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

MISSIONS AND ACTIONS SPECIFIC TO CYBERSPACE OPERATIONS

Petrişor PĂTRAŞCU

"Carol I" National Defence University, Bucharest, Romania
patrascu.petrisor@yahoo.com

Abstract: *Currently, the digitization of society has become a major phenomenon worldwide, making its mark in everyday life of people and the activities of most organizations. Significant contributions to the emergence of this phenomenon consisted of the continued availability of services offered by the global Internet network, the diversity, the number and the usefulness of digital devices and digital competence development of people. Thus, cyberspace has become a good opportunity for malicious people. Today, cyber-attacks are very complex and sophisticated, supported and used, by state actors in their own economic, political, military or informational interest. Military organizations are targeted by cybercriminals to get as much information as possible, and the more valuable is the information, the more the attacker's interest is increased. Investments in such actions are supported by state actors themselves. These actions are lasting, well organized and with an increased effort of human, financial and informational resources. In this context, cyberspace is identified as a domain of operations, recognized by NATO since 2016. With this accreditation, the world's states, whether or not they are members of the alliance, have changed their approach to cyber security, by getting involved both in the content of strategies, doctrines, procedures or other regulations, and in the establishment and development of specialized structures, having qualified personnel, technique and proper equipment meant to meet the current safety standards. Missions and actions specific to cyberspace operations involve special attention from government institutions accredited in the fields of country defence and national security. When taking into account elements related to cyber defence in the strategic planning process, an effective inter-institutional cooperation must be developed.*

Keywords: cyber-attacks, mission, action, cyberspace operations

1. Introduction

NATO's official recognition of cyberspace as an operational environment alongside the other four operational environments (air, sea, land and space) has led Member States to reconfigure their national defense strategies, military doctrines and capabilities. Moreover, investment in cyber defense have become an undeniable priority for many countries in the context of achieving the main national security objectives.

Once cyberspace progressed on the massive development, the increased interest of cyber attackers in obtaining both quantitative and qualitative information from military structures, especially those at the strategic level, has helped to design and develop sophisticated attack techniques that became difficult to counteract.

2. Description of the cyberspace operations

Particular attention from States, involving military force structures, is directed to the development of an optimal cybersecurity protection. This is outlined in a series of arguments. One of these is the evolution of

DOI: 10.2478/kbo-2019-0117

cyber-attacks on various critical infrastructure, including military infrastructure, aimed at destabilizing national security. Vulnerabilities of critical infrastructures are those weaknesses or cumulative circumstances that can be exploited by certain threats [1], so that the vulnerabilities of cyber infrastructures are targeted by various individuals, groups, state and non-state actors.

Another argument that supports the former argument is given by the possibility for state actors to use cyber-attacks in parallel with the conduct of military actions, as confirmed by the events in Georgia (2008), and subsequently by the hybrid warfare in Ukraine.

Also, another argument is the development of modern military equipment in line with the new information and communication technologies and the emergence of integrated systems (e.g. *Command, Control, Communication, Computers, Intelligence, Surveillance, Targeting Acquisition and Reconnaissance - C4ISTAR*), facilitating as much as possible command and control achievement. Last but not least, the orientation of several states towards a cyberwarfare, exploiting the new advantages, the acquired power and the player's status in cyberspace may be another argument.

Compared to the those exposed above, there is a strong need to implement cyber security policies specific to the design, training and operationalization of military cyber defence structures, as well as the preparation, organization and conduct of the cyberspace operations planning process.

From these considerations it is apparent that in order to develop and implement such measures, it is necessary to take into account the particularities and requirements of the military field as well as the essential missions that the military structures are required to carry out at the highest level, in order to achieve and maintain national security, safety and defense.

For example, cyber defence capabilities vary from state to state, from one military structure to another, but also from a state of peace and normality to a state of conflict. In terms of military action, achieving cyber defense is the basis of several factors.

First, the efforts of public and private institutions involved in cyber security are considerably increased and are directed to support the vital activities of society. In case of any cyber-attacks, it is recommended, if time permits, the intervention a specialized team (*Computer Emergency Response Team – CERT*).

Secondly, the attacks can be launched both before and during the conflict. That's why, cyber security measures are taken during the cyberspace operations planning process. Therefore, integrating cyber defence into the cyberspace operations planning process is essential, given that cyberspace meets the attributes of a new battlespace.

