DOI:10.33179/BSV.99.SVI.11.CMC.19.3.5

Pika Šarf

ZAKONITOST NIZKOINTENZIVNIH KIBERNETSKIH OPERACIJ PO MEDNARODNEM PRAVU

LEGALITY OF LOW-INTENSITY CYBER OPERATIONS UNDER INTERNATIONAL LAW

Povzetek Namen tega prispevka je obravnava mednarodnopravne ureditve nizkointenzivnih kibernetskih operacij. Čeprav mednarodna skupnost soglaša, da mednarodno pravo ureja ravnanje držav v kibernetskem prostoru, ni popolnoma jasno, kako se veljavna pravila mednarodnega prava uporabljajo v kibernetskem kontekstu. Večina pravnih strokovnjakov in strokovnjakov za nacionalno varnost ter vojaških strategov se je osredotočila na kibernetske operacije, ki dosegajo prag oboroženega spopada ali uporabe sile, vendar pa je le nekaj kibernetskih operacij v preteklosti ta prag tudi v resnici doseglo. Kibernetske operacije nižje intenzivnosti prevladujejo v kibernetskih odnosih med državami. Pri analizi skladnosti nizkointenzivnih kibernetskih napadov z veljavnimi pravili mednarodnega prava, zlasti z načelom ozemeljske suverenosti in načelom nevmešavanja, se članek opira na ugotovitve mednarodne skupine strokovnjakov, ki je pripravila t. i. Talinski priročnik uporabnega prava za področje kibernetskih operacij, in na mnenja drugih priznanih pravnih strokovnjakov.

Ključne besede ***Kibernetska operacija, mednarodno pravo, načelo ozemeljske suverenosti, načelo neintervencije.***

Abstract The purpose of this article is to discuss the international law regulation of low-intensity cyber operations. Although the international community agrees that international law governs the conduct of states in cyberspace, it is not entirely clear how the existing norms of international law apply in the cyber context. The majority of legal scholars, as well as national security experts and military strategists, have focused on cyber operations that reach the threshold of either armed attack or use of force; however, few cyber operations in the past have actually risen to that level. Cyber operations of lower intensity prevail in state cyber interactions. While analyzing the accordance of low-intensity cyber operations with the existing norms of international law, in particular with the principle of state sovereignty and non-intervention, the article

leans on the findings of the International Group of Experts which developed the Tallinn Manual on International Law Applicable to Cyber Operations, and writings of other recognized legal scholars.

Key words ***Cyber operation, international law, principle of territorial sovereignty, principle of non-intervention.***

Introduction

In the wake of the new millennium the prevailing assumption of the international community was that cyberspace presented a new threat, which would change not just the future of international conflicts but international relations in general. The world awaited an inevitable cyber-attack of apocalyptical dimensions that would cripple critical infrastructure and the economy. Cyber war was coming.

However, cyber war never happened. On the other hand, cyber operations of lower intensity are relatively common. The military employs a wide variety of cyber operations, both in the context of armed conflict and in times of peace, which serve various goals, from information gathering, deception and deterrence to disruption and destruction (Gill, 2016). The vast majority of military cyber operations do not meet the threshold of use of force or armed attack; however, this does not necessarily mean that they are legal under international law.

This article will examine how the focus of the international community and legal scholars has shifted from cyber war to low-intensity cyber operations. It will further provide an overview of the international law regime governing low-intensity cyber operations, arguing that although they fall below the threshold of use of force and armed attack, they may nevertheless violate other principles of international law, in particular principles of territorial sovereignty and non-intervention.[1] This article leans on the findings of the International Group of Experts that prepared the Tallinn Manual of International Law Applicable to Cyber Operations, and writings of other recognized legal scholars.

