

ISSN: 2450-6869

eISSN: 2719-6763

No. 11, 2021

DEFENCE SCIENCE REVIEW


<http://www.journalssystem.com/pno/>

DOI: 10.37055/pno/148424

Attributes of cyber conflict in the context of armed conflict – an outline of the problem.

Original article

Monika Szyłkowska^{1,A}

ORCID  0000-0003-3153-610X

Received: 2022-03-21

Revised: 2022-04-12

Accepted: 2022-04-12

Final review: 2022-04-12

¹ Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego w Warszawie

A – Research concept and design, B – Collection and/or assembly of data, C – Data analysis and interpretation, D – Writing the article, E – Critical revision of the article, F – Final approval of article

Abstract

Peer review:

Double blind

Keywords:

cyberconflict, armed conflict, digital war

Objectives: This article explains the concepts of cyber conflict attributes in relation to the classical attributes of armed conflicts. Problems related to the study of the causes of armed conflicts and wars, forms of their conduct, ending and ways of their resolution. This paper outlines selected definitions of conflict and war that have formed the basis of analysis for the attributes of cyber conflict - in particular the attributes of: nature, forms, sources, complexity, and the difficulty of uniquely identifying the "aggressor" if the attack is not "overt".

Methods: Statistical analysis, document analysis.

Results: The characteristics of a cyber conflict are, in particular: no certain identification of the aggressor, no possibility of an official declaration of war or official defense and retaliation.

Conclusions: The key determinant of defense – should be digital and electromagnetic offensive measures. Security threats and more frequent attacks in broadly defined cyberspace have unquestionably become the challenge of today's world – consisting of alliances, which the sum of security being the security levels of individual members and their defense capabilities. However only the level of commitment and cooperation can contribute to the achievement of a common goal, defined by the Alliance – including, above all, the elaboration of common, acceptable by all members – „modern” solutions. However, the common defense and deterrence potential equipped with real, though digital, both offensive and defensive resources would allow practical implementation of the challenge for art.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License

1. Concept of war and armed conflicts

In the literature on the subject, both the concept of war and armed conflicts is defined heterogeneously and interpreted in the same way. The word conflict comes from the Latin *conflictus* – a collision, however, for objective reasons – the original meaning has significantly expanded. The broadest and most general meaning is given in the *Universal Encyclopaedia*, which recognizes conflict as every kind of conflict of interests, a dispute, antagonism (*PWN Encyclopaedia*). According to T. Kęsoń: the analysis of the definitions of conflict adopted for scientific reflection reveals the scope, complexity and depth of problems that their creators had to face³⁵. In the literature on the subject, the definitions of war were determined by various criteria – the historical period, in which the following were created: Sun Tzu (600 BCE) in the “*Art. Of War*” treatise wrote: “War is a matter of the highest importance for the state, a matter of life and death, a path leading to survival or decline. Therefore, serious studies should be conducted on it. Everything is better than war, (...) every evil, even the worst, is better than the highest evil, and war is the greatest evil” (Sun Tzu). Cicero recognized war as: “dispute resolution by force”. For Carl von Clausewitz, “war is not only a political act, but a real tool of politics, a continuation of political relations, conducting them with other means. (...) Violence is armed with inventions of art and science to face violence. Slight, only worthy mentions of restriction, which are imposed on itself under the name of international laws, accompany it without actually weakening its strength (Clausewitz). In other sources, the war is defined as, among others: “a social phenomenon which dominant feature is the armed struggle between states, nations or social groups” (*Lexicon, PWN, 1972*), but also “a structured exercise of violence for individual political goals. When the leader of the state clarifies his national goals, the commander begins to outline his action plans” (*Britannica Encyclopaedia, 1978*).

On the basis of international law (Cesarz, 1993) the state of war does not necessarily mean conducting (commencing) the armed struggle, although in the strict legal sense, the scope of the war includes all manifestations of the armed struggle. Similarly – as in the case of the definition of armed conflict – it can also be run by parties that are not internationally recognized entities, and can take place, although military operations have not been officially declared. The moment of breaking the peace relations and the transition to war relations is recognized as the moment of commencing war.

Also the end of military activities is not synonymous with the end of the war.

The most common criteria referred to as “basic” include:

- the criterion of entities – conflicts between states,
- the criterion of will – in the form of recognizing the resulting dispute over the war by at least one of the states,
- the subject criterion – conflict with the armed forces of both parties,
- the goal criterion – the purpose of the war, which is to defeat the opponent and force him to accept the demands and conditions of the other party.

2. Definitions of wars

It is worth noting that among the various definitions of wars (Western studies), three of them have found a specific application, namely:

1. Practical approach to the definition of war used by the Stockholm Peace Research Institute (SIPRI) uses this concept to define a larger armed conflict, in which military units subordinate to two or more governments, or one government and at least one organized or armed organization, fight for a longer period of time¹.
2. Definition of war developed by the contemporary history professor at the Budapest University, Istvan Kende, according to which war is an armed conflict characterised by three features:
 - a. the armed forces of one or more parties take part in the fighting (at least in one case regular army, government army or police),
 - b. the fighting parties are organized according to a certain pattern and there is an organized structure of the military operations carried out,
 - c. activities of the parties involved in the conflict are conducted according to the adopted strategy².
4. The works containing discursive analyses (Cesarz, 1993) of the phenomenon of war and armed conflicts, the polemological approach is used³. “According to polemologists, the word: polemos {war} means a relatively strict and easily identifiable phenomenon, in contrast to the word {peace} implying a kind of ideal which requirements are undefined: (...) War destroys, mutatis mutandis – always the

¹ SIPRI also qualifies a given conflict as a war if at least 1000 people were killed because of it. This definition is so general that it allows to classify ongoing armed conflicts without much difficulties.

