2021, Vol. 10, Issue 1

Krzysztof Bobrowski*

PhD seminar participant at Kozminski University

CONVENTIONAL ATTACK VS DIGITAL ATTACK IN THE LIGHT OF INTERNATIONAL LAW

Abstract: International law does not currently possess adequate instruments to define aggression in cyberspace, as well as to identify and punish perpetrators. The classical definition of aggression is inadequate to the reality of cyberspace, in the area of legal doctrine and practice, the international law is not adjusted to the contemporary digital reality and the destinations in which the digital reality is heading. The current definition of aggression reflects past conflicts. Conventional aggression is related to the attack on the physical elements of a state (related to the territory). Whereas, a digital attack may, but does not have to, have a direct relation to the territory of the state. The nature of cyberspace varies from other spaces. The a-territorial character of cyberspace influences the assortment of difficulties in the international legal issues regarding cyberspace. Cyberspace is not an additional or a marginal field of the operations of units, organisations and the state, but an area to which the entire sphere of operations is transferring. The war of the future will take place to a large extent in cyberspace.

Keywords: conventional attack, digital attack, aggression in cyberspace, definition of aggression

* The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy or position of any institutions / agencies with which he cooperates.

1. The definition of aggression

One should begin with the definition of aggression[1] (Latin: *aggressio* – assault). In the international law, aggression[2] is defined as an armed assault of one or more countries on the other. In international law, aggression is a crime.[3] The country that is attacked has the right to defend itself. In 1928, in Paris, a key pact was concluded regarding aggression, the Kellogg-Briand Pact[4] dedicated to the withdrawal from war as the means of solving international conflicts. The key aspect for the determination of what aggression is, was the 1933 Convention for the Definition of Aggression, which was signed in London,[5] supplementary to the Kellogg-Briand Pact.[6] The Convention indicated the following acts of aggression: declaration

[1] A.M. Rifaat, *International Aggression. A Study of the Legal Concept: Its Development and Definition in International Law*, Almqvist & Wiksell International, Stockholm 1979, p. 19.

[2] W. Góralczyk, S. Sawicki, *Prawo międzynarodowe publiczne w zarysie* [An Outline of the Public International Law], LexisNexis, Warsaw 2009, pp. 358-359.

[3] C. Damgaard, *Individual Criminal Responsibility for Core International Crimes*, Berlin 2008, p. 60. Damgaard's approach is identical with the approach to the problem in literature, see, e.g.: M. Królikowski, P. Wiliński, J. Izydorczyk, *Podstawy prawa karnego międzynarodowego* [Bases of the International Criminal Law], Warsaw 2008, pp. 113-150; P. Grzebyk: *Odpowiedzialność karna za zbrodnię agresji* [Criminal Liability for the Crime of Aggression], Warsaw 2010; L. May, *Aggression and Crimes against Peace*, Cambridge 2008; O. Solera, *Defining the Crime of Aggression*, London 2007; *The International Criminal Court and the Crime of Aggression*, M. Politi, G. Nesi (eds.), Ashgate 2004; Y. Dinstein, *War, Aggression and Self-Defence*, Cambridge 2003; M.C. Bassiouni, *International Crimes: Jus Cogens and Obligation erga omnes*, 'Law & Contemporary Problems' 1996, vol. 59, no. 4, pp. 69-70, M.J. Glennon, *The Blank-Prose Crime of Aggression*, 'Yale Journal of International Law' 2010, vol. 35, no. 1, p. 109; A. Zimmermann, *Crimes Within the Jurisdiction of the Court,* [in:] O. Triffterer (ed.), 'Commentary of the Rome Statute of the International Criminal Court', Second Edition, Munich 2008, p. 135; M. Płachta, *Międzynarodowy Trybunał Karny* [International Criminal Court], vol. 1, Krakow 2004, pp. 450-509.

[4] J. Łaptos, *Pakt Brianda-Kelloga* [The Kellogg-Briand Pact], Wydawnictwo Naukowe WSP, Krakow 1988.

[5] Polish OJ 1933 no. 93, item 712. See also M. Matysiak, P. Domagała, *Międzynarodowe Trybunały Karne oraz instrumenty sprawiedliwości tranzytowej* [International Criminal Courts and Transitional Justice Instruments], Warsaw 2012, p. 52.

[6] H. Korczyk, *Traktat ogólny o wyrzeczeniu się wojny (Pakt Brianda–Kelloga). Geneza, zawarcie, recepcja, działanie* [General Treaty for Renunciation of War as an Instrument of National Policy (the Kellogg-Briand Pact). Genesis, Conclusion, Reception, Effect], Wydawnictwo Fundacji 'Historia pro Futuro', Warsaw 1993, p. 5 et seq.

of war against a different country, a military act committed with own military forces in foreign territory; even without the declaration of war, attack with the use of ground, naval or air forces against the territory, ships or planes of other country even without the declaration of war, naval blockade of a coast or ports of other state, support given to armed bands, who by organising within the territory, would perform an assault on the territory of other state as well as, a refusal, despite the request of the state that is subject to aggression, to deprive these bands of any aid or care. Aggression. On 14.12.1974, during the 29th session – the United Nations General Assembly adopted a resolution no. 3314 (XXIX) which included the definition of aggression based on the 1933 Convention and introduced some amendments. Aggression is the use of armed force by a state or a group of states against the sovereignty, territorial integrity or political independence of another state (regardless of whether the state belongs to the United Nations).[7]

> Article 1 Aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition.
> Article 2 The First use of armed force by a State in contravention of the Charter shall constitute prima facie evidence of an act of aggression although the Security Council may, in conformity with the Charter, conclude that a determination that an act of aggression has been committed would not be justified in the light of other relevant circumstances, including the fact that the acts concerned or their consequences are not of sufficient gravity.

While analysing the current definition of aggression, one must indicate that it still rings the bells of the past reflecting rather the nature of the conflict of the past and even the language, in which it was written, indicating its archaic nature and the lack of adjustment to the cyber present.

