sciendo International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXV No 3 2019

TERMINOLOGY AS A BARRIER TO NATO'S INTEROPERABILITY IN CYBERSPACE OPERATIONS

Robert JANCZEWSKI, Grzegorz PILARSKI, Maciej MARCZYK

War Studies University, Warsaw, Poland
r.janczewski@akademia.mil.pl

Abstract: *During Warsaw NATO summit cyberspace has officially become a new domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea. According to this declaration, NATO members must achieve abilities to conduct cyber operations. This declaration shows distinctly that partners in NATO need to have defensive and offensive capabilities to interoperate with allies during cyber activities. However, the proper functioning of armed forces in a multi and international environment, their cross-sectoral cooperation in time of peace, war, and a crisis situation depends on terminology and common language. Unfortunately, different NATO countries have their own set of terms and definitions. Sometimes cyber terminology is strongly distant. The lack of a unified conceptual apparatus for cyber activities poses a serious barrier to interoperate in cyberspace. The article presents a theoretical basis of cyber terminology based on research carried out by the authors. The paper is the added value since it presents and clarifies complex issues of cybersecurity terminology. Moreover, it also presents definitions of key terms and assures a strong theoretical basis and provides an incentive for further research on the referents of cyber terms.*

Keywords: cyberspace, cyberspace operations, interoperability, cyber terminology, cyber activities

1. Introduction

As a result of computerisation of human life, some new, so far unknown spheres of reality have come into being with a proper name given: cyberspace. This is exactly the domain where the military activity is being transferred from the physical dimension, namely the land, sea, air and space. Thus, cyberspace has become another domain of fight.

The authors have made an attempt to identify the terminology pertaining to operations in cyberspace. On the basis of the knowledge and experience to date, in order to determine and explain the state of science concerning terminology in the scope of cybersecurity, the main research problem has been formulated as a starting point. In order for it to be empirically justified, it has been formulated as an essential open question which requires narration: *What is the state of terminology in the field of cybersecurity?*

The authors of this paper aim at presenting the importance of terminology of NATO's cyberspace operations based on their research. The subject of research undertaken by the authors has not been explored yet and there are neither any studies in this field nor any practical solutions based on them.

2. Cyber terminology in NATO

The reason for the tendency to create still

DOI: 10.2478/kbo-2019-0113

new terms based on the root cyber is the term cyberspace, and not as it could be assumed cybernetics. The analysis and critical review of subject literature conducted by the authors revealed that words formed with the prefix-cyber are very popular terms of the turn of the 20th and 21st century. Nonetheless, regardless of their popularity, they have not been defined with the use of commonly accepted definitions. Different NATO member states use those concepts with varied meanings. Thus, it is impossible to provide unequivocal referent of cyberspace, which from the pragmatic point of view creates a barrier to NATO's interoperability at the time of cyberspace operations.

The obvious lack of explicitness in defining terms relating to operations in cyberspace allows to draw a conclusion that a piece of new reality formed as a result of civilization development of societies is not sufficiently defined and examined, if it is at all. Lack of clear-cut terminological convention is a serious obstacle for NATO's interoperability at the time of operations run in cyberspace.

Lack of agreement between both the scientists and practitioners in terms of one commonly accepted definition of a piece of reality called cyberspace contributes to disagreement in terms of one undisputable referent of cyberspace.

3. NATO's declaration on cyberspace

In Warsaw during the summit of the North Atlantic Treaty Organization (NATO), both the member states as well as the countries which do not belong to the organization officially agreed that cyberspace beside land, sea, and airspace is another operational domain. The heads of state and government participating in the meeting of North Atlantic Council on 8th and 9th July 2016 in Warsaw clearly declared: (…) Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea. This will improve NATO's ability to protect and conduct operations across these domains and maintain our freedom of action and decision, in all circumstances. It will support NATO's broader deterrence and defence: cyber defence will continue to be integrated into operational planning and Alliance operations and missions, and we will work together to contribute to their success. Furthermore, it will ensure more effective organisation of NATO's cyber defence and better management of resources, skills, and capabilities. This forms part of NATO's long term adaptation [1]. (…).Such pledge has become a confirmation of NATO's mandate of defence in the new domain.