² Such a criterion for classifying conflicts was used in the works by, among others, K. Gantzel, J. Meyer-Stamer, B. Moser, A. Charisius, R. von Dingemann.

³ Polemos – (Greek) war, conflict. Polemology – a field of science dealing with the scientific study of war. Created by the French philosopher, sociologist and lawyer, Gaston Bouthoul. The aim of the field of polemology is to analyse the conflicts of the past and present, to determine their nature, periodicity, intensity, duration,

same. Regardless of its sociological, ethnic, technical, political, economic and ideological context, it consists in the accelerated destruction of human life and material goods (...)”(Gałganek, 1986). Polemology is trying to answer the question: Why do societies at the specific moment of their history take up war activities? According to polemologists, war is the most controversial phenomenon of all social phenomena, but above all it is a destructive phenomenon. As a result of the war, civilizations fall down, and at the same time “the transition from one period in the history of nations to another is the result of extensive changes, which are almost always caused by war” (Gałganek, 1986). The contemporary concept of armed conflict – for objective reasons has changed both in the context of historical events, when the world changed its layout from bipolar – and with it the number of wars in the classical sense has decreased – as well as due to the technical and technological revolution. From an international point of view, the division of armed conflicts proceeds according to the criterion of their extent and impact on the international situation. The international dispute is characterized, above all, by the fact that it may potentially be one of the sources of armed conflict, but its regulation is usually carried out using legal means. To simplify matters, one can distinguish armed conflicts of the following nature (Balcerowicz, 2002):

- global, the participants of which are the largest states (superpowers), causing tension on a global scale,
- regional – participants are the largest countries in the region using significant armed forces, which results in generating tension of great strategic importance,
- local – small and poorly armed forces of states with little international significance are involved, which in effect does not cause major international effects.

There is no doubt that the boundaries between the different types of armed conflicts are fluid, because it is not difficult to imagine a situation when the internal conflict – as a result of intervention – will turn into external one or, for example, supplies of arms from outside, will make it become international in nature⁴. In the literature on the subject, different proposals of models and patterns of conflicts can be found, but among them the model of cyclic intensity levels prevails – i.e. increasing from the (relative) stabilization and peace to crisis and war,

forms, typology, the involvement of external forces and the reactions of the international community. The discourse of war and peace is the research tool in polemology.

⁴ Likewise, a local conflict may – at the time when favourable circumstances arise - turn into a regional or even a global conflict. In such cases, we talk about the phenomenon of internationalization of internal conflicts. This liquidity is mainly due to the dynamics of contemporary armed conflicts

and after this period again reducing the intensity to relative peace. Most scientists also agree that these cycles are repeated (other models distinguish escalation and de-escalation – then the conflict model takes the shape of the letter U or the reversed letter U).

3. The classical conflict typology

The classical conflict typology distinguishes:

- war,
- armed intervention,
- armed incident,
- military coup,
- armed blockade,
- demonstration of power.

In turn, the basic attributes of conflicts include:

- the nature of the entities and the environment in which they occur,
- space and ways of conducting war in it,
- concepts of conducting conflict and war expressed in strategies
- and doctrines,
- the laws of war.

The essential properties of the conflict are the existence of at least two parties, behaviors aimed at destroying or at least controlling the other party (whose effects are the profit of one party at the expense of the loss of the other party), the opposing action of the parties to the conflict (Mucha, 1978). At this point, one more category of conflict should be added, which currently includes terrorism. The following division of terrorism can be found in the literature on the subject:

- organized terrorism – conducted by states and social groups to intimidate and subordinate their interests – is a carefully thought-out policy tool considered as the cheapest and potentially most effective means leading to the goal,
- unorganized terrorism – chaotic, run by small but very active groups or units of an ad hoc nature, formed to perform a specific task (usually associated with professed values, ideology, etc.).

Summing up the deliberations on the definition of conflicts and wars, it is worth bearing in mind that – depending on the field of science – each of them will create its own conflict definitions (narrower or broader), which will best characterize this phenomenon for the needs of a given area and reference point, i.e.: purpose, type, kind, form, place or scale, and the level

of contradiction – including how to defend an own interests. The global political and economic system encompassing all political, economic, social, cultural, religious and social events – by its nature also contains a system of interrelationships between its entities, which is also often expressed in various (opposing) aspirations, ambitions and objectives of these entities. In such a conglomerate it is extremely difficult to achieve a balance at a satisfactory level for all parties (states, international organizations, etc.).

4. Cyberattacks attributes

In the outline of selected definitions of conflicts and wars presented above - cyberattacks occupy a special place. This is mainly due to their attributes in the form of: their nature, forms, sources, level of complexity and difficulties in uniquely identifying the “aggressor” if the attack is not “open”.

