12 To the Margin of the Theory of a New Type of Warfare

Examining Certain Aspects of Cyber Warfare

Ádám Farkas – Roland Kelemen[*]

Keywords
new types of security challenges, cyberspace, cyber warfare, cyber attack, cyber defense

Abstract
In the second half of the 20th century, humanity went through an unprecedented technical and technological development. As a result, technological innovations emerged in the course of the last third of the century which have now become indispensable parts of everyday life, the whole society and even the state. Among them, we must mention the IT sector, which has effectively enabled global contacts and communication between people and organizations across different parts of the world through various tools, programs and networks. Moreover, it also facilitates and simplifies everyday tasks both in the private and the public sector. Cyberspace is a unique and complex phenomenon, since it can be described with physical and geographical concepts, but in addition, its virtual features also have extraordinary relevance. As a result of its remarkable expansion, fundamental areas such as sociology, geopolitics, security policy or warfare must also be reconsidered. This paper provides an overview of the new types of security challenges for the 21st century, most notably security risks related to the cyberspace. In addition, some aspects of cyber warfare, such as cyber intelligence, cyber attack and cyber defense are examined. Particular attention is given to the question whether a cyber attack in itself can reach the level of an armed attack, and if so, what means can be used by the State under attack in defense.

12.1 Introduction

Over the past decades, one of the most important novelties in the field of military technology and warfare was the appearance of cyber warfare and the cyber battlefield. At the same

* Ádám Farkas: 1st Lieutenant of the Hungarian Defence Forces; associate professor, National University of Public Service, Budapest. Roland Kelemen: assistant lecturer, Széchenyi István University, Győr; assistant research fellow, National University of Public Service, Budapest.

time – endangering the very existence of the state – it poses perhaps the biggest security risk. Billions of civilians are present on this cyber battlefield – not unlike the traditional battlefields. But the scene is different, with hacktivists and terrorists engaging in partisan tactics hidden among civilians, as well as the administrative and military bodies of the state.

The weight of the security risk may be illustrated by the thoughts of Dennis C. Blair, Director of the National Intelligence (US), formulated in his senate report. Here, he highlights the real nature of the problem, namely the vastly increasing cyberspace – which is becoming uncontrollable – and the associated vulnerability of the fundamental social, economic, state and military infrastructures.[1] This line of thinking is further reinforced by James R. Clapper, who said that the constantly expanding cyber technology and the dependent governmental, commercial, military and social subdivisions are constantly exposed to the danger of cyber espionage or assault. In his words, these will cause a 'cyber Armageddon', but can nevertheless result in significant harms and costs to the economy and national security of the US and, must therefore be taken seriously.[2]

Based on the above, it is clear that the phenomena related to cyberspace are extremely significant, with the potential to have a relevant effect on the conventional space. Consequently, it is clearly necessary to develop legal, military and security concepts in this area as well. In this light, this study seeks to describe cyber warfare as security risk, to define and characterize cyberspace itself. Finally, it also investigates how the rules based on certain basic concepts of international law could be applied to the aspects of cyber warfare.

12.2 Complex Security – New Types of Challenges – The Cyberspace as a New Battlefield

The 21st century has brought a number of security changes that can either be symptoms or just phenomena of trends. International terrorism, international organized crime, hybrid warfare, or even attacks and threats from cyberspace are all included in these phenomena. It is worth considering these on a wider horizon, with the multidisciplinary approach offering a possible framework to analyze these phenomena. This framework is a complex[3]

1 Dennis C. Blair, *Annual Treat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence*, 12 February 2009, p. 38.

2 James R. Clapper, *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee*, 26 February 2015, p. 1.

3 The question of complex security brought about the renewal of security-related sciences at the end of the twentieth century. In respect of security police, it can be said that "the bipolar world order and the security architecture of the Cold War began to change rapidly after the fall of the Berlin Wall. […] In his study of 1991, Walt highlighted the following areas: At first, security studies have to pay more attention to the internal political affairs of each state, as it has been shown that there is a close connection between the

understanding of security and a broader interpretation of the security environment of our age. This broad understanding shows that we must adapt the legal aspects of defense against security challenges.[4]

Before the end of the twentieth century, the key element in the security approach was the preparation for war and maintaining a military power. However, this has changed irreversibly by the end of the twentieth and the beginning of the twenty-first century. No analysis focuses on military power without considering inner relations, positions emphasizing the international element and the avoidance of war can no longer be considered timely. The internal and external spheres, or with other words, law enforcement, military, national security and broadly conceived state defense come together in actions taken against new challenges. The increasingly comprehensive approach in the NATO also serves this purpose, just like the expansion of the regional defense cooperation with various non-classical military – *e.g.* anti-terrorist – elements. The new types of challenges are not only multifaceted but affect both the nation state and the international level at the same time, since they cannot be handled at nation state level only. The new challenges are prompting renewal in approach of the nation state as well as the different principles, institutions and tools of international law, for these are becoming ever more globalized.

Now our world has become truly globalized, as there is virtually not a square foot on Earth that is not a part of the world economy system, one way or another, and they all play a part in the power competition. Besides, with the explosive evolution of info-communication – in addition to some attempts and ambitions of restriction,– a complete information space has also emerged with the cyberspace: a secondary plane of existence in the information society. As a result, the emerging logic of the twentieth century's totality can be further enhanced by these. Of course, there may be a revolutionary scientific breakthrough in the future that will enhance our present situation, but with the changes that have already been made, all boundaries of influence (of tools for attack) can be effectively eliminated. This would mean that welfare infrastructures immediately become critical infrastructures, and our society is exposed to new threats. On the other hand, all the benefits of publicity and the world wide web would be accumulated in the hands of terrorists or those conducting

---

nature of the internal policy's institutional system and the foreign policy behavior of the states. Secondly, in terms of peace and cooperation between states, the role of international organizations ad regimes is inevitable. […]. Thirdly, the strengthening of the constructivist trend in the area of security studies also draw attention to the fact that ideas can influence foreign policy behavior. Fourthly, the close connection between economy and security is unquestionable […]." Ferenc Gazdag (ed.), *Biztonsági tanulmányok – Biztonságpolitika*, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2011, p. 18.