Moreover, during European Cybersecurity Forum – CYBERSEC 2018, which took place on 8th-9th October 2018 in Cracow, Assistant Secretary General for Emerging Security Challenges, NATO Antonio Missiroli announced that full NATO operational capability in the field of cybersecurity is to be attained in year 2023. To comply with this announcement, NATO member countries have to achieve interoperability capacity in cyberspace till year 2023.

However, the road from a declaration to actions is long and rough. Each NATO member state has its own solutions as for the organization, procedures, training, legal solutions, technical support (e.g. systems supporting the command and control of combat measures; methods, techniques, and tools) applied in cyberspace operations. NATO member states also elaborated their own conceptual apparatus in the field of operations in cyberspace. The multitude and inconsistency of terms and concepts creates barriers to the interoperability in the scope of activities performed in cyberspace.

So far, NATO has not prepared its own conceptual apparatus in the field of operations in cyberspace. Such state of affairs leads to a conclusion that communication between member countries will be much impeded.
The authors' conviction that only through consistent, common for NATO system of concepts pertaining to operations in cyberspace it is possible to ensure interoperability in the subject matter, this underlies the need for scientific research on the conceptual apparatus in the scope of military interoperability.

4. A referent of cyberspace

A common language is the basis for proper, effective, supra-sectional cooperation both at the time of peace and war as well as crisis situations. It should be consistent and univocal. Partners should use not only the same terms but also the definitions of the terms should have strict, univocal and identical semantic scopes.
Meanwhile, cooperation seems to be hindered since partners in NATO use various referents of cyberspace. This leads to the assumption that there is no agreement in terms of operational sphere. The definitions of cyberspace observed in the USA, Poland and Germany can be used as an example.
According to the views held in the US Armed Forces 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 [2]. Such definition is also included in the latest dictionary [3] determining standard US military terminology and the interrelated terminology applied in the activity of the US Armed Forces. The military and the interrelated concepts, alongside with their definitions, are approved by the US Department of Defense and are destined to be used universally by all components of the US Department of Defense.
According to the definition included in the Cybersecurity strategy for Germany [4] cyberspace is the virtual space of all information technology systems networked at the data level worldwide. The cyberspace is based on the Internet as a publicly accessible connection network, which can be extended by any other data network. Similarly to the German view, the European Union identifies cyberspace with virtual reality, which is envisaged in its definition where cyberspace as the virtual, global and common domain within the information environment consisting of all interconnected and interdependent networks of global, organisational, and national information infrastructure, based on the Internet and telecommunications networks, to be extended by other networks, computer systems and embedded processors, and containing also stand-alone systems and networks [5].
In the Polish doctrine cyberspace is understood as the space where information created by ICT systems is processed and exchanged together with the existing bonds and relations with users [6]. Where ICT systems are understood as groups of cooperating IT devices and software which assure processing, storing, as well as sending, and receiving of data through ICT networks with the use of an end device proper for a given type of ICT network designed to connect directly or indirectly to the end of the network.
The above examples show that cyberspace is understood at the same time as a domain, space, virtual space, a virtual domain. Thus, it is difficult to find a univocal referent.

5. A referent of cyberattack

The analysis of normative documents has shown that there is no agreement between

countries as for the meaning of a cyberattack.
In the National Strategy of Cybersecurity in Spain a cyberattack is defined as an attack resulting from threats in cyberspace. The Spanish believe that cyberattacks which take the forms of cyberterrorism, cybercrime, cyber espionage or hacktivism have become a powerful tool for attack on public and private institutions [7].
The Czechs define a cyberattack as an attack on IT infrastructures aimed at causing damage and acquiring sensitive or strategic information. It is usually launched in the context of politically or military motivated attacks. The Czechs also use a term cyber-counterattack. It means an attack on IT infrastructure as a reaction on a cyberattack. It is mostly launched in the context of politically and military motivated attacks [8]. What is surprising, a document National cybersecurity strategy of the Czech Republic for the period from 2015 to 2020 does not indicate what a cyberattack is at all [9].
The Germans claim that a cyber-attack is an impact on one or more other information technology systems in or through the cyber-space that seeks to wholly or partially compromise their IT security through information technology [4].
In the British view Cyberattack is deliberate exploitation of computer systems, digitally-dependent enterprises and networks to cause harm [10].
According to the Americansa cyberspace attack means actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires [2]. This definition is also included in the DOD Dictionary of Military and Associated Terms [3].
The quoted examples clearly indicate the lack of agreement between partners in NATO as far as cyberattack referents are concerned. It constitutes a serious barrier to the achievement of armed forces capability to run interoperational activities in cyberspace.