[7] A.L. Zuppi, *Aggression as International Crime: Unattainable Crusade or Finally Conquering the Evil?*, 'Pennsylvania State International Law Review' 2007-2008, vol. 26, no. 1, pp. 2-3.

2. The subjects of aggression

According to the current international legal state, the subject of aggression may be a state, including everything that is related thereto, i.e. military and civil infrastructure.

The aggressor may simultaneously be a state, which furthermore complicates the contemporary evaluation of the situation in terms of the international law. It essentially narrows down the number of entities encompassed by the definition, as well as the situations it defines. Already on more simple grounds, i.e. the conventional attack, a doubt arises, because, judging by the independence of activities undertaken by various organisations towards states, from the territory of which they operate, e.g. ISIS, states are not the sole aggressors. It seems inappropriate to narrow down the term aggressor solely to states. It raises numerous practical and legal issues already at the conventional level. The contemporary definition of aggression is archaic and inadequate. Cyberspace is not an additional or a marginal field of the operations of units, organisations and the state, but an area to which the entire sphere of operations is transferring. Cyberspace is an area of military operations parallel to the real world. The subject of the contemporary, aggressive military operations comprises not only states, but also independent organisations, the activities of which can neither be associated to those states, nor proved. The transfer of operations towards cyberspace causes even bigger autonomy. Additionally, one should underline that the substantial number of these operations is not actually associated with any state. These operations are performed by terrorist or criminal organisations.

The war of the future will take place to a large extent in cyberspace. Therefore, the international law should address these issues adequately.

3. The object of aggression

The object of aggression is the sovereignty, territorial integrity or political independence. Speaking of the territorial integrity element, one should specify that the object of attack comprises all that is related to the territory of a given state, i.e. aggression concerns the entire infrastructure of a state, both civil and military, private and public, i.e. everything that is located within the borders of a particular state and associated therewith.

However, one should distinguish the object of conventional aggression from the object of digital aggression. At this point the first issue occurs; something that can be the object of aggression may be, by mutual agreement, referred to as the state infrastructure, but it is not always narrowed down to the territory of this state. The aforementioned results from the fact that the whole digital infrastructure of a state does not have to be located within its territory.

Conventional aggression is related to the attack on the physical elements of a state related to territory. Whereas, a digital attack may, but does not have to, have a direct relation to the territory of the state.

The author would like to focus on the key source of the issue, that is, the a-territoriality of the digital space, which constitutes an issue in the international legal specification of the term aggression, so that it could be adequate to cyberspace.

3.1. The object of digital aggression

Digital aggression encompasses the entire digital infrastructure, i.e. servers, websites and digital control structures. The idiosyncrasy of this type of attack itself causes its partial de-physication. Additionally, transferring some of the activities and data to the virtual sphere causes the disconnection of the physical location from the factual one. The basic difficulty consists in the fact that the determination of the key element, i.e. the territorial element of the digital structure is difficult to identify.

Obviously, due to security reasons, states strive to locate their IT infrastructure, or at least the strategic components thereof, in their territory. However, a state as a whole is a highly complex and a multi-faceted structure and it encompasses a lot of elements, and here, there is no certainty that its structural placement is simply within the borders of a particular state. After all, they operate within a territory of a company or there are institutions constituting elements of structures of other global companies, therefore, the IT infrastructure cannot be reduced to a territory. Furthermore, the transfer of actions to a cloud causes their disconnection from a territory of a particular state.

4. The characteristics of a territory

In order to provide the international legal context, one should introduce or remind the concept of a territory. By territory we understand a generally specified geographical area or an area of human activity; however, it is mostly treated as a synonym of a state's territory. The state territory is an area subject to state power and limited with borders. J. Symonides distinguishes four categories in terms of defining a territory: objective (a territory constitutes an object of state authority), subjective (a state is a quasi-biological organism and the territory is its body), spatial (the space within which the authorities operate) and competence-oriented (if the state is a normative system then, the territory is a spatial sphere of the state's competence and constitutes the scope of its legal order validity.[8]

According to the author, as has been shown before, the a-territorial character of cyberspace influences the assortment of difficulties in the international legal issues regarding cyberspace.

The question about territory has always been crucial for the international legal system. It constitutes the core of the definition of the state and as is, it is related to the issue of jurisdiction and the scope of rights executed by the state. The territory is protected in compliance with par. 52 of the Charter of the United Nations, by the *uti possidetis iuris* norm.[9] In the international law, the conception of jurisdiction was traditionally strongly associated to the concept of sovereignty. Jurisdiction allows states to bestow the power of sovereign independence, which they possess in a global system of formally equal states. Sovereignty informs of the acquisition of international regulations that limit the execution of the jurisdiction of the state.[10] The state has jurisdiction over territory and its inhabitant

[8] R. Bierzanek, J. Symonides, *Prawo międzynarodowe publiczne* [The Public International Law], Wydawnictwo Prawnicze LexisNexis, 8th ed, Warsaw 2005.

[9] The UN Charter, Polish OJ 1947, no. 23, item 90.

[10] C. Ryngaert, *The Concept of Jurisdiction in International Law,* Professor of International Law, Utrecht University, pp. 1-2; F.A. Mann, *The Doctrine of Jurisdiction in International Law,* 'Recueil des Cours de l'Académie de Droit International de La Haye' 1964, vol. 111, p. 15 (stating that *'[j]urisdiction ... is concerned with what has been described as one of the fundamental functions of public international law, viz. the function of regulating and delimiting the respective competences of States ...*'). Also A.F. Lowenfeld, '*International Litigation and the Quest for Reasonableness*', 'Recueil des Cours de l'Académie de Droit International de La Haye' 1994, vol. 245, p. 29 ('*I believe that while we will not here address the cosmic issues of war and peace, of nuclear weapons and terrorist assaults, we will deal with*

population; however, there exist certain limitations in using own territory, such as those coming from the naval and aviation law.[11] The key issue here is, whether cyberspace is a territory subject to protection. Additionally, a more basic issue comes to mind, whether cyberspace can even be regarded as territory. According to the author, such a statement is illegitimate.