Apart from normative uncertainty, the cyber-realm is also facing a terminological gap, since the international community has failed to define any cyber-related terms. In the absence of shared definitions, different states and institutions understand terms differently, which makes debate at the international level particularly difficult (NATO CCDCOE, Cyber Definitions). The term cyber operation itself is poorly understood. The Glossary of the Tallinn Manual states that a cyber operation is the employment of cyber capabilities with the primary purpose of achieving objectives in or through cyberspace (Schmitt, 2013, p. 258). In the present article the term low-intensity cyber operations will only refer to cyber operations falling below the threshold of use of

[1] *Low-intensity cyber operations may also violate other international law norms, for example, human rights (in particular the right to privacy and freedom of expression) or norms relating to diplomatic and consular relations, but, due to the spatial limitations, the present article will only concentrate on violations of the principles of state sovereignty and non-intervention.*

force, although some authors also use this term for cyber operations amounting to the use of force below the threshold of armed attack.

1 FROM CYBER WAR TO LOW-INTENSITY CYBER OPERATIONS

In the late 1990s, cyber operations began to draw the attention of international legal scholars, as well as national security experts and military strategists. Arquilla and Ronfeldt wrote in their article, "Cyberwar is coming!", that "the information revolution will bring the next major shift in the nature of conflict and warfare" (1993, p. 143). In 2012, the Secretary of Defense of the United States and a former Director of the CIA, Leon E. Panetta, warned that "these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life" (Panetta, 2012). But he was far from being the only one to use such cyber doom rhetoric in the cyber security debate. Others have compared cyber attacks to the 9/11 terrorist attacks, major natural disasters or even nuclear weapons (Lawson, 2016). It is therefore not surprising that the entire legal community, fearing that states would in the near future engage in cyber warfare, focused their attention almost exclusively on cyber attacks amounting to either armed attack or use of force.

However, more than 25 years have passed since "cyber Pearl Harbor" was mentioned for the first time, but it still has not happened and it is highly unlikely that it will happen in the near future.[2] Regardless of all evidence that supports the opposite, some scholars are still asserting that the world is already in a state of cyber war.[3] Indeed, states and individuals alike are daily targeted by cyber attacks, but such attacks almost always fall within the categories of either cyber crime or cyber espionage. In fact in 2016, only 4.3% of all cyber attacks were conducted in relation to war or caused physical damage approaching the use of force. However, it must be noted that the number of such attacks almost doubled since 2015[4] (Passeri, 2016).

On the other hand, cyber operations of low intensity are quite common in state cyber interactions. Estonia gained the attention of global community in 2007, as it became the first country targeted by a series of low-intensity cyber attacks. Following the relocation of the Soviet memorial of the Bronze Soldier, the websites of the Estonian Parliament, Ministries, political parties, banks, news and broadcasters suffered

---

[2] *A comprehensive list of cyber attacks perpetrated by different states, which includes information about the targeted state or institution within a state, the alleged source of the attack and a description of the event, is included in the Appendix in: Shakelford S. J., 2014. Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. New York: Cambridge University Press.*

[3] *Dearden L., 2017. World Heading Towards 'Permanent Cyber War', France Warns. http://www.independent.co.uk/news/world/europe/cyber-war-world-warning-france-criminals-extremists-russia-countries-guillaume-poupard-anssi-a7767886.html, 23 August 2017; Ferguson N., 2017. Cyber War I has Already Begun. https://www.bostonglobe.com/opinion/2017/03/13/cyber-war-has-already-begun/dYE1vkpT1W3zKdhjxwH1QP/story.html, 23 August 2017.*

[4] *The share of cyber attacks falling within the category of "Cyber Warfare" was 2.4% in 2015.*

from various forms of distributed denial of service attacks (DDoS)[5] that prevented access to and defaced websites, as well as halting e-mail traffic. Considering the duration of the DDoS attack and Estonia's high reliance on information systems, the attack posed a significant threat; however, it resulted in mainly economic and communications disruptions (Czosseck, 2011; Watts, 2011). In 2008 Georgia was similarly attacked by a series of DDoS attacks, which coincided with the Russian military invasion and lasted for almost a month, much longer than the invasion and even postdating a ceasefire (Watts, 2011). Far less known is an attack on Azerbaijan in 2012 in which websites of government institutions and news agencies were hit by a politically motivated cyber attack by a group of hackers called "the Armenian Cyber Army" (UN Doc. A/66/897, 2012). These cyber incidents in Estonia, Georgia and Azerbaijan were undoubtedly wake-up calls for the international community on the new threats emerging from cyberspace.