6. A referent of cyber defence

Cyber defence is a concept which rarely appears in doctrinal documents of NATO member countries. The definitions cited below show what cyber defence means for the chosen countries.
The German Doctrine provides that cyber-defense comprises the defensive and offensive capabilities in the Bundeswehr within its constitutional mandate and the international legal framework for working in cyberspace, which are suitable and necessary for operational management or for the defence against (military) cyberattacks and thus to protect its own information, IT, as well as weapons and weapon systems. This also includes the use and co-design of cyber defence structures, processes and reporting under defence-relevant aspects and situations [3].
According to the Portuguese, cyber defence refers to the use of security measures in order to defend and protect the elements of ICT infrastructure against cyberattacks, with cyberattacks treated as a ‘forms of cyber war which can take place in connection with a physical or non-physical attack aimed at hindering the operation of the enemy’s information systems’ [11].
The Americans use a compound term‘ cyberspace defense’ which is defined as actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures and include actions to detect, characterize, counter, and mitigate threats, including malware or the unauthorized activities of users, and to restore the system to a secure configuration [2], [3].
The above examples of definitions of cyber defence lead to a conclusion that it is

difficult to provide cyber defence collectively if each participant of joint actions understands the performed activities in a different way.

7. Conclusions

The above presented examples as well as the authors' analysis and critique of doctrinal documents of NATO member countries revealed that there are no paradigms in the field of cybersecurity. However, there is multitude of cyber terminology. Concepts are given different meanings. Sometimes such differences observed in them point to different referents of the same concepts. Such a state of affairs poses a barrier to the interoperability in cyberspace. Lack of common conceptual apparatus in unfavourable conditions can lead to the infeasibility of effective cooperation. Lack of understanding of what is e.g. cyberspace, cyberattack, or cyber defence can significantly impede or even preclude the achievement of a common goal.

Taking into consideration the above one should be aware that for 'good job' it is well grounded to achieve a common ground of understanding. While in the technical dimension of cybersecurity it is clear what a router, an ARP board, an IP address, or a worm or virus is, operational concepts, generally speaking, are not clearly cut, and more interestingly there is no agreement in this field among practitioners as well as theoreticians in terms of the views on this dimension of running military operations.

References

[1] https://www.nato.int/cps/en/natohq/official_texts_133169.htm
[2] Joint Publication 3-12, Cyberspace Operations, 8 June 2018, p GL-4.
[3] DOD Dictionary of Military and Associated Terms, January 2019, p. 59.
[4] Cyber-Sicherheitsstrategiefür Deutschland, Bundesministerium des Innen, November 2016, s. 46.
[5] EUMC Glossary of Acronyms and Definitions - Revision 2018, Brussels 2019, p. 68.
[6] Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej, BBN, Warszawa, 22 stycznia 2015, s. 7.
[7] National Cybersecurity Strategy, Gobierno de Espana, Presidencja del Gobierno, 2013, p. 7.
[8] P. Jirásek, L. Novák, J. Požár, Cybersecurity Glossary, Policejníakademie ČR v Praze, Českápobočka AFCEA, Praha 2015.
[9] National cybersecurity strategy of the Czech Republic for the period from 2015 to 2020, National Security Authority, National Cybersecurity Centre, February 2015.
[11] Estratégia da informação e segurança no ciberespaço, Instituto da Defesa Nacional, Dezembro de 2013, p.11.