ESTONIA CYBER-ATTACKS AND THE IMPACT ON NATO

Alexandra Elena TIMOFTE*

Abstract

Out of all the industrial or technological revolutions that ever occurred throughout the history the latest one marked all the components of human life. But development comes with diversification of vulnerabilities and threats. Thus, the providers of security are forced to have the proper response facing all kind of threats, conventional and non-conventional (hybrid threats) starting with the military dimension to the digital or cyber space.

9/11 and the cyber-attack against Estonia were both conducted through non-conventional means, they were both affecting the civil population and not only the government or the politicians, both were aiming to weaken the national security of the countries targeted. But what impact did these two events have on NATO? How was each perceived at the level of the Alliance and what was their outcome? A terrorist attack is producing way much greater impact upon the public compared to a cyber-attack which can hardly cause such major visual effect. However, the latter, in the context of the fast digitalization of the present days, can seriously damage the government services and decrease peoples trust. In this realm a real and comprehensive response to the new threats is required, not only from the states as sovereign entities but also from the organization at the international level.

Keywords: *cyber-attack, cyber defense, non-conventional means, non-conventional threat, terrorist attack.*

Introduction

A terrorist attack caused by crashing a plane into a building is having way much greater impact upon the public compared to a cyber-attack which can hardly cause a major visual impact. However, the latter, in the context of the fast digitalization of the present days, can seriously damage the government services and decrease people's trust (Ciolan, 2014).

* National School of Political Studies and Public Administration, timofte.alexandra26@gmail.com.

On this realm a real and comprehensive response to the new threats is required, not only from the states as sovereign entities but also from the organizations at the international level. The subject of this paper is the cyberspace (especially the cyber defense) analyzed from the perspective of one of the most influential military Alliances still existing nowadays: NATO. The reason why I choose this topic is due to its growing importance, but most of all, due to the events that occurred within this domain: the cyber-attack on Estonia in 2007. These events generated important discussions regarding the behavior of the actors in the cyber space and the level of jurisdiction that can be applied to this domain.

The questions of the following research are: Why in the American case Article 5 was triggered and in the Estonian case not? What were the consequences of these two events on NATO, especially after the 2007 cyber-attack? The method I will apply will be comparison. I chose to compare the impact that the 9/11 terrorist attacks had on the Alliance (that moment being the first and the only one when the Article 5 of the Alliance was invoked) with the events from Estonia, which did not trigger the Article 5 of the Alliance. Nevertheless, as it will be shown, the latter event brought cyber-security problems on the diplomatic agendas of NATO officials, generating important changes within the organizational framework and on the political perspective of the cyber space.

I choose to compare the two events due to the different impact they had despite the similarities between them. As I will illustrate in the following pages, 9/11 and the cyber-attack against Estonia were both conducted through non-conventional means, they both affected the civil population and not only the government or politicians, both were aiming to weaken the national security of the countries targeted. After this process I will analyze the impact on NATO and the actions taken by the Alliance. At this level I will illustrate the main differences reflected not in the manner that were conducted, but in the way they were perceived at the level of the Alliance: in the first case we have a clear response, a day after the attack, while in the second case we have no immediate response, but a step by step approach focused on defensive measures.

The paper is structured in four parts. The first chapter will introduce the concepts of non-traditional threats and non-traditional actors and the emergence of these two during the 21st century as part of a larger subject – the hybrid war. The second chapter will present the two selected cases in which the concept of non-traditional threats is exemplified: the terrorist attack on 9/11 and the cyber-attack on Estonia conducted in April 2007. In the third chapter I will compare the two cases, and I will identify differences and

similarities from a NATO perspective and will emphasize the main actions undertaken by NATO as a possible response to the cyber-attack on Estonia. The last of the paper will be reserved for a series of final remarks.

