SAFETY&DEFENSE
ISSN 2450-551X

Nation-State Cyber Operations Legal Considerations: An Estonian Case Study

Agata MAŁECKA

General Tadeusz Kosciuszko Military University of Land Forces, Wroclaw, Poland;
agata.malecka@awl.edu.pl, ORCID: 0000-0002-5519-9681

DOI: https://doi.org/10.37105/sd.139

Abstract

States use cyberspace as one of the platforms for pursuing national interests, also in the context of armed conflict. Due to their inherent purpose, certain principles of international law also apply to the activities of entities (state and non-state) in cyberspace. The main research problem was defined as the following question: under what conditions could the terms in international law be used to describe the events in Estonia in 2007 that imply the possibility of eventual responses or demands by victim parties consistent with international standards? In the article, the events in Estonia in 2007 were compared to existing methods of cyber warfare. The main research methods that were used to achieve the essential objective were: analysis of legal documents and critical analysis of the literature on the subject. 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 defense, Estonia, nation-state cyber operations, prohibition of the use of force

Submitted: 05.07.2021 Accepted: 19.07.2021 Published: 31.12.2021

1. Introduction

In the present day, there is nothing new in states conducting cyber operations. The number of nation-state cyber operations is rising significantly – from 12% in 2018 to 38% in 2020 (Verizon Communications, 2020) and takes many forms. For example, according to terminology that shows how actors can leverage information systems to disrupt political systems, cyber operations can take the forms of disrupting data sources in physical and logical systems, manipulating algorithms used in the processing of signals, manipulating interpretations associated with information, and weaponizing information systems (Desouza et al., 2020).

In this context, it is important not to consider cyber-attacks as an outlaw form of exerting influence in the international environment (Koh, 2012). In cyberspace, we are also dealing with types of acts that can be classified as "armed attacks" and/or unlawful "use of force" under the doctrine of *jus ad bellum* or as "attacks" under the doctrine of *jus in bello*. This is important in terms of the rise of certain legal consequences.

The research aimed at defining the nature of the events in Estonia in 2007 and determining if terms such 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) could be applied. The main research problem was defined as the question: under what conditions could the terms in international law be used to describe the events in Estonia in 2007 that imply the possibility of eventual responses or demands by victim parties consistent with international standards? In the author's opinion, the juxtaposition of international law norms on cyber-attacks with the practice of states using cyberspace to achieve national goals is important for the ability of the affected party to react. The case of Estonia is one of the first examples of the collision of these norms with a real violation of the nation state's cyberspace.

The research methods used in the research process were based on the qualitative analysis of publicly available sources, including a critical analysis of the literature on the subject and analysis of acts of international law. This article does not exhaust the entire broad and complex issue of hostile activities of state and non-state actors in cyberspace. Instead, it represents an attempt to offer an initial, general overview of the issue of state-supported cyber operations classification in international law context (UN Charter and international humanitarian law), based on the example of events in Estonia which is useful for analysts of the international security system and broadly defined international relations.

2. Events in Estonia in spring 2007 – facts, figures, context

Cyber operations that targeted Estonian governmental and private (belonging to banks, schools, media, and citizens) servers took place between April 27 and May 18 2007. The choice of cyberspace as a platform for hostile actions was not accidental. It should be seen in the context of the high level of computerization of Estonian society, which is visible in the percentage of banking transactions conducted over the Internet, which amounted to 95% at that time (Tikk et al., 2010). The nature and intensity of the cyber operations varied throughout the period. The main type of hostile action was DDoS (Distributed Denial of Service) attacks, based on a botnet, suggesting a bottom-up hacker initiative. During the most intense

actions (between 9 and 19 May), about 85,000 infected computers were involved in the operations. At that time, among others, the largest Estonian banks became the target, and one of them – Hansapank – lost the ability to provide online services for a few hours (NATO Strategic Communications Centre of Excellence, 2017). The operations were carried out mainly outside Estonia's territory, so some Estonian banks stopped handling foreign transactions. A technical analysis of hostile actions in the Estonian cyberspace indicated the use of the Russian language and political motivations. That is all the more interesting as detailed instructions on carrying out attacks on Estonian servers and websites appeared on many Russian-language websites and internet forums (Ottis, 2008).