4 About its emergence in scholarly thinking about national defense in Hungary, *see* Ádám Farkas, *Tévelygések fogságában*? *Tanulmányok az állam fegyveres védelmének egyes jogtani és államtani kérdéseiről, különös tekintettel Magyarország katonai védelmére*, Magyar Katonai és Hadijogi Társaság, Budapest, 2016; Ádám Farkas & Pál Kádár (eds.), *Magyarország katonai védelmének közjogi alapjai*, Zrínyi, Budapest, 2016; Szabolcs Till, *A honvédelmi alkotmányosság 30 éve Magyarországon 1988-2017*, Zrínyi, Budapest, 2017.

a hybrid war, allowing them to reach a new level of propaganda, as emphasized by numerous analyses on the Islamic State[5] as well as papers analyzing hybrid warfare operations in Ukraine.[6] These phenomena were further enhanced by the challenge of cyberspace as a factor capable of supporting the majority of the forms of illegitimate violence, but they are also significant in themselves.

The importance of this – namely the information world – cannot be overstated, since it has changed our worldview completely, affecting our everyday life, in addition, it is the framework for influencing entire societies or social groups. Numerous scholars have drawn attention to this, among others, Manuel Castells and Nico Stehr whose thoughts must be mentioned in connection with the relevance of knowledge and information acquisition and refinement shaping our world. For Manuel Castells speaks of nothing less than the world of knowledge. Recommending some rationality, but with proper weighting, he states that

> "The problem is that the futurists have confused us by that things what they imagined about the internet-based world. The world is indeed based on the Internet; but because of this, geography, history and institutions are not disappearing; places will be preserved, but in networked form, just like people and companies, and some states still operate on the basis of bombing their enemies. But without information, you cannot know who, what and where to bomb […]. So, the main thing is that communication and knowledge are higher value-creating activities, but no value can be separated from the material world. The information itself and the knowledge itself lie in it, and that is why and how

5 For the terrorist organization called the Islamic State and terrorism in a broader sense, *see* Loretta Napoleoni, *Terrorism and the Economy, How the War on Terror is Bankrupting the World*, Seven Stories Press, New York, 2010; Loretta Napoleoni, *Terror Incorporated, Tracing the Dollars Behind the Terror Networks*, Seven Stories Press, New York, 2005; Péter Tálas (ed.), *A terrorizmus anatómiája*, Zrínyi, Budapest, 2003; Péter Tálas (ed.), *A globális terrorizmus: Biztonsági kihívások és stratégiai válaszok*, Nemzeti Közszolgálati Egyetem, Budapest, 2013.

6 With regard to hybrid warfare and especially the Ukrainian crisis, *see* Heather A. Conley *et al., The Kremlin Playbook. Understanding Russian Influence in Central and Eastern Europe. Center for Strategic and International Studies*, Chatham House, Washington, 2016; *Russia's 'New' Tools for Confronting the West. Continuity and Innovation in Moscow's Exercise of Power. Chatham House*, The Royal Institute of Foreign Affairs, London; Mikkel Vedby Rasmussen *et al., The Ukraine Crisis and the End of the Post-Cold War European Order: Options for NATO and the EU*, Centre for Military Studies, University of Copenhagen, Copenhagen, 2014; Andrew Wilson, *The High Stakes of the Ukraine Crisis*, at www.currenthistory.com/Wilson_Current_History.pdf; Dmitri Trenin, *The Ukraine Crisis and the Resumption of Great-Power Rivalry*, Carnegie Moscow Center, Moscow, 2014; Péter Tálas, 'A jelenlegi ukrán válságról 2.0', *NKE Stratégiai Védelmi Kutatóközpont Elemzések*, Vol. 3, Issue 8, 2014; Péter Tálas, 'Folytatódó ukrán válság', *Nemzet és Biztonság*, Vol. 7, Issue 4, 2014, pp. 63-74.

> the Internet is important; it connects the material reality with the processing of signs."[7]

Grasping the very essence of the issue, he also points out that the totality of cyberspace is in connection with material reality, so it obviously has a repercussion for the material world, whether it is propaganda goals, warfare recruiting to the new partisanship,[8] express cyber attacks or influencing order. Examining the relationship between knowledge and freedom, and more broadly, the relationship between knowledge and the modern state and society, Nico Stehr takes a clear position in his immersive work stating that

> "I would like to define knowledge as an ability to act (acting capacity) as a possibility to 'make something to move'. The ability to act (in opposition to – habitual – behavior) is not only about the possibility of creating something in the meaning of material-physical performance. […] This making-something-to-move can also absolutely relate to the ability to create symbolic products, for example to create a hypothesis, organize the literature of a topic or defend a thesis against 'new facts'. […] The direct power of knowledge is manifested only through the realization of the ability to act…"[9]

By doing so, however, it means a significant power capable of influencing social and dominant relationships, has a defining weight in the economy in supplying population, in guaranteeing safety and in nurturing the scientific sphere. Putting something in motion can also be actually applied to the creation of symbolic products, for example, formulating a hypothesis, sorting out the literature of a topic, or defending a thesis against 'new facts'.

Twentieth-century totality that had unfolded with world wars thus gained a new meaning at the beginning of the twenty-first century. Namely, the separation of serious security challenges from the state took place in the globalized, networked, and therefore

7 Manuel Castells, *A tudás világa*, Napvilág, Budapest, 2006, pp. 138-139.

8 Carl Schmitt, in his work on the Partisan theory, analyzed partisans, and essentially described all non-state actors who depart from the logic of classical inter-state conflicts to challenge international peace and security. While he showed that partisans were tied to states as a consequence of interstate conflicts, in his work he expected that there will be a time when partisans will be separated from the state. However, this question was not analyzed further by science as he was shunned due to his Nazi years. Schmitt's thoughts, however, have drawn the basic contours of most of today's challenges, which can be interpreted as a new partisan approach, irrespective of whether they include radicals, international terrorists, cyber criminals, cyber terrorists or even hybrid warlords. This question emerges in respect of most challenges. As Carl Schmitt said: "The modern partisan is neither legitimate nor does he expect pardon from the enemy. He turned away from the conventional hostility of the war encircled by the defamed defense institutions, and took his way to another territory, the territory of the real enemy, which is intensified with terror and counter-terror right to destruction." Carl Schmitt, *A politikai fogalma*, Osiris-Pallas Stúdió-Attraktor, Budapest, 2002, p. 31.

9 Nico Stehr, *A szabadság a tudás leánya*, Gondolat, Budapest, 2017, p. 21.

totalized world (including transport and information flow), meaning that a new threat horizon appeared, including cyber terrorism, Islamic terrorism and hybrid warfare. The challenges represented by non-state actors,[10] intertwined with the exposure of the economic, communicational and technical development and the exposure of the society coming from its addiction to infocommunication have fueled totality, and also confused military, law enforcement, national security and state administration boundaries of security challenges in the force field of complex security.