Both state and non-state actors will in the future most likely engage in low-intensity cyber attacks, since they are tactically and strategically attractive for numerous reasons. A low-intensity cyber operation is unlikely to provoke a response from a target, especially because the target will not always be aware that an attack has happened at all. Even if the attack is detected, states employing low-intensity cyber operations spread the effects of the operation by attacking various targets over long periods of time, so the attacks appear random and unrelated. Watts therefore compares low-intensity cyber operations to death by a thousand cuts (Watts, 2011). Moreover, cyber operations are usually far cheaper than traditional military operations. The technology required is widely available and inexpensive, which also enables the cooperation of non-state actors, such as cyber militias, offering services for profit or political advantage (Ibid.). For all of these reasons low-intensity cyber operations are no longer used only by cyber criminals and cyber terrorists, but are becoming a powerful means for states to achieve a wide variety of political, military and economic goals and to project national power.

2 OVERVIEW OF MILITARY INVOLVEMENT IN THE CYBER DOMAIN

The internet, one of the main components of cyberspace, was designed by the US Department of Defense Advanced Research Project Agency (ARPA, later known as DARPA) as a Cold War military project that would provide a decentralized communications system which would enable communication even if the Soviet Union successfully destroyed the telephone system. The result of this project was ARPANET, the first predecessor of the modern internet, which consisted of only four computers. In its first two decades it was primarily used in the academic environment as a tool to exchange ideas and knowledge. For security reasons the network split into two domains in 1983: ARPANET remained the network of academia and later

[5] *In a distributed denial of service attack, an attacker attempts to make an online service unavailable to its users by overwhelming it with traffic from different sources, which makes it impossible to stop the attack by simply blocking a single IP address.*

became the internet as we know it today,[6] and MILNET evolved into a network devoted entirely to military communications (Naughton, 2016).

For a very long time military engagement in the cyber domain was mostly seen through the prism of its involvement in the development of the internet, and cyberspace was considered as the military's new and safe communications system capable of surviving a devastating attack. However, in one very early case malicious code was used as a real cyber weapon, which is still considered probably the most damaging cyber operation to date, even though it was perpetrated by the CIA and not by the military. In 1982 CIA agents covertly provided the Soviet Union with infected SCADA software, which they desperately needed in order to operate their newly built Urengoy-Surgut-Chelyabinsk pipeline. The software infected the control systems, which resulted in a massive explosion, comparable to the blast of a small nuclear device (Rid, 2012). During the Kosovo crisis in 1999 it became clear that cyber operations would play an important part in international conflicts in the future. Just three days after NATO air strikes began, NATO websites, servers and the cyber infrastructure of NATO member states were the target of a coordinated cyber attack in order to disrupt NATO communications systems (Shackelford, 2014). According to US officials, the United States also resorted to cyber operations during the crisis, but refrained from launching a more aggressive attack that would destabilize the Serbian leader Slobodan Milošević, mostly because they were "worried about the legal implications of launching the world's first cyber war" (Borger, 1999; Ibid.).

However, cyberspace as such was still not seen as a war-fighting domain. It was not until during the international conflict between Georgia and Russia in 2008, when cyber operations were launched alongside conventional kinetic operations, that the international community realised that cyberspace is a domain in which you can engage with and defend against an adversary (Ziolkowski, 2013). In 2011 the United States became the first country to officially recognise cyberspace as the fifth operational domain, along with land, sea, air and space (DoD Strategy for Operating in Cyberspace, 2011). More importantly, NATO recognized cyberspace as a domain of operations during the Warsaw Summit in 2016. Representatives of NATO states and other nations, including Montenegro, Ukraine, Georgia, and Russia, agreed, that "[they] recognize cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea" (Warsaw Summer Communiqué, 2016).