Cyberattack can determine the use of IT tools and means (computers, systems and ICT networks and other means of storing or transferring data and information), the purpose of which are devices, systems and ICT networks. The attack of this type will be, for example, hacking into systems and computer networks through software or hardware to destroy them, prevent the operation, modification or manipulation of data, information, system or network functionality in whole or in part. The attack also includes physical destruction of components caused by manipulation or modification of software (Doctrine of Information Operations SZ RP). The targets and methods of attacks may be different, and also the strategic goals of their conduct may be different: from propaganda, through the attempt of causing panic – to permanent damage or destruction of key infrastructure elements (power plants, transport network, communication systems, etc.). However, attacks of this kind can also serve as sources of information, dissemination of disinformation or technological intelligence. Regardless of motives and willingness to achieve the intended goal – each of the conducted cyberattacks will be a key element of cyber conflict of cyber war – depending on the adopted point of reference and definition, because the very essence of cyberattack assumes the purposeful use of a properly programmed tool or a whole range of tools (breaking security, data modification, data theft, destruction or taking control of the system) for a specific purpose. The key feature of cyberattacks is the unique difficulty in detecting their initiators (and perpetrators), which results from the possibility of programming cyber-bugs so that it not only blurs traces, but also leads to the wrong sources. Specific examples show the actions that contributed to the realization of the concept of cyberwar - through attempts to destabilize IT systems of high complexity: in 2003, IT systems in the USA were attacked by hackers from

Russia and China (the so-called Titan Rain and Moonlight Maze); in June 2010 a bug called Stuxnet was detected, which aim was to spy and reprogram industrial installations and the Flame virus⁵, in May 2007 a cybernetic attack on Estonia took place (hackers attacked the Estonian parliament, government agencies, banks and the media); in 2007–2008 (most probably) Chinese hackers interfered four times with the US government satellites via a ground station in Norway (interference from outside into the Landsat-7 observation satellite for a total of 12 minutes, and the Terra AM-1 satellite for two minutes in June 2008 and 9 minutes in October 2008). Cyberattacks – according to classically conceived concepts – will be primarily asymmetric attacks – both in military and nonmilitary terms⁶. In asymmetry, cyber conflict attributes will be identical to asymmetric wars, whose characteristics are: secretiveness, variability, surprise and unlimited range. An additional obstacle is the globalization of the modern world: all the conveniences of modern technology and techniques are a hindrance in such cases. T. Szubrycht, paraphrasing the words of H. Kissinger, aptly described the nature and essence of today's asymmetric conflicts: the contemporary asymmetric opponent wins if he does not lose, and the international community loses if it does not win⁷.

Asymmetrical threats – as a rule – are characterized by behaviour different from the opponent's behaviour and action – a characteristic and essence at the same time – is the difficulty of identification mentioned earlier. It is also worth paying attention to yet another aspect of cyberattacks - namely the concept of balance of power and the impact it will have on international relations in the future. In the shortest terms, the balance of power is defined as the pursuit of states to maximize their own power, or balancing the growing power of other states. In the (already historical) Cold War period, the spiral of arms has, paradoxically, led to the balance by reaching a climax – global awareness and total destruction. In the case of cyber threats, it will be difficult to achieve this kind of balance: for now it is difficult to imagine a situation in which states will overtly outdo each other in the production of computer viruses capable of destroying the military or economic potential of the opponent. However, this is possible in the case where the first such situation becomes the point of inflammation, with an

⁵ The Flame program was recognized a definition of cyber war and a synonym for cyber-espionage. Its work consisted in the fact that after infecting the system, it started a lot of complex operations, which included primarily eavesdropping of network traffic, capturing characters entered from the keyboard, taking screenshots, recording audio conversations – after which all the acquired data was available for its operations via the link to the Flame control servers.

⁶ Symmetry concerns – besides the inequality of opponents in terms of potentials (economic, military) – also the legitimacy of the form of their formal and legal status in the area of international regulations).

explicit admission of one country to carry out an effective attack in cyberspace – which would basically deny its essence, however it is not excluded as a source of the opponent's provocation to initiate military retaliation. However, with the concept of balance of power, one more thing has to be kept in mind – a paradox. James J. Writz claims that it occurs when the weaker countries instead of trying to balance the powers with balancing measures will seek a strategy that will otherwise weaken the existing disproportions, for example, through an asymmetrical strategy. The first application that comes to mind is the information technology. Such actions obviously provoke the dominant states to counteract to eliminate or balance the existing or potential threats. However, with the balance of power assumed in this way – treating it as providing security and protection against the outbreak of war is unfounded. In the context of asymmetric attacks it is assuming that strategies of the future should be strategy by startling the opponent along with the awareness of readiness to use a wide arsenal of strengths and resources. Asymmetrical threats are difficult to identify and neutralize – all the more that not all are driven by rational premises, and classic answers are usually ineffective (as demonstrated by the example of the war on terrorism). As a consequence, these actions led to the increase of the global threat, instead of its minimization, and the power is not so much deterring as provoking, thus becoming its paradox. The attributes of cyberconflicts fit in smoothly with their classic counterparts in the whole complexity of the above considerations. This is best demonstrated by the conclusions of a report by a group of experts and security lawyers from the US Cybernetic Command and the International Committee of the Red Cross called the so-called “Tallinn manual”⁷. Its authors stated that the cyberattack may turn into a conventional war, at the same time starting from the assumption that nowadays the understanding of concepts such as “armed conflict” or “war” is extended, because the ICT attack, leading to physical damages, differs from classical methods of conducting a war only with form, and not the results. Therefore, after analysing the resolutions of the UN Security Council and other international law acts, they concluded that the countries attacked in the event of a breach of their national security have the right to legally use force in self-defence against persons who supported states in launching an ICT attack on the NATO members⁸. However, it was emphasized that the use of force could only

⁷ Ultimately, it may be the beginning of the doctrine of the application of international law to military operations in cyberspace. Polish Institute of International Affairs, NATO 2020 Assured security. Dynamic involvement (“Albright report”). Source: <http://www.pism.pl/zalaczniki>

⁸ This applies to direct assistance, for example, informing the third country about gaps in the system, support for a specific action, creating software that, with its knowledge and in accordance with its intentions, will be used to attack.

occur in specific situations: the attack on critical infrastructure and only if there were victims (wounded and killed) – a combined premise – or high risk that they will occur.