Thus, with the eve of the twenty-first century, total security challenges have emerged, which have no defining and unique attributes, but have complex characteristics related to many segments of security and also to the various sectors of the state's defense apparatus entrusted with upholding order. Another aspect is the escalating ability and the increasing mobility that can change the dominant character of security challenges within a short period time, including the system of tools needed to manage them. Thus, a domestic security challenge – be it the ISIS or the Ukrainian anti-government riot – can escalate within a short period of time into a conflict involving several states necessitating an armed and military approach (such as the nationalization aspiration of the ISIS in the case of Iraq and Syria, and the hybrid war in the case of Ukraine). This, following a relative resolution, requires co-operation, a comprehensive approach, namely civil-police-military-national security cooperation and even renewed international action.

This kind of transformation only intensifies when the evolution of the partisan –a group of phenomena caught under an umbrella concept – is coupled with changes in the world. As Márton Szabó writes:

> "Schmitt, however, describes the guerilla, the revolutionary and the terrorist as the three basic historical variants of the type in which the partisan develops from the role of the 'home's defensive primordial defender' into the character of the 'aggressive activist who tries to dominate the world'."[11]

He also underlined that

> "certainly terrorists signify the possibility of unregulated and uncontrolled violence; they represent the process of getting through the privatized struggle and the nature of the war that has been completely liberated from the obligations

10 *See* Erica Chenoweth & Adria Lawrence (eds.), *Rethinking Violence: States and Non-State Actors in Conflict*, MIT Press, Cambridge, 2010; Gábor Kajtár, *A nem állami szereplők elleni önvédelem a nemzetközi jogban*, ELTE Eötvös, Budapest, 2015; Gábor Sulyok, *A humanitárius intervenció elmélete és gyakorlata*, Gondolat, Budapest, 2004.

11 Márton Szabó, 'A politika fogalmának elmélyítése Carl Schmitt partizánelméletéről', *Világosság*, Vol. 44, Issue 7-8, 2003, p. 70.

> of international law. So, the question is not how noble or insolent the idea is in light of which the terrorists are acting; but rather that they have a self-identity that makes the separation of armed struggles final, not even from the law and the state, but also from the civil society, as the terrorist occasionally kills even those whom he represents, what is more, he incorporates the suicide warrior into his system."[12]

Building on the thoughts of Márton Szabó, as a kind of thought experiment we could say that from the trope of total war the theory of total security challenges has been developed by now. This experiment was cemented by Carl Schmitt himself in his partisan theory, in the perspective and concepts of the final stage. Namely, he had foreseen the possibility that the partisan's interpretation framework must be independent from the state and its regular war, that is to say, as a non-state actor, he has to become an independent threat on the international stage.[13] However, this also means that the traditional role and the regulatory system of the states war can no longer provide an adequate interpretation framework for these challenges, which are not-only-state, or non-state challenges, but have international impacts. Based on the above, the total security challenges are the following: *(i)* they can generate and combine threats in all spheres of security; *(ii)* they use tools, achievements and rights for the benefit of the welfare society with the purpose of an attack; *(iii)* they can use significant living and inanimate resources to enhance the fight to an extreme; *(iv)* they blur the boundaries between the individual states and the acts must be treated by the tools of the government, police, military and national security; and *(v)* they are coupled with exceptional escalation factor.

In this scenario, the challenge of cyberspace should to be highlighted, for on the one hand, it may be an independent threat, and on the other hand, it will clearly be the part of the inter-state or state-driven conflicts of the twenty-first century, too. Cyberspace is now – in NATO's interpretation – a battlefield, so it is also necessary to map it in the regulatory system related to warfare, and at the same time shape the regulation of non-state cyber challenges and possibly the framework for action against them.

By now, the total war can be interpreted as the war being waged in surface, water, air and cyberspace that does not know the heartland-front line, nor does it know– or just with reservations – the civil-military confinement: It must therefore be interpreted as the final stage of hostility, and in a truly totalized world of complex security, it is to be complemented by total security challenges capable of breaking away from the total state. The only solution against these could be the re-thinking of protection and its adjustment to totality while

12 Id. p. 72.
13 *Cf.* Schmitt 2002, pp. 145-162.

also maintaining proper constitutional guarantees, and at the same time creating the opportunity for operational, rapid and effective action.

It is time to recognize that the total security challenges of our age have surpassed our nation-state defense solutions based on classical sharp delineations and our international legal instruments based on inter-stateness just like the total war surpassed the previous periods of armies' war in the twentieth century. As for the development of the state – according to the ideas of the good state and the good government – a comprehensive state reform, and strategic thinking with an aspiration for cost efficiency, in addition to the increase of efficiency are necessary. These require coordinated development and renewal is also necessary in the field of armed protection, including the reform of international legal instruments. This is not about radical change, but rather about the willingness to develop, since total security challenges require absolutely completely new type of task management. In fact, they did not strive for total rule. Just the opposite. The new types of security challenges are, in essence, combined with the earlier classical security challenges, and they even use these as tools. As such, the situation requires a new kind of approach and solutions in accordance with proven procedures, principles and tools. While all of the total security challenges build on every form of black economy, the commission of classical public law offenses, indications of various social tensions and conflicts, migration, the proliferation of weapons and organized crime, it cannot be excluded that they will try connect these with the proliferation of nuclear, chemical and biological arms and to the reinforcement of certain natural threats in order to have a social impact and ultimately, to carry out an attack.[14]

In this altered security force field it seems obvious that the challenges driven by states or non-state participants who are acting individually in major powers' buffer zones, as well as the cyber challenges which constitute individual challenges in many respects, and also support actions that endanger international peace and security in many respects are those, which require increased attention. Dealing with the former was inspired in many ways by increasing international terrorism since the 2000s, gaining new impetus by hybrid warfare. In the latter case, however, we believe that there are many fundamental questions to be clarified, investigated and explored, further underlined by the fact that cyberspace is now officially a battlefield in the thought system of the world's largest military alliance.

14 For more information on classic security challenges *see* Péter Deák, *Biztonságpolitikai kézikönyv*, Osiris, Budapest, 2007; Béla Galló, *A túlélés tudománya*, Helikon, Budapest, 2000.

12.3 A Draft Conceptual Overview of Cyberspace and Cyber Warfare

Cyberspace and its processes "radically change social, cultural, political, institutional and economic life."[15] This statement is absolutely right in that today's modern state apparatus, military, social network, economic life and people in their daily lives are 'managing' essential vital functions through cyberspace, changing their centuries-old dynamics. The social tensions of the traditional space – be they political, religious, ideological or criminological – also appear in this global internal cyberspace. Meanwhile, these tensions in these personalized global communities appear with increased intensity. The increasing social tension is also manifested in social movements, setting their own tools: globalizing technology and culture in opposition to the networking world. Thus, exploiting the opportunities offered by cyberspace, some terrorist organizations reinforce their transnational character and emerge as a new hybrid security problem and challenge.[16]

This security problem is compounded by the fact that certain economic and financial factors, as well as the institutions of nation-state and supranational communities are connected to the global cyberspace. Thus, the above-mentioned actors connected to cyberspace may also become a direct target of interstate conflicts, the conflicts themselves stemming from social tension.