The events in Estonia in the spring of 2007 are not without a political echo. At the same time, the Tallinn authorities decided to move the monument to the Soviet soldiers who died in clashes in Estonia during the Second World War from the center to the nearby military cemetery. Rioting broke out, in which the Russian minority representing nearly 25% of Estonia's population took part. One person died in street clashes, 100 were wounded, and 1,300 were arrested (Rid, 2013). The communication capabilities of social media and other Russian-language websites, which contributed to the radicalization of the Russian-speaking minority's mood, were not without significance. The dates of events also indicate the political background to the operations in Estonia's cyberspace. The second, more technologically advanced wave of cyber operations began on May 4, with its culmination on May 9 – the day of the Russian public holiday commemorating the victory over Nazi Germany (Herzog, 2011).

3. "Armed attack", "attack" and the "use of force" in international relations in the context of cyberspace

The term "cyber-attack" can be used in the context of international law. Moreover, it is important to distinguish between two interpretive approaches: *jus ad bellum* and *jus in bello* (Schmitt, 2012a). *Jus ad bellum* refers to "armed attacks" (which is not the equivalent to the term "use of force", because not all uses of force are armed attacks) and is related to the exceptions to the principle of the prohibition of the use of force set out in the United Nations Charter (Article 51 UN Charter – self-defense and UN Security Council authorization of the use of force). It must be remembered that the provisions of the UN Charter apply only to state entities. The *jus in bello* considers the concept of "attack" as a type of armed operation, covered by international humanitarian law, mainly written in Additional Protocol I to the Geneva Conventions. This distinction is crucial to the response options of the injured party (Schmitt, 2011).

The term "armed attack" includes kinetic military force and should result in effects specific to armed operations – death (or the risk thereof) or injury to persons or damage to or destruction of property and objects. These conditions allow the victim state to respond militarily on the basis on Article 51 of UN Chapter, which describes the conditions of the right to individual or collective self-defense (Schmitt, 2012a). In contrast, the term "attack" describes a military operation covered by the rules of international humanitarian law and is the same as "combat action" referring to physical force. Both "armed attack" and "attack" are consequence-based terms. This means that cyber operations that result in effects analogous to those caused by kinetic armed attacks should also be treated as an armed attacks. The methods of using force are not as significant as their effect – exceeding a certain degree of harm (Schmitt, 2012a).

The prohibition of the use of force in international relations, based on Article 2(4) of the UN Charter, is not the equivalent of "armed attack". The "use of force" may be illegal without exceeding the "armedness" condition. Article 51 of UN Chapter does not apply in this situation and victim-states can use only non-forceful countermeasures (Schmitt, 1999). Article 2(4) of the UN Charter is also applicable in cyberspace, which was confirmed by The International Court of Justice 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 (Legality of the Threat or Use of Nuclear Weapons, 1996). The term "use of force" refers to an armed force (every armed attack is use of force) and includes kinetic force. In addition, use of force can have a non-kinetic character, like arming and training guerrillas (Nicaragua v. United States of America, 1986). The framework for the use of force is not clearly defined, even more so when it comes to cyber operations that do not result in death or injury to persons or damage to or destruction of property and objects. That is why states have adopted informal criteria based on the analysis of the effects of cyber operations – the scope, scale and effects of a cyber operation comparable to an attack by traditional methods. They include severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement and presumptive legality (Schmitt, 2017).

4. The events in Estonia in 2007 – unlawful use of force or cyber-attack from the perspective of international humanitarian law?

The analysis of hostile actions in cyberspace towards Estonia in terms of the appearance of unlawful use of force features requires the confirmation of three essential conditions – state involvement, a military character, and an exceeded damage threshold. These criteria are decisive for the status of unlawful use of force, regulated in Article 2(4) UN Chapter, and apply to operations in cyberspace as well.

Identifying the main actors involved in the conflict is a crucial determinant of their statehood due to Article 2(4) UN Charter, which applies only to states. Unfortunately, meeting this condition is problematic and reduces the effectiveness of the application of international law due to the difficulty in determining the nature of the parties involved in present-day conflicts. Moreover, the dominant trends in the area of armed conflicts clearly point to their "de-nationalization" – in 2019, only 2 out of 54 active state-based conflicts have been interstate in nature (Pettersson & Öberg, 2020). Therefore, the term "new war" is increasingly often used in relation to contemporary armed conflicts to describe a new type of violence, characteristic of privatized, informal, internal, and low-intensity conflicts of the late 20th and early 21st centuries (Kaldor, 2012).