In the last few years states have been urging the development of military capabilities in cyberspace, which could be compared to past cases of arms races (Craig, 2016). The militarization of cyberspace is evident from strategic documents and increasing investment in cyber military capabilities. Research conducted by the United Nations

[6] *ARPANET was officially decommissioned in 1990, when the network became privatised with commercial companies called Internet Service Providers controlling and operating the network. The creation of the World Wide Web and a graphical browser that was easy to use were the final steps towards the internet as we know it today.*

Institute for Disarmament Research showed that, in 2012, 114 UN Member States had cyber security programmes, and 47 of these gave some role to the armed forces (UN Doc. UNIDIR/2013/3, 2013). While defence is the primary goal of the majority of cyber security programmes, there are a great number of states capable of launching an offensive cyber operation.[7] One of the main reasons the number is higher each year is that it is very hard to protect against vulnerabilities in cyberspace; meanwhile, detecting and exploiting them is considerably easier. General Michael Hayden, the former director of the NSA and the CIA, stated that "we have built the internet in such a way that it's very hard to defend it. It's built on openness. It's built on access. It's built on agility. None of those things help the defense" (Hayden, 2010).

3 LEGALITY OF LOW-INTENSITY CYBER OPERATIONS

Neither the international community nor legal scholars agree completely on how the existing rules of international law, including the principles of territorial sovereignty and non-intervention, apply to states' behaviour in cyberspace. In the absence of any cyber-specific customary or treaty law, the opinions of recognized international scholars are of the utmost importance.[8] Among dispersed academic debate, the Tallinn Manual on the International Law Applicable to Cyber Warfare, and its follow-up project, the Tallinn Manual on International Law Applicable to Cyber Operations (Tallinn Manual 2.0), which were written by an International Group of Experts on the initiative of the NATO Cooperative Cyber Defense Centre of Excellence, must be mentioned as the key contributions in clarifying the current state of international law as it applies to cyberspace.

The following section will briefly explain the international law principles of state sovereignty and non-intervention, and it will continue by addressing the question of when those principles are violated by state conduct in or by using cyberspace.

3.1 Low-intensity cyber operations and the principle of state sovereignty

The principle of state sovereignty and its correlate, the principle of non-intervention, are fundamental principles of international law. In its first judgment the International Court of Justice noted that "between independent states, respect for territorial sovereignty is an essential foundation of international relations" (Corfu Channel, 1949, p. 35).

The principle of territorial sovereignty gives a state the exclusive right to exercise its powers in the territory of a state, which includes land territory within state

[7] *States believed to be in a possession of offensive cyber capabilities are the United States of America, Israel, Russia, China, Iran, the United Kingdom, Australia, Canada, Denmark, Sweden and the Netherlands.*

[8] *It must be noted, that according to Article 38 (1)(d) of the Statute of the International Court of Justice, which is universally recognized as the definitive statement of sources of international law, teachings of distinguished scholars, just like judicial decisions, are not regarded as a source of international law, but as a subsidiary means for the determination of international law (Statute of the International Court of Justice, 1945).*

boundaries, internal waters, territorial sea, the air space above the territory, and the subsoil beneath it (Military and Paramilitary Activities in and against Nicaragua, 1986, §212). Judge Max Huber noted in the Island of Palmas case that "sovereignty in the relations between states signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other state, the functions of a state" (Island of Palmas, 1928, p. 838).

Before addressing the question of the legality of low-intensity cyber operations, we must understand that the international community and legal scholars have not always agreed whether existing rules of international law apply to states' behaviour in cyberspace. In the early days of the internet many scholars argued that the internet could not and should not be regulated, while others advocated self-regulation instead of state regulation. Later, legal scholars advocated that cyberspace is a common heritage of mankind or *res communis omnium*, much like the high seas or outer space, and is therefore an area outside the sovereignty of states subjected to a specific regime of regulation and exploitation (Segura Serano, 2006). Today the international community agrees that the norms of public international law, including the UN Charter, also apply to state conduct in cyberspace[9] (Schmitt, 2013; UN Doc. A/68/98, 2013; UN Doc. A/70/174, 2015). International law has the ability to address in a timely manner the challenges posed by new technologies, such as cyberspace, through the interpretation of the established international norms. Since the interpretation reflects the contemporary values of the international community, international law evolves as the values in the community change (Schmitt, 2013). Therefore, although the application of international law to cyberspace is undisputed, the interpretation of these norms in order to understand their exact scope will need some additional clarification.