Then it will be a “hostile act” (armed conflict or war) because there is no difference between a virtual and a physical attack if the consequences of both are identical. In practice, this means that hostile activities in the form of, for example, disinformation or breach, as well as activities that result in the paralysis of websites or theft of data – do not qualify for a forced response. According to the provisions of the Geneva Conventions – cyberattacks conducted or supported by states should not be directed against a civilian strategic infrastructure, such as hospitals or nuclear power plants. According to the adopted rule, even if the cyberattack is carried out from the state network, it is not a sufficient proof to recognize that the state is responsible for a specific action. It should be emphasized that the report called the “Tallinn manual” is not an official NATO document, only a report of independent experts, which was not recognized as a doctrine but rather a voice in the discussion that is just beginning. This is due to objective reasons: it is still not known how to locate ICT “enemies”, which makes it impossible to identify the entity responsible for the attack. Also, no recommendations have yet been developed as to what proportional physical force should be used in the event of detection and identification of a perpetrator (Czulda, 2018). As part of the deliberations on the attributes of cyberconflicts, which arsenal is a broadly understood cyber-weapon – it is worth pointing to another issue: the possibility of military use of cyberattacks as one of the types of weapons that is currently no longer a futuristic concept detached from reality. On the other hand, it is not difficult to imagine a situation in which the cyberattack becomes the beginning of a conflict (constituting the above-mentioned element of provocation). The dynamics of the changing global world – including also in the area of armaments industry orders to ask the question not “whether” this type of weapon will be used, but “when”? In the context of armed conflict, cyberattacks still occupy a theoretical position, however, it is not difficult to get the impression that it is only a matter of time when the theatre of actions will change its plane to a virtual one with very real effect in non-virtual reality. The reality and the rank of cyber threats are best demonstrated by the fact that the American military doctrine includes the possibility of using conventional means of defence (e.g. missiles) in response to cyberattacks on military or governmental facilities, and the fact that in the next few years, the USA intends to increase the number of their defence forces several times against cyberattacks (CYBERCOM – the command of the US armed forces dealing exclusively with the ICT security of the country is expected to each approx. 4000 people, and it is to create three additional operational cells: two defensive ones – for the tasks of protecting IT networks and ensuring the security of critical

infrastructure and the third one being offensive – to attack on foreign networks and their penetration in order to obtain information (the so-called IT triad). Cybernetic war viruses – until recently recognized as the weapons of the future – are increasingly used as an element of activities such as recognition or disinformation. On the one hand, cybernetic weapons will be more and more complex, refined and invisible – on the other, they will exert the most real effects: Consequences of cybernetic war in which governments are involved can be appalling (...) Software similar in its operation to Flame is getting cheaper in production – thousand times cheaper than a traditional arsenal, but its effects may be just as real and destructive – it can attack energy networks, infrastructure, financial institutions – and destroy them effectively (<https://www.nytimes.com/2017/09/13/us/politics/kaspersky-lab-antivirus-federal-government.html?searchResultPosition=1>). An attempt to traditional approach to cyberconflicts as armed conflicts (e.g. the recognition of hostile activities in cyberspace as a possible reason for declaring war) shows, on the one hand, the seriousness with which cyberthreats are treated by states, on the other, it shows some kind of misunderstanding of their scattered (<http://www.cs.put.poznan.pl/>) and asymmetrical nature, which not only makes it difficult, but may even make it impossible to identify aggressors. One can imagine a situation when the cyberattack will be carried out in such a way as to confuse the identification of its source and direct the suspicion to another country as an aggressor. According to experts, such spectacular cyber operations as Stuxnet⁹ and Flame are – and will rather be in the near future – a deviation from the norm, and not the norm, which is due to their nature: cyberwar will prefer anonymity rather than publicity. However, the use of combat methods in cyberspace is the most real and – every day it becomes more serious, which is confirmed by, among others, the fact of introducing the provisions concerning offensive, digital defense measures into the legal regulations or doctrines. Currently, the cyberwar can still be seen as an extension of traditional actions (espionage or sabotage) – their instrument, but not an agent in itself. However, it is hard to resist the impression that the proverbial “matter of time” is not as distant as it may seem. However, the attitude, i.e. the IT security will remain the key (in offices, ministries, armed forces), in line with the principle that every closed network is as secure as its weakest link.

⁹ Stuxnet virus changed the operating speed of the centrifuges in such a way that its operation would remain unnoticed for many months.