The state character of participating entities is ambiguous and often impossible to demonstrate (Goldsmith, 2013). The aspect of statehood is also debatable in the case of cyberspace. Enemy cyber activities in Estonia in 2007 are a perfect example of that. The Kremlin officially opposed the blaming of the Russian authorities for hostile actions in Estonia's cyberspace, attributing the initiative to hackers acting on private grounds.

Undoubtedly, the cyber operations in Estonia were connected with the relocation of the monument to Soviet soldiers to the military cemetery on the outskirts of Tallinn and had a political background. Moscow took these actions as disrespect for the Red Army soldiers killed there. At the same time, Russia denied its participation in hostile cyber activities. Nonetheless, all events accompanying the aggression in cyberspace signaled Russian activity. High Estonian state officials officially pointed to at least Moscow's indirect involvement: "IP addresses have helped to identify that the cyber terrorists' attacks against the Internet

pages of Estonian government agencies and the Office of the President have originated from specific computers and persons in Russian government agencies, including the administration of the President of the Russian Federation" (Government Office of Estonia, 2007). Why, then, can the statehood criterion, which would determine whether events in Estonia in 2007 are an unlawful use of force, not be considered to be fulfilled? That is due to the specificity of activities in cyberspace, which makes it challenging or impossible to identify the culprit, despite the identification of methods and tools. The reasons why there would be a possibility to attribute the perpetration of hostile cyber operations against Estonia to Russia are not entirely credible. For example, evidence in the form of the IP addresses of the computers from which the attacks were made and which were located in Russia can be questioned. The fact that hackers used botnets infected with malicious software as the main method of operations resulted in computers all over the world being taken over and used for hostile actions. As Dmitry Peskov, First Deputy Press Secretary of the Russian President in 2004-2008, said: "[There is] no way the [Russian] state [could] be involved in cyber terrorism [...]. When one looks at the IP addresses showing where the attacks are coming from, there is a wide selection of states from around the world. However, it does not mean that foreign governments are behind these attacks. Moreover, as is probably known, IP addresses can be fake" (BBC News, 2007). In a situation where the Kremlin officially opposes blaming Russia for the destabilization of Estonia's cyberspace, the condition of the state character of the initiator of cyber operations is entirely questionable. Similary, the condition of the military character – another of the criteria used to define the use of force in international relations.

The involvement of military actors in cyber operations in Estonia cannot be proved. While Moscow's inspirational and mobilizing role in the political dimension is distinct, the participation of Russian secret services in the events in Estonia in 2007 is not evident. On many occasions, accusations of controlling botnet networks to achieve political goals, including the initiation of DDoS attacks on the websites of Russian opposition parties, led by Garry Kasparov, were directed at the Russian authorities. The event took place a few weeks before the cyber operations in Estonia, and Arbor Networks – a company tracking DDoS-type activity in the network – confirmed the participation of the same botnet elements in both operations (Davis, 2007). Contrary to the Kremlin's official position, Russian oppositionists reported specialized government units initiating aggressive actions in cyberspace. According to Denis Bilunov, the United Civil Front executive director: "There is a specific department within the FSB – the successor to the KGB – that specializes in coordinating Internet campaigns against those they consider a threat. They have attacked Chechen rebel sites, us, and now it appears they have attacked Estonia" (Davis, 2007). However, there are doubts again about the qualification of governmental actions of individuals carrying out tasks in cyberspace as activities involving features of either cyber conflict or cyber espionage. The latter type of state operation in cyberspace is not regulated by international law unless it is part of armed conflict (Schmitt, 2017).

With regard to determining the degree of harm necessary for an act to be considered as an unlawful use of force, it is fundamental to analyze whether the criteria of severity and invasiveness are met. Although people have not been killed or injured as a result of cyber operations in Estonia, hostile actions have had a negative impact on Estonian society as a whole, especially when considering its rate of computerization. The effects of the aggressive acts in Estonian cyberspace have manifested themselves in physical form and cannot be regarded as "common" methods of exerting political pressure. The question is to what extent, as a result of cyber operations, have the state's essential interests been affected and has the functioning of the state's critical infrastructure been disrupted to the extent that it would have been in the case of an invasion by "traditional" methods? The activities of hackers in Estonian cyberspace did not cause any disruption to the functioning of the military, energy, or transport systems. The loss of Estonia's image as the leading country in transforming a

former Soviet republic into a modern and computerized country can be discussed. However, this is not a key area of the functioning of the state.