Although cyberspace is a non-physical, virtual space, it is nevertheless a man-made environment that requires physical architecture to exist, and as such can be subject to state regulation (Buchan, 2016). Cyberspace can be described by using three interconnected layers[10]:

1. *A physical layer:* physical cyber infrastructure used to communicate and connect (hardware and other physical network components);
2. *A logical (virtual) layer:* software, data and protocols that allow the exchange of data across the physical layer across various geographical locations;
3. *A social layer:* individuals and groups as part of cyberspace (Gill, 2016; Schmitt, 2017).

---

[9] *Not all states agree that the whole body of public international law applies to cyberspace and therefore cyber operations. China and Russia, for example, oppose the applicability of international humanitarian law (Schmitt, 2014).*

[10] *Sometimes this multi-layered system is also seen as consisting of five layers, with an additional cyber persona layer, which enables people to connect to the logical layer (e.g. e-mail addresses, social media accounts) and a geographical layer, which is the location of the physical layer (Gill, 2016).*

States may not claim sovereignty over cyberspace *per se*, but they enjoy sovereignty over cyber infrastructure located on their territory, as well as activities associated with that infrastructure (Schmitt, 2017; Von Heinegg, 2012). As a consequence, states have the right to enforce domestic legislation and to protect cyber infrastructure and safeguard cyber activities that are located in or take place in their territory, regardless of whether the cyber infrastructure belongs to the government, private entities or individuals, or the purposes it serves (Schmitt, 2017). On the other hand, states also bear an obligation to prevent their territory or cyber infrastructure under governmental control to be used to violate the rights of or produce detrimental effects on other states.[11] State regulatory power extends beyond the physical layer, which understandably falls under state sovereignty. Cyber activity of both legal and natural persons located in the territory of a state may also be regulated, and the state may prohibit or restrict certain online content in accordance with other applicable international law norms[12] (Ibid.).

As a result of states exercising territorial sovereignty over the physical layer of cyberspace located in their territory, some authors believe that any cyber attack on cyber infrastructure located in the territory of a foreign state violates its territorial sovereignty (Buchan, 2016; Ohlin, 2015). In support of that theory they argue that in the cyber context physical damage is irrelevant, since a cyber operation may have perceptible effects even though they are not physical in nature (Ziolkowski, 2013). The majority, however, do not agree with this wide interpretation of the rule. The International Group of Experts that prepared the Tallinn Manual 2.0 analyzed in detail which cyber operations constitute a violation of state sovereignty.

State sovereignty is violated in the event that a cyber operation results in physical damage or injury (Schmitt, 2017). The Stuxnet virus, which caused substantial damage to the centrifuges in the Iranian uranium enrichment facility at Natanz by changing the rotor speed, would therefore constitute a clear violation[13] (Buchan, 2012). A cyber operation that interferes with the functions of a foreign state which are inherently governmental in their nature also amounts to a violation of state sovereignty. On the other hand, a cyber operation that results in the loss of functionality of cyber infrastructure located in a foreign territory in some cases constitutes a violation of state sovereignty; however, in the absence of sufficient *opinio juris* it is not settled precisely when this threshold is reached (Schmitt, 2017).

---

[11] *The duty of due diligence is a general principle of international law deriving from the principle of sovereignty of states, which has been confirmed in many cases of the International Court of Justice, most famously in the Corfu Chanel Case in which the Court stated that "every state has the obligation not to knowingly allow its territory to be used for acts contrary to the rights of other states" (Corfu Chanel, 1949, p. 22).*

[12] *Special attention should be paid to the freedom of expression enshrined in Article 19 of the International Covenant on Civil and Political Rights, which may be subject to restrictions only if certain conditions stipulated in Article 19(3) are fulfilled. Restrictions on the operation of websites, blogs or any other internet-based content must be content-specific and all generic bans are prohibited (UN Doc. CCPR/C/GC/34, 2011).*

[13] *The question of whether the attack against Iran amounted to an unlawful use of force or armed attack is beyond the scope of this article. Solving this question is not only legally complicated, as the exact impact of the Stuxnet virus has never been entirely identified.*

The line between a low-intensity cyber operation that amounts to a violation of state sovereignty and one that does not is therefore very thin, and the legality of such an operation would depend on the circumstances of the particular case.