Third, cyberspace becoming a battlespace, adopts the basic rules of an armed conflict. Thus, the objectives and missions of cyber defence adapt to these rules, and during operations, military forces engaged in fighting, if they have offensive capabilities, may apply the principle that the best defence is a good offense. Based on recommendations written in the Tallinn Manual [2], a state has the right to react, including through cyber-action, to a cyber-attack, as a response to the violation of the international law of another state, in order to determine that state, to respect its obligation to comply with applicable international law in the cyberspace by protecting the legal rights of the affected State.

Another peculiarity that can be taken into account, within multinational operations is highlighted by the compatibility and integration of the communication and information systems of the participating forces as well as the consistency between their cyber security policies. In this situation, there is a need for multinational cyber defence exercises specific to cybersecurity structures, as well as exercises in a physical (kinetic) dimension, within a common, national or multinational environment.

3. Layers of cyberspace interdependency

From a NATO's perspective, cyber defence is integrated into operational planning and Alliance operations and missions, jointly supported by Member States, to contribute to their success. In addition, this will ensure a more effective organization of NATO's defence against cyber-attacks and a better management of resources, abilities and capabilities.In the military field, in order to have a clearer and broader vision of cyber defence, it is necessary to focus on the three levels of cyberspace outlined in Figure 1.