Taking these circumstances into account, for the sake of the protection and safety of cyberspace, and as a corollary the traditional space, it is necessary that the armed defense systems of individual spaces, including their military-like bodies[17] – and researchers of this area – create their own cyberspace concepts, thereby helping the organizations to define their role and place in cyberspace processes. The need for this narrow interpretation of cyberspace is also confirmed by the fact that

> "anyone can put an end to life with information […] because devices connected to Internet and telecommunication networks can lead to the same result as weapons do […] the instrument, scale and social impact of destruction can be compared more likely to the legally-only judged consequences of wars or industrial and natural disasters."[18]

15 Martin Dodge & Rob Kitchin, *Mapping Cyberspace*, Routledge, London-New York, 2001, pp. 1-33.

16 *See* Sándor Magyar & László Simon, 'A terrorizmus és indirekt hadviselés az EU kibertérben', *Szakmai Szemle*, Vol. 15, Issue 4, 2017, pp. 57-68; László Simon & Sándor Magyar, 'A terrorizmus és indirekt hatása a kibertérben', *Nemzetbiztonsági Szemle*, Vol. 5, Issue 3, 2017, pp. 89-101.

17 On the concept of military-like bodies, *see* Ádám Farkas, 'A katonai büntetőjog és igazságszolgáltatás helye, szerepe, létjogosultsága az állam és társadalom rendszereiben', *Hadtudomány*, Vol. 22, Online issue, 2012, pp. 3-6.

18 László Simon, 'Az információ mint fegyver?', *Szakmai Szemle*, Vol. 14, Issue 1, 2016, pp. 34 and 41-42.

Recognizing this, NATO classified cyberspace as the fourth battlefield. In their work, Steve Winterfeld and Jason Andress said that in cyberspace, the battlefield includes networks, computers, hardware (this includes weapon systems with embedded computer chips), software (developed commercially and by the government), applications (like command and control systems), protocols, mobile devices and people that run them.[19] According to the definition by the US Department of Defense, cyberspace is

> "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[20]

Summarizing the concepts and features above, it may be concluded that this cyberspace is an ever-expanding entity, easily accessible to everyone but difficult to describe with conventional geographic space concepts. It has a real impact on the self-image of the individual and society, on social reflections and the global economy, and in this space, administrative and military-like organizations of the states appear as active players. Through this cyberspace, a massive amount of information flows through within a single minute. "It is clearly predictable that cyberspace systems are getting bigger, faster and more complex,"[21] but their vulnerability lies exactly in this complexity. Our traditional viewpoint on warfare was fundamentally revised when cyberspace appeared. As warfare changed, new equipment and warfare methods emerged, which cannot be considered as weapons based on their basic function, however many practical examples show that they may indeed be used as weapons (The case of Estonia in 2007, Stuxnet 2010). Operations carried out in cyberspace can be classified as information operations.

> "Information operations mean those coordinated activities which are capable of supporting decision makers via effects on opponents' information and telecommunications system in order to reach the aimed political and military objectives, besides they can also utilize and protect their own similar systems effectively."[22]

19 Steve Winterfeld & Jason Andress, *The Basics of Cyber Warfare Understanding the Fundamentals of Cyber Warfare in Theory and Practice*, Elsevier, Waltham, 2013, p. 22.

20 Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms, at https://fas.org/irp/doddir/dod/jp1_02.pdf, p. 57.

21 Tibor Babos, '"Globális közös terek" a NATO-ban', *Nemzet és Biztonság*, Vol. 3, Issue 3, 2011, p. 42.

22 Zsolt Haig & István Várhegyi, 'A cybertér és a cyberhadviselés értelmezése', *Hadtudomány*, Vol. 18, Online issue, 2008, p. 2.

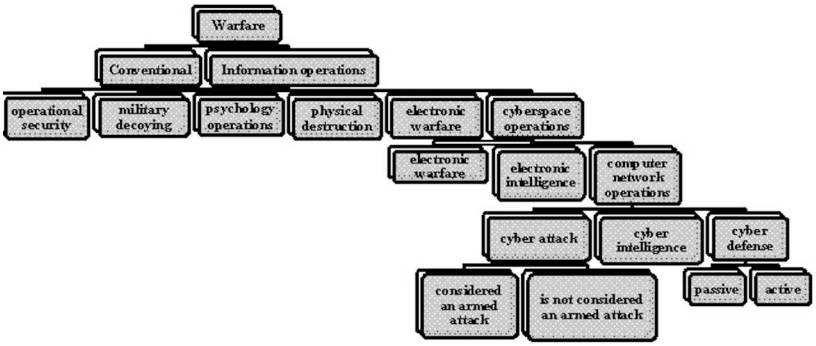
Information warfare became fully developed[23] around the time of the Gulf War.[24] The purpose of information operations is "to influence, disrupt, destroy or limit the decision making processes of enemies or potential opponents, and to protect our own decision making process."[25] In order to achieve these purposes, information operations are explicated in physical, informational and cognitive dimensions. During the realization of these dimensions

> "informational operations create harmony among pre-existing and those informational actions that were achieved through military means. Therefore, its components are made by these, supplemented by new features that appeared concurrently with IT innovation and their appearance on the battlefield (for example the appearance of computer networks on battlefields)."[26]

For these reasons the components of information operations generally are: *(i)* operational security, *(ii)* military deception, *(iii)* psychological operations, *(iv)* physical destruction, *(v)* electrical warfare, *(vi)* computer network operations.[27] So, as demonstrated above, one of these information operations is computer network operations, which is a subfield of cyber operations. Cyber operations can be further expanded to two more areas: electrical warfare and intelligence, but these can be interpreted as such inside a networked info-communications environment.[28] For this reason, in this study we will only consider computer network operations to be cyber operations – according to the broad social perspective – and we treat these two concepts as synonyms.

23 Some of its elements like intelligence or deception were already typical in the early wars of humanity.
24 Zsolt Haig, 'Az információs hadviselés kialakulása, katonai értelmezése', *Hadtudomány*, Vol. 21, Issue 1-2, 2011, p. 13.
25 Zsolt Haig *et al., Elektronikus hadviselés*, Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest, 2014, p. 19.
26 Haig 2011, p. 18.
27 Haig *et al.* 2014, p. 18.
28 Id. p. 28.