3.2 Low-intensity cyber operations and the principle of non-intervention

The principle of non-intervention prohibits states from arbitrarily interfering in affairs falling within the sole responsibility of another sovereign state. The prohibition of intervention "is a corollary of every state's right to sovereignty, territorial integrity and political independence" (Jennings, 1992, p. 428). Its status as a rule of customary international law has been confirmed in numerous United Nations documents[14] and judgments of the International Court of Justice[15].

The Court noted that "the principle forbids all states or groups of states to intervene directly or indirectly in internal or external affairs of other states. A prohibited intervention must accordingly be one bearing on matters in which each state is permitted, by the principle of state sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones" (Military and Paramilitary Activities in and against Nicaragua, 1986, §205). Determining whether an area lies solely in the responsibility of the domestic state is particularly difficult, but in general all matters that are not regulated by international law fall within the category of domestic affairs. In a globalized and interconnected world where cooperation between states is of key importance, few matters remain purely domestic (Kunig, 2008).

A line between friendly persuasion, which is a normal part of international relations, and political interference prohibited by international law is extremely difficult to draw. According to Oppenheim, "the interference must be forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question. Interference pure and simple is not intervention" (Jennings, 1992, p. 432). The element that distinguishes between interference and prohibited intervention is coercion. Only acts of a certain magnitude, which force a state to adopt a decision with regard to its policy that it would not otherwise adopt, qualify as coercive and violate the principle of non-intervention. The element of coercion is most obvious in cases of the unlawful use of force, which always constitutes a violation of the principle of non-intervention, but acts that do not involve direct physical coercion may also violate the principle (Military and Paramilitary Activities in and against Nicaragua, 1986).

---

[14] *Since 1957 the UN General Assembly has adopted more than 30 resolutions addressing the issue of a prohibition of intervention in the internal affairs of states. The most important is the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (UN Doc. A/RES/25/2625, 1970).*

[15] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America); Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania); Armed Activities on the Territory of Congo (Democratic Republic of Congo v. Uganda).*

The International Group of Experts that prepared the Tallinn Manual 2.0 agreed that activities which merely involve influence by cyber means must be distinguished from prohibited interventions. A cyber attack launched by a state or a non-state actor, whose acts are attributable to a state and which is directed against cyber infrastructure located in the territory of another state and involves the element of coercion clearly amounts to prohibited intervention (Schmitt, 2013; Schmitt, 2017). The cyber attacks on Estonia in 2007 and on Azerbaijan in 2012 are examples of prohibited cyber interventions, since both attacks were politically motivated and aimed at changing policy in the attacked state, which clearly shows the presence of an element of coercion.

The Tallinn Manual provides some other examples of actions of a state that would constitute prohibited interventions:
- Using cyber operations to remotely alter electronic ballots and manipulate an election;
- Employing cyber means to alter electronic diplomatic communications between a state's Ministry of Foreign Affairs and its negotiators during the course of fragile talks involving another state, in order to compel the abandonment of the talks;
- Launching disruptive DDoS operations against a state in an attempt to compel it to withdraw recognition of another state;
- Providing cyber weapons to a non-state actor engaged in an insurgency against the government of another state (Schmitt, 2017).

On the other hand, in the view of the International Group of Experts, certain acts do not qualify as wrongful interventions since they are lacking the coercive element. One of the most undisputed examples is cyber espionage, which does not amount to a prohibited intervention, even if it requires remote breaching of protective virtual barriers, e.g. breaching of firewalls or cracking of passwords. Another example is operations conducted by a state to protect its nationals who are in jeopardy abroad, if the territorial state is not offering adequate protection (Schmitt, 2017). The question of whether cyber operations in support of humanitarian intervention that was not consented to by the state or authorized by the UN Security Council would violate the prohibition of intervention remains unanswered, since the experts could not agree on the existence of an exception of humanitarian intervention in international law (Ibid.).