The emergence of non-conventional threats on the international arena

During the last decades, the security field suffered some changes, being widened both horizontally (including more domains) and vertically (including different kind of actors). Horizontally, besides the political and the military fields, economic, cultural and environmental ones were added (Buzan, 2014). While in terms of actors, the limitation to the state was overcome by the introduction of the individual. However, at the international level a wide variety of actors exist, from states and individuals, to different types of organizations and groups of individuals. But the widening concept of the security field meant a variety of the possible threats. Specifically, the diversification of the nature of the actors present on the international arena and the possible threats and challenges posed by them in the 21st century gave birth to a new category of threats: the so called non-traditional ones. For example, in a 2014 article published in the *International Journal of Development and Conflict* it is argued that "rise of non-state actors, intra-state wars, environmental degradation and climate change, demographical changes and cyber-conflict pose a greater security threat to the nation-states in the 21st century than armies of other states." (Srikanth, 2014)

The non-traditional threats are the opposite of the idea of solely conventional threats seen especially as organized military components. The hybrid threats are included in this category. The causes of emergence of these threats are various: from globalization, to technological revolution and the spread of democracy. My main focus is to see which are these new threats and their impact, with a special focus on NATO. The definitions of these new types of threats vary from one author to another. For example, from the perspective of a military practitioner the hybrid threats are represented by the actions of an opponent that "simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism and criminal behavior in the battle space to obtain their political objectives." (Hoffman, 2009)

Other see the hybrid actions as including also cyber offensive and psychological operations (Hunter, Pernik, 2015). Figure 1 – Hybrid threats (Purton, 2015) depicts the hybrid threats as representing the core of a combination of actions such as conventional, irregular and criminal means, but also acts of terrorism.

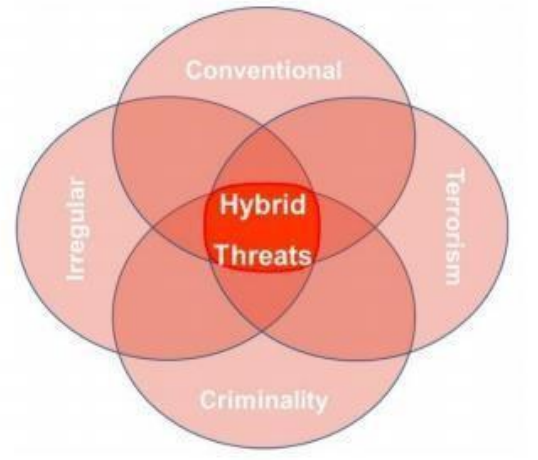

Fig. 1 Hybrid threats

An even more comprehensive view of what the hybrid threats is provided by NATO: "multimodal, low intensity, kinetic and non-kinetic threats to international peace and security including cyber war, low intensity asymmetric conflict scenarios, global terrorism, piracy, transnational organized crime" (Richterová, 2015).

Fig. 2: Hybrid threats – NATO perspective

Not only the action *per se* has been analyzed, but also the actors involved. The importance of the actors in the case of hybrid war is essential for understanding this type of threats. At the international level we have two main categories of actors: state and non-state actors. If in the first case the understanding is clear, in the second case things are more complicated. In the category of non-state actors, just as the term is saying, the actors that do not speak in the name of the state are included. The problem arises from the multiplicity of non-state actors that can be represented either by organizations (international relations), corporations (international economic relations) or by individuals or groups of individuals. At the same time, at the international level we encounter official and unofficial positions of states regarding the problems present. For example, even though some non-state actors, such as terrorist organizations or hackers, are declaring they are acting on their own behalf, in some cases they are supported and/or sponsored by state actors. In both cases – actions conducted by terrorists or hackers – the link between states and these non-state actors is very fragile and very difficult to be tracked down. The blurred line between the two is making the process difficult. However, the two types of actors are more often included in the non-state category.

From a security perspective, the most important problem is when a non-state actor is challenging the legitimacy of a state actor by using violent means. The challenges posed by the non-state are not necessary new, but in the 21st century this phenomenon gained more and more attention because we are witnessing a particular mixture between the non-state actors and the new technological tools. Due to this last component, weak non-state actors (such as individuals or group of individuals) are posing a real threat to the security of a state. Even though the power of a state in terms of military means is greater than the power of any individual or group of individuals, the use of irregular and nonconventional tactics by the latter, in some cases, overcome the damages they can produce to the former. However, the irregular or non-conventional tactics in order to defeat the opponent are not used only by non-state actors. Historically, even states appealed to these tactics as source of power in order to defeat a stronger combatant. According to this perspective, it can be argued that the hybrid war is the instrument of the weaker part in combat with a stronger force. At the same time, some specialists assert that the hybrid war may be seen, in the near future, as "a smart and nimble tactic." (Hoffman, 2009, p. 34)

