




## CYBER-OPERATIONS UNDER INTERNATIONAL LAW

### Cyberoperacje w świetle prawa międzynarodowego

Agata Małecka  
General Tadeusz Kościuszko Military University of Land Forces  
e-mail: [agata.malecka@awl.edu.pl](mailto:agata.malecka@awl.edu.pl)  
ORCID  0000-0002-5519-9681

#### Abstract

States around the world are constantly conducting (or participating in conducting) cyber-operations, using cyberspace to achieve national goals. Defensive and offensive actions in cyberspace are officially the part of strategic documents of the biggest state players in the international relations. Nevertheless, activities in cyberspace are regulated not only by national legislation, norms of international law apply to them also. The text attempts to determine the nature of such terms as: armed cyber-attack (under Article 51 of the UN Charter), use of force (under Article 2(4) of the UN Charter), cyber-attack and cyber-conflict (under international humanitarian law) and answer the question: under what conditions could the different cyber-operations be attributed to these terms, that imply the possibility of eventual responses or demands by victim parties consistent with international standards? The analysis is interdisciplinary in nature and will be particularly useful to researchers of international political and/or military relations and those interested in aspects of international security.

**Keywords:** cyber-attack, cyber-conflict, cyber-war, international law, prohibition of the use of force.

#### Streszczenie

Państwa na całym świecie nieustannie przeprowadzają lub biorą udział w przeprowadzaniu cyberoperacji, wykorzystując cyberprzestrzeń do realizacji interesów narodowych. Działania defensywne i ofensywne w cyberprzestrzeni są oficjalnie częścią dokumentów strategicznych największych państwowych graczy w stosunkach międzynarodowych. Niemniej, działania w cyberprzestrzeni nie są uregulowane jedynie przepisami krajowymi, odnoszą się do nich również normy prawa międzynarodowego. W niniejszym tekście podjęto próbę określenia charakteru takich pojęć, jak: cyberatak zbrojny (na gruncie art. 51 Karty Narodów Zjednoczonych), użycie siły (na gruncie art. 2 ust. 4 Karty Narodów Zjednoczonych), cyberatak i cyberkonflikt (na gruncie międzynarodowego prawa humanitarnego) oraz odpowiedzi na pytanie: pod jakimi warunkami można przypisać różnorodne cyberoperacje do tych w/w terminów, które implikują możliwości ewentualnych odpowiedzi czy też żądań stron pokrzywdzonych zgodnych z międzynarodowymi standardami? Analiza ma charakter interdyscyplinarny i będzie przydatna szczególnie dla badaczy międzynarodowych stosunków politycznych i/lub wojskowych oraz osób zainteresowanych aspektami bezpieczeństwa międzynarodowego.

**Słowa kluczowe:** cyberatak, cyberkonflikt, cyberwojna, prawo międzynarodowe, zakaz użycia siły.

## Introduction

The popularization of the prefix "cyber" and the beginning of adding this term to almost all activities and actions transferred to the network has led to the definition chaos, the mixing of concepts and meanings and the conviction that the existing legal state cannot apply to the new reality. The meaning of the prefix "cyber" should be placed primarily in the paraphysical space, where the internet plays an essential role (information, communication, social, and programming) with all technical elements such as servers and links. Therefore, the prefix "cyber" is used to define new, dynamically changing forms of communication using the latest technologies (e.g., mobile telephony).

Cyberization has also affected the sphere of research on war and peace, armed conflicts, and competition between countries. In this context, one should consider the category of cyber-attacks, which are not taken out of the law. In fact, any hostile activity in cyberspace initiated by state or non-state actors can be correctly interpreted and attributed to a specific group of activities to which provisions of international and/or national laws apply (Koh, 2012).

Aggressive acts in cyberspace have become a permanent method in the canon of political influence tools. Some of them are characteristic of so-called "soft power", used by states to gain predominance in the international system. The international community lacks coherent tools accepted by all states to deal with cyber-attacks. A need to transfer peacekeeping principles in physical space to cyberspace – the so-called "cyberpeacekeeping" – is gaining supporters (Dorn & Webb, 2019). Until appropriate mechanisms are developed, states have the ability to follow existing norms of international law. There are forms of acts in cyberspace that can be classified as "armed attacks" and/or unlawful "use of force" under the doctrine of *ius ad bellum* or as "attacks" under the doctrine of *ius in bello*, which creates specific legal consequences.