According to the territorial sovereignty principle, the state holds sole and explicit power over own territory. Therefore, only a given state is allowed to exercise jurisdiction, particularly by the submission of objects and subjects in its own territory to the state legislation and to execute these provisions. Moreover, the state has the right to control the access to own territory. Territorial sovereignty protects the state from various forms of intervention of other states.[12]

4.1. Space in the international law

From the issue of territory one should proceed to the concept of space. From the legal viewpoint the aviation space is divided into domestic and international:[13]

- the space of a given country encompasses its territory (land, internal marine waters and territorial waters). Within its own space, the state is sovereign;
- international aviation space encompassing the rest of the world, including the open sea and the areas beyond anyone's jurisdiction. All countries may use it on equal terms.

---

legitimate and serious concerns of private persons and of States, and surely of lawyers, embraced within what Story calls the comity of nations.').

[11] J.L. Brierly, *The law of nations. An introduction to the international law of peace*, Oxford at the Clarendon Press, 1936, p. 142.

[12] W. Heintschel von Heinegg, *Legal Implications of Territorial Sovereignty in Cyberspace,* 4th International Conference on Cyber Conflict 2012, p. 8.

[13] According to the *Convention Relating to the Regulation of Aerial Navigation* signed in Paris on 13.10.1919 (Polish OJ 1929, no. 6, item 54) *every Power has complete and exclusive sovereignty over the airspace above its territory* (Article 1). The Convention on International Civil Aviation of 1944 specifies that *the territory of a State shall be deemed to be the land areas and territorial waters adjacent thereto* (Article 2). The United Nations Convention on the Law of the Sea states that; *1. The sovereignty of a coastal State extends, beyond its land territory and internal waters and, in the case of an archipelagic State, its archipelagic waters, to an adjacent belt of sea, described as the territorial area. 2. This sovereignty extends to the air space over the territorial sea as well as to its bed and subsoil.* (Article 2).

5. The characteristics of cyberspace

However, cyberspace is perceived as a virtual social and multi-faceted space dedicated to indirect contact. Cyberspace is at the same time a method of social contact. Despite the great advantages of cyberspace, it may be used against the user's will or interest. Cyberspace collects and uses information (also private) without consent, knowledge and contrary to the interest of the interested entities. On the one hand, in cyberspace, the human rights are being exercised, but on the other hand, it constitutes a threat to exercising them. Moreover, there are instances of a lack of control over the virtually processed personal data and the inability of erasing them.[14] The key aspects of cyberspace consist in the difficulty of identifying the perpetrator or the decisive factor, and the double nature of the technology – good and destabilising.[15] Cybersecurity is the key element of global security.[16] Cyberspace is the host for the communication between computers and transfer channels (mobile or wire-based). Any such communication requires hardware and any such information is then physically directed through a territory of one or few states (and, potentially, through the outer space), before it reaches the recipient. Here, we notice a significant territorial bond of any activity in 'cybernetic space' with at least one state. Whereas, the connection may last for nanoseconds and the state has no way of countering, controlling or preventing this transfer. The phenomenon of transferring information via various jurisdictions in cyberspace is still not a new form of 'outer space'. However, in cyberspace, no state, in compliance with the international law, can exercise its jurisdiction effectively. Full control of cyberspace by the state is technically impossible.[17] Cyberspace

[14] See *Człowiek w świecie rzeczywistym i wirtualnym Nowy wymiar zagrożeń w świecie realnym i wirtualnym* [A Human in the Real and Virtual World. The New Dimension of Threats in the Real and Virtual Worlds], [in:] A. Andrzejewska, J. Bednarek, S. Ćmiel, J. Sozański (ed.), 'Unijne regulacje praw człowieka w cyberprzestrzeni a korzyści, zagrożenia i postulaty, Cyberprzestrzeń a system ochrony prawnej Unii Europejskiej' [Union Regulations on Human Rights in Cyberspace vs Benefits, Threats and Postulates. Cyberspace vs the European Union's System of Legal Protection], Wydawnictwo WSGE Józefów 2013, p. 158.

[15] Department of State International Cyberspace Policy Strategy, March 2016, Public Law 114-113, Division N, Title IV, Section 402, p. 3.

[16] *Ibidem,* p. 4.

[17] See A Zimmermann, *International Law and 'Cyber Space'*, ESIL Reflections 2014, vol 3, no. 1 (http://www.esil-sedi.eu/node/481, accessed 4.1.2021).

comprises of a co-dependent structure of IT structures, including the Internet, telecommunication networks, computer systems and built-in processors and controllers. That makes cyberspace to not be a physical place. The physical bind of cyberspace with servers and computers is often illusionary. Cyberspace is anonymous and omnipresent. Cyberspace should be considered as common, therefore, legally, as *res resisis omnium*. However, these characteristics only justify the obvious conclusion that cyberspace in its entirety is not subject to a single state or a group of states. Due to its features it resists acquisition.[18] Cyberspace is an illusion of the real world created with the use of ICT tools.

5.1. The difference of aggression in cyberspace

The contemporary definition of an attack is not coherent with cyberspace attack. The nature of a cyberspace attack is related to the infection of the computer infrastructure, programmes, servers used for various purposes e.g. a programme that maintains power stations, waterworks, mobile communication or financial system. The characteristics of cyberspace creates an issue in each of the elements. The problem in cyberspace consists in the various categories of perpetrators: state – a particular state that inspires the attack, organisations inspired without the knowledge of state authorities, organisations or natural persons who are autonomous in relation to the state. Additionally, the technical executor of the attack, e.g. the hacker, may not know of the actual perpetrator. On the one hand, cyberspace provides the instruments for anonymous commission of such criminal acts, and on the other hand, it allows for efficient masking of the one commissioning the attack. Therefore, what is characteristic, is the difficulty in identifying the actual perpetrators and those who inspired them. The difficulty comes from a-territoriality. Additionally, the institutional perpetrators are separated from the autonomous and 'individual perpetrators'. Additionally, cyberspace constitutes a difficulty in identifying perpetration, a difficulty in connecting the individuals with institutions, additionally, virtual inability of proving the state perpetration. At times, the executor may be unaware of acts committed through the agency of his computers. The attack must not only have a hostile intention, but may result in aggression, e.g. hackers'

[18] W. Heintschel von Heinegg, *Legal…*, p. 9.

breaking into the servers of the general staff of the army of the foreign state.