Looking at the criteria of immediacy and directness, there are circumstances under which the events in Estonia can be considered as a use of force. The most significant losses occurred in the banking sector due to the blockade of services of Estonia's largest bank for several hours. Government websites also became non-functional. The lack of ability to perform essential functions of a financial (banking) or social nature (blocking access to social benefits) demonstrates the immediacy and directness of the cyber operations under study (Schmitt, 2011). On the other hand, it is impossible to establish a direct link between hostile actions in Estonian cyberspace and the injured and the one person killed. There are also doubts about fully meeting the immediacy criterion because of the nature of cyber incidents, which are part of a more general operation with political and national roots. The economic impact of cyber operations in Estonia, especially in the private sector, is even more challenging to be determined. However, it should be kept in mind that, in the context of the finding of violations of the ban on the use of force in international relations, the impact of cyber operations on non-state actors is not taken into account (Schmitt, 2017).

In addition, the damage caused by cyber operations in Estonia in 2007 is unmeasurable due to the denial of service technique, which is characterized by a lack of access to a network service as a result of flooding the network with huge amounts of data. If the methods used resulted in the destruction of data, the range of damage would be easier to measure.

Considering the previous analysis of the terms "use of force" and "armed attack", some researchers concluded that the cyber operations in Estonia in major aspects exceeded the degree of harm and could be considered by the international community as an unlawful use of force (Schmitt, 2011; Buchan, 2012). However, a necessary condition for this recognition would have to be Russia's indisputable and unequivocal responsibility. Furthermore, under Article 2, paragraph 4 of the UN Charter, the recognition of the use of force is based on a finding of material damage (property, death, or injury). In this context, consideration should be given to ethical controversies concerning the possibility of classifying cyber-attacks as forms of informational violence going beyond physical borders and subject to international law (Haataja, 2017).

Another issue is the analysis of the events in Estonia in 2007 from the point of view of the legitimacy of using the term "attack" in *jus in bello* terms and the necessity of applying the principles regulated by international humanitarian law. The interpretation of the term "act of violence" is a key factor in determining whether an act was an attack or not. Acts of violence include not only physical force but also the neutralization of objects in order to gain military advantages. The term "military" also plays an important role. The rules of international humanitarian law (e.g. requirement to take precautions in attack) concern attacks on military targets. All attacks on civilian objects are unlawful. In this context, using the term "cyber-attack" to describe the events in Estonia would seem reasonable, regardless of the state or non-state nature of the aggressors. However, in reference to Additional Protocol II, non-international groups conducting attacks should be organized and "under responsible command" (Protocol I, art. 1, 1977), which did not occur in the case of Estonia.

5. Events in Estonia in 2007 – an attempt to classify

An analysis of the events in Estonia in 2007 led to the conclusion that they cannot be considered as use of force in international relations (even more so as an armed attack) within the meaning of the *jus ad bellum*, mainly because of the difficulty of determining the state

character of the actors involved. For the same reason, the term "cyber war" should not be used to describe cyber-attacks in Estonia (or use it only as a descriptive, non-legal term).

Nor can the events in Estonia be categorized as a cyber conflict under international humanitarian law. The distinction between international armed conflicts and non-international armed conflicts is not essential. It is more important to analyze the term "organized", "armed" and "protracted" (the degree of the organization of the of participating groups), because non-international conflicts are described as "protracted armed violence between governmental authorities and organized armed groups or between such groups within a State" (Prosecutor v. Dusko Tadic aka "Dule", 1995). Cyber operations, like these in Estonia, conducted by individuals, are not included in non-international armed conflicts – they were neither conducted by organized nor an armed group.

The organization criterion is related to the possibility of undertaking military activities in a coordinated manner in accordance with the goals of the group, not individuals. Thus, to talk about a non-international cyber conflict under international humanitarian law, its parties should be characterized by a certain degree of organization, measured by factors such as formal command structure, mission planning, issuance of orders, imposing discipline (Schmitt, 2012b). The cyberspace environment does not exclude such organized groups – virtual leadership can function without the physical inherence of its members, but not without concentration of all fellows to achieve the group's goals.