The article constitutes a problem analysis and aims to show that hostile actions in the cyberspace environment are regulated by international law analogous to other "traditional" forms of violence carried out by state and non-state actors. The text attempts to determine the nature of such terms as: armed cyber-attack (under Article 51 of the UN Charter), use of force (under Article 2(4) of the UN Charter), cyber-attack and cyber-conflict (under international humanitarian law). Victim parties are not deprived of legitimate means of response and can take preventive and defensive measures, depending on the characteristics of acts of cyber violence. The difficulty lies not in the lack of tools to detect and prevent hostile cyber activity, but in identifying the initiators and their targets (Rid & Buchanan, 2015).

This article does not exhaust the entire, broad, and complex issue of international law in cyberspace. Rather, it presents a general view of the application of selected international law rules to state-initiated hostile actions in cyberspace, that should be

useful to analysts of the international security system and broadly defined international relations.

### **Terminology**

An important aspect of this paper was the use of appropriate terminology. This was crucial to the analysis presented in this article because of fundamental legal differences between the different interpretations of the phrase "attack", which condition the various options for affected parties to respond to cyber-operations. The term "cyber-attack" can be used both in the context of international law and in a common meaning – including political usage. In the first case, it is important to distinguish between two interpretive approaches: *ius ad bellum* and *ius in bello*. In the second, "cyber-attack" appears as a non-legal term used in everyday language to describe a computer attack (Schmitt, 2012a). *Ius ad bellum* refers to "armed attacks" and is closely related to the exceptions to the principle of the prohibition of the use of force in international relations set out in the United Nations Charter (Article 51 UN Charter – self-defence, UN Security Council authorization of the use of force).

The *ius in bello* considers the concept of "attack" as a type of armed operation, covered by international humanitarian law (the law of armed conflicts), mainly written in Additional Protocol I to the Geneva Conventions (the legality of attacks because of the manner in which they are carried out and the status of the targets of attacks). Both interpretive approaches are legally founded in post-war international law. Nevertheless, they are applicable in assessing the nature of present-day acts of aggression in cyberspace. The spectrum of response options for victim parties depends on this assessment. If a cyber-operation qualifies as an "armed attack" in UN Charter terms, the possible response will be based on the principles of *ius ad bellum* - necessity, proportionality, and immediacy. Similarly, cyber-operations treated as "attacks" will be characterized by the use of physical violence and will be regulated by the norms of international humanitarian law *ius in bello* (based on the principle of distinction between civilians and military). In the context of cyberspace, however, it is not only the manners of carrying out attacks that are examined, but primarily their consequences. Therefore, both interpretive approaches *ius ad bellum* and *ius in bello* are applicable to cyber-operations that result (or were assumed to result) in the same consequences as the use of conventional forces (Schmitt, 2011).

### **Cyber-operations under international law**

Although the hostile activity of state and non-state actors in cyberspace is a phenomenon characteristic of the 21st century, it is important to realize, that it is a subject to the "old" (20th century) regulations of international law. In this context, it is difficult to talk about cyber-warfare; it can take place only in the ordinary sense of the word, and

with all the knowledge that war is officially being waged between state entities. It is more reasonable to use the term cyber-conflict or cyber-attack as an element of the former to describe hostile actions in cyberspace. That has legal implications in the form of the application of UN Charter and international humanitarian law, particularly the four Geneva Conventions and the Additional Protocol I.