5.2. The threat of digital space

The main challenge for the governments is to ensure that the population is protected from Internet crime and espionage. One must at the same time indicate that most of the cyber-attacks are not conducted by government-funded hackers, but by autonomous criminals who focus on the theft of trade and financial secrets.[19]

Cyber-terrorism is among the main threats, i.e. intended actions undertaken to the detriment of ICT networks via the disruption of the systems' operations, the unauthorised entry, copying, modification or erasure of data, breaching security in order to take control over the particular elements of the network.

The most frequent cyber-terrorist attacks include[20]:

- entering foreign computers (*hacking*) or IT systems (*cracking*) for financial gains,
- software that allows entry into the server while circumventing security (*back door*),
- interception of information between computers, particularly passwords and logins (*sniffing*),
- posing as a different computer (*IP spoofing*),
- sending computer viruses,
- extracting confidential information (*phishing*).

Cyberspace comprises all ICT systems and networks, as well as associations and relations between them and users thereof, as well as between users themselves. Cyberspace is used by various users, financial institutions, private companies and individuals. Therefore, cyberspace security has become one of the basic strategic aims in the area of security of each state. The freedom of migration, trade, information and capital in a physical world was associated to the freedom of cyberspace transfer.

[19] University of Notre Dame Law School, *US, International Law: Meeting Summary, Cyber Security and International Law*, Chatham House, p. 3.

[20] T. Pączkowski, *Słownik Cyberbezpieczeństwa* [Dictionary of Cybersecurity], Szkoła Policji w Katowicach, Katowice 2017.

The aims of cyberterrorism may vary – they may be both, political and material. The aim of cyberterrorist attacks may be state institutions, social organisations, companies, research institutes, private persons and other structures. However, the main target mostly comprises state ICT systems that ensure proper functioning of: state administration, military forces and other institutions engaged in national security, institutions responsible for the internal and external security of the state, communication and telecommunication networks, supply networks regarding energy, water and gas, the financial networks and institutions and emergency services.

IT operations involving computers or other network devices that are located in a different territory of the state do not constitute a violation of the international law *per se*. It seems the clearest, when such an activity in the territory of a different state yields no or little results. In some circumstances cyberspace activities of one country in the territory of other country may be a violation of the international law.[21] Often, it is difficult to determine, who or what is responsible for a given cybernetic event. The aforementioned leads to an often raised and discussed 'issue of attribution' in cyberspace. The states concerned with the challenge related to attribution in the technical sense, would inform other states of a particular cybernetic incident. A different issue is the matter of the state's decision on the publication and indication of the other state as the entity responsible for the particular cybernetic incident and condemnation of the action as intolerable.[22] The behaviour of the state in cyberspace remains rooted in the existing legislative frameworks, including the international law. States are held responsible for the determination of how the certain cyberspace legal frameworks work.[23]

In terms of the international law, the phenomenon of cyberwarfare does not exist in the legal vacuum, but it is subject to various rules; however, in the opinion of the author, unadjusted to the challenges of the modern times.[24] Cyberspace is a time-dependent assortment of connected IT systems and users, who engage in interactions with the systems. The implications between two or more parties, where at least one cyberattacks

[21] B.J. Egan, *International Law and Stability in Cyberspace*, 'Berkeley Journal of International Law' 2017, vol. 35, no. 1, pp. 173-174.

[22] *Ibidem,* p. 176.

[23] *Ibidem,* p. 180.

[24] N. Melzer, *Cyberwarfare and International Law,* 'Cyberwarfare and International Law' 2011, UNIDIR Resources, p. 36.

the other party, influence the ability to locate offensive and defensive activities swiftly in cyberspace, the efficiency of cyberspace mapping and the need for continuous patrolling and recon.[25]

The definition of the state according to the international law is the territory and the population represented by an effectively operating government. Territory efficiently determines the population and the greatest denominator of the government's legal power (jurisdiction) is the territory. Governments are increasingly taking control over domestic cyberspaces and while the territory principle states that the state holds jurisdiction over servers and networks of own territory, the communication between servers and computers takes place in international networks supported mainly by private networks that are not controlled by any government, with an abundance of information being stored on foreign servers.[26] In cyberspace the differentiation of storing data in or beyond a state is artificial. States hold sovereignty over their appointed cyberspaces *mutatis mutandis*. However, states can also undertake operations in foreign cyberspace, e.g. in reaction to terrorism and other crimes. Many means of such type are encompassed by international conventions against international crime and terrorism. Thus, countermeasures against crime and terrorism, which may be applied on foreign soil, will be perfect for the cooperation with local officials of law enforcement agencies based on the convention or *ad hoc* agreements. The state may feel an urge to take action of pursuing or combating terrorism without the proper authorisation from other interested country.[27]

5.3. The Nature of Cyberspace

The author would like to indicate that the nature of cyberspace varies from other spaces due to the following elements:

- virtual actors in cyberspace;

[25] R. Ottis, P. Lorents, *Cyberspace: Definition and Implications*, Cooperative Cyber Defence Centre of Excellence, Tallinn (https://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf, accessed: 4.1.2020).

[26] P. Wrange, *Intervention in national and private cyberspace and international law*, [in:] J. Ebbesson, M. Jacobsson, M. Klamberg, D. Langlet, P. Wrange (eds.), 'International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi', Brill/Nijhoff, Leiden 2014, p. 2.

[27] *Ibidem,* p. 5.