Figure 12.1 Warfare in the 21st Century (Based on the above-mentioned work of Haig et al. 2014; created by Roland Kelemen.)

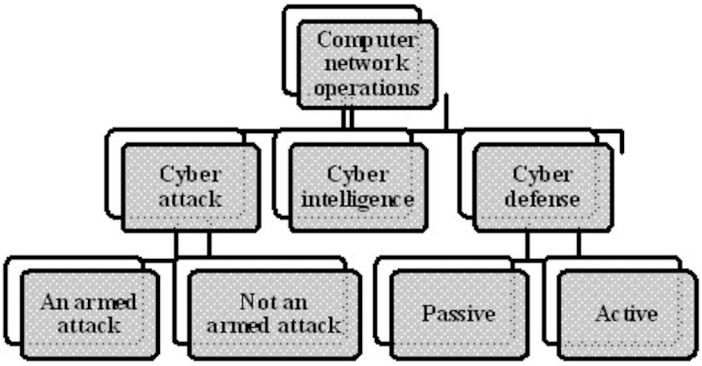


According to Zsolt Haig's definition, a computer network operation

"on the one hand is aimed at influencing, destroying or shutting down the opponent's networked IT system, on the other hand it is to maintain the operability of a similar, own system."[29]

Based on these, three areas can be separated: *(i)* cyber intelligence, *(ii)* cyber attack, *(iii)* cyber defense.

Figure 12.2 Typology of Cyber Operations (Made by Roland Kelemen.)



29 Zsolt Haig, 'Számítógép-hálózati hadviselés rendszere az információs műveletekben', *Bolyai Szemle*, Vol. 15, Issue 1, 2006, p. 60.

12.4 Cyber Intelligence/Gathering of Cyber Information – Espionage in Cyberspace

The Hungarian cyber defense concept regards attack and intelligence as the same concept despite of their markedly different object and intensity. According to the concept's definition, a cyber attack can mean

> "an attack via cyber space aimed at interrupting, shutting down or destroying an information environment or infrastructure, or gaining its authority, destroying the integrity of data handled, or taking data out from under control."[30]

The concepts created by Zsolt Haig highlight the sharp difference between the two activities.

> "Computer network intelligence means penetration into the opponent's computer systems and networks via hardware or software, in order to access data and information that are stored in databases, and to use them for reconnaissance purposes. Computer network attack means penetration into the opponent's computer systems and networks via hardware or software, in order to destroy, modify or manipulate data that are stored in databases, or to make them inaccessible, or to make the whole system or network inaccessible. This attack can also mean physical damage, achieved by modifying or manipulating software."[31]

It is clear that while intelligence is nothing more than acquiring data and information required for an operational objective, the aim of an attack can be diverse from an operational perspective, because it can be directed at terminating the system or the disinformation of enemies, or to make those data inaccessible that would be necessary for the operation to make relevant decisions.

Based on our conventional military operational concepts, cyber intelligence[32] can mostly be considered spying. The handbook called Tallinn Manual – made by NATO experts (expert evidence) – also sharply separates intelligence and data acquisition from activities

30 Instruction of the Minister of Defense to the Publication of the Hungarian Army's Professional Concept of Cyber Defence 60/2013. (IX. 30.), Appendix 1, Section 2(7).

31 Haig 2006, pp. 60-61.

32 Such devices are the diversion of data transferred on Ethernet and Token Ring local networks by switching relays to promiscuity state, the devices aimed at cracking passwords, the L0phtCrack network monitoring program, the Server Message Block, and the Van Eck-Monitoring, which makes electromagnetic systems' electromagnetic signs perceivable (*e.g.* monitors).

deemed to be attacks, especially armed attacks.[33] According to the opinion of Katharina Ziolkowski, "spying alone is not against international law, so it is not an action that violates international law."[34] By contrast, Anikó Szalai states that "the first written international rights conventions of war (Hague Conventions 1899, 1907 and Geneva Conventions 1949, 1977) are actually not to prohibit spying, only the case when spies had been caught."[35] Furthermore, "international law does not contain almost any rules for spying, it is situated on the boarder of legality and illegality."[36]

> "The existing – uncertain – rules did not follow the technological innovations, and for example the Vienna Convention of 1961 about diplomatic relations can be interpreted to the current situation in spirit only."[37]

However, the responsibility of the spying country or individual can be established and the insulted country can take actions against it, but this action cannot be armed violence and only passive cyber defense tools can be used. Against such countries non-armed sanctions can be used only (political, economic, and diplomatic), meanwhile, punishment against individuals may be enforced.

12.5 Cyber Attack – Can It Be Classified as an Armed Attack?

Cyber attacks, as mentioned above, can satisfy a wide range of operational needs. Furthermore, in case of each attack, from the point of view of its legal assessment, the issue of intensity associated with the goal is extremely important, as well as the attributability to state(s).

Why is it important to examine these two criteria from legal point of view? To answer this, we have to go back to a *ius cogens* rule of international law, the absolute prohibition of violence. The absolute prohibition of violence covers not only war but all acts that are directed against the territorial integrity or political independence of another state, or manifests in any form of violence or threatening with violence are inconsistent with the

33 Michael N. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013, p. 55.

34 Katharina Ziolkowski, 'Peacetime Cyber Espionage – New Tendencies in Public International Law', *in* Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy*, Tallinn, NATO CCD COE Publication, 2013, p. 456.

35 Anikó Szalai, *Kémkedés: nem tilos, mégsem szabad*, at http://drszalaianiko.hu/2013/11/22/kemkedes-nem-tilos-megsem-szabad/.

36 Szalai 2018.

37 Anikó Szalai, *Az 1979-es iráni forradalom éleslátása*, at http://drszalaianiko.hu/2013/11/04/az-1979-es-irani-forradalmarok-eleslatasa/.

purposes of the UN.[38] It follows from the definition of the term that the Charter prohibits all forms of armed violence irrespective of their weight, intensity and the nature of the weapon used.[39]

There are only two exceptions to the absolute prohibition of violence: the use of armed force upon the authorization of the UN Security Council and the exercise of the right to individual and collective self-defense. In the system of collective security, these binding decisions of the Security Council take precedence over the right to self-defense and its exercise. In addition, Article 39 authorizes the Security Council to introduce all the necessary measures in case of act of aggression. The Security Council is entitled to identify the act as an aggression, for which the Charter provides a wide margin of maneuver. This difficult concept is attempted to concretize by the UN General Assembly Resolution No. 3314, adopted in 1974. The decision defines the concept of aggression as follows:

> "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations."[40]

The decision contains a list of the possible acts of aggression. It then states that this list is not exhaustive, and that the Security Council may also classify other acts as such. The significance of the decision is that it indicates the fact of that the intensity of armed violence is of relevance in international law, and that armed violence also can be committed indirectly. Finally, it reinforces the interstate nature of violence (here: aggression).