In this context, it would be appropriate to clarify the principles of *ius ad bellum* and *ius in bello* applicable to cyber-operations. As mentioned before, the *ius ad bellum* analyses the concept of "armed attack", which is not the equivalent to the term "use of force" (not all uses of force are armed attacks). Thus, a cyber-operation must be considered as an "armed attack" in order for the provisions of the UN Charter to apply (in the context of the ability of the victim party to respond and defend itself). An analysis of Article 51 of UN Charter, which describes the conditions of the right to individual or collective self-defence, is the key to explaining the term "armed attack". The term "armed attack" is a narrower term than "use of force" and includes kinetic military force. "Armed attack" should be also understood in the context of effects, specific to armed operations – death (or risk of) or injury to persons or damage to or destruction of property and objects. Recognizing an "armed attack" is crucial to the possibility of an armed response by the victim state. If an unlawful use of force is identified and it is not an "armed attack", forceful defensive action cannot take place (more about "in-kind" responses to cyber-operations conducted by states in: Schmitt & Johnson, 2021).

It would seem that the United Nations Charter, that in Article 51 is act-based, does not include cyber-operations, because they do not generate negative effects by release of kinetic force. However, it should be considered that the intention of the drafters of Charter was to avoid certain effects, that is, to discourage states from initiating armed attacks, which consequences for the affected states were severe enough to respond militarily as well. This consequences-based approach means that all cyber-operations with effects analogous to those caused by kinetic actions considered as an armed attack will also be treated as an armed attack. The condition, however, is that a certain degree of harm is exceeded – death or injured (also illness and severe suffering) to individuals or damage or destruction of objects (Schmitt, 2012a).

*Ius in bello* analyses the term "attack", which is used to describe a military operation covered by the orders and prohibitions of international humanitarian law. *Ius in bello* is based on the principle of the distinction between civilians and combatants, which is crucial for the protection of the civilian populations during an armed conflict and/or a military operation. In the context of cyberspace, international humanitarian law will apply when a cyber-operation is considered as an "attack". According to the International Committee of Red Cross interpretation of the provisions of Article 49 of the Additional Protocol I, "'attack' means acts of violence against the adversary, whether in offence or in defence" (Sandoz et al., eds., 1987). Term "attack" is the same as "combat action" and refers to physical force. However, similar to the *ius ad bellum*, this will not

exclude all cyber-operations, which are in general non-physical, from the jurisdiction of international humanitarian law, due to the application of a consequence-based approach (Schmitt, 2012a). Thus, the main condition for an act to be classified as a cyber-attack is appropriate scale and effects. Importantly, the degree of harm for cyber-attacks can go beyond the strict understanding of physical damage, such as the appearance of disease due to poisoning of water, air, or soil. Similarly, a cyber-attack may occur in the form of the neutralization of the computer system on which the functionality of a specific object is based. Any interference with military computer networks, treated as an attempt to influence an adversary's military capabilities, may exceed the degree of harm (Schmitt, 2017). Cyber-operations against civilian targets that reach the certain degree of harm, defined above, are prohibited from the perspective of international humanitarian law. For military objects, a cyber-attack should follow certain rules (e.g. rule of proportionality, precautions in attack). It is important to remember that reaching the certain degree of harm applies to both conflicts between states (international armed conflicts between states) and non-state conflicts (non-international armed conflicts between state and an organized armed group or between organized groups) (Schmitt, 2012b). International humanitarian law applies to acts in cyberspace that would be considered as "attack" in the first place. Therefore, the use of the term "cyber-attack" is unjustified, for example, when using malicious software for criminal purposes. The failure to exceed the damage threshold and the civil nature of a cyber-attack are decisive on conferring the status of a cyber-attack.

### **Prohibition of the use of force in international relations in the context of cyberspace**

The prohibition of the use of force in international relations, which is based on Article 2(4) of the UN Charter, is not without significance for a full analysis of the legitimacy of the use of the terms "cyber-conflict" and "cyber-attack" in public debate. Importantly, "use of force" is not the same as "armed attack", and "armedness" is not necessary to make "use of force" illegal. The occurrence of an "armed attack" is relevant to the nature and conditions of defence, as defined in Article 51 of UN Chapter. In case of use of force, which did not rise to the level of an armed attack, victim-states can use only non-forceful actions and countermeasures (Schmitt, 1999).