- theoretically, the actions appear in real-time. That means, that the computers, systems and servers are in a territory of interest, but the area of the cyberattack in a particular territory may be strictly temporary;
- some operations in cyberspace may occur on particular computers or servers (i.e. on a specified territory), largely without the knowledge of their owners;
- inconsistency between the features of the encapsulated territory and the open cyberspace;
- the inability to control cyberspace, therefore, the inability to exercise jurisdiction over this 'territory';
- some countries attempt to impose control over this space by censorship and controlled access;
- abundance of instruments allowing to operate within cyberspace: computers, smartphones, players, all modern home appliances (e.g. refrigerators, vacuum cleaners etc.) and a growing assortment of devices that allow access to cyberspace;
- cyberspace gives a feeling of anonymity. This aspect is of course disputed and there is an opinion that all actions can be monitored. However, I do not share this opinion due to the following reasons:
- broad scope of possibilities of accessing cyberspace;
- well-developed techniques of masking the end access point, anonymous instruments of access to cyberspace, such as smartphones with unregistered cards (i.e. in Poland the registration of all used mobile phone cards was imposed in 2017, and one should agree that it is not a global standard) or Internet cafes etc.;
- efficiency of identification is not in fact significant;
- immediate transfer capability in cyberspace;
- existence of enormous areas outside of the efficient international jurisdiction. First of all, it results from the fact that servers are often located in countries that do not cooperate in terms of combating crime. Secondly, none of the countries can control all computers and servers located within their territories;
- ability to distinguish between the territorial location of the final perpetrator and the territorial area, from which the actual attack is taking place;
- all negative actions e.g. the promotion of terrorism and other negative ideas, criminal activity can be easily located and relocated;

- actual jurisdiction of the state over cyberspace is, to a significant degree, fictional or at least incomplete, considering the fact that the state is unable to control all the 'impulses' that occur in cyberspace, for which the state may theoretically be responsible regarding the actions undertaken from a given territory;
- semi-automation of certain activities in cyberspace, i.e. the perpetrator does not have to control and direct particular activities, while remaining the initiator of further activities;
- it is easier to conceal actual activities, it is much easier than concealing in real territory;
- to a certain extent, a rather symbolic impact of the impulse on a particular territory, which may be even counted in nanoseconds;
- some wrong (black) activities may be performed with complete lack of awareness.

5.4. The differences between cyberspace and territory

The territorial sovereignty principle also applies to cyberspace and protects the IT infrastructure located in a state territory. States are obligated not to allow for conscious exploitation of their territories for activities violating the territorial sovereignty of other country, if the cyberattacks have been conducted from a government IT infrastructure of the state of origin. However, the properties of cyberspace and the necessity of maintaining the functionality of the Internet connection require consensual limitations of exercising local competences.[28]

The second consequence of applying the territorial sovereignty principle to cyberspace is the domestic law of a state dedicated to the cybernetic infrastructure and digital activity, and applied by legislative, executive or judicial means.[29] These issues are associated with countless other digital problems which we face in our foreign policy every day, such as digital security, e-trade, human rights in cyberspace, and the public diplomacy through cybernetic instruments.[30]

[28] W. Heintschel von Heinegg, *Legal...*, p. 8.

[29] *Ibidem,* p. 13.

[30] H. Hongju Koh, *International Law in Cyberspace*, 'Yale Law School Legal Scholarship Repository' 2012, p. 13.

One should indicate that there is a shortage of treaty law specific for cybercrime. Therefore, the general international law should be applied. All interpretation efforts are uncertain and vague. This lack of normative legal clarity encourages states to take certain interpretative positions. The objective view of the state regarding the law may affect the legal position it takes; however, it would be naive to deny that political and ethical influences have impact on such arrangements. Only in special circumstances, their prescriptions may cross the boundaries of international law. However, where the boundaries are unclear, there may be certain common political principles or ethical norms in effect, in order to determine the external boundaries of the acceptable activity in cyberspace. As IT activity is a relatively new phenomenon, policies and ethical norms may serve the purpose of determining boundaries that are more restrictive than those of the international law, aiming at the limitation of the activities of other states. In time, these non-legal norms may mature through codification into treaty law or clarify in the form of customary law, so that they formally determine the boundaries of cybernetic activities. In the meantime, cyberspace will remain the environment of an eager and often multi-directional, normative development.[31] Digital warfare is not a technical legal term, it is misleading and useless. Cyber warfare has certain significance for regulations regarding the use of force, as it may be applied for the justification of self-defence against other states and non-state entities accused of conducting a cyber-attack against the state.[32]

The international law assumes that the right to sovereignty and the due diligence must be in balance. Therefore, the state is required to take measures that go beyond its capabilities or are otherwise unsubstantiated. The state does not have to take burdensome measures to prevent the malicious use of own cybernetic infrastructure, such as monitoring the entire cybernetic activity. The principle of sovereign equality means that other states have the same obligation. Therefore, they have the legal motivation to ensure that the malicious digital operations are not conducted from their territories. If they do not meet their obligations of due diligence, the affected state may react directly against them or indirectly, by performing

[31] M.N. Schmitt, L. Vihul, *The Nature of International Law Cyber Norms, International Cyber Norms: Legal, Policy & Industry Perspectives*, NATO CCD COE Publications, Tallinn 2017, pp. 46-47.

[32] C. Lotrionte, *State Sovereignty and Self-defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, 'Emory International Law Review', vol. 86, p. 826.

operations against the non-state entities involved.[33] The specific properties of cyberspace do not constitute an obstacle for applying this law. There is an urgent need of explaining, or even adjusting the traditional law. Due to the co-dependence of networks, there is a large possibility that hostile states take measures against neutral countries. Such measures may endanger the essential aim and the aim of the neutrality law – preventing the escalation of an international armed conflict.[34]

5.5. The issues of jurisdiction in cyberspace

The nature of communication in cyberspace is a new phenomenon for the international law and, due to its particular technical features, it poses new challenges to the international law. The traditional ways of creating norms of the international law, be it multilateral treaties or development of the rules of customary international law, may not be able to address this issue. Additionally, there is a hostility of states and even non-state entities, such as international corporations that have the technological advantage in 'cyberspace', against the regulation of their activities in 'cyberspace' by defined principles based on treaties. These entities rather benefit from the lack of efficient international regulation of their activities. Due to the same reason, considering the enormous technological gap between the highly industrialised states and international companies, and the small and less developed states, many of them is incapable, de facto, of maintaining at least a minimum form of control over cyberspace activities, originating of afflicting their territory. Additionally, the nature of cyberspace activities, where information is directed through numerous states and territories, as well as, the sheer amount of the created information, lead to the lack of efficient regulative mechanisms, that could be applied by the states, in terms of detecting malicious cyberspace activities. The results of cyberspace activities, even if they come from certain states, take place abroad, which in many cases, raises the question whether the international obligations (based on a treaty or on a custom), that the state accepted, are still in force in such transboundary and extraterritorial conditions, while the

[33] M.N. Schmitt, *In Defense of Due Diligence in Cyberspace*, 'The Yale Law Journal Forum' 2015, p. 86.