Conclusion

States are increasingly important actors in cyberspace and low-intensity cyber operations offer appealing opportunities to exploit the vulnerabilities of their adversaries, since they are highly effective, extremely affordable, especially compared to classic military operations, and also deniable, because of the difficulties with their attribution. Low-intensity cyber operations raise significant issues, even more so because almost the entire academic debate on state activities in cyberspace is focused on cyber operations which amount to the use of force or armed attack, and low-intensity cyber operations are often completely forgotten. In the last few years this situation has improved as more and more legal scholars recognize the

importance of determining the legality of low-intensity cyber operations. This was also reflected in the field of study of the International Group of Experts in the second edition of the Tallinn Manual, which no longer focuses on the international regime governing cyber warfare, but provides an extensive study of the legal regime for peacetime activities of the states in cyberspace.

Low-intensity cyber operations do not fall through a gap in international law, as some may argue. Although they do not rise to the level of use of force or armed attack, their legality may be assessed through the international law principles of state sovereignty and non-intervention. The key issue that still needs to be resolved is how these two fundamental principles of international law, which were adopted in an entirely different time and circumstances, should be interpreted in the cyber context. In this position of normative uncertainty, states need to be encouraged to articulate their positions on how current international law applies in cyberspace. Their silence leads to unpredictability, which could give rise to misinterpretations and miscalculations by other states and eventually escalate into international conflict. However, we cannot rule out the possibility that in the future states will show willingness to start negotiations in order to comprehensively codify the international law of cyberspace. In the meantime cyberspace will remain an environment haunted by uncertainty and ambiguity.

Bibliography

1. *Armed Activities on the Territory of Congo (Democratic Republic of Congo v. Uganda), Judgment, [2005] I.C.J.Rep.168.*
2. *Arquilla J., Ronfeldt D., 1993. Cyberwar is coming! Comparative Strategy. 12/2, pp. 141-165.*
3. *Borger J., 1999. Pentagon Kept the Lid on Cyberwar in Kosovo. https://www.theguardian.com/world/1999/nov/09/balkans. 4 August 2017.*
4. *Buchan R., 2012. Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions. Journal of Conflict and Security Law. 17/2, pp. 212-227.*
5. *Buchan R., 2016. The International Legal Regulation of State-Sponsored Cyber Espionage. In: Osula A., Rõigas H. (Eds.), 2016. International Cyber Norms: Legal, Policy & Industry Perspectives. Tallinn: NATO CCD COE Publications, pp. 65-86.*
6. *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania), Merits, [1949] I.C.J. Rep.4.*
7. *Craig A., Valeriano B, 2016. Conceptualising Cyber Arms Races. In: Pissanidis N., Rõigas H., Veenendaal M. (Eds.). 8th International Conference on Cyber Conflict. Tallinn: NATO CCD COE Publications, pp. 1-18.*
8. *Czosseck C., Ottis R., Talihärm A., 2011. Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. International Journal of Cyber Warfare and Terrorism. 1/1, pp. 24-34.*
9. *Dearden L., 2017. World Heading Towards 'Permanent Cyber War', France Warns. http://www.independent.co.uk/news/world/europe/cyber-war-world-warning-france-criminals-extremists-russia-countries-guillaume-poupard-anssi-a7767886.html, 23 August 2017.*
10. *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, 1970. Resolution of the General Assembly of the United Nations, 2625(XXV), UN Doc. A/RES/25/2625.*

