized with armed conflicts. The conflicts in Georgia and eastern Ukraine are model examples of this. These operations were often focused on restricting the other party's infocommunication systems, and through them, they caused serious damage in the operation of some critical infrastructures.

Thus, in 2008, the Georgian parliament and government websites became unavailable, and in December 2015, after annexation of the Crimea, there was a service outage in the Ukrainian power supply, caused by a backdoor malware called BlackEnergy [18]. Both cases were linked with actual military operations, and based on this, both Georgia and Ukraine assumed that Russia was behind the attacks. Either regular and irregular forces, or even civilian hacker groups can carry out these types of cyberspace operations in order to support military operations and political goals.

However, thanks to today's networked society, the use of cyberspace operations is not solely related to military operations. Today, we encounter news on a daily basis, which report various hacker groups carry out cyberattacks against government agencies, institutes, economic organizations, etc. in hopes of achieving political goals or economic benefit. Attacks in this physical and logical layer induce service outages, database alterations, data theft etc. in the networked infrastructure of the attacked organization, and their effects also appear in the physical and logical layer of cyberspace.

In addition, nowadays we are more frequently encountered with such cyberspace effects, where the purpose is not to cause malfunction in some kind of information infrastructure, but to influence the network users and through them the public opinion. These "soft attacks" do not damage the data and information, nor the hardware and software elements of the infocommunication system. Instead, by disseminating politi-

cal and ideological messages on the network, they attempt to achieve such influencing effects in the people and in a wide range of society that serves the interests of the disseminator of messages and news. All of these also prove that the cyberspace operations remove the sharp boundaries between the war in Clausewitzian sense and the peacetime activities for political purposes. Therefore, this is one of the most important characteristics of cyberspace and cyberspace operations.

Tab. 1, which summarizes the usable information capabilities in cyberspace, illustrates the targets (target groups) of each capabilities, the applicable offensive activities against the targets, the protection methods and influencing effects, as well as the relationship of these activities to the layers of cyberspace. Accurate, real-time, and relevant intelligence is essential for the effective application of each capability. Therefore, although intelligence is not part of information operations and thus cyberspace operations, the table also includes the cyberspace appearance of electronic based intelligence.

Technical information capabilities are basically related to the physical and logical layers of cyberspace, they are realized in them and their effects also prevails there. In contrast, the cognitive information capabilities focus on the humans to form and shape the attitudes, opinions, thinking, behavior of people and social groups. Thanks to modern network technologies, the usage of targeted messages delivered via the internet, especially social networks, has now become almost commonplace. Based on this, the scene of applying cognitive information capabilities can also be the cyberspace, even its physical and logical layers, and the messages transmitted through them have an effect in the cyber-persona layer.

6 Conclusions

Nowadays, the amount of data generated and managed in networks is constantly growing. The new network technology, characterized by IoT and cloud computing, not only generates large amounts of data, but it also offers more efficient data storage and processing solutions than before. Thanks to IoT and M2M connections, full interconnection has come true in networks with cyber physical sensors and actuators, as illustrated, e.g. by smart home and smart city concepts.

The data management benefits of sensor networks, IoT and cloud technology are also having an impact on military networks. The integration of sensors, embedded devices, database technology, and software analysis into a battlefield network closely reflects the essence of IoT. Compared to the past, IoT based sensor networks provide significantly more data on the position, technical means and capabilities of the opposing party, as well as changes in the battlefield environment. As a result, cloud-based data storage, processing, and information sharing enable more efficient command and control, and decision-making. Based on this, we can recognize such nature of cyberspace where humans, computers, and smart objects are pervasively interconnected. It means that today cyberspace is not only a domain for interpersonal relationships, but also for human-machine and machine-machine connections.