There is no doubt that cyberspace is a new security environment, and the effectiveness of its protection requires and depends on the involvement of the widest possible group of users of the global network. According to K. Liderman, it should not be forgotten that: “although the threats in cyberspace constitute a different category of legislative and organizational challenges, the problems they create largely resemble those generated by other asymmetrical threats, such as terrorism”(Grzelak, Liedel, 2018). A common feature of this kind of threats is “forcing state structures to evolve towards less hierarchical and more flexible solutions”(Ibid.), because today network is one of the most important concepts of the new security paradigm at all levels. According to experts, in the future, wars will take place mainly in cyberspace. The global network will become an arena of struggles in which rapid reactions will play a key role. According to Prof. Brzeziński, states are increasingly making implicit acts of violence without a formal declaration of war, giving, among others, hacker attacks on foreign institutions and private companies, spreading computer viruses, or commissioning secret attacks on foreign leaders and scientists involved in research into the development of weapons as examples. In addition, some countries are currently developing methods of attack in cyberspace, which are able to paralyse the “socio-economic system and the most important institutions of the attacked state” and thus “contribute to the prevention of disaster on an unprecedented scale”. The conclusion of this observation is that the governments of technologically advanced states should establish rules that will help prevent the tendency to carry out non-public acts of aggression.

It is no longer a secret or a new discovery that the war in cyberspace continues – it has various sources, surfaces, forms and methods of fight. And although it defies the classic concepts with which war is identified – its effects can be seen in practically every sphere. However, its attributes will remain unchanged.

4. NATO Strategic Concept

The best example of emanation tackle common challenges at the international level has become records of cybersecurity in the new NATO Strategic Concept of November 2010. In June of 2011 NATO defense ministers adopted a document: NATO`s policy in the area of cyber defense (The NATO Policy on Cyber Defence) and action plan (The Cyber Defense Action Plan). First of those documents was the first in the history of the Alliance developed by defining a formal policy, which was adopted in January 2008, and established the three main pillars of the Alliance in cyberspace. These pillars are: subsidiarity, avoiding duplication and security. Subsidiarity means that the necessary support is provided only upon request,

while in other cases the principle of self-responsibility of a sovereign state. Avoiding duplication – means avoiding unnecessary duplication of structures or capabilities – at international, regional and national levels. Security – this area of cooperation based on trust, taking into account the sensitivity of the information system, which must be available, as well as their potential vulnerability. Pillars are derived from the broader context of the concept – in terms of synthetic basic tasks of the Alliance – include: collective defense; crisis management, and undertaking actions for international stability. Confirmed in this respect, especially the wording of Article binding 5, which states: “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 (,,) (Article 5 of North Atlantic Treaty) ”. Allies have committed to take in such a situation, individually and collectively, “such action as it deemed necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area”(Article 5 of North Atlantic Treaty). In practice this means that the legal commitment to collective self-defense under Article 51 of the Charter of the United Nations. Article 5 is a legal instrument designed to provide:

- a. the effective protection of the country against the threat of military aggression in the form or attack, the consequences of which are comparable to an armed attack (e.g. a cyberattack);
- b. attack protection, which would constitute an existential threat to the existence of a sovereign state and its territorial integrity.

Article 5 effectiveness is based on four fundamental principles:

1. Inevitability (assist for the victim of aggression).
2. Automatism (assist for the victim of aggression or threatened by such aggression).
3. Priority access to NATO resources in case of attack.
4. Adequacy of actions and measures that will be able to effectively prevent and alleviate aggression and neutralize its effects.

Conceptually, the new perception of system collective security is – in principle – to neutralize a potential assault one of the Member States of the system, while being a defensive alliance is to ensure the safety and protection of the state against attack from outside.

NATO fulfills the fundamental objectives and core functions in the defense dimension:

- protection of members (security guarantees);
- deterring a potential aggressor (mainly nuclear deterrence);
- the ability to intervene, especially in the area of terrorist threats (expeditionary missions) and

- preventive and stabilizing function on a global scale.

There is no doubt that in the era of globalization, the idea that organizes a system of international security is the interdependence of countries – different sizes, with different structures and systems of governance. Madeleine Albright concluded: Combination of internal security and dynamic engagement outside of borders is the cornerstone of NATO in the coming decades (Rotfeld, 2010).

Nowadays, the security of the Member States – and thus the entire Alliance – may be affected by less conventional (and asymmetric) threats, which include i.e.: bombings, attacks with weapons of mass destruction and attempts to destabilize society with cyberattacks or contradictory the law disruption major transport routes. In order to defend against these threats, which may, but need not – exhaust the significant of the attack within the meaning of Article 5 – NATO had to revise and update the approach to the defense of allied territory. According to the new and updated Strategic Concept of NATO Policy in the field of cyber defense, cyber threats is defined as a potential reason to take collective defense in accordance with Article 5 of the Treaty. Furthermore, both the Policy and Action Plan NATO countries provide clear guidance to the agreed list of priorities for improving the Alliance's cyber defense – including strengthening coordination within NATO and with its partners. In the so-called. Mrs. Albright report stated, that the Alliance should intensify efforts, able to respond to cyberattacks: both by protecting its own communications and command systems, developing the ability to defend against cyberattacks, (to ensure their efficient detection), as well as providing allies to help prevent attacks and removing their effects. Due to the fact that the international security environment will change in both predictable and unpredictable way today – a vision of NATO in 2020, provides for the need to ensure the safety of all members and dynamic engagement beyond the treaty area to minimize threats. The dynamism of globalization and technological development and modern technology makes that there is a sudden and uneven growth of the international flow of information, goods, services, people, technology, ideas, habits, but also crime (including weapons). NATO experts predict that the deepening global interdependence strengthen ties, but not necessarily induce the public to peaceful coexistence. The reason is the emerging disproportions: strengthening the position of some actors while marginalizing others. From a security standpoint, this means that incident in one part of the world can interact in other regions (e.g. the state of chaos and anarchy engulfed can become a place of terrorists) – which, unfortunately, already confirmed by real examples from the region of the Middle East. Referring directly to asymmetric digital threats, it should be emphasized that the destabilizing chaos caused by the cyber-attack of one city