[34] W. Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 'International Legal Studies' 2013, vol. 89, p. 155.

obligations regarding human rights are particularly important. As has already been mentioned, in cyberspace it is often difficult or even impossible to examine the activities and associate them to a given state in accordance with the existing norms of the international law. This in turn requires the international law to develop detailed norms that would properly solve this issue. Another challenge regarding cyberspace is related to the states' (and actually private entities') capability of the efficient gathering of comprehensive data on every person that is active in the Internet, in any way. The last challenge is related to the lack of any form of efficient international structure of managing cyberspace.[35]

The question, whether the traditional principles and the principles of international law are applicable to cyberspace activity is nothing new. The issue of applying international customary law in cyberspace gained significance. Currently, the binding international law does not have to submit to the challenges related to cyberspace. The states agree that the international customary law is actually applicable in cyberspace, however, it requires a consensus.[36]

5.6. The legal aspect of jurisdiction in terms of cyberspace

The formal situation of activities in cyberspace, the location of conducted activities, decide on the used responsibility and jurisdiction, and the difficulty lies in the fact that not all of these actions conducted in a given territory were performed by permission or to the knowledge of government authorities.[37] According to the conception of territorial jurisdiction, states have the right to regulate IT activity on their territory and apply domestic law. States have the right to apply territorial jurisdiction in order to conduct IT activity and maintain IT infrastructure on their territories. However, there is a need of arranging, at the international level, the means of executing territorial jurisdiction with regard to cyberspace.[38] The unique attributes of network technology demand explanation, how

[35] See A. Zimmermann, *op. cit*.

[36] W. Heintschel von Heinegg, *Legal…*, p. 8.

[37] D.G. Post, *Governing cyberspace*, 'Wayne Law Review' 1996-1997, vol. 43, p. 155; J.R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 'Emory Law Journal' 1996, vol. 45, p. 911.

[38] W. Heintschel von Heinegg, *Legal…*, p. 19.

norms of the international law apply to them, and whether they should be supplemented.[39] One should underline that cyberspace is not a law free zone.[40] States that conduct activities in cyberspace must consider the sovereignty of other states, including beyond the context of an armed conflict.[41] Additionally, one should indicate that sovereignty does not only mean rights, but also obligations. The state must not consciously allow the use of the IT infrastructure present in its territory or under its exclusive government control, for activities that have an unfavourable and illegal impact on other states.[42] The international law is fully applicable, and fully developed in regard to cyberspace activity, and it is particularly important when one understands, that IT activities encompass persons using material objects in physical domains that have been subject to the normative architecture of the international law for years.[43]

5.7. The examples of digital attacks

One may point out a few cases of digital attacks:

- in the middle of December 2014, in the media, information had appeared about the breaches into computer systems of the operator of South Korean nuclear power plants. The hacker demanded the shutdown of the nuclear reactors. Still, the South Korea authorities assure that their 23 nuclear reactors are safe[44];
- in 2007, a wave of cybernetic attacks against Estonia was noted. It was the first case in history, when an independent state had fallen victim to a cybernetic attack on such a scale. Websites, servers and IT systems of the Estonian parliament, government institutions, banks and media were attacked by hackers, who had been at first suspected as working for the Russian government.

[39] M.N. Schmitt, *International Law in Cyberspace*: *The Koh Speech and Tallinn Manual Juxtaposed*, 'Harvard International Law Journal' 2012, vol. 54, p. 14.

[40] *Ibidem,* p. 15.

[41] *Ibidem,* p. 31.

[42] *Ibidem,* p. 32.

[43] *Ibidem,* p. 36.

[44] See J. Snow, *5 najsłynniejszych cyberataków*, [Five most notorious cyberattacks] http://plblog.kaspersky.com/five-most-notorious-cyberattacks/10015/; M. Mejssner, *Zabójcze kody* [Lethal codes] www.polska-zbrojna.pl/home/articleinmagazineshow/7454?t=ZABOJCZE-KODY (accessed 4.1.2020).

Although eventually, it turned out, that the attack was initiated by the 20-year-old Estonian student, these events showed that cybernetic attacks may pose a threat for the functioning of a state similar to traditional terrorism or armed aggression;

- Georgia-Russia, 2008: It was the first known use of the Internet during a conventional armed conflict for the purpose of disrupting the civil use of the Internet. It took place in a Georgian enclave of Southern Ossetia. The disruptions lasted for approximately a month. The physical fight lasted for approximately a week;
- Stuxnet,[45] 2009-2010: a computer virus, called Stuxnet, infected Siemens computers used in the Iranian nuclear program. Probably, the virus was created by the United States military with help from Israel and Siemens' scientists. The result was that centrifuges worked too fast;[46]
- in the middle of September 2009 an attempt of an organised cybernetic attack on the servers of Polish government institutions occurred. The attempt was thwarted due to the so-called cyber-patrols of the Internal Security Agency, who detected suspicious traffic in the network on time (the Internal Security Agency's patrols protect cyberspace of more than 50 government and local government institutions).

6. Conclusions

The author would like to indicate that the international law fails to keep up with the changes in reality, applying old models resulting from being attached to the inadequate understanding of the concept of territory. The author would like to underline that as has been shown, cyberspace significantly differs from the space defined by the international law. Additionally, the strategic issue with cyberspace consists in, first of all, codification, and secondly, effective application and execution.