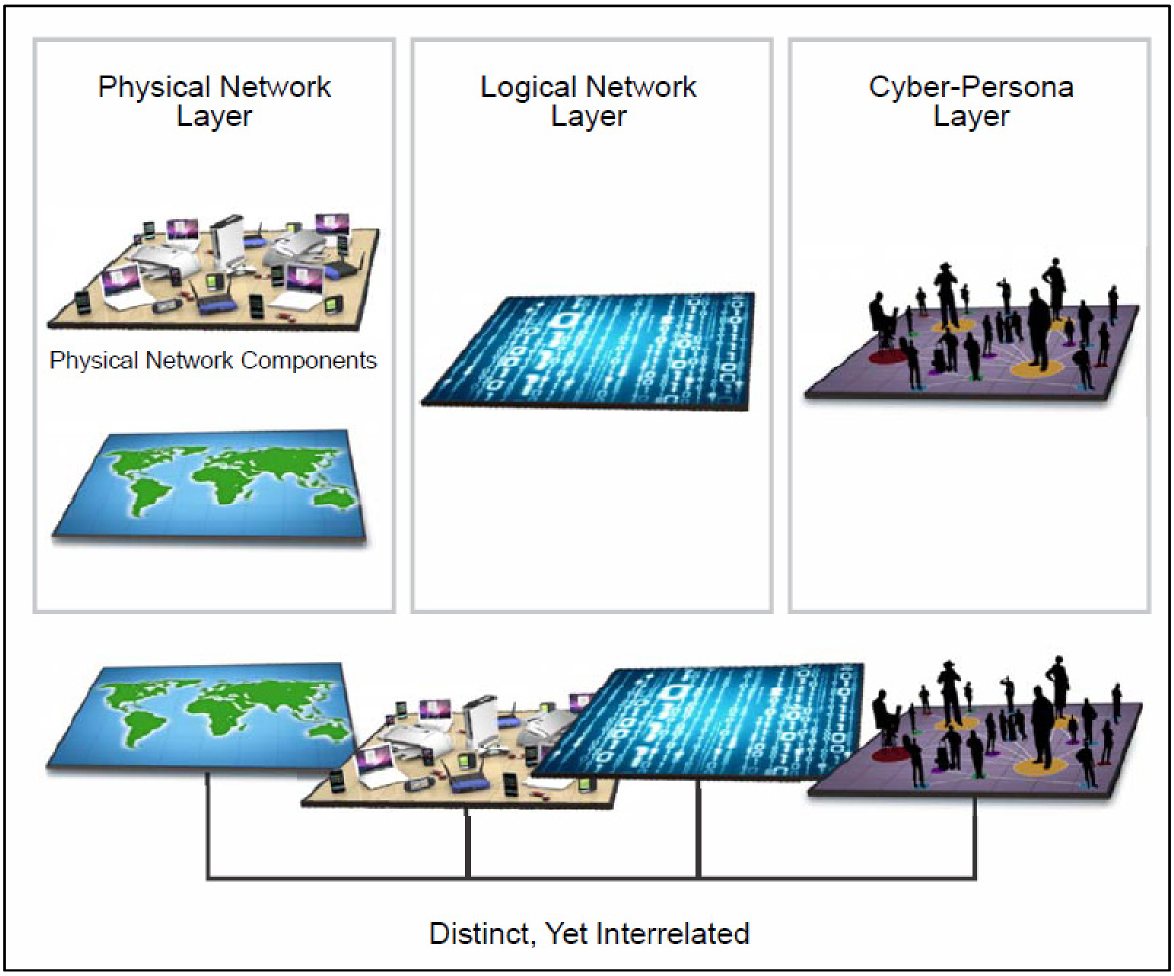

Figure 1: The Three Interrelated Layers of Cyberspace[3]

Physical level provides data circulation and consists of two components of the cyber network, namely: the geographic component and the physical network component. The geographic component has the role of hosting cyber infrastructures in its specific environments (soil, water, air and space), while the physical network component is made up of cyber infrastructures that are supported by connectors for the physical network which are a combination of wired and wireless links and satellites. From here, one can observe the need to retain the proper level of operational cyber security, each category of forces being provided with cyber defence mechanisms (e.g. the US Army).

However, logical construction also occurs at this level to ensure security by primary methods, such as providing information or VPN for cyberspace security. Consequently, they are targets for SIGINT OSINT, MASINT, HUMINT, GEOINT, including communications network infrastructure.

The second level is that of the logical network, in which the components are linked in ways that are extracted from the physical network. For example, network nodes related to one another in the form or relationships that are not tied to an individual, specific path, or node. Another example is the content of websites hosted on servers in multiple physical locations that can be accessed by a single uniform resource locator (URL) or a single web address.

The third level, *cyber-persona* represents a higher level of abstraction of logical network and uses its rules to develop a digital representation of the identity of individuals or entities in cyberspace. This level consists of people with the status of network users with one or more identities that can be visible and actionable. These identities may include e-mail addresses, social network identities, Internet protocols, mobile phone numbers, accountancies, etc.

Military users with *cyber-persona* profile can create and maintain multiple cyber-characters through separate email addresses (on private and at work), through different identities on forums and on social networks. At this level, changes can be made more quickly than changes associated with the physical level.

The access possibilities of a military user to several computer systems connected to networks are increasingly large and delimited in two categories: personal or military purposes. Private opportunities are those that give him the right to use applications offered by Internet service providers for personal purposes. Instead, military options entitle him to use military cyber infrastructure to manage data and information for work, depending on the obtained security credentials. Moreover, a cyber-persona[4] is an online identity that facilitates decision making, communication and the influencing of audiences in the cognitive dimension.

4. Cyberspace operations missions

The missions'characteristic of cyber defence structures aim to achieve the objectives by completing actions that involve cyberspace. Several cyber defence specialists have prevailed a number of approaches to the classification of cyberspace operations missions. However, a sustained approach to an extensive area of cyber defence structures in the context of planning and conducting military operations is given by *Joint Publication 3-12: Cyberspace Operations*, the US Army. Starting from the above-mentioned publication, cyber missions can be categorized as: offensive, defensive and proactive, noting that the last mission listed is called *DODIN operations* (Department of Defense Information Network). By their contents, DODIN can be assimilated as proactive missions to generalize and eliminate the peculiarities of this structure.

Therefore, proactive missions are characterized by operations that assure, maintain and support the cyber security of critical infrastructures, as well as the network configuration, management and expansion. Another peculiarity consist of testing and evaluating security in order to eliminate any vulnerabilities and threats. Proactive operations are permanent through regularly scheduled events.

Defense Cyberspace Operations – ***DCO*** involve internal defense, authorized by standing order, including cyber elements of redirection or isolation of advanced persistent threats and cyber elements of reconstruction or restoration of the security of degraded, compromised or affected cyber infrastructure. Defensive missions can acquire a different form, so cyber defence can be represented on a broader level, leading to private networks or mission partners. In the present context, a central military defence structure cannot guarantee the robustness of the security standards applied to those networks, and this uncertainty has to be taken into account during the risk analysis by establishing coordination between structures and prioritization of cyber defence systems.