may inspire others to similar actions in elsewhere. Report confirmed that it is impossible to predict “how technology will change the battlefield due to breakthroughs in scientific research, but now should be closely monitored for potentially harmful changes in such rapidly developing fields of information and communication technologies, cognitive and biological sciences, robotics and nanotechnology. The most destructive periods of history are usually those in which the offensive measures have achieved superiority in the art of war” (Rotfeld, 2010).

5. Prediction of threat

The most likely threats in the near future included the unconventional nature, in particular:

1. international terrorist groups attacks,
 2. attacks with ballistic missiles (e.g. with a nuclear warhead),
 3. cyber-attacks,
 4. disruption of supply lines,
 5. the financial crisis (also caused by the destabilization of a cyberattack).
- Anticipated threats have a direct impact on the way of development and preparing concrete actions of NATO - including to define the key concepts of: security, attack in the context of Art. 5 of the Treaty; or adapting the strategy of deterrence.

The recommendations of the Group of Experts of NATO stated: “NATO, the EU and other entities should provide capabilities that will provide the greatest possible added value for the proper solution, so that NATO should strive agreement with the leaders of the EU with regard to plan regular joint participation in meetings, full communication between military staffs and enhanced coordination of crisis management, risk assessments and sharing of resources” (Rotfeld, 2010).

The partnership with the United Nations was also found as a fundamental in order to „unite efforts for collective defense and ensure peace and security” (Rotfeld, 2010). The role of NATO is to be continued as it did before – to support the United Nations in strengthening its ability to carry out the mission entrusted by the international community – in particular through operational support and security.

In the area of cyber defense capabilities considered as necessary:

- developing the capacity of all allies including early warning through the development of sensor networks to monitor the functioning of the IT infrastructure throughout the

area, – Preparation of a rapid response group of experts who will be able to be sent to the member state threatened or affected by a major cyberattack,

- developing a set of capabilities to defend against cyberattacks fully corresponding to their potential range, containing active and passive components.

Should be emphasized that classical doctrine of war cannot be easily translated into cyberwar. The main priority is to develop an international definition of cyberwar and identify what is effective cyber-defense, and how adequate response to the attack. In conventional military operations were certain rules of behavior that are not in cyberspace¹⁰.

Under the current NATO policy in the ICT dimension – it focuses primarily on defending and supporting Member States in helping countries to develop national capacity building interoperability and cyber defense, for which they are responsible under the protection of national infrastructure. That serve the objectives of such institutions as: CDMB or agency of the NATO Communications and Information Agency, NCI. In March 2013 there was established a project to develop multinational capabilities to cyber-defense (Multinational Cyber Defence Capability Development Project, MCDCDP). For significant reform was considered to develop a specific decision-making process in the event of an attack on telecommunication networks: in particular situations the North Atlantic Council, NATO could invoke Article 5 of the Treaty. The current strategy focuses primarily on the element of deterrence and defense – but the response to threats ICT is not only defense but also attack – therefore, hence heard more and more about the construction of offensive measures: cyber equivalents an element of a strategy of deterrence and „certain destruction”.

6. Conclusions - response for cyber-attack

According to unconfirmed official information – NATO has „the means to answer in the case of a cyberattack, „allowing the” overwhelming response”(scale compared to nuclear attack). However, each Member State has a different regulations, procedures, doctrines and strategies in cyberspace. Taking into account the different interests of these countries and different perspective perception of risks, agreeing on a common position on the conduct cyber offensive would be extremely difficult. in addition, still have not defined precisely the relationship between Article 5 and the activities in cyberspace. This issue will very likely be part of the action national instruments, and not centralized NATO (Multinational Cyber Defence Capability Development Project, MCDCDP) forum. In additional: „The greatest danger does not relate to strictly military matters. Cybercrime and cyberespionage allows to

get valuable political and economic information. Unfortunately, there is also a high risk of a terrorist cyberattack. Terrorist groups are increasingly shifting their activities (communication, propaganda, recruitment) to the network. Even if they lack the capacity for offensive action, it can always hire a specialist to criminals act” (Multinational Cyber Defence Capability Development Project, MCDCDP). The new concept of the Alliance recognizes the changes in the security sphere – including in particular identified new types of threats arising outside the NATO Treaty (unconventional and asymmetric). Both the new threats, as well as how to create a security environment – are and will be increasingly determined by the development of new technologies. Regardless of global change and new challenges most important is the acknowledgment of the Strategy, the territorial defense and solidarity allies in the event of an attack is a fundamental task in accordance with Article 5 of the Washington Treaty, which means the immutability of NATO