These new types of threats have drawn the attention of the North-Atlantic Organization as well. However, compared with United States, the Alliance had a belated response. For example the United States mentioned

the term hybrid threats since the first decade of this century, while in the NATO documents we encounter this especially starting with 2010. Even if in the 2010 NATO *Strategic Concept*, the word hybrid is never mentioned, there are clear specifications regarding the security challenges existing at the international level. Besides the acknowledgement that "the Euro-Atlantic area is at peace and the threat of a conventional attack against NATO territory is very low" (NATO, Strategic Concept, 2010, p. 3) the 2010 *Strategic Concept* expresses a clear concern regarding the "new threats": proliferation of chemical and biological weapons, missiles, terrorism, modern technology in the hands of terrorists, illegal arms trafficking, narcotics and people, cyber-attacks (NATO, Strategic Concept, 2010, p. 3). Apart from the graphic pictured above, within the Alliance, the hybrid threats are defined as "those posed by adversaries, with the ability to simultaneously employ conventional and non- conventional means adaptively in pursuit of their objectives." (Bi-Sic Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats", 2010, p. 2) The definition accepted by NATO resembles to some extent the one given by Hoffman. What is important though: none of the definitions is pointing to a specific category of actors. They can both encompass state and non-state actors which can use a mix between conventional and non-conventional means in combat. Moreover, in the NATO chart, the inclusion of both terrorism and cyber-attacks on the non-kinetic category can be noticed. I am making this observation because it is of vital importance for understanding the following part of this paper which includes case studies for two important events: the 9/11 terrorist attacks on USA and the cyber-attacks on Estonia in April 2007.

The non-conventional aspects of the 9/11 and April 2007 attacks and their impact on NATO

The beginning of this century has been marked by one of the most terrifying events in the recent history: the terrorist attacks on 11th of September 2001. Four commercial planes were hijacked by 19 individuals. Two of the planes were crashed into the symbolic buildings of US power: The World Trade Center; another one hit the headquarters of the US Department of Defense, the Pentagon; the fourth plane crashed somewhere in Pennsylvania, not reaching its target (BBC, The 9/11 terrorist attacks). The entire operation was claimed by Al-Qaeda, a terrorist organization located in Afghanistan. The impact of this event was huge. With almost 9000 casualties (Plumer, 2013), 3000 dead and 6000 wounded, the 9/11 attacks represent a turning point in history. The US president at that time, George W. Bush,

labeled the events as "evil, despicable acts of terror" (BBC, The 9/11 terrorist attacks) and stressed that United States is facing a new and different kind of enemy (*The 9/11 Commission Report*, p. 330).

Six years after this event, another important incident occurred: the cyber-attack against Estonia. At the end of April and beginning of May 2007, Estonia was the target of one of the most powerful cyber-attacks in history. Since the technological revolution at the end of the XX century, other cyber-attacks were conducted, but the one against Estonia had some particularities due to the features of the targeted country. Estonia is one of the most wired countries on the Earth. The range of activities done by internet is widespread and it includes sectors as: e-government, e-voting, e-taxes, e-parking, e-banking, e-identification systems. That is why Estonia is a country that admits the access to internet as being part of the basic human rights (almost the entire country is covered by free Wi-Fi networks) (Laasme, 2011, pp. 58-63). The wide coverage of the Internet and the use of it in almost every daily activity comes with major responsibilities for the state, measured in terms of the capacity to secure the networks and to prevented the collapse. In this sense, the digital space is becoming a part of the national security. Thus, when, in April 2007 a near-catastrophic botnet hit almost the entire electronic infrastructure of Estonia, the national security of this state was threatened. (Laasme, 2011, p. 60) The relevance of this incident is highlighted by the fact that, never before, an entire country happened to be a digital target. (Laasme, 2011, p. 60)

As it can be noticed, both cases, the 9/11 and the events from 2007 that occurred in Estonia can be included in the category of non-traditional threats. In the first case we encounter the use of non-military means (theft of passenger aircrafts crushed into targets strategically chosen) in order to affect and challenge the security of a state. In the second case, we also have a new type of threat, distinct from the conventional, military one: cyber-means used in order to affect the security of an entire state in terms of electronic infrastructure. From a NATO perspective both events have had impact on the Alliance. In the following pages I will summarize the most important measures undertaken by NATO, first, after the terrorist attacks on 9/11 and second, after the April 2007 cyber-attack. Both cases will be analyzed only from the perspective of non-traditional threats.

In the case of 9/11, the answer from NATO was out of hand. In less than 24 hours the Secretary General of the Alliance at that time, Lord Robertson notified the UN Secretary General about the decision made by NATO member states: to invoke the principle of Article 5 from the Washington Treaty (NATO, "Collective defense – Article 5"). This was the first and the

single time in the history of the Alliance when the principle of collective defense was invoked. Even though it was not an armed attack in term of means, the major consequences of these actions lead to a firm and immediate response from the Alliance. In October 2001 NATO agreed on eight measures proposed by US that were tackling: the intelligence information sharing, the support to the countries that are subject or possible subject of any terrorist attack as a result of their involvement in combating this phenomenon, increased security on their territory to any facility provided by the allies, the access to any ally to their ports and airfields for operations against terrorism, the deployment of the Alliance Standing Naval Forces to the Eastern Mediterranean, the readiness of the Alliance to deploy part of its Airborne Early Warning Force in order to combat terrorism (NATO, "Collective defense – Article 5"). Starting the same month operation *Eagle Assist* was launched – the first anti-terror operation, consisting of patrols over the sky of United States.

One of the most important actions of the Alliance was the empowerment of NATO to take the lead of the International Security Assistance Force (ISAF) mission in August 2003. Due to the fact that Al-Qaeda was localized mainly in Afghanistan, the international coalition transformed this country in the main target of the anti-terrorist actions. The aim of the ISAF mission was to help the Afghan government to provide security to the country and in the same time to ensure that Afghanistan will never become a *safe-haven* for the terrorists (NATO, ISAF mission in Afghanistan (2001-2014)).

In the case of Estonian cyber-attacks we have a different range of actions and measures taken by the Alliance. Even though the attack affected the national security of Estonia, the way in which the attack occurred did not represent a case to trigger the Article 5. In 2008, in the declaration of the summit held in Bucharest was stated for the first time the need to strengthen the key Alliance information system against cyber-attacks (NATO, "Bucharest Summit Declaration", 2008).

Furthermore, in the strategic concept issued in 2010 the fact that the cyber-attacks are more and more frequent and the impact of such attacks on the government administration, business and critical infrastructure of the Allies can be very disruptive is highlighted (NATO, Strategic Concept For the Defense and Security of the Members of The North Atlantic Treaty Organization, 2010, p. 3). In response to these threats, in the same document the need of a centralized protection of the Alliance and enhanced coordination of cyber-capabilities of the member states was specified (NATO, Strategic Concept For the Defense and Security of the Members of The North Atlantic

Treaty Organization, 2010, p. 3). Beside these measures, maybe the most important one is the decision of the Alliance to "recognize 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" taken at the Warsaw summit held in July 2016 (NATO, "Warsaw Summit Communique", 2016). At the operational level, the Alliance's preoccupation for the cyber-space started in 2002 when the NATO Computer Incident Response Capability (NCIRC) was initiated[1], but which was fully operational in 2008. The same year the Allies ratified NATO Cyber Defense Policy and decided to create the Cyber Defense Management Authority in Brussels. In May 2008, the Cooperative Cyber Defense (CCD) Center of Excellence (COE) was established in Tallinn (NATO opens new center of excellence on cyber defense, 2008). CCD COE aim is to give support to its member states and NATO members in the fields of technology, law, strategy and operation (CCD COE, "About Cyber Defense Center"), but it does not belong to the NATO military command or force structure (CCD COE, "About Cyber Defense Center"). It is widely accepted that all these measures were hasted by the events that occurred in Estonia in 2007.

Comparison: similarities – differences

If the previous chapter I presented the main aspects of the two events I chose to compare. In the second part I described the impact that the events had for NATO and the direction the Alliance choose after both of them. The following comparison will be in regard only the two cases from the perspective of NATO and the perceived non-traditional threats.

On the one hand we have the 9/11 terrorist attack which triggered the Article 5 of the North-Atlantic Treaty. The attack was conducted by the terrorist organization Al-Qaeda by appealing to nonconventional means: they transformed three passenger aircrafts into weapons, hitting strategic targets inside United States, causing a great number of casualties. On the other hand, we have the use of cyber-instruments as non-conventional means targeting the entire electronic network of a country. Estonia's electronic infrastructure was struck by almost one million computers at the same time, attack which was coming from hijacked computers from United States by unknown elements inside Russia. (Laasme, 2015, p. 60) In this case, even the Estonian officials linked the attack with the decision to remove a Russian statue which

[1] It is the main instrument developed by NATO in order to protect the networks of the Alliance. It includes Rapid Reaction Teams which are designed to help the member states in protection of the networks.

was commemorating the Russian victims from WWII. At the level of NATO there was no declaration that the Russian Federation is behind this attack.

Until this moment we can identify a series of similarities. First, both actions are included on the list of non-conventional means that can be used by any adversary in a combat. There has not been used any military infrastructure in order to undermine the national security of the two countries. Second, the nature of the actors: in the 9/11 case we have a group of individuals labeled as terrorist organization (non-state actor), in April-May 2007 attack we do not have a clear identification of the attacker. In this case, even if we do not know who conducted the attack, at least the possibility to be a state actor was not fully acknowledged. Of course, the second similarity is having some weaknesses due to the fact that the actor involved was not identified at all.

Nevertheless, it is important that NATO did not rush in linking the attack to Russia. As I mentioned above, the terrorist organizations or the hackers can be supported or controlled by states, but in the cases in which the link between them cannot be demonstrated, hackers are remaining non-state actors.

A third similarity is the target of the attacker. In the case of 9/11 the terrorists hit civilian buildings and caused casualties among civilians in a deliberate way. The Pentagon was also hit, a building of the government, but this cannot be considered part of the military or combatant in a conventional war. In the Estonian case, due to its widespread use of digital space, also the civil population was highly affected because, as I mentioned above, Estonia is using: e-government, e-banking, e-identification system and the list continues. Even though the Estonian government was also the target, the attack paralyzed the entire country which was forced to cut down all the ties with the outside networks, thus affecting not only a limited number of people such as politicians or any other group, but the daily activity of the civilians.

On the other hand, in terms of differences, we can identify some important ones from NATO perspective. The consequences that the events of 9/11 had (9000 casualties), compared to the cyber-attack which caused no deadly victims, but affected the electronic infrastructure of a country. This is a difference at a general level, but at the level of the Alliance the fact that in 2001 NATO chose to take military action and in 2007 not, the difference can be tracked down in the documents of the Alliance. For example, in the Strategic Concept of 1999 was clearly stated:

> *Any armed attack on the territory of the Allies, from whatever direction would be covered by Article 5 and 6 of the Washington Treaty. However the Alliance must take into*

> *consideration the global context. Alliance security interest can be affected by other risks of a wider nature, including acts of terrorism, sabotage, organized crime, and by other disruptions of flows of vital resources.* (NATO, "The Alliance's Strategic Concept")

These specifications from the Strategic Concept from 1999 were an argument in favor of triggering the Article 5 in the case of 9/11. More exactly, in the press release from 12th of September 2001, NATO member states "condemned terrorism as a serious threat to peace and stability and reaffirmed their determination to combat it in accordance with their commitments to one another, their international commitments and national legislation." (NATO, "Statement by the North Atlantic Council")

Thus, in terms of legal framework, the Alliance was entitled to consider 9/11 actions as covered by the principle of collective defense stated in the Washington Treaty.

Another difference is that the events that occurred in Estonia triggered no military actions. Here we can identify the most important difference between the two events from NATO perspective. While the 9/11 event was covered by legal framework, the Estonian case was not. Every decision related with the cyber-space in terms of legal framework was taken post factum. In other words, if there were any specifications in the official documents of the Alliance tackling the issue of cyberspace/cyber-attacks the attitude of the Allies towards this kind of threats, other kind of actions would have been taken. But in this case, only years after, when the member states became aware of the damages that can be produced through cyber means, agreed to include the cyber space on the list of other three (land, sea, air) covered by the collective defense principle.

NATO after 2007: strategy, means and policies

The Article 5 from the Washington Treaty specifies "the Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all" and all the necessary means, "including the use of armed force." (NATO, "The North Atlantic Treaty (1949)")

To consider cyber-space as part of the collective defense principle means that to a cyber-attack even an armed attack as a response is possible. This specific issue brought the attention of the parties involved. That is why one of the most important issues that NATO is struggling to establish is a threshold: to what extents a cyber-attack will be considered as requiring a

military response? In this regard, at the invitation of NATO Cooperative Cyber Defense Center of Excellence a group of international law experts elaborated the Tallinn Manuals which are trying to set these thresholds and the way in which international law can be applied to cyber-space.

Another important issue that is discussed within NATO is the identification of the attacker. Cyberspace is very attractive due to the fact that the user can choose to remain anonymous. To track down the source of an attack in cyberspace is very difficult, thus responded it is very unlikely.

In this regard, NATO strategy for cyber defense is focusing on "the resilience of NATO's and Allies' Communication and Information System (CIS)." (Ducaru, 2016, p. 20) To this strategy is contributing the NATO Computer Incident Response Capability and the affiliated cyber defense Rapid Reaction Teams. In strong relation with increased resilience of the Alliance and its members is the awareness and early warning policy endorsed by NATO, but also the cooperation and exchange of information between the Allies. For the cooperation part we encounter the agreement between NATO's Cyber Defense Management Board (CDMB) and the national cyber defense authorities, while in the case of early warning NATO developed the Cyber Threat Assessment Cell (CTAC). (Ducaru, 2016, p. 19.) In its efforts to secure the cyberspace NATO also developed important instruments of cooperation with other organizations such as: United Nations, Council of Europe, Organization for Security and Cooperation on Europe. One of the most relevant steps towards this aim was made in 2016 when NATO and EU signed a Technical Arrangement on Cooperation in the Cyber Domain. "This Technical Arrangement provides a framework for exchanging information and the sharing of best practices between emergency response teams." (NATO, "NATO Cyber Defense", p. 2)

Conclusions

At the beginning of this paper I proposed to answer two questions:

1. Why in the American case the Article 5 was triggered and in the Estonian case not?

2. What were the consequences of these two events on NATO, especially after the 2007 cyber-attack?

The analysis was conducted from the NATO perspective and the impact of non-traditional threats on the Alliance. Applying a comparative method I succeeded to answer both question during my analysis. For the first question I identified the nature of the means involved in the attack, and I concluded that in both cases non-conventional means were used. This was one of the

similarities of the two cases. But the answer to the question *Why in the American case the Article 5 was triggered and in the Estonian case not?* relies on the differences between the 9/11 attack and the cyber-attack upon Estonia. It can be said that for the events of 9/11 the Article 5 was triggered because the legal framework developed until that moment was encompassing a terrorist attack. In the Estonian case, even if the attack affected the entire electronic infrastructure of the country, the Article 5 could not be triggered due to the fact that no specifications were made up until that point in the official documents of the Alliance. Thus, the main argument in applying the collective defense principle was not the nature of the conflict, but the possibility to justify the actions at the level of NATO.

The answer to the second question is closely linked to the answer to the first question. On the one hand, in the 9/11 case there was a clear military action taken by NATO and its involvement in the anti-terrorist missions, both the actors involved and their location being known. On the other hand, the cyber-attack upon Estonia was not followed by such clear and decisive actions, the entire situation being surrounded by uncertainty. Nevertheless, both events had major impact on NATO. In the 9/11 case we have the first NATO out-of-area mission. In the Estonian case we witnessed a totally different approach of the cyberspace and the cyber defense, the main change being the inclusion of the cyberspace on the list of those which has to be defended alongside sea, land and air.

The 9/11 events can be viewed as a turning point in the policy of NATO if we take into consideration the actions that followed and the declared position of NATO in fighting terrorism. At the same time, the cyber-attack against Estonia is a turning point in the policies of NATO regarding the digital space. The fact that until 2007 very little progress was made at the level of the Alliance in order to tackle the cyber issue, and after the events of the year major changes have occurred, represents an argument in the sense that the cyber-attacks upon Estonia generated the entire flow of improvements at the NATO level.