Also, a second category of defensive missions is identified by **DCO-RA** (*Defense Cyberspace Operations-Response Action*) response to cyber-attacks in conflict situations, and even the use of physical force to destroy critical enemy infrastructure is possible, taking into account the certainty of the threat and the magnitude of the damage caused. A well-coordinated military command, a careful analysis of the scope, strictly following the employment standards rules (ROE), is recommended in this type of mission.

Offensive Cyberspace Operations – ***OCO*** missions are intended to design cyber power over opponents by undertaking actions to support the achievement of the ultimate goals. Offensive missions can produce controlled and cascading effects on the enemy's physical environment, more precisely on its weapons systems, command control, strategic objectives, and cyber infrastructures. Offensive missions are directed entirely to the enemy, requiring careful analysis of the scope, military coordination, quantifiable goals, and compliance with ROE.

5. Cyberspace actions

Performing any of the tasks mentioned above involves performing actions that use cyber space capabilities, thereby fully contributing to the effects of cyberspace [5]. According to the same publication [6], JP 3-12, these actions involves cyberspace *security*, *defense*, *exploitation* and *attack*

In the context of cyber security, *security actions* are designed to block unauthorized access in order to protect cyber infrastructures and the information they contain in order to ensure confidentiality, availability, integrity, authentication and non-repudiation. Security actions have the role of reducing or eliminating the vulnerabilities that can be exploited by potential opponents by implementing security policies and measure and increasing security by adding solutions and promoting a security culture for users.

Cyber defense actions are applied to combat the threats of opponents as they have breached or are about to breach security measures and include detection, description, control, and mitigation of threats.

The exploitation actions are identified by INTEL activities of enemy interpretation and acquisition of the situation, discovery of vulnerabilities, support in the planning of operations, maneuvering, especially those in the current and future preparation of military operations. Their purpose is to obtain and maintain access to military cyber infrastructures, network nodes, maneuvering for advantageous positions, and the employment of cyberspace capabilities to facilitate subsequent actions without producing far-reaching effects.

The attack actions are designed to produce remarkable reluctance effects, resulting in denial in physical operational environments. The attack action is a form of strike as part of an offensive or defensive mission response. They are categorized as deny for blocking access and manipulation. In turn, denials are done through degradation, dismantling or destruction. Handling, control or exchange information with certain components of the opponent's cyber infrastructure are carried out using techniques of deception, forgery, conditioning, spoofing, and the like.

The objectives of cyberspace operations missions are met through a combination of one or more of these actions. In planning, authorizing and evaluating cyberspace operations missions, it is important that the decision maker, together with the planning team, take into account the actions that are authorized. The most part, defensive missions provide initial cyberspace operations missions, while OCO or DCO-RA missions are episodic and may require clandestine or visible maneuvers. Therefore, the authorization of missions must be conducted separately.

6. Conclusion

The magnitude of cyber threats has managed to turn the attention of specialized structures to the field of national and international security. Once cyberspace has become an operational environment, NATO's member states have assimilated their main elements of cyberwarfare both in the planning of military actions and in the establishment of military structures for cyber defence. In principle, taking into account the components of strategic level of operational design, cyber defence missions and actions are designed to achieve the desired final state. At present, sensitive and controversial cyber defence issues, such as the fact that states don't assume the cyber-attacks in the context of lack of regulation and global consensus, as well as the way the decision are made for offensive missions, remain some of the main topics of interest to the cyberspace operational environment.

References

[1] D. Roman, F. Repez, E.V. Popa, *Infrastructura critică – Reglementări legislative și de planificare a protecției*, Editura CTEA, București, pp. 93, 2017.

[2] The Talinn Manual, *On the International Law Applicable to Cyber Operations*, 2nd edition, Cambridge University Press, pp. 111-122,2017.

[3] Joint Publication 3-12*, Cyberspace Operations*, U.S.Army, pp. I-3, 2018.

[4] JFODS 5: *The Joint Forces Operations & Doctrine SMARTbook*, 5th edition, The Lightning Press, pp. 6-8, 2017.

[5] The U.S. Army War College, *Strategic Cyberspace Operations Guide*, 2018, available on https://csl.armywarcollege.edu/USACSL/Publications/Strategic_Cyberspace_ Operations_Guide.pdf.

[6] Joint Publication 3-12*, Cyberspace Operations*, U.S.Army, pp. II-5, 2018.