bases in this area. It should be recognized that although theoretically there would be a possibility in accordance with Art. 5. North Atlantic Treaty – however, given the complex nature of cyberattacks, including in particular the huge problem of determining the „aggressor” – at the moment it seems unlikely. This situation, however, does not interfere with taking actions aimed at sanctioning modern (new) forms of attack – especially for preventive purposes. It seems unlikely that an aggressor will be revealed in the case of cyberattacks. This is due to a simple reason – the essence of this type of attack lies precisely in the possibility of blurring the traces of its source. Time, and above all the practice and the latest technique will show whether there will be the possibility of unambiguous and unmistakable indication of the source. It would be highly advisable that by that time there would be some legal formulas regulating the possibility of responding to an attack in cyberspace. The thesis that it can be applied the existing rules – with the difference that it should be clearly stressed that the possibility of conventional defense depends on the type of losses caused by this type of attack, and the answer in the classical form would be at least proportional (proportional) – is highly risky. NATO decision-makers lack interpretation when it comes to cyber-matter – state alliance have appropriate operating procedures in the event of a physical attack on their territory, but lacks instruments when it comes to the impact of ICT. Analyzing the „case of Tallinn” group of experts and lawyers from the safety of the US Cyber Command and the International Committee of the Red Cross has prepared report, which estimated that ultimately may be the beginning of the doctrine – the so-called. Tallinn manual on the application of

¹⁰ <http://polska-zbrojna.pl/home/articleinmagazineshow/10171?t=ATAK-W-WIRTUALU>

international law to military action in cyberspace. The group tried to make the interpretation of existing international law through the prism of activities and events in the network. For the purposes of the adopted concept of *ius ad bellum*¹¹ virtual reality has been analyzed several treaties. The authors of „manual” found that cyberattack can turn into a conventional war, starting simultaneously with the assumption that today is the extension of understanding of concepts such as „armed conflict” or „war”, because the attack ICT, leading to physical damage is different from classical methods of warfare, only the form but not the effects. The paper emphasized that their aim was not to answer all the questions, but take a relatively coherent and useful part in the discussion on IT security, threats or methods of defense from the perspective of already existing international law – creating a deeper interpretation. After an analysis it was concluded that the affected countries in the event of a breach of national security have the right to legally use force in self-defense against those who support the state in making IT an attack on NATO members. This also applies to direct assistance – for e.g. inform the third country to gaps in the system, support a specific action or create software that will be used to attack. In those cases, the assisting entity loses the status of a civilian and thus the protection of international law (also apply to civilian networks which can be the target of legal attack if they are used for „military purposes”). According to the interpretation contained in the Tallin`s manual – legitimate target is not the person who wrote the malware, placed it on the Internet which was used in a cyberattack. The document also notes the main limitations: the prohibition of unlimited use of physical force or killing.

The basic method of the response are and will continue to arrest criminals and terrorists operating in cyberspace, and sentencing them by the law. Tallin`s manual recognizes that people consciously supporting ICT attacks are „unlawful belligerent” (e.g. Al-Qaeda in Afghanistan), which means that after detention do not receive the status of a prisoner of war under the Geneva Conventions, so they can be tried as criminals according with the provisions of the national penal codes, and also for those acts that are legal under the law of war if they have been carried out by “lawful belligerent “– means the armed forces participating (involved) in the conflict (III Geneva Convention Relative to The Treatment of Prisoners Of War Of 12 August 1949: http://www.un.org/en/genocideprevention/documents/atrocities-crimes/Doc.32_GC-III-EN.pdf”). It was considered that the use of force can occur only in

¹¹ *Ius ad bellum* (Latin for “right to war”) is a set of criteria that are to be consulted before engaging in war, in order to determine whether entering into war is permissible; that is, whether it is a just war. the right to wage war by the state. Previously the attribute of international legally subjectivity vested in each State, legally allowing to war as a means to resolve the international dispute.

specific situations (combined premises) in the event of an attack on critical infrastructure and only when recorded casualties (dead and wounded) or high risk of that. In that case then it will be a hostile act (armed conflict or war). There is no difference between the virtual and the physical attack, if the consequences of both are identical. In practice, this means that such hostile actions as disinformation, burglary, as well as activities that result in paralysis websites or data theft, do not qualify for force response. This also applies to business intelligence that cannot be treated as aggression. In accordance with the provisions of the Geneva Conventions, cyber-attacks carried out or supported by government should not be directed against civilian strategic infrastructure, such as e.g. hospitals or nuclear power plants (according to this interpretation, the governmental attack of the Stuxnet virus on the Iranian nuclear system should be considered incompatible with international law). According to the adopted rule, even if the cyber-attack is carried out from the state network, it is not constitute sufficient evidence to conclude that the state is responsible for a specific action (e.g.: theft of valuable military and economic information, or sabotage). The “Tallinn manual” is not an official NATO document and is not yet an official doctrine, but it is an important start of the discussion. This is due to objective reasons: there are still no precise guidelines to locate and identify IT intruders or enemies, which makes it impossible to identify certain entities responsible for the attack. Furthermore, no recommendations have yet been made about possibility of use proportional physical force in the event of detection and identification of an assailant (Czulda, 2019). Zbigniew Brzezinski stated that should be created the principles of operation in cyberspace, and the need to establish principles of coexistence – was considered increasingly urgent: “At a time when wars move to cyberspace and acts of aggression are carried out implicitly and anonymously, it is necessary to create a new principles” (<http://article.wn.com> and <https://www.tvo.org/transcript/2104174/zbigniew-brzezinski-the-new-rules-of-cyber-war>): “Advanced methods of use of violence against distant targets, as well as cross-border, state-sponsored terrorism blur the clear boundaries between what is acceptable and what is not. (...) Technological progress has increased the scope of activities that the perpetrators can be difficult to detect and which cannot be stopped in time” (<http://article.wn.com> and <https://www.tvo.org/transcript/2104174/zbigniew-brzezinski-the-new-rules-of-cyber-war>). According to Brzezinski, the states increasingly perform implicit violence without formal declaration of war (<http://article.wn.com> and <https://www.tvo.org/transcript/2104174/zbigniew-brzezinski-the-new-rules-of-cyber-war>). In addition, the governments are developing methods of attack in cyberspace, that are able to paralyze the “socio-economic system and the most important institutions of the attacked