References:

1. "Bi-sic input to a new NATO capstone concept for the military contribution to countering hybrid threats," 2010, accessible on-line on http://www.act.nato.int/the-countering-hybrid-threats-concept-development-experiment

2. CCD COE, "About Cyber Defense Center", accessible on-line on https://ccdcoe.org/aboutus.html.

3. NATO, „NATO Cyber Defense", accessible on-line on http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet- cyberdefence-eng.pdf.

4. NATO, "The North Atlantic Treaty (1949)", accessible on-line on http://www.nato.int/nato_static/assets/pdf/stock_publications/20120822_nato_treaty_en_light_20 09.pdf.

5. NATO, "The Alliance's Strategic Concept", accessible on-line on http://www.nato.int/cps/on/natohq/official_texts_27433.htm.

6. NATO, "Statement by the North Atlantic Council", accessible on-line on http://www.nato.int/docu/pr/2001/p01- 124e.htm.

7. NATO, "NATO opens new center of excellence on cyber defense", 2008, accessible on-line on http://www.nato.int/docu/update/2008/05-may/e0514a.html

8. NATO, "Warsaw Summit Communique", 2016, accessible on-line on http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

9. NATO, "Strategic Concept for the Defense and Security of the Members of The North Atlantic Treaty Organization", 2010, accessible on-line on http://www.nato.int/lisbon2010/strategic-concept-2010- eng.pdf.

10. NATO, "Bucharest Summit Declaration", 2008, accessible on-line on http://www.nato.int/cps/in/natohq/official_texts_8443.htm.

11. NATO, "ISAF mission in Afghanistan (2001-2014)", accessible on-line on http://www.nato.int/cps/eu/natohq/topics_69366.htm.

12. NATO, "Collective defense – Article 5" accessible on-line on http://www.nato.int/cps/cn/natohq/topics_110496.htm#.

13. "The 9/11 terrorist attacks", accessible on-line on http://www.bbc.co.uk/history/events/the_september_11th_terrorist_attacks

14. "Wartime", *The 9/11 Commission Report*, p. 330, accessible on-line on https://911commission.gov/report/911Report.pdf.

15. Buzan, Barry, (2014), *People, states and fear*, Cartier, Chișinău.

16. Ciolan, Ionela, "Defining cyber security as the security issue of the twenty first century. A constructivist approach" in The Public Administration and Social Policies Review, Vol. VI, 1(12), 2014, accessible on-line on http://revad.uvvg.ro/files/nr12/8.Ionela_Ciolan.pdf

17. Ducaru, Sorin, (2016), „The Cyber Dimension of Modern Hybrid Warfare and its Relevance for NATO", in *Europolity – Continuity and Change in European Governance*, Vol. 10, No. 1.

18. Hoffman, G. Frank, (2009), „Hybrid warfare and challenges", JFQ, Issue 52, 1st quarter.

19. Hoffman, G. Frank, „Hybrid vs compound war", (October 2009*), Armed Forces Journal – Military Strategy, Global Defense Strategy*.

20. Hunter Eve, Pernik, Piret, (2015), "Military Balance 2015, International Institute of Strategic Studies", in *Challenges of Hybrid Warfare*, *International Center for Defense and Security*.

21. Jitka Richterová, (2015), *NATO – Hybrid threats*, Prague, accessible on-line on https://www.amo.cz/wp- content/uploads/2016/01/PSS-Hybrid-Threats-NATO.pdf

22. Laasame, Häly, (2011), "Estonia: Cyber Window into the Future of NATO", *Joint Forces Quarterly*, Issue 63, 4th Quarter, pp. 58-63.

23. Plumer, Brad, (2013), "Nine facts about terrorism in the United States since 9/11", *Huffingtn Post*, accessible on-line on https://www.washingtonpost.com/news/wonk/wp/2013/09/11/nine-facts-about-terrorism-in-911/?utm_term=.ef807ae0f78fhttps://www.washingtonpost.com/news/wonk/wp/2013/09/11/nine-facts-about-terrorism-in-the-united-states-since-911/?utm_term=.ef807ae0f78f

24. Purton, Simon, (2015), "Future Capabilities, Research and Technology, Allied Command Transformation, NATO: "Why half of winning an Irregular War is agreeing on what it is…" in *Background Raport* – "NATO hybrid threats", Prague, accessible on-line on https://www.amo.cz/wp- content/uploads/2016/01/PSS-Hybrid-Threats-NATO.pdf