The current ban on the use of force in international relations has its origins in attempts by states to restrict the use of armed force as a method of conducting foreign policy, as was initiated in the 19th century. The commitment to applying peaceful means to settle international disputes was enshrined successively in the Hague Conventions, the League of Nations Pact, and the Kellogg- Briand Pact. Finally, in the United Nations Charter, the signatories agreed to refrain "in their international relationships from the threat or use of force against the territorial integrity or independ-

ence of any state" (*United Nations Charter*, 1949). The terms "territorial integrity" and "independence" are essential. They derive from the general principle of sovereignty – currently a fundamental rule of international law. Principle of sovereignty refers to the supreme authority of the state and signifies independence. Thus, its connection to the prohibition of the use of force in international relations and non-intervention is unquestionable (International Court of Justice, 1986). The analysis of Article 2(4) of the Charter makes it possible to conclude that the prohibition of the use of force in international relations applies to:

1. states and relations between them, which automatically precludes the application of the Charter's provisions to non-state actors;
2. all states, including those which are not members of the United Nations;
3. both the use of and threatened use of force;
4. exclusively armed force, and therefore does not apply to activities of, for example, economic nature;
5. the so-called 'recourse to war' and the use of force, which cannot be attributed to warfare (for example, one-off military operations) (Simma et al., eds. 2013; Dinstein, 2017).

The provisions of the United Nations Charter interpreted in this way are applicable in cyberspace. Also, the general principle of sovereignty which is related with state's control over cyber infrastructure, persons, and cyber activities located on their territory (internal sovereignty) and/or jurisdiction over cyber infrastructure and activities abroad (external sovereignty). External sovereignty in cyberspace context means that states are free to engage in cyber activities (including cyber-operations) as a part of their foreign policy subject to rules of international law (e.g., the prohibition on violating the sovereignty of another state by using force in cyberspace) (Schmitt, 2017). The International Court of Justice has taken the standpoint that the prohibition of the use of force in international relations applies to any use of force, regardless of the type of weapon used (International Court of Justice, 1996). All cyber-operations that bear the hallmarks of the use of force or threats thereof against the territorial integrity and independence of a state are subject to UN Charter. At the same time, states enjoying sovereignty over their cyber infrastructure, bear responsibility for cyber-operations that exploit it. However, the use of government cyber infrastructure does not mean that the state is involved in conducting cyber-operations. Considering the issue of responsibility for violations of international law, it is important to properly attribute and define cyber-operation actors as any entity that initiates an attack, supports any aspect of attack planning (e.g., by providing funds or computer or human resources – experts), conducts the actual attack, knowingly supports the cover-up the attack or its source, or unknowingly reinforces the attack (Desouza et al., 2020). It should also be noted that the link between the prohibition of the use of force in international relations and the United Nations mission has resulted in a presumption of

illegality of those activities that do not directly threaten the integrity of the state (Schmitt, 2017).

The term "use of force" unquestionably refers to an armed force (as it was examined earlier – every armed attack is use of force) and includes kinetic force. However use of force can have non-kinetic nature – e.g. arming and training guerrillas (International Court of Justice, 1986). This standpoint is based on General Assembly resolution 3314 (XXIX), with the Definition of Aggression annexed to it ("aggression is the use of armed force by a state against sovereignty, territorial integrity or political independence of another state [...]"; UN General Assembly, A/RES/3314/XXIX, 1974). The catalog of acts of aggression listed in Article 3 is open and Security Council "may determine that other acts constitute aggression under the provision of the Charter" (article 4, UN General Assembly, A/RES/3314/XXIX, 1974). This allows certain cyber-operations to be considered as an act of aggression/use of force.

Thus the framework for the use of force is not clearly defined, cyber-operations that kill or injure persons or physically damage or destroy objects are definitely use of force, but other cases are not so explicit. The same problem surfaces in case of cyber-operations. A solution may be the application of informal criteria by the states, under which it seems more reasonable to qualify a particular act as the use of force. Yet they do not constitute official law, and the practice of states' responses to cyber threats is still in progress (Ney, 2020). These criteria are the outcome of an approach based on the analysis of the effects of cyber-operations – the damage and the impact on the state's functioning (the benchmark for individual assessment is the scope, scale and effects of a cyber-operation, comparable to an attack by traditional methods and means). They include: severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement and presumptive legality (Schmitt, 2017). It should be also mentioned that the willingness of states to apply the so-called Tallinn rules is not clear and the interest in promoting legal certainty in cyberspace is uneven (Efrony & Shany, 2018).

The criterion of severity refers to physical damage in the form of death, injury and/or destruction of critical infrastructure. Hence, it reflects the damage threshold already mentioned. The possibility for the state to pursue national vested interests in a cyber-operation situation is to be analyzed. The more likely a cyber-operation is to be considered as a use of force, the more it hampers the ability of the state to function efficiently in internal and external aspects.

Immediacy relates to the period, measured from the moment a cyber-operation occurs until its effects appear. In the case of cyber-operation, it appears extremely difficult to analyze the immediacy criterion and determine the relationship between the event and its consequences. The possible consequences of a cyber-operation may occur with considerable delay, especially when facing economic and financial conse-

quences. Also, determining the temporary link between a cyber-operation and its social implications does not fulfill the immediacy criterion.

As another criterion for considering a cyber-operation as a manifestation of the use of force, directness is tricky and ambiguous to identify as well. It is defined as the emergence of a close relationship between hostile actions in cyberspace and their effects, which manifests in the earlier determination of immediacy. The fact that cyber-operation affect various spheres of state functioning causes complications within the framework of directness. The economic and financial aspects are an excellent example of this – the economic slowdown resulting from a cyber-operation on the banking sector, for example, will occur over some, longer than immediate, time.

To determine the criterion of invasiveness, the determinant of "statehood" of individual systems of state functioning applies. In the case of cyber-operations that interfere with the proper operation of the most critical elements of the state (military systems, governmental domains, critical infrastructure, etc.), it is highly likely that they will be considered a manifestation of the use of force.

Measurability refers to a clear identification of the scale of impact of a cyber-operation. It is expressed in numbers – the amount of maliciously infected computers or stolen data.

Similarly, the criterion of a military character as classifying hostile activity in cyberspace as a group of armed conflicts refers to determining the degree of involvement of military entities. The possibility of qualifying a cyber-operation as a manifestation of the use of force increases with the probability of military nature of the party initiating it.

The prohibition of the use of force in international relations applies only to state actors. The criterion of statehood will, therefore, be met for cyber-operations initiated by or acting on behalf of state institutions and bodies.

The principle that what is not prohibited is allowed creates the essence of the presumption of legality. Acts not expressly prohibited by the treaty or adopted customary law meet the criterion of presumption of legality. That includes, but is not limited to, psychological and propaganda actions and activity aimed at creating economic pressure.

All the above criteria are taken into account when state entities consider the issue of qualifying cyber-operation to manifest the use of force in international relations. The difficulty lies in the determination of immediacy, directness, and measurability, which is due to the specific features of cyber-activities and their effects over time. Cyber-operations, which affect the capabilities of the national interests pursued by states, will be considered as methods of conducting armed conflicts. That means that cyber-operations are subject to analysis and interpretation on a case-by-case basis in terms of the applicability of international law.



### **Application of international humanitarian law in cyberspace**

A consequence-based approach is also used to analyze a particular cyber-operation under the *ius in bello*. In contrast to the assumptions of *ius ad bellum*, the *ius in bello* does not consider the "right or wrong" purpose of attack or "right to use of force" by a state. Instead, it determines how armed actors (state or non-state) may exploit military forces and who or what may be the target. An important term, which determines the applicability of international humanitarian law is "act of violence", which denotes a physical force. Again, in cyberspace context, the analysis deals with the consequences – violent consequences. "Act of violence" includes all cyber-tools (worms, viruses, malware, etc.) that result in physical damage, but also neutralization of military objects if it leads to a military advantage for the aggressor (Schmitt, 2012a). Thus, every cyber-operation which results in (or it was expected to result in) death or injury of individuals or destruction or damage of object and is aimed at military targets should be conducted in accordance with the principles of international humanitarian law (Gisel et al., 2020). These principles include: The Fourth Hague Convention of 1907 and the Geneva Convention relative to the Protection of Civilian Persons in Time of War of 1949, together with Protocols I and II of 1977.

From the point of view of cyberspace, it is vital to analyze the so-called Martens Clause in the preamble to the Fourth Hague Convention of 1907 (International Committee of the Red Cross, 1907). It reads: "Until a more complete code of the laws of war has been issued, the High Contracting Parties deem it expedient to declare that, in cases not included in the Regulations adopted by them, the inhabitants and the belligerents remain under the protection and the rule of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity and the dictates of public conscience" (International Committee of the Red Cross, 1907). The above gives the possibility to apply the provisions of the Fourth Hague Convention to cyber-operations.

Also, the provisions of Protocol I and Protocol II to the Fourth Geneva Convention for the Protection of Civilian Persons in Time of War (1949), indicate that certain cyber-operations are covered by international law. Protocol I (International Committee of the Red Cross, 1977a) and II (International Committee of the Red Cross, 1977b) supplement the rules on the treatment of civilians in times of conflict with the rule of limiting the use of methods and means of harming the opposing party – Protocol I to conflicts of an international nature, Protocol II – non-international ones. The wording of the Preamble that the provisions of the Geneva Conventions and this Protocol must be applied in all circumstances, to all protected persons, irrespective of the nature or causes of the armed conflict (International Committee of the Red Cross, 1977a) and Article 1 of Protocol I that in cases not covered by Protocol I and other international agreements, civilians and combatants are protected by international law (International Committee of the Red Cross, 1977a), give the possibility to apply the provisions of the

Fourth Geneva Convention to cyber-conflicts. Similarly, the wording of part of the Preamble of Protocol II: "[...] in cases not covered by the law in force, the human person remains under the protection of the principles of humanity and the dictates of the public conscience" (International Committee of the Red Cross, 1977b).

International humanitarian law shall also apply in the case of cyber-warriors, generally defined as highly qualified, trained and specialized individuals or groups who engage in aggressive and/or defensive cyber-operations (Li & Daugherty, 2015; Maurer, 2018; Somer et al., 2019). International humanitarian law applies to cyber-warriors regarding the determination of the status of a combatant, under the conditions laid down in Articles 43 and 44 of Protocol I. It is required to demonstrate affiliation to the armed forces of one of the parties to the conflict to obtain such status. An important issue is that cyber-warriors are subject to a specific command – the existence of a subordination relationship. According to Protocol I, the armed forces of the parties to a conflict consist of all armed and organized groups which are under a command responsible to that party. Importantly, the party to the conflict may be represented by a government or an authority not recognized by the opposing party (International Committee of the Red Cross, 1977a). Hence, all non-governmental entities (in the case of cyber activities - private agencies acting on behalf of governmental authorities) that are part of the regular armed forces are covered by international law.

The second condition for a cyber-warrior to be considered a combatant is that he can be distinguished from a civilian, for example, through the appropriate marking of his uniform. The specificity of cyber-activities makes it impossible to identify and recognize an entity physically. However, the provisions of Protocol I point to an exception in the application of the principle described above in a situation where due to the nature of military operations an armed combatant cannot distinguish himself from the civilians. Then such a combatant retains a combatant status under the two conditions – that during each military engagement he carries his arms openly and he is visible to the adversary at the time of a military deployment preceding the launching of an attack (International Committee of the Red Cross, 1977a). If the use of computers, information systems, or computer programs by cyber-warriors is openly considered as carrying weapons, this condition can be considered to meet. It is essential to be aware of the purposefulness of the Protocol. Appropriate, distinctive marking of the uniform of a member of one of the parties' armed forces is an indicator of identification, which is a critical element in identifying the parties to a conflict and attributing responsibility, among other things, for violations of international law by a state entity.