state”, therefore an open debate on new threats to global stability can “contribute to the prevention of disaster on an unprecedented scale.” It is postulated that the governments of technologically advanced countries should establish rules that will prevent the tendency to carry out secret acts of aggression. Summing up considerations should be emphasized as a powerful challenge are cyber-threats for Art. 5 of NATO Treaty. Given their nature and above all, the specificity of the digital arms and deep cyberspace same considerations and precautions have to be the ability of cyber-attack as part of collective defense and force response for this type of attack. That kind of possibility exists under the condition of open (overt) action, and, in essence, attacks of this kind prefer undetectability with hiddenly from the source. Another issue is the provision of assistance. Digital warfare munitions is very expensive in production – analogous to classic - but it gives what is the most important – potential advantage over the foe. For this reason, it is unlikely to become an element that will be subject to “aid transfer” (in accordance with Article 3). In addition, use of this type of digital weapon will make the attacked foe be able to analyze it (source code), refine and use it as part of retaliation. Consideration should be given to the possibility of creating Digital Conventions – and law of cyber-war (*Ius ad digital bellum*). Unspeakable war continues in cyberspace – its sources are different, it is run on different planes, which takes various (digital) forms and (digital) methods of struggle. And although it escapes classic concepts of war – its effects can be seen in practically every – also non-virtual – sphere of life¹². Undoubtedly, the creation of a legal framework would require the development of a common, universal definition – including digital state border – containing both elements of the physical infrastructure and the matter goes spatial elements – including systems, software and networks. The key and fundamental element of protection and defense would be an information, because regardless of the form it adopts (e.g.: graphic, audio) – it is the essence of cyberspace – the source and the potential target of the attack. Therefore, the definition of cyberspace should include this key element – a constitutive determinant of security. Therefore, cyberspace is the communication space created by the system (internal and / or external) – logical and physical network connections. The key element of cyberspace is information: generated, processed, transferred and stored by ICT systems. Protection and defense of cyberspace is the protection of information in this space – regardless of the type of network and the form in which it operates.

¹² *Ius ad bellum* (Latin paraphrase for “right to war”)

Reaction and threatening sanctions will depend – on the type of threat and potential damage to information (eg theft, deformation, damage to the critical infrastructure system). However, a key determinant of defense – should be digital and electromagnetic offensive measures. Security threats and more frequent attacks in broadly defined cyberspace have unquestionably become the challenge of today’s world – consisting of alliances, which the sum of security being the security levels of individual members and their defense capabilities. However only the level of commitment and cooperation can contribute to the achievement of a common goal, defined by the Alliance – including, above all, the elaboration of common, acceptable by all members – „modern” solutions. However, the common defense and deterrence potential equipped with real, though digital, both offensive and defensive resources would allow practical implementation of the challenge for art. 5th North Atlantic Pact in such a strategic way for all areas, which is cyberspace.

References

- Balcerowicz, B. (2002) *Peace and non-peace*. Bellona, p. 160.
- Kęsoń, T. (1999) *Contemporary armed conflicts in the aspect of forecasting military threats of the Republic of Poland – doctoral dissertation*. AON – Warsaw, p. 21.
- Sun Tzu (1994) *The art of war*. Przedświt, p. 7, 13.
- C. von Clausewitz (1958) *About war*. Warsaw, p. 15.
- Cesarz, Z. (1993) *Contemporary political problems in the world*. University of Wrocław, p. 30–31.
- Gałganek, A. (1986) *Polemology – studies on war and peace*. International Affairs, 6, p. 112.
- Rotfeld, D. (2010) *NATO 2020. Zapewnione bezpieczeństwo. Dynamiczne zaangażowanie („Raport Albright”)*. Polski Instytut Spraw Międzynarodowych, Warszawa.

Electronic sources

- Brzeziński, Z. (2013) *The New Rules of Cyber-War. Tvo Today*.
<https://www.tvo.org/transcript/2104174/zbigniew-brzezinski-the-new-rules-of-cyber-war>
- Czulda, R. (2013) *Virtual attack*. Polska-zbrojna.pl. <http://polska-zbrojna.pl/home/articleinmagazineshow/10171?t=ATAK-W-WIRTUALU>.
- III Geneva Convention Relative to The Treatment of Prisoners Of War Of 12 August 1949:
http://www.un.org/en/genocideprevention/documents/atrocities-crimes/Doc.32_GC-III-EN.pdf
- Grzelak, M., Liedel, K. *Security in cyberspace. Threats and challenges for Poland – an outline of the problem*. <http://www.bbn.gov.pl>.
- Rosenberg, M., Nixon, R. (2017) *Kaspersky lab antivirus software is ordered Off U.S. government computers*. <https://www.nytimes.com/2017/09/13/us/politics/kaspersky-lab-antivirus-federal-government.html?searchResultPosition=1>.