Another exception to the *ius cogens* rule of the absolute prohibition of violence is the right to self-defense, in respect of which the Charter declares that

> "[n]othing in the present charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a member of the UN, until the Security Council has taken the measures necessary to maintain international peace and security."[41]

The basic condition for the exercise of the right to self-defense is armed attack, but the concept of the same is not defined by either the Charter or the subsequent documents, and therefore the classification of such an act in practice "is based on an extremely subjective

38 Article 2(4) of the UN Charter.

39 Orsolya Bartha, 'A fegyveres összeütközések fogalma, fajtái és elhatárolásuk', *in* Tamás Ádány *et al., A fegyveres összeütközések joga*, Zrínyi, Budapest, 2009, p. 20.

40 GA Res. 29/3314, The Definition of Aggression, Article 1.

41 Article 51 of the UN Charter.

decision; the same fact can be attributed to different classifications under the same law."[42] The subjective nature of the decision is reinforced by the fact that it is the resolution of the contested state that is relevant and there is no need for a decision adopted by the Security Council. Deeming this to be a condition would hollow out the essence of self-defense; even without this, the state can begin to use violence for self-defense purposes.

Armed attack is the only exception in the Charter where states or their communities have the option of using armed violence. "However, as the Charter does not include the definition of armed attack, there is nothing to exclude the possibility of using self-defense by analogy."[43] Armed attack must meet two conditions: *(i)* the act must have an extraordinary weight or intensity, and *(ii)* the act of the offending persons must be attributable to another state.

In determining the level of armed violence, the easiest way is to start from the concept of aggression, as both are a subset of violence. The ICJ declared that armed attack is the most serious case of violence.[44] "Because of this, only the most serious cases of aggression are classified as an armed attack."[45] So, these concepts are in a cause and effect relationship with each other. Another characteristic of an armed attack is that an attack must always be attributable to another state. So, armed attacks can only be committed by a state. It is obvious that if a state's regular troops commit an attack of a specific intensity, then in this case it will be classified as an armed attack. However, it is questionable whether the attack by individuals or their groups can be attributed to the state, and if so what level of relationship should this be? It is accepted that the acts of individuals and their groups can only be attributed to a state if they act under the instruction, guidance or control of the state. However, the level of control is not specified. In its judgment the ICJ in *Nicaragua* stated that an effective control was necessary,[46] while according to the international tribunal set up for investigating acts in violation of humanitarian rights in the former Yugoslavia declared that the overall control of the state is sufficient.[47] However, in the case of Bosnia and Herzegovina and Serbia and Montenegro the ICJ confirmed the principle of effective control, adding that the use of overall control as a criterion would significantly broaden the scope of the right to self-defense, which would be contrary to its original purpose.[48] In

42 Gábor Sulyok, 'Az egyéni vagy kollektív önvédelem joga az Észak-Atlanti Szerződés 5. cikkének tükrében', *Állam- és Jogtudomány*, Vol. 43, Issue 1-2, 2002, p. 108.

43 Gábor Sulyok, 'A terrorcselekmény elkövetéséhez használt polgári légi jármű lelövésének nemzetközi jogi és alkotmányjogi megítélése', *Fundamentum*, Vol. 9, Issue 3, 2005, p. 34.

44 *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States)*, Judgement of 27 June 1986, ICJ Reports 1986, pp. 64-65, para. 191.

45 Gábor Kajtár, 'A terrorizmus elleni önvédelem a XXI. században', *Kül-Világ*, Vol. 8, Issue 1-2, 2011, p. 10.

46 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States)*, Judgment of 27 June 1986, ICJ Reports 1986, pp. 64-65, para. 115.

47 *Prosecutor v. Dusko Tadic*, Judgment, Appeals Chamber, Case No. IT-94-1, 15 July 1999, para. 145.

48 *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Summary of the Judgment of 26 February 2007, para 406.

the opinion of the International Law Commission, the desired level of control should be assessed on a case-by-case basis. "So, determining the responsibility of the state requires the precise knowledge of the details of the preparation."[49] In the light of the above, we must consider the following question: can cyber attacks be classified as armed attacks?

A cyber attack can be of several types; there are attacks which are aimed at disabling communication or making data or information inaccessible, while another group of attacks is destined for destruction; destruction of the system itself or the infrastructure controlled and managed by the system. "A cyber attack which is only intended to cause damage can be sophisticated or primitive, depending on the capacity of the attacker and the target of the attack."[50]

> "Hence, in the arsenal of warfare the instruments and methods of attack appeared in cyberspace – in the world of computer networks. At the same time, not only large, regular armies are capable of using these but also small countries which are much poorer in armaments and financial resources, or groups and cells that are driven by political goals or even terrorist organizations,"[51]

as well as some well-trained and well-equipped individuals. It is therefore necessary to examine whether the state has the right to self-defense in the case of an attack in cyberspace, and when can the attack be considered an armed attack? A cyber attack in itself is not necessarily sufficient to put a state in a position of self-defense because the intensity of the attack is one of the decisive factors. As we indicated above, there is no widely accepted concept of armed attack, but we can agree with the approach that attacks endangering the life of a large number of people or putting an end to their life, or those attacks that cause significant damage to the infrastructure can be considered armed attacks.[52]

Therefore, cyber attacks whose result reaches this intensity must be considered an armed attack. It is to be noted that according to the editors of the Tallinn Manual, cyber attacks should be compared to the use of radioactive, biological and chemical weapons,[53] which means that the authors are of the view that existing rules of international law must be applied by analogy.

In cyberspace, an attack leading to such a result could be an attack on a nuclear power plant or nuclear reactor, and there were several examples for this: the Blaster worm in 2003 and the Stuxnet virus in 2010. The Blaster worm caused a power outage in the US and in

49 Sulyok 2005, p. 35.
50 Ákos Orbók, *A kibertér, mint hadszíntér*, at www.biztonsagpolitika.hu/documents/1375084295_Orbok_Akos_A_kiberter_mint_hadszinter - biztonsagpolitika.hu.pdf.
51 Haig 2006, p. 66.
52 Schmitt 2013, p. 55.
53 Id. p. 54.

Canada on 14 August 2003; "since the critical alarm systems has failed, the employees of the FirstEnergy have not stopped the series of events, because they did not know what was happening."[54] In just over an hour, the Blaster crashed the main server computer that operated the full alarm function, so the workers did not realize that the system's functioning was in danger, or even that the system's conditions had changed. It was fortunate that the Blaster did not carry out any malicious destruction in the infected machines, but only consumed their resources. The Stuxnet virus did not mean a direct threat to the power plants; its targets were the Iranian uranium enrichment facilities which had been so effectively attacked by the virus that it set back the nuclear program of the Iranian state by several years.