The provisions contained in the supplementary documents to the Fourth Hague Convention and the Fourth Geneva Convention indicate that international humanitarian law applies to all operations, irrespective of the location and nature of the participating entities, provided that the damage threshold is exceeded. Cyber-operations of a military nature resulting in people's injury or death or destruction of critical infra-

structure are therefore subject to international law, regardless of the state or non-state nature of the parties involved. These rules, established in the mid-20th century, are the basis for protecting victims of cyber-attacks and punishing their perpetrators. They also enable states to respond following international standards and take appropriate preventive and protective measures. International humanitarian law assumes that the list of subjects of conflicts and methods of their conduct is open, which excludes the need for the continuous legal regulation of new measures used in external policy. Existing provisions of the law of armed conflicts also prevent the "what is not prohibited is allowed" principle, which poses a threat to the observance of the international ban on the use of force in international relations and towards the international security system in general. Humanitarian law applies regardless of technological changes that arise in the methods and means of conducting an armed activity. That allows for the inclusion under the jurisdiction of international bodies that uphold world peace and security, non-traditional conflicts in the form of the so-called hybrid warfare, and internationalized armed conflicts. Cyber-operations can be part of a more extensive, planned military operation in such specific types of conflicts.

### **Conclusion**

Activities in cyberspace by both state and non-state actors stay under the jurisdiction of international law. Under certain conditions, specific articles of the UN Charter or principles of international humanitarian law can be applied to them. The analysis of individual cases of hostile acts in cyberspace makes possible the identification of ways in which the victim party can respond, in accordance with international law.

The problem that needs to be worked out outside the current norms of international law is attribution of cyber-operations. It is difficult and time-consuming to attribute responsibility to state actors for cyber-actions below the use of force level. In the future, therefore, it will be up to states themselves to define the cyber-security limits of their own critical infrastructure, which will help in establishing international standards for protection against nation-state cyber-operations (Banks, 2017). Defensive actions in cyberspace were officially the part of strategic documents of the biggest state players in the international relations, and for several years, offensive cyber-operations are used to reach national interests too. U.S. National Cyber Strategy (The White House, 2018) and Department of Defense Cyber Strategy (Department of Defense Cyber Strategy, 2018) both emphasize the importance of military cyber defence and offensive capability development to the country's national security. The "strategy of persistent engagement" and the "defend forward" operational concept implemented by Pentagon and the United States Cyber Command (USCYBERCOM) are responses to the hostile activities in cyberspace, particularly those below the threshold of "armed attack" and the "use of force" level.

The article attempts to show that the particular cyber-operations can be classified as an armed attack (in the view of Article 51 of the UN Charter), an attack (in the view of international humanitarian law) or an unlawful use of force (in the view of Article 2(4) of the UN Charter). All these terms are consequence-based, which is one of the main condition to consider certain cyber-operation as an act under the rules of international law. It means that Article 51, 2(4) of the UN Charter and international humanitarian law are applicable to cyber-operations result in effects analogous to those caused by kinetic operations. The issues under consideration include such conditions as: statehood (bearing in mind that statehood is a questionable criterion for the characteristics of modern armed conflicts), exceeding the damage threshold, direct causal link, and military character. This is fundamental to the direction of present and future international competition between states, in view of fact that cyberspace offers much more effective, cheaper, and safer (in the context of establishing an attribution) methods of such competition.

## REFERENCES

1. Banks, W. (2017). State responsibility and attribution of cyber intrusions after Tallinn 2.0. *Texas Law Review*, 95(7), 1487–1513. <https://texaslawreview.org/state-responsibility-attribution-cyber-intrusions-tallinn-2-0/>
2. Department of Defense Cyber Strategy (2018). U.S. Department of Defense. [https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER\\_STRATEGY\\_SUMMARY\\_FINAL.PDF](https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF)
3. Desouza, K.C., Ahmad, A., Naseer, H., Sharma, M. (2020). Weaponizing information systems for political disruption: The Actor, Lever, Effects, and Response Taxonomy (ALERT). *Computers & Security*, 88. <https://doi.org/10.1016/j.cose.2019.101606>
4. Dinstein, Y. (2017). *War, Aggression and Self-Defence*. 6th ed. Cambridge University Press. <https://doi.org/10.1017/9781108120555>
5. Dorn, A.W., Webb, S. (2019). Cyberpeacekeeping: New ways to prevent and manage cyberattacks. *International Journal of Cyber Warfare and Terrorism*, 9(1), 19–30. <https://doi.org/10.4018/IJCWT.2019010102>
6. Efrony, D., Shany, Y. (2018). A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. *American Journal of International Law*, 112(4), 583–657. <https://doi.org/10.1017/ajil.2018.86>
7. Gisel, L., Rodenhauer, T., Dormann, K. (2020). Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross*, 102(913), 287–334. <https://doi.org/10.1017/S1816383120000387>
8. International Court of Justice (ICJ). (1986). Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America). Merits, I.C.J. Reports. <https://www.refworld.org/cases,ICJ,4023a44d2.html>
9. International Court of Justice (ICJ). (1996). Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion. I.C.J. Reports.
10. International Committee of the Red Cross. (1949). *Convention (IV) relative to the Protection of Civilian Persons in Time of War. Geneva, 12 August 1949.*