[45] See K. Zetter, *Stuxnet. Początek ataku na infrastrukturę krytyczną świata* [Stuxnet. The beginning of the attack on the world's critical infrastructure] http://wszystkoconajwazniejsze.pl/kim-zetter-stuxnet/ (accessed 4.1.2020).

[46] University of Notre Dame Law School, US, International Law: Meeting Summary, Cyber Security and International Law, Chatham House, pp. 3-4.

The nature of a cyberspace attack causes that, while the location of the attacks may be determined, with the application of the appropriate technological level of the perpetrators, one is unable to determine neither the perpetrators, nor the actual location, from which they attack. In the opinion of the author, the difficulty of the issue of aggression in the international law primarily results from doctrinal issues, when the conceptual apparatus used for the purpose of defining aggression in the international law does in no way reflect the current digital reality. The second issue is the difficulty with determining the territory from which the attack and aggression were performed, as well as the legal and factual territory of attack. Additionally, a situation is possible, when a given state places its own servers on a territory of other state, however, not within the vicinity of its diplomatic mission.

Therefore, it is difficult to state that these assets are subject to diplomatic protection assigned to diplomatic facilities. The aforementioned creates *lege ferenda*, whether 'territory' with the servers should not be considered as owned by the state that actually performs operations in this area. That would create the necessity of establishing a certain tax residence, i.e. an actual location of executing given actions, from the IT location of performing these tasks. This creates an abundance of legal complications.

However, the author sees a difficulty in a different area as well. The issue at hand may be reduced to two aspects. First, the practical detectability of the actual perpetrators. Second, the actual impossibility to persecute the perpetrators. The aforementioned causes doubts regarding the effective application of the international law to increase even more. Actually, as shown by numerous cases of cyberspace aggression, apart from the presumption of guilt, such determination is impossible. Obviously, the state authorities do not remain unprotected against those attacks, as they apply countermeasures. Still, the aforementioned leads to a situation, in which the reaction to non-legal activities of one of the parties consists in actual activities (in a form of a reaction or proactive activities), also in the undetectable digital area.

As this area is too crucial to leave it unregulated, it seems that the key matter is to establish the standards of proceeding in cyberspace, which would limit the grey and black zones of operation. Such peculiar soft law which, through standardisation of action, would allow for the establishment of certain standards, which would some day turn into an international convention.

At the same time, the author would like to indicate that there are certain risks of extending the definition of aggression, as, when the act

of aggression is identified as such, the state will be forced to react to such activities. Additionally, autonomous, non-state attacks against other states, or against portions of the state, yet, against the state itself as a legal structure, pose a challenge.

The characteristics of cyberspace, as demonstrated above, leads to the final conclusion that it is not territorial, where territory is perceived in a traditional way. While the openness of cyberspace should be generally perceived as a positive element, its nature provides incredibly large possibilities of wrongdoing, such as cybercrime, or the spread of terrorism.

Both, the international community, as well as states, should strive to tackle these negative elements, however, the subject at hand creates a difficult and crucial dilemma between freedom of operating in the network and the control of negative phenomena. This nature of cyberspace will be a challenge for both, the international and the domestic (internal) law. It seems that the tightening of cooperation between the international community is the only instrument that imposes actual control over the negative aspects of cyberspace.

While the international law provisions are applicable to cyberspace and its infrastructure located in a given territory, the efficiency of the jurisdiction of a given state therein is doubtful. It is rather a suggestion to develop new principles of efficient practice of the states in cyberspace, than to expect the states to hold complete jurisdiction in cyberspace. It is neither realistic, nor doable, while *ad impossibilia nemo obligatur*.

Additionally, apart from the theoretical and doctrinal issues related to cyberspace, there is a large assortment of practical problems. Primarily, there is a difficulty in relating aggression to a state. In a conventional attack, one may see the aggressor, the attack is executed by people who are identifiable with the use of equipment that allows identification of the attacking country. However, cyberspace attacks, while maintaining a certain level of security, impede such identification. It is demonstrated by the course of numerous attacks which left us only with presumptions regarding the perpetrators, who were never truly identified. The difficulty with determining the actual perpetrators and the dislodgement of the location from which the attack comes is the key aspect here. In the extreme case, the instrument of attack may be computers, the users of which are not aware of participating in the attack.

7. *Lege ferenda* postulates in the issue of cyberspace aggression

Therefore, a new definition of aggression in cyberspace should be created as *lege ferenda*, as an action behind which an institutional activity of a given state stands, if, of course, such an indirect perpetration can be proven. Similar to anti-mafia regulations, a conception of the indirect perpetration in cyberspace had to be developed. It results from the fact that the perpetrator in cyberspace is not only a soldier or an official of the state but may also be a 'person on a contract' who performs certain activities.

As *lege ferenda*, the international law must specify the following areas:

- extension of the definition of an aggressor to non-state entities, as without it the demonstration of contemporary challenges will not be addressed properly;
- one should extend the scope of the meaning of aggression. One should define that the object of an attack is the entire military and civil infrastructure, including IT systems related to the strategic elements, such as e.g. energy, finance;
- redefinition of what should be considered as territory subject to an attack. Here, an objective difficulty arises, whether one may extend the definition of a territory of a state to all elements of the IT infrastructure, i.e. servers present in other country. However, assuming that computers are not located in the area of a diplomatic facility, they cannot be simultaneously considered as elements of a territory of other state. In order to properly define this issue, one should create, for the sake of cyberspace, a concept of a functional state territory, i.e. a factual arena of IT operations. The aforementioned dualism is necessary, as otherwise, we would have to hold on to the current territorial definition that does not meet the requirements of cyberspace, or develop an overly broad definition of a territory (as extended with the physical location of servers). Such a functional territory would be under the protection similar to the traditional territory;
- the territory from which the attack comes must be specified and must be an actual territory of the aggressor's operations, his residence, and not his servers (or intermediary links) from which the attack was launched;
- one should define what cyberspace aggression is. The classic components should include: network, computer or server infection

that would cause actual harm to the state's sovereignty, political or economic interests. However, the results of the attack should be of a material value or have strategic effects. For example, causing the dysfunction of the state's energy system would be an aggression, while impeding the work of waterworks in a small town would not be considered as such. Obviously, it is a discretionary issue. We possess international legal structures of organisation, which are able to determine the scope of such an attack and provide an authoritative evaluation of whether it is an aggression (the United Nations Security Council). Additionally, due to the complexity of the contemporary relations, one should divide the attacks into those causing state and private effects. Whereas, in the case of identifying a private attack or something that may be regarded as an autonomous attack in regard to a state, the state would be obligated to take counteractive measures against these activities, while not taking responsibility for these actions, but it would be only responsible for the omission of activities in the case of not taking action against the repetition of such attacks in the future.