"The possibility that there was a state behind the Stuxnet is underlined by the fact that the software itself was very complex and sophisticated, and during its activity it applied a targeted differentiation in the scope of the pre-selected controlling systems."[55]

That 2012 case is less known, when a malware virus was transmitted to a power plant management system in the US that accessed all vital networks; again, luckily, the purpose of the action was not an attack. These cases reveal that attacking power plants with cyber instruments is not an impossible business; in all of the above cases if destruction had been the primary goal, it would have been achieved. Obviously, a cyber attack causing the destruction of a nuclear power plant would be classified as an armed attack by all states, and the consequence of the attack would be the same as the nuclear weapons' effect (nuclear radiation).

Another type of cyber attack is when the impact it produces does not reach the threshold that would qualify them as an armed attack, but the consequences of the attack can already go beyond that extent and therefore, the original attack may be classified as such. Such an attack can be one that attacks a state's drinking water system or water purification system. The direct impact of this attack is that the infrastructure is not functioning properly, but its indirect impact is the contaminated drinking water, which can have serious consequences for the civilian population. Such an attack was committed against the drinking water system of Haifa.[56]

---

54 Bruce Schneier, *Schneier a biztonságról*, Budapest, HVG, 2010, p. 144.

55 Tamás Lattmann, 'A nemzetközi jog lehetséges szerepe az informatikai hadviselés területén', *in* Zsuzsanna Csapó (ed.), *Emlékkötet Herczegh Géza születésének 85. évfordulójára – A ius in bello fejlődése és mai* problémái, Pécs, Kódex Nyomda, 2013, p. 211.

56 Benedikt Pirker, 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace', *in* Ziolkowski (ed.), 2013, p. 56.

Such an attack may result in the deaths of tens of thousands of civilians, or it can have millions of victims depending on the size of the network.[57] In case of an attack like this, an analogy can be drawn with biological or chemical attacks. As both tactics are forbidden by a large part of the international community in multilateral agreements,[58] such an attack can be classified as an armed attack even in case of a small number of victims.

Unlike previous cases, an attack purely conducted in cyberspace that paralyzes a state's communication network can be classified as an armed attack, but of course the appropriate intensity is also necessary. As a result of this type of attack simulated by the US, "the controlling system of the attacked country and its functioning collapsed within two to four days",[59] which resulted in the dissolution of public order. The attacked country sank into anarchy, and its social network collapsed. The outcome is exacerbated by the fact that the attack "leads to distrust towards their own software running systemized tools and causes serious insecurity by raising uncertainty and decreasing the sense of security."[60]

A similar attack was launched against Estonia in 2007 and Georgia in 2008, which were not sufficiently intensive and lengthy to achieve the results above, but they predicted the system of such attacks, including the paralyzing of governmental bodies, the complete paralysis of the banking network, the police and military communication and then the civilian communication system. It cannot be predicted that how much infrastructural and humanitarian damage such an attack would cause beyond the economic and political consequences. There is also the possibility that in the event of such an attack the attacked state would not be able to exercise its right to self-defense.

According to the facts outlined above, it is clear that certain cyber attacks may be classified as armed attacks based on their intensity, but for this to hold water, it is necessary to examine the other criterion, whether it can be attributed to a state or not.

In the case of cyber attacks where a state body conducts the attack, if it reaches the required intensity, we can clearly talk about an armed attack. However, it is also necessary to investigate that scope of cases when individuals or groups of individuals commit attacks. Any of the three above mentioned elements, that is, guidance, instruction or control will mean that it can be attributed to the state. In the context of control, we can only imagine effective control in the case of the cyber attacks, since the application of the theory of overall control would, on the one hand, greatly extend the scope of attributability, and

57 Other circular infrastructures, such as natural gas network can be mentioned in this regard.

58 Convention of 1971 on the Prohibition and Destruction of the Development, Production and Storage of Bacteriological (Biological) and Toxin Weapons (158 states parties); Convention of 1993 on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons, signed in Paris on 13 January 1993 (184 states involved).

59 Zsolt Haig & László Kovács, 'Fenyegetések a cybertérből', *Nemzet és Biztonság*, Vol. 1, Issue 5, 2008, p. 67.

60 Lattmann 2013, p. 212.

beyond that it would obviously result in a restriction on the freedom of the internet, presupposing a much stricter state control.

It is necessary to examine what cases may fall within the scope of effective control. Since there is no international practice in this field, it is worth using analogy again and examining the practice regarding terrorist organizations. In Gábor Kardos' opinion, there is effective control in case of terrorist organizations, if the state provides resources, endures training bases or provides shelter for members of such organizations.[61] These criteria can also be applied to offenders of cyber attacks or their groups, with the addition that the provision of recruitment would also result in attributability. However, this scope of cases is questionable when the state 'only' knew about the activity, but has not done anything, or was not able to do anything. In relation to a similar case, Tamás Lattmann and Boldizsár Nagy noted that

> "the targeted state can act with violence if the territorial state is unable to control the attackers on its territory, and the international community (Security Council, in the form of coercive measures) does not act. Then defense is legitimate if it is proportionate and its implementation is in accordance with the rules of warfare."[62]

This category of cases also makes cyber attacks attributable. This is confirmed by the fact that

> "according to the current practice of states, rules on the use of violence and the right to self-defense are evolving in parallel in order to prevent the dangers arising with the use of violence."[63]

For this reason, it is necessary to take into account the mandatory standards of international law in the exercise of the right to self-defense, in particular the international rules of humanitarian law. In case of an armed attack, not only the right to self-defense, but also the humanitarian law will apply, including the "the *sic utere tuo* principle, the obligation of the states to prevent malicious computer activities that may harm the right of states."[64]

---

61 Gábor Kardos, 'Vannak-e jogai a terroristáknak?', *in* Péter Tálas (ed.), *Válaszok a terrorizmusra II. A politikai marketing csapdájában*, Mágustudió, Budapest, 2006, p. 89.

62 Tamás Lattmann & Boldizsár Nagy, 'Támadható-e Bejrút vagy Tel-Aviv?', *Élet és Irodalom*, Vol. 50, Issue 33, 2006, p. 2.

63 Zachary Newland, 'Collusion and Confusion: Evaluating the Right of Self-defense Against Private Actors', *Stellar*, 2009, at www.okcu.edu/uploads/arts-and-sciences/english/docs/stellar2009.pdf.

64 Katharina Ziolkowski, 'General principles of International Law as Applicable in Cyberspace', *in* Ziolkowski (ed.), 2013, p. 185.

In this category of cases, it is necessary to point out emphatically that attributability can only be confirmed solely and exclusively on the basis of the assessment of all circumstances of the case.

12.6 Cyber Defense, or Self-Defense in the Scope of Cyber Attacks

The normative concept of cyber defense is provided by the cyber defense concept of the Hungarian Defense Forces, according to which cyber defense is

> "the use of security measures designed to create cyber security against intentional impacts aimed to the designated critical infrastructural elements that can cause service interruption, termination or limitation, or unauthorized data handling, coming through a network or appearing in any other form. The most important tasks of defense are prevention, detection, analysis, evaluation, reaction, recovery and service improvement."[65]

The tools of defense can be divided into two main categories; passive and active protection.

> "Passive defense tools and methods can be firewalls, antivirus software, access control, intrusion detection and adaptive response tools. The following can be classified as active defense methods: pre-emptive attacks, counter attacks and active deception."[66]

From the viewpoint of cyber defense's legal assessment, the cases of cyber intelligence and cyber attacks conducted by a state must be separated from attacks and intelligence conducted by individuals and their groups, including terrorist organizations. State rules are defined by the principles of international law and the rules on the law of war, while the framework of actions to be taken against individuals and terrorist organizations are mainly set out by internal law rules, which must comply with guarantees laid down in universal and regional documents of fundamental rights.

In the case of states, passive defense tools can be used even in the case of cyber intelligence, and also in the case of both armed and non-armed attacks. However, active cyber defense tools can only be used legally in case of an armed attack and even then, only under specific conditions. The set of conditions are basic, *i.e.* the active cyber defense must be

65 Instruction of the Minister of Defence to the Publication of the Hungarian Army's Professional Concept of Cyber Defence No. 60/2013. (IX. 30.), Appendix 1, Section 2(9).

66 Haig 2006, p. 68.

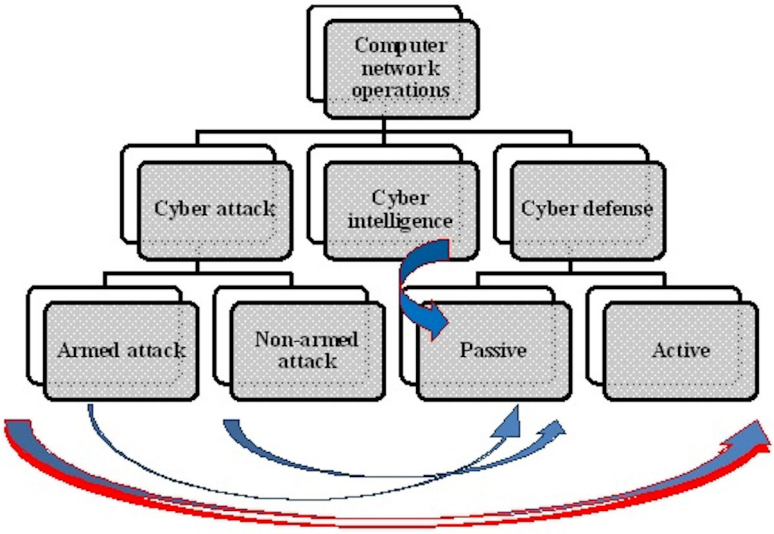
necessary and proportionate, and it must comply with international law's current rules. The exercise of the right to self-defense can only serve to deflect and reflect the attack;

> "therefore, the use of armed violence should not be retaliatory, punitive or generally preventive of any future attacks. These are classified as self-help with the use of unlawful armed violence, or as unlawful armed repression."[67]

The principle of proportionality means that the violence used by applying the right to self-defense must be adapted to the extent of the armed attack in question.

The current rules of international law on self-defense deny the use of preventive defense tools or the use of pre-emptive attacks, so under no circumstances can pre-emptive attack-type cyber defense procedures be used, on the other hand, active cyber defense tools can only be used in the case of an armed attack and only until measures of the Security Council are implemented.

Figure 12.3 Typology of Cyber Operations (Made by Roland Kelemen.)



In the case of individuals, personnel actively involved in the attack and intelligence have to be separated from passive persons who provide resources. This separation also appears in the Tallinn Manual, which divides the individuals involved in the attack into active

67 Kajtár, 2011, p. 14.

offenders who demonstrate intentional attitude and into passive, careless offenders. In the case of the former, it declares that the civilian person loses his protection and becomes subject to attacks by IT and other lawful methods. These other legitimate methods have not been defined, however, since in this case too, the exercise of the right to self-defense can only be proportionate and reasonable, it is obvious that the use of these tools can only achieve the degree of contribution to the result. Otherwise a person may be eliminated who concedes the resources of his machine to complete the operation, alongside with hundreds, thousands or even hundreds of thousands of other users.

The Manual does not refer to any possible actions against passive offenders; this silence indicates that the attacked state is not authorized to take action against them. In our view in the case of exercising self-defense, cyberspace actions solely aimed at self-defense can be carried out against passive offenders to the necessary and proportionate extent, if this is indispensable to overcome the danger, but the responsibility of the passive participant cannot be determined for the armed attack.

The issue of pre-emptive cyber defense arises in case of both the active and passive circle of persons. Here, in the absence of international rules, in order to protect itself and its citizens, the state is able to prevent these actions – whether committed or not, but being at least in the preparatory or experimental phase – by possible pre-emptive defense tools to the extent necessary and proportionate. An example would be to prevent the activation of huge zombie networks or cyber attacks prepared against critical infrastructure. However, it is also necessary to emphasize the criterion of proportionality and necessity here, and the restriction of fundamental rights can only take place in accordance with the law.

12.7 Conclusion

The appearance of cyberspace and its worldwide nature made it possible for human society to become truly global and the existence of interactions that transcend continents and oceans within a fraction of the moment. This cyberspace is an ever-expanding entity that is difficult to describe with conventional geographic terms, and it has a significant impact on the life of individuals and the society and the relationships at large. Active players of this space are states that also claim a legitimate monopoly of policing this medium.

As a result, in line with conventional space, the state's administrative and militaristic bodies also appear in cyberspace, creating a new type of warfare in the twenty-first century; this is a specific type of information warfare, namely, computer network operations. Within this operation type, the triad of cyber intelligence, cyber attack and cyber defense can be distinguished, each of which can be identified by one single move of conventional warfare. Based on this, the exact rules of warfare applicable in this space to such acts are yet to be

created. Building on analogy can be the way forward, taking into due consideration the non-standard nature of cyberspace, which requires a precise, appropriate regulation.