11. *Department of Defense Strategy for Operating in Cyberspace, 2011. http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf, 3 August 2017.*
12. *Ferguson N., 2017. Cyber War I has Already Begun. https://www.bostonglobe.com/opinion/2017/03/13/cyber-war-has-already-begun/dYE1vkpT1W3zKdhjxwH1QP/story.html, 23 August 2017.*
13. *Gill T. D., Fleck D. (Ed.), 2016. The Handbook of the International Law of Military Operations. New York: Oxford University Press.*
14. *Hayden M., 2010. Hackers Force Internet Users to Learn Self-Defense. http://www.pbs.org/newshour/bb/science-july-dec10-cyber_08-11/, 3 August 2017.*
15. *Heintschel von Heineg W., 2012. Legal Implications of Territorial Sovereignty in Cyberspace. In: Czosseck C., Ottis R., Ziolkowski K. (Eds.), 2012. 4th International Conference on Cyber Conflict. Tallinn: NATO CCD COE Publications, pp. 7-19.*
16. *HRC General Comment No. 34 (2011), UN Doc. CCPR/C/GC/34.*
17. *Island of Palmas Case (Netherlands v. United States of America), RIAA, Vol. II.*
18. *Jennings R., Watts A. (Ed.), 1992. Oppenheim's International Law, Volume 1 – Peace. Longman, Harlow.*
19. *Kunig P., 2008. Intervention, Prohibition of. Max Planck Encyclopedia of Public International Law. http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434?prd=EPIL, 3 August 2017.*
20. *Lawson S.T., Yu H., Yeo S. K., Greene E., 2016. The Cyber-Doom Effect: The Impact of Fear Appeals in the US Cyber Security Debate. In: Pissanidis N., Rõigas H., Veenendaal M. (Eds.). 8th International Conference on Cyber Conflict. Tallinn: NATO CCD COE Publications, pp. 65-80.*
21. *Letter dated 6 September 2012 from the Chargé d'affaires a.i. of the Permanent Mission of Azerbaijan to the United Nations addressed to the Secretary-General, 2012. UN Doc. A/66/897.*
22. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA), Merits, [1986] I.C.J. Rep.14.*
23. *NATO Cooperative Cyber Defence Centre of Excellence, Cyber Definitions. https://ccdcoe.org/cyber-definitions.html, 23 August 2017.*
24. *Naughton J., 2016. The Evolution of the Internet: From Military Experiment to General Purpose Technology. Journal of Cyber Policy. 1/1, pp. 5-28.*
25. *Ohlin J. D., Govern K., Finkelstein C. (Eds)., 2015. Cyber War, Law and Ethic for Virtual Conflicts. Oxford: Oxford University Press.*
26. *Panetta L., 2012. Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security. http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136, 30 July 2017.*
27. *Passeri P., 2016. 2016 Cyber Attacks Statistics. http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics, 2 August 2017.*
28. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2013. UN Doc. A/68/98.*
29. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015. UN Doc. A/70/174.*
30. *Rid T., 2012. Cyber War Will Not Take Place. Journal of Strategic Studies. 35/1, pp. 5-32.*
31. *Schmitt M. N. (Ed.), 2013. Tallinn Manual on the International Law Applicable to Cyber Warfare. New York: Cambridge University Press.*
32. *Schmitt M. N. (Ed.), 2017. Tallin Manual on the International Law Applicable to Cyber Operations. New York: Cambridge University Press.*

33. *Schmitt M.N., 2013. Cyberspace and International Law: The Penumbral Mist of Uncertainty. Harvard Law Review Forum. 126, pp. 176-180.*
34. *Schmitt M. N., 2014. The Law of Cyber Warfare: Quo Vadis? Stanford Law & Policy Review. 25, pp. 269-300.*
35. *Segura Serano A., 2006. Internet Regulation and International Law. In: Bogdandy A., Rüdinger W. (Eds.), 2006. Max Planck Yearbook of United Nations Law, Volume 10. The Hague: Brill Nijhoff, pp. 192-272.*
36. *Shakelford S. J., 2014. Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. New York: Cambridge University Press.*
37. *Statute of the International Court of Justice, 26 June 1945, 33 UNTS 993.*
38. *UNIDIR (2013). The Cyber Index – International Security Trends and Realities. UN Doc. UNIDIR/2013/3.*
39. *Warsaw Summit Communiqué Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw, 2016. https://ccdcoe.org/sites/default/files/documents/NATO-160709-WarsawSummitCommunique.pdf.*
40. *Watts S., Low-Intensity Computer Network Attack and Self-Defense. In: Pedrozo R., Wollschlaeger D.P. (Eds.). International Law Studies, International Law and the Changing Character of War, Volume 87. Naval War College Press, pp. 59-87.*
41. *Ziolkowski K. (Ed.), 2013. Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy. Tallinn: NATO CCD COE Publication.*