The international law does not currently possess adequate instruments to define aggression in cyberspace, as well as to identify and punish perpetrators. The classical definition of aggression is inadequate to the reality of cyberspace. Both, in the area of legal doctrine and legal practice, the international law is not adjusted to the contemporary digital reality and the destinations in which the digital reality is heading.

Bibliography

1. Andrzejewska A., Bednarek J., Ćmiel S., Sozański J. (eds.), *Unijne regulacje praw człowieka w cyberprzestrzeni a korzyści, zagrożenia i postulaty*, Wydawnictwo WSGE Józefów 2013
2. Bassiouni M.C., *International Crimes: Jus Cogens and Obligation erga omnes*, 'Law & Contemporary Problems' 1996, vol. 59, no. 4
3. Bierzanek R., Symonides J., *Prawo międzynarodowe publiczne*, 8th edition, Wydawnictwo Prawnicze LexisNexis, Warszawa 2005
4. Brierly J.L., *The law of nations. An introduction to the international law of peace*, Oxford at the Clarendon Press 1936
5. Damgaard C., *Individual Criminal Responsibility for Core International Crimes*, Berlin 2008
6. Dinstein Y. (eds.), *War, Aggression and Self-Defence*, Cambridge 2003

7. Egan B.J. *International Law and Stability in Cyberspace,* 'Berkeley Journal of International Law' 2017, vol. 35, no. 1
8. Glennon M.J., *The Blank-Prose Crime of Aggression*, 'Yale Journal of International Law' 2010, vol. 35, no. 1
9. Góralczyk W., Sawicki S., *Prawo międzynarodowe publiczne w zarysie*, LexisNexis, Warszawa 2009
10. Grzebyk P., *Odpowiedzialność karna za zbrodnię agresji*, Warszawa 2010
11. Hongju Koh H., *International Law in Cyberspace*, 'Yale Law School Legal Scholarship Repository' 2012
12. Korczyk H., *Traktat ogólny o wyrzeczeniu się wojny (Pakt Brianda–Kelloga). Geneza, zawarcie, recepcja, działanie*, Wydawnictwo Fundacji 'Historia pro Futuro', Warszawa 1993
13. Królikowski M., Wiliński P., Izydorczyk J., *Podstawy prawa karnego międzynarodowego*, Warszawa 2008
14. Lotrionte C., *State Sovereignty and Self-defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, 'Emory International Law Review', vol. 86
15. Lowenfeld A.F., *'International Litigation and the Quest for Reasonableness'*, 'Recueil des Cours de l'Académie de Droit International de La Haye' 1994
16. Łaptos J., *Pakt Brianda-Kelloga*, Wydawnictwo Naukowe WSP, Kraków 1988
17. Mann F.A., *The Doctrine of Jurisdiction in International Law*, 'Recueil des Cours de l'Académie de Droit International de La Haye' 1964
18. Matysiak M., Domagała P., *Międzynarodowe Trybunały Karne oraz instrumenty sprawiedliwości tranzytowej*, Warszawa 2012
19. May L., *Aggression and Crimes against Peace*, Cambridge 2008
20. Melzer N., Cyberwarfare and International Law, 'Cyberwarfare and International Law' 2011, UNIDIR Resources
21. Ottis R., Lorents P., *Cyberspace: Definition and Implications*, Cooperative Cyber Defence Centre of Excellence, Tallinn
22. Pączkowski T., *Słownik Cyberbezpieczeństwa*, Szkoła Policji w Katowicach, Katowice 2017
23. Płachta M., *Międzynarodowy Trybunał Karny*, vol. 1, Kraków 2004
24. Post D.G., *Governing cyberspace*, 'Wayne Law Review' 1996-1997, vol. 43
25. Reidenberg J.R., *Governing Networks and Rule-Making in Cyberspace*, 'Emory Law Journal' 1996, vol. 45
26. Rifaat A.M., *International Aggression. A Study of the Legal Concept: Its Development and Definition in International Law*, Almqvist & Wiksell International, Stockholm 1979
27. Schmitt M.N., Vihul L., *The Nature of International Law Cyber Norms, International Cyber Norms: Legal, Policy & Industry Perspectives*, NATO CCD COE Publications, Tallinn 2017
28. Schmitt M.N., *In Defense of Due Diligence in Cyberspace*, 'The Yale Law Journal Forum' 2015

29. Schmitt M.N., *International Law in Cyberspace*: *The Koh Speech and Tallinn Manual Juxtaposed*, 'Harvard International Law Journal' 2012, vol. 54
30. Solera O., *Defining the Crime of Aggression*, London 2007
31. von Heinegg W.H., *Legal Implications of Territorial Sovereignty in Cyberspace,* 4th International Conference on Cyber Conflict 2012
32. Wrange P., *Intervention in national and private cyberspace and international law*, [in:] Ebbesson J., Jacobsson M., Klamberg M., Langlet D., Wrange P. (eds.), 'International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi', Brill/Nijhoff, Leiden 2014
33. Zimmermann A., *Crimes Within the Jurisdiction of the Court,* [in:] O. Triffterer (ed.), 'Commentary of the Rome Statute of the International Criminal Court', Second Edition, Monachium 2008
34. Zuppi A.L., *Aggression as International Crime: Unattainable Crusade or Finally Conquering the Evil?*, 'Pennsylvania State International Law Review' 2007-2008, vol. 26, no. 1