A group should be militarily active to be "armed", this means the existence of a purpose of carrying out armed activities. Conducting "attacks" should be the primary goal of an armed group. Therefore, as long as individual group members carry out attacks on their own and not on the group behalf, the armed criterion cannot be met (Schmitt, 2012b).

There is also difficulty in finding "protraction" in the Estonian case. International law stipulates a few factors which could give an answer to whether the conflict was or was not "protracted" – intensity and gravity of the attacks, the collective character of the warfare, the need to increase forces in the face of the ongoing crisis (Schmitt, 2012b). In the context of cyberspace, it is also important to determine the time over which the hostilities have taken place. Cyber-attacks do not need to be continuous, but they should be frequent and related to be considered as "protracted". In other words, protracted cyber-attacks have to occur regularly over time (Schmitt, 2012b).

Given that only a political, planned, and deadly act of violence in cyberspace can be considered a symptom of cyberwar (with the criterion of statehood) or a cyber conflict, such forms of fighting in cyberspace did not occur in Estonia. It is highly probable that they will not appear in the near future either (Rid, 2012). In addition, there are doubts about the effectiveness of cyber operations (in situations when they are part of a larger military operation) as a tool that significantly impact the battlefield area (Kostyuk & Zhukov, 2019). So if the events in Estonia in 2007 were not a cyber conflict, how can they be named and qualified?

Cyber operations in Estonia were one of the examples of using cyberspace to achieve national goals by the state (Chung, 2018). Nowadays, it is a well-known method of political struggle for some international state actors. Analyzing the Cyber Operations Tracker (tool made by Council on Foreign Relations, which shows the scope of publicly known state-sponsored cyber incidents since 2005), it can be found that cyberspace is the main domain to achieving nationals goals for some countries (https://www.cfr.org/cyber-operations/). In the 2005-2020 period, the five most active states (China, Russia, Iran, North Korea, United States) suspected for sponsor cyber incidents were involved in almost 400 cyber operations targeted different sectors. It should be noted that those data is most likely heavily underestimated, because of basing on publicly available reports and including cyber incidents affecting states where English is widely spoken. In 2020, there were sixteen registered and publicly known cyber operations which could be treated as sponsored by Russia Federation.

Moscow has found a way to move the competition from domains where adversaries (mainly U.S.) have an advantage (military, economic and diplomatic sphere) on a domain where the opponents' strength is not dominant (cyberspace). In this way, the "Russia's Indirect Grand Strategy" is implemented (Clark, 2019). Modern cyber operations launched or supported by Russia are a continuation of the methods of penetrating the other countries' cyberspace initiated in the 21st century. Estonia was one of the first examples, and it is clear that cyber operations in this country were aimed at political destabilization. Since then, Russia has developed a specific cyber operations toolbox – selection of targets, techniques used and the long-term nature are based on Russia's interests and intelligence needs (e.g. GRU cyber operations against the World Anti-Doping Agency (WADA) in September 2016 and International Olympic Committee (IOC) in January 2018) (Estonian Foreign Intelligence Service, 2018).

On the one hand, Estonia became a place to try and present Russian capabilities of conducting cyber operations. On the other hand, it was a testing ground for the other players' response to cyber operations (especially U.S., Alliance and the EU). In the context of international law, the character and methods of responding are the key issues, as they depend on the classification of a particular cyber operation as either an "attack" or an "armed attack".

6. Conclusion

The study was aimed at demonstrating that the events in Estonia in 2007 cannot be classified as an armed attack (in the view of Article 51 of the UN Charter) and unlawful use of force (in the view of Article 2(4) of the UN Charter). In the first case, the cyber operations in Estonia did not meet the criteria of an "armed attack". In the second, despite likely exceeding the degree of harm, they did not meet the criterion of state involvement. Presumably, cyber operations in Estonia could be called an "attack" in the sense of *jus in bello*, which would mean that they are subject to the rules of international humanitarian law. However, in contradiction to this statement lie the international principles outlining the "profile" of non-state actors in armed conflict, highlighting the organized and armed character of groups conducting cyber operations.

The problematic case of Estonia leads to a search for other solutions to its possible classification. It seems that Estonia has become the first place where a non-state entity (Russian hackers) has achieved the policy objectives of the external state entity (the Kremlin). As the present-day shape of cyber operations shows, cooperation between these two actors in performing cyber operations is a real and challenging threat to be eliminated for contemporary international relations. Despite the fact that the scope and harmfulness of cyber operations are still growing, states do not decide on armed self-defense, which is not only due to attribution problems. Nevertheless, the issues of nation-state cyber operations are changing dynamically, in contrast to the norms of international law.