11. International Committee of the Red Cross. (1907). *Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land*. The Hague, 18 October 1907.
12. International Committee of the Red Cross. (1977a). Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.
13. International Committee of the Red Cross. (1977b). Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977.
14. International Criminal Tribunal for the former Yugoslavia (ICTY). (1995). Prosecutor v. Dusko Tadic aka "Dule" (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction). (IT-94-1). <https://www.refworld.org/cases,ICTY,47fd520.html>
15. Koh, H.H. (2012). International Law in Cyberspace. Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD. *Harvard International Law Journal, Online*, 54, 1–12. [https://harvardilj.org/2012/12/online\\_54\\_koh/](https://harvardilj.org/2012/12/online_54_koh/)
16. Li, J.J., Daugherty, L. (2015). *Training Cyber Warriors. What Can Be Learned from Defense Language Training?* RAND Corporation.
17. Maurer, T. (2018). *Cyber mercenaries: the state, hackers, and power*. Cambridge University Press.
18. Ney, P.C. (2020). Some Considerations for Conducting Legal Reviews of U.S. Military Cyber Operations. *Harvard International Law Journal*, 62, <https://harvardilj.org/2020/11/some-considerations-for-conducting-legal-reviews-of-u-s-military-cyber-operations/>
19. Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35(1), 5–32. <https://doi.org/10.1080/01402390.2011.608939>
20. Rid, T., Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, 38(1-2), 4–37. <https://doi.org/10.1080/01402390.2014.977382>
21. Sandoz, Y., Swinarski, Ch., Zimmermann, B. (Eds.) (1987). *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. International Committee of the Red Cross.
22. Schmitt, M.N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *The Columbia Journal of Transnational Law*, 37(3), 15.
23. Schmitt, M.N. (2011). Cyber Operations and the Ius Ad Bellum Revisited. *Villanova Law Review*, 56(3), 569–606. <https://ssrn.com/abstract=2184850>
24. Schmitt, M.N. (2012a). 'Attack' as a Term of Art in International Law: The Cyber Operations Context. *4th International Conference on Cyber Conflict*, C. Czosseck, R. Otis, K. Ziolkowski (Eds.). Tallinn, 283–293. <https://ssrn.com/abstract=2184833>
25. Schmitt, M.N. (2012b). Classification of Cyber Conflict. *Journal of Conflict and Security Law*, 17(2), 245–260. <https://doi.org/10.1093/jcsl/krs018>
26. Schmitt, M.N. (Eds). (2017). *Tallinn Manual (2.0) on the international law applicable to cyber operations*. Second edition. Prepared by the International Group of Experts at the Invitation of the NATO, Cooperative Cyber Defence Centre of Excellence. Cambridge University Press.
27. Schmitt, M.N., Johnson D.E. (2021). Responding to hostile cyber operations: the "in-kind" option. *International Law Studies*, 97(1), 97–121. <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2951&context=ils>
28. Simma, B., Khan, D., Nolte, G., Paulus, A., (Eds.) (2013). *The Charter of the United Nations (3rd Edition): A Commentary*, Vol. I. Oxford University Press.

29. Somer, T., Ottis, R., Lorenz, B. (2019). Developing military cyber workforce in a conscript armed forces: Recruitment, challenges and options. *14th International Conference on Cyber Warfare and Security*, ICCWS 2019, 413–421.
30. The White House (2018). *National Cyber Strategy of the United States of America*. <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>
31. UN General Assembly (1974). *Definition of Aggression*. (A/RES/3314/XXIX). <https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/IMG/NR073916.pdf>