However, due to the nature of wireless technology, the military application of IoT (IoMT, IoBT) and cloud technology also faces many vulnerabilities, such as modifying or compromising sensor data, unauthorized access to data, jamming network communication, etc. From the aspect of military operations in cyberspace, these technological developments and new vulnerabilities required the redefinition of cyberspace and its structure. Accordingly, beside the purely logical conception, the physical

space, including the electromagnetic spectrum as well as the cognitive domain are also important parts of cyberspace.

Tab. 1 Information capabilities of cyberspace operations

Capability	Targets	Activities	Layers of cyberspace	
			Activity	Effect
Electronic based intelligence	Networked electronic devices; Wireless communication	Signal intelligence; Measurement intelligence, Open source intelligence, etc.	Physical	Physical
Computer network operations	Network, Hardware; Software; Operating systems; Databases; Cyber-physical devices	Computer network exploitation, attack and defence, e.g. Malware, DDoS, deleting and modification of databases, etc.	Logical	Logical; Physical
Electronic warfare	Networked electronic devices; Sensors; Wireless communication; Navigation; Cyber-physical devices	Electronic intelligence; Electronic jamming;, Electronic deception; Electronic neutralization; Electronic protection	Physical	Physical
Physical destruction	Hardware; Elements of networked information infrastructure;	Destruction and damage of information targets	Physical	Physical
Operation security	Elements of networked infrastructures; Databases; People Communication;	Electronic information security, Physical security; Personal security; Encryption Security awareness, etc.	Physical; Logical; Cyber-persona	Physical; Logical; Cyber-persona
Deception	Network; Sensors; Databases; People; Community groups; Communication;	Electronic deception; disinformation; Spoofing, Social Engineering, Fake news.	Physical; Logical; Cyber-persona	Physical; Logical; Cyber-persona
Psychological operations	People; Community group	Influence via internet, news portals, social media, e-mail; Social engineering	Physical; Logical; Cyber-persona	Cyber-persona
Civil-military cooperation	People; Community group; Government and administrative organizations	Cooperation and relationship building via internet, news portals, social media, e-mail.	Physical; Logical; Cyber-persona	Cyber-persona
Public affairs	People; Community group	Information via internet, news portals, social media, e-mail; Social engineering	Physical; Logical; Cyber-persona	Cyber-persona

The main result of this paper is that it presents that the approach of three-layered (physical, logical and cyber-persona) structure of cyberspace provides an opportunity to interpret cyberspace operations in a more complex way, which is not limited to only CNO (e.g using malwares, DDoS attack, antivirus software, etc.). The essence of this is that in a similar way to information operations we also use integrated technical and cognitive information capabilities that take advantage of each other's effects in cyberspace.

Based on the above, the research results confirm (see the Tab. 1) that the cyberspace operations are carried out in all the three layers of cyberspace as follows:

- in the logical layer using logical information activities and tools, such as malwares, DDoS attacks, firewalls, antiviruses within the networks,
- in the physical layer, namely in the electromagnetic spectrum with methods of electronic intelligence, electronic attack, as well as physical and electronic protection, and
- in the cyber-persona layer, i.e. in the cognitive domain with cognitive capabilities based on real and credible or misleading information.

Therefore, we can conclude that information activities in cyberspace now point beyond the traditional CNO, and thanks to wireless technologies, effective attack and defense solutions can be applied within the confines of EW, as well as in the cognitive domain due to the spread of social media. Moreover, according to a novel interpretation of cyberspace, cognitive influence can be accomplished much more effectively in a human-created social networking environment. In addition, thanks to the networked opportunities provided by the cyberspace, we can experience the information operation capabilities and effects appear not only in military operations, but also in political and economic conflict situations.

Based on the evolution of network technologies and information operations, and the analysis of cyberspace and cyberspace operations, as well as the cyberspace events in recent years, we can state:

- the interpretation of networks has now fundamentally changed and expanded with network of cyber-physical devices based on M2M connections as well as social networks,
- the physical, logical, and cyber-persona layers of cyberspace are equally important, and cyberspace activities can be accomplished in all of them,
- both technical (e.g. CNO, EW) and cognitive (e.g. PSYOPS, deception with fake news) information activities appear in cyberspace, and thus all capabilities of information operations can be interpreted in it as well.

In accordance with the principle of information operations, all these information activities are significantly more effective if they are also applied in cyberspace in an integrated and coordinated manner, and thus they can be used for influence, countermeasure and defense.

References

[1] *Number of Internet of Things (IoT) Connected Devices Worldwide in 2018, 2025 and 2030* [online]. January 2021 [viewed 2021-01-27]. Available from: https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/

[2] FULLER, J.R. *The 4 Stages of an IoT Architecture* [online]. May 2016 [viewed 2021-01-29]. Available from: https://techbeacon.com/4-stages-iot-architecture

[3] *Forecast Number of Mobile 5G Subscriptions Worldwide by Region from 2019 to 2026* [online]. January 2021 [viewed 2021-01-17]. Available from: https://www.statista.com/statistics/760275/5g-mobile-subscriptions-worldwide/

[4] *DARPA Wants to Militarise the IoT* [online]. [viewed 2021-01-21]. Available from: https://internetofbusiness.com/darpa-wants-militarise-iot/

[5] *Military Applications of Internet of Things* [online]. NATO Science and Technology Organization, 2016 [viewed 2021-01-21]. Available from: https://www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=16536

[6] RELIA, S. *Cyber Warfare: Its Implications on National Security.* New Delhi: Vij Books India, 2015. ISBN 978-93-84464-82-0.

[7] *Overview of Cybersecurity* [online]. April 2008 [viewed 2020-12-06]. Available from: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items

[8] *DoD Dictionary of Military and Associated Terms* [online]. June 2020 [viewed 2020-12-06]. Available from: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

[9] KE X., Q. YI and Y. KUN. A Tutorial on Internet of Things: From A Heterogeneous Network Integration Perspective. *IEEE Network,* 2016, **30**(2), pp. 102-108. DOI 10.1109/MNET.2016.7437031.

[10] FM 3-12, *Cyberspace and Electronic Warfare Operations* [online]. April 2017 [viewed 2020-12-06]. Available from: https://fas.org/irp/doddir/army/fm3-12.pdf

[11] JP 3-12, *Cyberspace Operations* [online]. June 2018 [viewed 2020-12-06]. Available from: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

[12] PORCHE III, I.R., C. PAUL, C.C. SERENA, C.P. CLARKE, E.-E. JOHNSON and D. HERRICK. *Tactical Cyber. Building a Strategy for Cyber Support to Corps and Below.* Santa Monica: RAND, 2017. ISBN 978-0-8330-9608-1.

[13] *Cyber Primer* [online]. 2nd ed. Swindon: Ministry of Defence, 2016 [viewed 2020-12-06]. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf

[14] *Aspects and Pillars of Cyber Security* [online]. [viewed 2020-12-06]. Available from: https://www.usna.edu/CyberDept/sy110/calendar.php?type=class&event=2

[15] *Terms & Definitions of Interest for DoD Counterintelligence Professionals* [online]. May 2011 [viewed 2020-12-06]. Available from: https://www.dni.gov/files/NCSC/documents/ci/CI_Glossary.pdf

[16] *Joint Doctrine Note 2/13 Information Superiority* [online]. Swindon: Ministry of Defence, 2013. [viewed 2020-12-05]. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819814/archive_doctrine_uk_info_superiority_jdn_2_13.pdf

[17] HAIG, Zs. *Information Operations in the Cyberspace* (in Hungarian). Budapest: Dialog Campus, 2018. ISBN 978-615-5945-04-5.

[18] LIPOVSKY, R. and A. CHEREPANOV. *BlackEnergy Trojan Strikes Again: Attacks Ukrainian Electric Power Industry* [online]. January 2016 [viewed 2020-12-06]. Available from: https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/