Declaration of interest

The author declares that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

References

1. BBC News. (2007, May 17). *The Cyber Raiders Hitting Estonia*. http://news.bbc.co.uk/2/hi/europe/6665195.stm
2. Buchan, R. (2012). Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? *Journal of Conflict and Security Law*, *17*(2), 212–227. https://doi.org/10.1093/jcsl/krs014
3. Chung, J. J. (2018). Nation-states and their cyber operations in planting of malware in other countries: Is it legal under international law? *University of Pittsburgh Law Review*, *80*(1), 33–67. https://doi.org/10.5195/lawreview.2018.593
4. Clark, J. R. (2019). Russia's Indirect Grand Strategy. *Orbis – A Journal of World Affairs*, *63*(2), 225–39. https://doi.org/10.1016/j.orbis.2019.02.002
5. Davis, J. (2007, August 21). *Hackers Take Down the Most Wired Country in Europe*. Wired. https://www.wired.com/2007/08/ff-estonia/
6. 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
7. Estonian Foreign Intelligence Service. (2018). *International Security and Estonia 2018*. https://www.valisluureamet.ee/doc/raport/2018-en.pdf
8. Goldsmith, J. (2013). How Cyber Changes the Laws of War. *The European Journal of International Law*, *24*(1), 129–138. https://doi.org/10.1057/9F781137455550_4
9. Government Office of Estonia. (2007, May 1). *Declaration of the Minister of Foreign Affairs of the Republic of Estonia*. Government Communication Unit, Government Office of Estonia. https://www.valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia
10. Haataja, S. (2017). The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. *Journal Law, Innovation and Technology*, *9*(2), 159–189. https://doi.org/10.1080/17579961.2017.1377914
11. Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, *4*(2), 49-60. http://dx.doi.org/10.5038/1944-0472.4.2.3
12. Kaldor, M. H. (2012). *New & old wars: organized violence in a global era*. Stanford University Press.
13. Koh, H. H. (2012). International Law in Cyberspace. *Harvard International Law Journal*, *54*, 1–12. https://harvardilj.org/2012/12/online_54_koh/
14. Kostyuk, N., & Zhukov, Y., M. (2019). Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? *Journal of Conflict Resolution*, *63*(2), 317–347. https://doi.org/10.1177/0022002717737138
15. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Rep. 1996. https://www.refworld.org/cases,ICJ,4b2913d62.html
16. NATO Strategic Communications Centre of Excellence. (2017). *Hybrid Threats: 2007 cyber attacks on Estonia*. https://www.stratcomcoe.org/hybrid-threats-2007-cyber attacks-estonia
17. Nicaragua v. United States of America, I.C.J. Rep. 14 (1986). https://www.refworld.org/cases,ICJ,4023a44d2.html
18. Ottis, R. (2008). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

19. Pettersson, T., & Öberg, M. (2020). Organized violence, 1989–2019. *Journal of Peace Research*, *57*(4), 597–613. https://doi.org/10.1177/0022343320934986
20. Prosecutor v. Dusko Tadic aka "Dule", Case No. IT-94-1 Int. Crim. Trib. for the Former Yugoslavia (1995). https://www.refworld.org/cases,ICTY,47fdfb520.html
21. Protocol Additional to the Geneva Conventions of August 12 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977.
22. 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
23. 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
24. 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), XV.
25. Schmitt, M. N. (2011). Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review*, *56*(3), 569-606. https://ssrn.com/abstract=2184850
26. Schmitt, M. N. (2012a). *'Attack' as a Term of Art in International Law: The Cyber Operations Context*. https://ccdcoe.org/uploads/2012/01/5_2_Schmitt_AttackAsATermOfArt.pdf
27. 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
28. Schmitt, M. N. (Ed.). (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*. Cambridge University Press.
29. Tikk, E., Kaska, K., & Vihul, L. (2010*). International Cyber Incidents: Legal Considerations*. Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf
30. U.N. Charter art. 2, para. 4.
31. U.N. Charter art. 51.
32. Verizon Communications, Inc. (2020). *The Verizon Business 2020 Data Breach Investigations Report*. https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf