https://doi.org/10.22364/jull.13.06

Reducing the Threat of Cyber Warfare Through a Suitable Dispute Resolution Mechanism

Dr. **Muhammad Asif Khan**
Faculty of Law, Bahria University, Islamabad, Pakistan
Senior Assistant Professor at the Department of Law
E-mail: *aasif.buic@bahria.edu.pk*

With each step of technological advancement, we are entering a global technological domain susceptible to cyber infiltration. The individual privacy and security are supposed to be protected by the states governed by laws that are specifically a part of the national legal systems. The transnational cyber infiltration targeting the state actors by using the cyberspace creates a new plethora of questions. The issue has been highly debated, whether the *jus ad bellum* is sufficient in regulating the various types of cyber infiltrations. The matter of classifying the cyber-attacks as armed attacks has been furtively debated on contextual basis. The legal principles governing the laws of war have been held insufficient by some in order to include the new forms of attacks conducted through global cyberspace. In the midst of such debate, one conclusion can be derived that the cyber operations globally are causing a threat to state sovereignty and security. The focus on issues related to transnational cyber operations is based upon the existing legal principles and laws. The debate conjures up a few problems which need to be addressed. This article analyses the different perspectives of the cyber warfare and the identified problems related with the issue. According to the current problems faced by the states, a measure of the remedial system for states in international law is taken into consideration. The current system of remedies fails to accommodate the grievances of the states with regard to the cyber operations. Hence, a new platform for the state remedies is suggested and proposed.

Keywords: cyber warfare, cyber-attacks, *jus ad bellum*, International Humanitarian Law; just war.

Contents

Introduction

The invasion of privacy through the medium of cyberspace is rapidly increasing. The rise in such invasions is directly related to the increasing virtual dependence. This dependence on the advanced technologies by public and private sector organizations in a sense incites the cyber experts to get involved in a technical but safer mode of attacks for personal gain. The attacks are often internal matters of a state to be regulated by the state laws, however, these attacks create more operational issues, when they adversely affect subjects on foreign grounds. The effects of these cyber-attacks can be devastating financially and from the perspective of international security. According to an estimate, the cyber-attacks have cost more than € 500 billion in damages worldwide only in 2016.[1] Similarly, the increasing reliance on technologies makes the civilian and military infrastructures more vulnerable to the outside attacks.[2] The ammunition required for such attacks can be acquired relatively cheaper, easier and lawfully in any location around the world.[3] The severity of the attacks involving cyberspace will increase keeping in view the dissemination and increasing reliance on advanced technologies.[4] This increases the risks of cyber-attacks leading to a kinetic warfare in the contemporary world. Although the attribution of these attacks to a state is problematic, in several cases it has been noted that there has been an apprehension of states being accomplices in certain cyber-attacks. China, for instance, has been suspected of several cyber-attacks committed against the United States.[5] In the Estonian cyber-attacks, a major governmental machinery including websites, newspapers, TV stations, banks and other targets was shut down for three weeks, allegedly by Russian attackers.[6] A similar attack was committed against Georgia's networks in 2008.[7] The attack on Iran's nuclear refining operations was committed through a Stuxnet virus program, allegedly

[1] See: Cyber Security: A Pillar of our Digital World. 2019. Available: https://new.siemens.com/global/en/company/stories/research-technologies/cybersecurity.html#30yearsofcybersecurity [last viewed 07.04.2020].

[2] The United States National Security Strategy. 2010. Available: www.whitehouse.gov/sites/defsult/files/rss_viewer/national_security_strategy.pdf [last viewed 07.04.2020], p. 27.

[3] Ibid., p. 6.

[4] See, for instance, McAfee Report: In the Crossfire – Critical Infrastructure in the Age of Cyber War. 2010. Available: Available:http://resources.mcafee.com/content/NACIPReport [last viewed 07.04.2020], p. 11.

[5] *Shackelford, S. J.* From Nuclear War to Net War: Analogizing Cyber-Attacks in International Law. *Berkeley Journal of International Law*, No. 27, 2009, pp. 192, 204.

[6] *Hollis, D. B.* Why States Need an International Law for Information Operations. *Lewis and Clark Law Review*, No. 11, 2007, 1023, pp. 1024–1025.

[7] *Swaine, J.* Georgia: Russia Conducting Cyber War. *The Telegraph*, 11 August 2008. Available: Available:https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html [last viewed 07.04.2020].

initiated by the American and Israeli intelligence services with Dutch support.[8] In a more recent venture, the United States claimed to have used cyber-attacks against Iran in retaliation for the shooting down of a US drone.[9]

The importance of cyber security with regard to states is now found unfolded and the threat of cyber warfare seems real. The concern by the international community is shown in the General Assembly resolutions admitting that the means of information technology can be influential in affecting the interests of the international community.[10] It has also been acknowledged that the state actors may be deeply affected by the misuse of information technologies.[11] Importantly, the states have agreed that international peace and security may be at potential risk, if such technologies are used purposefully to achieve adverse objectives.[12] The threat of cyber warfare is illuminating, in a sense that unregulated activities within cyberspace may lead state actors into situations where an act of aggression might become unavoidable. However, the legality of actions or reactions of states to the attacks using cyberspace remains ambiguous and open to the interpretation of existing legal norms and principles. An attempt by scholars has been made to clarify these ambiguities. For instance, the Talinn Manual on the International Law Applicable to Cyber Warfare[13] is a step towards guiding states in cyber operations during conflicts.

The current article is an attempt to present a workable solution of the problems related specifically to the cyber operations having transnational effects. The modes of cyber-attacks, which may lead to cyber warfare are described through the different approaches within the relevant scholarly work. The already existing views regarding both terms are analyzed in order to understand their legal standing. No attempt has been made to introduce new variables for finding a newer version of definitions attached to these terms. As the laws of conflict are distributed in two sets of rules, i.e., *jus ad bellum* and *jus in bello*, this article deals with the applicability of *jus ad bellum* within the cyber warfare. The complications of the applicability of the *jus ad bellum* to cyber warfare are discussed and the major issues are identified. In the midst of these complications, the access to remedies for a state adversely affected by the cyber-attacks is analyzed. The cyber warfare can have devastating effect, if the states found themselves without accessible remedies or a forum to seek reparations. Hence, keeping the real threat of cyber warfare in view, and the laws pertaining to regulating the warfare and providing a forum for the states to access remedies is proposed. The final part of the article deals with the importance of a separate Arbitration and Enquiry Tribunal for Transnational Cyber Operations (AETTCO). This article does not

[8] Dutch Intel Aided U.S.-Israel Stuxnet Cyberattack on Iran. *Haaretz*, 03 September 2019. Available: https://www.haaretz.com/middle-east-news/iran/dutch-intel-aided-u-s-israeli-stuxnet-cyberattack-on-iran-report-reveals-1.7793561 [last viewed 07.04.2020].

[9] British Broadcasting Corporation (BBC). US launched cyber-attack on Iran Weapons Systems. 2019. Available: https://www.bbc.com/news/world-us-canada-48735097 [last viewed 07.04.2020].

[10] See GA Res 55/28 (20 November 2000); GA Res 56/19 (29 November 2001); GA Res 59/61 (3 December 2004); GA Res 60/45 (8 December 2005); GA Res 61/54 (6 December 2006); GA Res 62/17 (5 December 2007); GA Res 63/37 (2 December 2008); GA Res 64/25 (2 December 2009).

[11] See the Preambles of GA Res 55/63 (4 December 2000); GA Res 56/121 (19 December 2001);

[12] GA Res 58/32 (8 December 2003); GA Res 59/61 (3 December 2004); GA Res 60/45 (8 December 2005); GA Res 61/54 (6 December 2006); GA Res 62/17 (5 December 2007); GA Res 63/37 (2 December 2008); GA Res 64/25 (2 December 2009).

[13] *Schmitt, M. N.* (ed.). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press, 2013.

intend to clarify the modes of operations for AETTCO, but to mark its value and a possible way out for states from ambiguities of the applicable laws (*jus ad bellum*) within cyber warfare.

1. From Cyber-Attacks to Cyber Warfare

The notion of cyber-attacks, which may lead to cyber warfare describes a phenomenon that occurs within the cyberspace. Cyberspace has been defined by Kuehl as "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies."[14] The whole system of cyberspace works through independent computer networks. A large number of individuals working in official capacity for national, transnational, public or private organizations are involved as active actors within the cyberspace. In addition, millions of individuals in private capacity are a part of cyberspace involved in activities related to information systems which might have transnational effects. On the whole, the cyberspace may be termed as a single system based upon interconnected networks, whereas the actors involved with the system do not work under a single code of conduct, and their actions are not limited to standardized boundaries. The invasion of individual or organizational privacy using cyberspace would lead to cybercrimes. Many of the cyberspace abusers are involved in criminal activities for private gains.[15] The issue of cybercrimes is regulated through domestic laws of the states,[16] and the nature of the transnational activities involved has driven the states to adopt an international convention on the issue.[17] The issue of cyber-attacks against states or state entities is dealt with through the existing set of international laws. It is pertinent to understand the nature and modes of cyber-attacks in order to address the issue when the attacks may lead to cyber warfare.

1.1. Understanding Cyber-Attacks

It is difficult to define the term 'cyber-attack' or other relevant terminologies; a consensus has not been reached on a single definition of such terms.[18] In general, the usage of cyberspace in some adverse manner may amount to a cyber-attack. According to Schmitt, cyber-attacks come under the ambit of a broader category of "information operations".[19] The information operations include the systematic usage of the different operational systems including electronic and computer networks in agreement with other relevant capabilities in order "to influence, disrupt, corrupt, or usurp any negative human and automated decision

[14] *Kuehl, D. T.* Cyberspace to Cyberpower: Defining the Problem. In: Cyberpower and National Security, *Kramer, F. D., Starr, S. H., and Wentz, L.* (eds.). Washington: Potomac Books, 2009, p. 27.

[15] *Roscini, M.* Cyber Operations and the Use of Force in International Law. Oxford: Oxford University Press, 2014, p. 4.

[16] According to United Nations Conference on Trade and Development (UNCTAD), a total of 138 states have enacted legislation dealing with cybercrimes. Available: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx [last viewed 07.04.2020].

[17] Convention on Cybercrimes 2001, ETS No. 185.

[18] *Roscini*, above n. 15, pp. 10–16.

[19] *Schmitt, M. N.* Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, No. 37, 1999, pp. 885, 890–891.

making while protecting our own."[20] This usage of cyberspace in the information operations can be of an offensive or defensive nature. A cyber-attack would come under this broader perspective and may amount to actions of a different nature including, among others, attacks on nuclear reactors, military communication systems, the air traffic control systems, automated weapons etc. However, a simpler definition may be an "attack initiated from a computer against a web site, network, or individual computer that compromises the confidentiality, integrity, or availability of that system or stored information."[21] The purpose of the attack is to harm any person or organization or a state in a broader category, whereby the harm may be inflicted intentionally or resulting through the wider effects of an action because of lack of expertise, *inter alia*.[22] Some state actors encourage a wider and broader approach towards defining cyber-attacks. The Shanghai Cooperation Organization[23] has expressed an opinion that the use of new technologies in the information and communication systems (including the social media apparatus) can be a threat to the "security and stability in both civil and military spheres."[24] This approach seems to adopt an expansive vision of cyber-attacks to include the use of cyber-technology to undermine political stability. Some experts fear that this approach is adopted for targeting the political speech and justifying its censorship.[25] Hence, the scope of the cyber-attacks seems to be undefined and open to relative definitions adopted. A commonality between the approaches is merely teleological. The purpose or object of the attacks is to inflict harm on others, while the extent and nature of the harm is, however, undefined.

The modes of cyber-attacks can differ technically according to the resources and proficiency of the person(s) involved. The attacks are mostly based upon computer network operations. These operations include Computer Network Attack (CNA), Computer Network Defense (CND), and Computer Network Exploration (CNE).[26] The CNA operations are directed towards incapacitating a communication system or even damaging the external computer networks.[27] The CND is a defensive action against an adversary's CNA. The CNAs may involve the distributed denial of service (DDoS), trojan horses and logic bombs and viruses. DDoS attacks are mostly used for the corruption of the hardware. It isolates targets from the said network by flooding them with a large amount of

---

[20] United States National Military Strategy for Cyberspace Operations. 2006. Available: www. dtic.mil/doctrine/new_pubs/jp3_13.pdf [last viewed 07.04.2020].

[21] *Springer, P. J.* (ed.). Encyclopedia of Cyber Warfare. California: ABC-CLIO, 2017, p. 40.

[22] See *Hodges, D.* and *Creese, S.* Understanding Cyber Attacks. In: Cyber Warfare: A Multidisciplinary Analysis, *Green, J. A.* (ed.). London: Routledge, 2015, p. 33.

[23] Shanghai Cooperation Organization is a security cooperation group composed of China, Russia, and most of the former Soviet Central Asian republics, as well as observers including Iran, India, and Pakistan.

[24] Shanghai Cooperation Organization, 61st plenary meeting, Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, 2008.

[25] *Gjelten, T.* Seeing the Internet as an Information Weapon, 2010. Available: http://www.npr.org/templates/story/story.php?storyId=130052701 [last viewed 07.04.2020].

[26] U.S. Department of Defense, The National Military Strategy for Cyberspace Operations, 2006. Available: www.dod.gov/pubs/foi/ojcs/ 07-F-2105doc1.pdf [last viewed 07.04.2020], 3.

[27] *Roscini, M.* World Wide Warfare – *Jus ad Bellum* and the Use of Force. In: Max Planck Yearbook of United Nations Law, *Bogdandy, A. and Wolfrum, R.* (eds.). Leiden: Martinus Nijhoff Publishers, 2010, pp. 85, 93.

information and data, which causes a collapse of the network.[28] As a consequence, the system collapses and malfunctions. In the attacks against Estonian (2007) and Kyrgyzstan's (2009) systems, the DDoS mode of attacks was used.[29] Similarly, other means of attack are employed by getting access to different networks through emails, hacking, chipping or even using the Universal Serial Bus (USB).[30] These methods may lead to the complete or partial destruction of opponent's computer network systems, resulting in disabling of major logistics or administrative infrastructure. The CNE operations include different forms of activities targeted towards obtaining classified information. These activities may be classified as cyber espionage.[31] The espionage activities are not unlawful under the international law, but a criminal offence in most of the domestic legal systems.[32] The use of cyberspace for such covert operations opens up a new plethora of legal questions. The activity may be legal in the state from where the CNE operations are carried out, whereas illegal in the state where they are carried out. The state's territorial jurisdiction may apply to take action against the attackers; the likelihood of arresting the persons involved in cyber espionage is very low without the cooperation of the other state. The issue becomes of high importance when the military and state departments are targeted through CNE operations.[33] The investigation of such activities due to a complex nature of cyberspace is also not possible without joint co-operation.

1.2. Understanding Cyber Warfare

The concept of cyber warfare is a contemporary phenomenon and difficult to define, it would not constitute a war in its traditional concept.[34] A war is usually a form of collective violence between two or more states that is ordered and performed by professionals to achieve an economic, political, or religious aim that could or would be prevented by the antagonist group. The aim of a military in modern warfare is to target and subdue the armed forces of the opponent.[35] A war in cyberspace does not correspond to such a definition, since a single person with a laptop and an Internet connection could start a war in this environment by attacking a foreign government using methods well-known from diverse cybercrimes.[36] The approach of defining the cyber warfare in order to include the cyber-attacks into the ambit of warfare may be twofold. Firstly, some authors would define this phenomenon through the subject-based approach. Jeffrey Carr

[28] *Springer*, above n. 21, p. 40.

[29] See *Hollis*, above n. 6, pp. 1024-1025.

[30] *Roscini*, above n. 27, at p. 93; *Cox S.*, Confronting Threats through Unconventional Means: Offensive Information Warfare as a Covert Alternative to Preemptive War. *Houston Law Review*, No. 42, 2005, pp. 881, 888–889.

[31] See, for instance, *Stiennon, R.* A Brief History of Cyber Warfare. In: *Green J. A.* (ed.). above n. 22. Stiennon identifies various means of cyber espionage that actually have been used, where different state actors were involved in the operations.

[32] United States Department of Defense Memo. 2015, p. 516; *Tubbs, D., Luzwick, P. G. and Sharp, W. G.* Technology and Law: The Evolution of Digital Warfare. *International Law Society*, No. 76, 2002, pp. 7, 16; *Chesterman, S.* The Spy Who Came in from the Cold War: Intelligence and International Law. *Michigan Journal of International Law*, No. 27, 2006, p. 1071.

[33] See *Springer*, above n. 21, p. 58. In 2014, the Chinese attackers allegedly stole information related with the US F-35 fighter jet program. The action has a huge economic and national impact.

[34] See *Rid, T.*, Cyber War Will Not Take Place. *Journal of Strategic Studies*, No. 35, 2012.

[35] See Declaration Renouncing the Use, in Time of War of Explosive Projectiles Under 400 Grammes Weight. 1868. Available: http://www.icrc.org/ ihl.nsf/FULL/130? [last viewed 07.04.2020].

[36] *Springer*, above n. 21, p. 90.

offers a definition of cyber warfare as an "art and science of fighting without fighting; of defeating an opponent without spilling their blood."[37] This notion of defining warfare is not new, as Sun Tzu has written that the objectives of military forces are not limited only to the battlefields, he stated that "to win a hundred victories in a hundred battles is not the highest excellence; the highest excellence is to subdue the enemy's army without fighting at all".[38] These new weapons and a ground away from the territorial battlefield bring this old phenomenon of warfare back into practice. This approach may be miscalculated with regard to the cyber warfare, as it may involve the destruction of state infrastructure leading towards affecting (and even killing) hundreds of people by adversely affecting their lives. Secondly, the approach may be object-based and based upon the amount and modes of techniques used. The approach towards defining a cyber-attack by some scholars is through taking the computers and networks as objectives.[39] For instance, Richard Clarke, special advisor on cyber security to US president Bush (2001–2003), defines cyber war as "actions by a nation state to penetrate another nation's computers or networks for the purpose of causing damage or disruption".[40]

Taking the international law related to the armed conflicts, the object-based definition of cyber warfare would come into discussion. The damage or disruption caused by the cyber-attacks would then amount to an attack. The attacks are defined and understood separately in the realm of *jus in bello* and *jus ad bellum*. *Jus in bello*, which deals with the law during an armed conflict, has its own principles of describing attacks. Attacks are defined in the Article 49(1) of Additional Protocol I as "acts of violence against the adversary, whether in offence or defense." The violence would then be taken as an objective matter, i.e. a consequence of an act, if not the direct consequence. In cases where it results in consequences such as destruction of property, damage to civilian or military objects, they are attacks satisfying the criterion of an armed conflict.[41] Consequently, if we take the example of the Stuxnet attacks on Iran in the context of the laws of war, the actual damage to the centrifuge would amount to an attack. On the other hand, the laws related to the armed conflicts (*jus in bello*) are applied on the basis of their own principles, the inclusion of cyber-attacks into these principles create further specific difficulties to assess and apply the law.

---

[37] *Carr, J.* Inside Cyber Warfare. 2nd ed., California: O'Reilly, 2012.

[38] *Tzu, S.* The Art of Warfare. In: *Giles, L.* (transl.), Sun Tzu on the Art of War, 2000: "the expert in using the military subdues the enemy's forces without going to battle, takes the enemy's walled cities without launching an attack, and crushes the enemy's state without a protracted war".

[39] *Nguyen, R.* Navigating *Jus ad Bellum* in the Age of Cyber Warfare. *California Law Review*, No. 101, 2013, pp. 1079, 1085.

[40] *Clarke, R. A. and Knake, R.* Cyber War: The Next Threat to National Security and What to Do About It. New York: Harper Collins, 2010.

[41] *Schmitt, M.* Cyber Operations and the *Jus in Bello*. In: International Law and the Changing Character of War, *Pedrozo, R. A. and Wollschlaeger, D. P.* (eds.). Newport: U.S. Naval War College 2011, pp. 89, 92–94. It has been suggested that operations falling below the threshold may also qualify; International Committee of the red Cross, Report 31IC/11/5.1.2, International Humanitarian Law and the Challenges of the Contemporary Armed Conflicts. 2011 (hereinafter ICRC Report); *Dörmann, K.* Applicability of the Additional Protocols to Computer Network Attacks. 2004. Available: http://www.icrc.org/eng/assets /files/other/applicabilityofihltocna.pdf [last viewed 07.04.2020]. The paper delivered at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm.

2. Application of *Jus ad Bellum* to Cyber Warfare

In order to deal with the application of *jus ad bellum* to cyber warfare, we will rely upon the assessment of both the subject-based and object-based approach towards cyber warfare. The reason is that the current laws of war do not specifically address the issue of cyber warfare. There are no treaties or conventions, which explicitly address the issue of cyber-attacks; the Charter of the United Nations also is silent about the legality of such attacks. However, the Additional Protocol I to the 1949 Geneva Conventions does make the point clear to an extent that the principles applicable in *jus ad bellum*[42] regarding the legality of weapons will apply to the cyber-attacks as it does to any other new weapons.[43] However, neither the extent of its application, nor the mode thereof have been determined. This lack of clarity in the laws may raise the issue of cyber-attacks as permissible under international law by the application of the *lotus principle* claiming "what international law does not prohibit, it permits."[44] Hence, we must look into the application of the existing principles to the cyber-attacks from both object-based and subject-based purposes. This approach brings the mode of the attack and the purpose of the attacks into question, according to which the *jus ad bellum* will apply, if the attack qualifies according to a certain principle, criteria. The ambiguity in application of the rules will still remain in the absence of direct laws. In the absence of direct laws or state practices, the states have historically developed new laws or regulatory regimes in order to extend the existing laws to include the new weapons.[45] Currently, the *jus ad bellum* has been termed as insufficient; the improvement to bring cyber-attacks into the realm of international law has been termed necessary.[46] Furthermore, as most parts of the *jus ad bellum* have been derived from the customary international law and to an extent the UN charter, they create the starting point for any discussion regarding the regulation of state practice related to cyber-attacks.[47] Therefore, to study the cyber warfare from the perspective of *jus ad bellum* and to know whether these laws are applicable to cyber-attacks, we have to determine the legality (or illegality) of these attacks. After meeting the criteria, the attacks must be attributed to the state in order to incur state responsibility.

---

[42] *Jochnick, C. and Normand, R.* The Legitimation of Violence: A Critical History of the Laws of War. *Harvard International Law Journal*, No. 35, 1994, pp. 49, 52.

[43] Article 38, Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I).

[44] See *Silver, D. B.*, Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter. *International Law Society*, No.76, 2002, pp. 73, 75 (discussing CNA and the prohibition on the use of force); *Haslam, E.* Information Warfare: Technological Changes and International Law. *Journal of Conflict and Security Law*, No. 5, 2000, pp. 157, 165 (use of force paradigm applies "only with difficulty"); Office of General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (Nov. 1999), reprinted in *International Law Society*, No. 76, 2002, pp. 459. Available: http://www.nwc.navy.mil/cnws/ild/studiesseries.aspx [last viewed 07.04.2020] [hereinafter DOD GC Memo]; *Brown, D.* A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict. *Harvard International Law Journal*, No. 47, 2006, pp. 179, 181.

[45] *Hollis*, above n. 6.

[46] Ibid., p. 1041.

[47] *Swanson, L.* The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict. *Loyola of Los Angeles International and Comparative Law Review*, No. 32, 2010, p. 303.

2.1. Question of an Armed Attack

In order to come under the ambit of the *jus ad bellum*, the cyber-attacks must pass the test of being an 'armed attack'.[48] The criteria laid down in the UN Charter must be fulfilled. The cyber-attacks have the potential to engage in actions within cyberspace, an action, which militaries have been carrying out through other destructive methods. The militaries can engage in depriving the opponents of infrastructure that may be helpful in military operations, for instance, disrupting the electrical or communication systems. The cyber-attacks also offer the advantage of achieving such targets without as much collateral damage, e.g., temporarily disabling an electrical grid. The purpose of these attacks comes into debate when it signifies a political objective. The targets go beyond the military objectives and the adverse activities within the cyberspace bring the purpose of activities to the foreground.[49] The current rule-based system can be interpreted differently by taking literal meaning or adopting an object-based approach. In order to know, whether the cyber-attacks are compatible with the notion of the 'use of force' under Article 2(4) of the UN Charter or an 'armed attack' under Article 51, if the literal meaning is taken, the cyber-attacks will not qualify under this test.[50] The purpose of the attacks is not taken into account, when this approach is applied. A cyber-attack objectively may not amount to a serious act, which may trigger the 'use of force' amounting to an 'armed attack', while the effects of the act in itself may be serious enough to trigger such rules. These apprehensions create doubts while applying the rules of war in cyber warfare. The ICJ has also discussed the question of what may amount to an armed attack in different cases. However, it has not given a direct account of what armed attack might be, it has only restricted itself to the attribution of attacks to the states.[51]

Three different possibilities may arise when analyzing the issue of a cyber-attack taken up as an armed attack. Firstly, as described, the cyber-attacks are not considered as armed attack because of the lack of direct physical force involved. [52]This approach relies upon the literal meaning and interpretation of the UN Charter. The text of the article 41 of the UN Charter can also be presented as an evidence of cyber-attacks does not involve any armed force.[53] A textual interpretation of Article 41 would suggest that cyber-attacks can never be regarded as armed attacks, since other means of communication do not involve

---

48 Article 51, Charter of the United Nations.

49 *Hollis*, above n. 6, p. 1035.

50 *Green, J. A.*, The Regulation of Cyber Warfare under the *Jus ad Bellum*. In: *Green J. A.* (ed.), above n. 20, p. 102.

51 See *Ruys, T.* Armed Attack and Article 51 of the UN Charter: Evolutions in Customary Law and Practices. Cambridge: Cambridge University Press, 2010; see also Case Concerning Military and Paramilitary Activities in and Against Nicaragua (*Nicaragua v. United States of America*), Merits, International Court of Justice (ICJ), 27 June 1986; see also Case Concerning Armed Activities on the Territory of the Congo (*Democratic Republic of Congo v. Uganda*); Request for the indication of Provisional Measures, International Court of Justice (ICJ), 1 July 2000.

52 *Kanuck, S. P.* Information Warfare: New Challenges for Public International Law. *Harvard International Law Journal*, No. 37, 1996, pp. 272, 288–89; *DiCenso, D. J.*, Information Operations: An Act of War?, Air and Space Power Chronicles, July 2000, Available: http://www.iwar.org.uk/iwar/resources/airchronicles/dicenso1.htm [last viewed 07.04.2020].

53 UN Charter, Art. 41. Since "means of communication" would include not only interpersonal communication (e.g., on the Internet) but how an operating system communicates with the infrastructure it controls, almost all CNA could qualify as targeting "means of communication."

the use of force.[54] Besides the normative discrepancies it has also been suggested that cyber-attacks cannot be regarded as armed attacks, if the cyber-attacks are not launched with the aim of taking lives; and the response to such attacks with the use of force in self-defense would be disproportional and therefore a cyber-attack could practically never reach the threshold of an armed attack.[55] This approach is based upon the damage caused by examining whether that damage would have typically been caused by a kinetic attack.[56] The effect is then used as the basis for assessing the aim or purpose of the attack. This kind of effect-based approach has long been used to separate traditional armed force from economic or political pressure.[57] The effects of an attack are calculated through a simple deductive analysis of creating a criterion to maintain whether a cyber-attack qualifies the test of an armed attack; however, it has seen criticism of not being an adequate tool because of a very simplified approach.[58] The major focus is on looking into the cyber-attack as an armed attack through the normative framework which identifies attack through physical force.

Secondly, according to some scholars, the targets of the attacks may be taken into consideration, when some critical national infrastructure is attacked, even without significant destruction or casualties.[59] Walter Sharp argues that an attempt to infiltrate the major computer systems controlling any state instalments should be considered as a hostile act.[60] Jensen is another scholar of a similar view; he regards the target of the attack as what should define the threat and appropriate response.[61] The amount of physical force is not taken as an indicator of whether a cyber-attack amounts to an armed attack. The ICRC also does not consider physical damage as a requirement of an attack.[62] Hence, many actors take the notion of physical force resulting in physical damage out of the question when drawing a yardstick for a cyber-attack amounting to an armed attack. Many states have also taken up this stance of relying upon the future consequences of attacks rather than the immediate consequences' approach. The Russian Federation in submitting its views to the Secretary General of the United Nations, declaring that the cyber-attacks "can have devastating consequences comparable to the effects of weapons of mass destruction".[63] A spokesperson for the Russian

---

[54] *Holmberg, E. J.* Armed Attacks in Cyberspace. Thesis on file at Stockholm University, 2015. Available: http://www.diva-portal.org/smash/get/diva2:854660/FULLTEXT01.pdf [last viewed 07.04.2020], p. 32.

[55] *May, L.* The Nature of War and the Idea of Cyberwar. In: Cyberwar, Law and Ethics for Virtual Conflicts, *Ohlin, J. D., Govern, K., and Finkelstein, C.* (eds.). Oxford: Oxford University Press, 2015, pp. 1, 14.

[56] *Graham, D. E.* Cyber Threats and the Law of War. *Journal National Security Law and Policy*, No. 4, 2010, pp. 87, 91.

[57] *Handler, S. G.* The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare. *Stanford Journal of International Law*, No. 48, 2012, pp. 209, 226–227.

[58] *Schmitt*, above n. 17, at 911-912.

[59] See, e.g. *Sharp, W. G.* Cyberspace and the Use of Force. 1999, pp. 129–32; *Jensen*, *E. T.* Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense. *Stanley Journal of International Law*, No. 38, 2002, pp. 207, 229; *Condron, S. M.* Getting it Right: Protecting American Critical Infrastructure in Cyberspace. *Harvard Journal of Law and Technology*, No. 20, 2007, pp. 403, 415–416.

[60] *Sharp*, ibid., p. 130.

[61] *Jensen*, above n. 57, p. 234.

[62] ICRC Report, above n. 39, p. 37.

[63] *Johnson, P. A.* Is it the Time for a Treaty on Information Warfare? In: Computer Network Attack and International Law, *Schmitt, M. N. and O'Donnell, B. T.* (eds.), 2001, p. 443.

Military have also specified that "the use of warfare against the Russian Federation or its armed forces will categorically not be considered a non-military phase of a conflict whether there were casualties or not".[64] In another instance, the United Kingdom undersecretary for security and counter terrorism also declared that the attacks on a power station would be considered as an act of war.[65] The Estonian Defense minister has compared the cyber blockades to naval blockades on ports, which prevent the access of a state to the rest of the world.[66] However, most of the instances described within this approach might come under the violation of the principle of non-intervention in international law.[67] Consequently, the targeting of critical infrastructure will not trigger the right to self-defense in every instance, but only where it amounts to an armed attack. The targeting may amount to violation of principle of non-intervention, which equals a wrongful act but not a justification for an armed attack in self-defense. This approach perceives any targeting of the critical infrastructure with a hostile intent as an armed attack, which is apparently a flawed approach. It has also been criticized for establishing a dangerous standard by triggering the right to self-defense when a sensitive computer system is malfunctioning.[68] It is not always clear, whether a cyber-attack has taken place and even if it might seem like it has, such malfunctions can be a result of defective software or operator errors. Moreover, an event of cyber espionage will also amount to an armed attack under this approach. As discussed earlier, cyber espionage is not prohibited under international law.[69] It has been suggested that espionage involving "unauthorized access to servers and other computers in a foreign state generally constitutes illegal interventions into the sovereignty of that state" and might trigger the principle of non-intervention.[70] However, the operations pertaining to cyber espionage and other related actions which lack a coercive element will not amount to the violation of even the non-intervention principle.[71] Hence, only the cyber espionage operations, which are of a coercive nature, will amount to the breach of the principle of non-intervention.[72] However, based upon the targeting of critical

---

[64] Quote from a speech of Russian Military Officer. In: *Jenkins, M. A.* Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places? *Naval Law Review*, No. 51, 2005, pp. 132, 166.

[65] *Doward, J.* Britain Fends off Flood of Foreign Cyber Attacks. *The Observer*, 7 March 2010. Available: https://www.theguardian.com/technology/2010/mar/07/britain-fends-off-cyber-attacks [last viewed 07.04.2020].

[66] NATO Parliamentary Assembly, NATO and Cyber Defence, 2009, para. 59.

[67] The principle of non intervention is not a UN Charter principle except for a short mention in article 2(7). It is a customary international law principle approved by the ICJ in *Nicaragua* 1986 (para 2015); see also the UN General Assembly Resolutions e.g. GA Res 25/2625 (1970); GA Res 31/91 (1976), paras 1, 3 and 4; GA Res 36/103 (1981), paras 1 and 2; see also Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty (UN Doc. A/RES/20/2131 (1965), paras 1 and 2; See also *Schmitt, M.* Legitimacy Versus Legality Redux: Arming the Syrian Rebels. *Journal of National Security, Law & Policy*, No. 7, 2014, pp. 139–59.

[68] *Robertson, H. B.* Self-Defense against Computer Network Attack under International Law. In: *Schmitt and O'Donnell*, above n. 63, p. 137.

[69] *Dinniss, H. H.* Cyber Warfare and the Laws of War. Cambridge: Cambridge University Publishers, 2012, p. 81.

[70] *Wrange, P.* Intervention in National and Private Cyberspace and International Law. In: International Law and Changing Perceptions of Security, *Ebbesson, J. et al.* (eds.), 2014, pp. 307, 322.

[71] *Tallinn Manual*, above n. 13, p. 44.

[72] *Roscini*, above n. 15, p. 65.

infrastructure theory, the cyber espionage operations will amount to an armed attack. This broader interpretation will cause more destruction than good to the overall international peace and security.

Thirdly, in establishing an armed attack, the reliance strictly placed upon the consequences of the attack. Thereby, an intention to cause an effect which a kinetic force could have instituted, will then constitute an armed attack.[73] The intention to cause a physical damage to persons or other tangible objects is then accepted as a yardstick for an armed attack.[74] The Tallinn Manual has also described the armed attack according to the consequences of the actions; the actions which "injures or kills persons or damages or destroys property" are considered as armed attacks.[75] Schmitt takes a step further and develops a seven point criteria to distinguish other forms of coercion that supplement the one which amounts to the use of force.[76] The right of self-defence under Article 51 of the UN Charter may be invoked in response to such acts of coercion.[77] However, there is a further consideration that any cyber-attack leading to an armed attack, according to this doctrine, which is based on consequences, will be a part of coordinated attacks, and the other elements of attacks will undoubtedly constitute an armed attack. An isolated cyber-attack in such context would be of little or no importance.[78] For instance, the acts including the cyber espionage, cyber theft and a brief interruption of non-essential cyber services would not qualify as armed attacks.[79] This view supports the object-based definition of the cyber-attacks ending up in cyber warfare. This approach encounters difficulties in cases where there are no direct physical incursions by a state through cyber-attacks amounting to violations of state sovereignty and territorial integrity. For example, the July 2009 attacks on South Korea and the United States were directed against a large amount of computers without involving any kind of physical territorial incursion.[80] The attacks posed a real threat to both states, but because of no physical incursions they would not qualify as 'armed attacks', unless a real physical damage was incurred.

3. Attribution of Cyber-Attacks

The most important obstacle in application of *jus ad bellum* to cyber-attacks is the difficulty of attributing a cyber-attack to a state. Attribution is defined by Wheeler and Larsen as "determining the identity or location of an attacker or an attacker's intermediary".[81] Identifying this identity becomes a tricky job in cases of cyber-attacks. In the case of Estonia it was demonstrated that the actor(s)

---

[73] DOD Memo, above n. 32, p. 483; *Silver*, above n. 44, p. 85; *Dinstein, Y.* Computer Network Attacks and Self Defense. *International Law Studies*, No. 76, 2002, pp. 99, 105; *Robertson*, above n. 68, p. 133; see also *Schmitt*, above n. 19, p. 913.

[74] Schmitt, ibid., p. 935.

[75] *Tallinn Manual*, above n. 13, para. 6.

[76] See *Schmitt*, above n. 19; the criteria include severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy and responsibility.

[77] Ibid., 935.

[78] *Schmitt*, above n. 17.

[79] *Tallinn Manual*, above n. 13, para. 6. See *Schmitt*, above n. 17.

[80] *Sudworth, J.* New "cyber-attacks" hit S. Korea. *BBC News*, 9 July 2009. Available: http://news.bbc.co.uk/1/hi/world/asia- pacific/8142282.stm [last viewed 07.04.2020].

[81] *Wheeler, D. A. and Larsen, G. N.* Techniques for Cyber Attack Attribution, Institute for Defense Analysis, IDA Paper P-3792, p. 1.

committing a cyber-attack can hide their identities and conceal the origins of an attack by ensuring that the attack is identified as coming from another source.[82] The attacks originated from countries such as the United States, Egypt, Peru and the Russian Federation. In the 1998 Solar Sunrise attack against the United States Department of Defense, people of different origins were involved through a computer based in another state.[83] In some situations, the cyber-attack may be a furtive act, whereby the victim has no knowledge of an attack, or it imitates effects of normal behavior, such as a simple software malfunction.[84] Anyone launching cyber-attacks can disguise their origin. The attackers remain anonymous, the attacks simply may point towards one origin, while the real origin might be different. Thereby, this does not necessarily point towards the state or even the computers involved in the attacks as the original perpetrators.[85] This circumstance makes the attribution more challenging in cases of cyber-attacks. The qualities of anonymity, usage of multiple resources, and quickness of action in cyberspace makes the question of attribution more significant.[86]

In cases where the perpetrators of a cyber-attacks can be identified, the attribution of their actions to a state becomes the leading question. The *jus ad bellum* principles and rules can only be applied, where modes of the law of the state responsibility can be fulfilled. As identified earlier, the cyber warfare does not follow the conventional warfare mechanism. Multiple actors can be involved, as the modes of attack are simpler than those of conventional warfare.[87] In cases where the attacks cannot be attributed to a state, the attacks may still be considered as an act of war if they qualify according to the criteria of warfare.[88] However, for the execution of remedies available to the state attacked, it is necessary that the attacks amounting to a wrongful action be attributed to a state or a non-state actor. In cases of a wrongful action by a state, the state entails international responsibility.[89] The state practice and *opinion juris* so support this notion of state responsibility.[90] For instance, the ICJ in Corfu Channel case, while dealing with the issue of attribution held that a state is under an obligation "not to allow knowingly its territory to be used for acts contrary to the rights of other states."[91] The attribution of wrongful actions to a state incurring state responsibility may have twofold dimension. Firstly, the attribution for actions of state organs; secondly, the attribution for the actions of non-state actors.

---

82 See *Schmitt*, above n. 17, p. 892.
83 See *Shackelford*, above n. 5, 204.
84 *Jensen*, above n. 59, pp. 212–213.
85 *Brenner, S. W.* At Light Speed: Attribution and Response to Cyber- Crime/Terrorism/Warfare. *Journal Criminal Law and Criminology*, No. 97, 2007, p. 424.
86 *Tsagourias, N.* Cyber Attacks, Self-Defence and the Problem of Attribution. *Journal of Conflict and Security Law*, No. 17, 2012, pp. 229, 233.
87 *Schmitt and O'Donnell* (eds.), above n. 63, p. 181.
88 *Whetham, D. and Lucas, G. R.* The Relevance of the Just War Theory to Cyber Warfare. In: *Green J. A.* above n. 22, p. 166.
89 Draft Articles on the Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/CN.4/L.602/Rev. July 26, 2001.
90 *Corfu Channel Case* (*U.K. v. Albania*), 1949 I.C.J. 4 (Apr. 9).
91 Ibid.

3.1. Responsibility of a State when Attack is Carried Out by a State Actor

The state responsibility for the actions of its organs is clearly mentioned within the ILC Draft Articles on State Responsibility.[92] State organs include the individuals or any entities making up the organization of a state.[93] A state is thus considered fully responsible for its agents, even when those agents act outside the scope of their duties. Discussing the question of responsibility the ICJ in Armed Activities on the Territory of the Congo held that "according to a well-established rule of a customary nature a party to an armed conflict shall be responsible for all acts by persons forming part of its armed forces."[94] This rule also applies to a person or entity that is not an organ of the state but nevertheless exercises elements of governmental authority.[95] In cases where a person, group of persons or an organization is involved in activities related to cyber information, this rule will apply. After the recent developments in cyberspace technology, a number of states have indulged in developing cyber units within their military or intelligence organs. For instance, China has formed cyberspace units and organs,[96] Israel also is involved in organizing an "Internet warfare" team,[97] the United States have recently established a military Cyber Command, to counter cyber-attacks,[98] Germany has also developed its own cyber unit called the Department of Information and Computer Network Operations,[99] while Italy is reported to be considering establishing one.[100] It is apparent that the conduct of such organs will be attributable to the state of which they are *de jure* organs.[101] Article 4 of ILC Draft Articles on State Responsibility state that "the conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State". Apparently, tracing of cyber-attacks is a tough challenge, but if the involvement of such cyber units is proven, the concerned state will be held responsible.

3.2. When Attacker is a Non-State Actor

The cyber-attacks may be conducted by individuals or corporations hired by states, or in some cases in their own personal capacity.[102] For instance, it is argued

[92] Draft Articles, Article 4, above n. 89.
[93] Ibid., Article 2.
[94] Case of the Armed Activities on the Territory of the Congo (*Dem. Rep. Congo v. Uganda*), 2005 I.C.J. 116, 214 (Dec. 19).
[95] Draft Articles, Articles 4 and 8, above n. 89
[96] *Condron, S. M.* Getting It Right: Protecting American Critical Infrastructure in Cyberspace. *Harvard Journal of Law and Technology*, No. 20, 2006–2007, pp. 373, 405; see also *Jensen*, above n. 59.
[97] *Eshel, D.* Israel Adds Cyber-Attack to IDF. 10 February 2010. Available: www.military.com/features/0,15240,210486,00.html [last viewed 07.04.2020].
[98] *Beaumont, P.* US Appoints First Cyber Warfare General. *The Observer*, 23 May 2010.
[99] *Goetz, J., Rosenbach, M. and Szandar, A.* National Defense in Cyberspace. *Spiegel Online International*, No. 2, 2009. Available: https://www.spiegel.de/international/germany/war-of-the-future-national-defense-in-cyberspace-a-606987.html [last viewed 07.04.2020].
[100] *Kington, T.* Italy Weighs Cyber-Defense Command. *Defense News*, 31 May 2010. Available: www.defensenews.com/story.php?i=4649478 [last viewed 07.04.2020].
[101] Draft Articles, Article 4, above n. 89.
[102] *Ophardt, J. A.*, Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield. *Duke Law and Technology Review*, No. 9, 2010; see also *Watts, S.* Combatant Status and Computer Network Attack. *Vancouver Journal of International Law*, No. 50, 2010, p. 392.

that the Russian Business Network (RBN) has been involved in the cyber-attacks against Georgia.[103] In such cases, the Article 8 of the ILC Articles provides that "the conduct of a person or group of persons shall be considered an act of a state under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that state in carrying out the conduct." This principle, also known as the "effective control" principle, is derived from the Nicaragua case, where the ICJ argued that for a state to be responsible it is to be proven that a state had "effective control of the military or paramilitary operation in the course of which the alleged violations were committed."[104] This effective control test has also been reaffirmed by the ICJ in the Genocide case.[105] The effective control points towards the fact that the non-state actors cannot be considered under the effective control of a state merely by "financing, organizing, training, and equipping the actors."[106] In contrast to the effective control test the ICTY in Tadic case applied an overall control test to attribute responsibility.[107] The overall control meant not only the "equipping and financing of the group, but also the coordinating or helping in the general planning of its military activity".[108]

In cases of cyber-attacks, some argue for the effective control test to be applied, while others contend that the overall control test is more suitable. Roscini argues in favor of the effective control test due to the clandestine nature and identification problems of cyber-attacks. He explains that the effective control test should be adopted in cyber-attacks cases, as it would prevent states being 'frivolously and maliciously' accused of cyber-attacks.[109] He also argues that the ICTY has applied the overall control test to organized and hierarchically structured groups, but such cyber groups are non-existent. Therefore, the difference of approach between the arguments of the ICTY and the ICJ do not have a bearing on cyber-attacks; the effective control test will continue to apply to them.[110] On the other hand, commentators like Shackleford maintain that the overall control test, which is more flexible and less restrictive, is more suitable for cyber-attacks given the technical challenges to identify the perpetrator in cyber-attacks, and should be adopted "as part of a future international regime" for cyber issues.[111] Under the effective control test, which is more restrictive, victim states may not receive justice even in a worst-case scenario.[112] In some cases, the 'due diligence' principle would apply as stated in the Corfu Channel case,

[103] *Markoff, J.* Before the Gunfire, Cyberattacks. *The New York Times*, 13 August 2008. Available: https://www.nytimes.com/2008/08/13/technology/13cyber.html [last viewed 07.04.2020].

[104] *Military and Paramilitary Activities in and Against Nicaragua* (*Nicaragua v. United States*), ICJ Reports 1986, at para. 115.

[105] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (*Bosnia and Herzegovina v. Yugoslavia (Serbia and Montenegro)*); Order of the Court on Provisional Measures, International Court of Justice (ICJ), 13 September 1993, paras 402–406.

[106] Nicaragua case, above n. 104, para. 115.

[107] *Prosecutor v. Dusko Tadic* (Appeal Judgement), IT-94-1-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 15 July 1999.

[108] Ibid., para 131.

[109] *Roscini*, above n. 15, pp. 39–40.

[110] *Schmitt, M. N.*, Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, No. 54, 2014, pp. 698, 709.

[111] *Shackelford, S. J.* State Responsibility for Cyber-attacks: Competing Standards for a Growing Problem. *Georgetown Journal of International Law*, No. 42, 2011, pp. 971, 987–988.

[112] Ibid., 993.

namely, when a state breaches its "obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[113] The 'due diligence principle' is also adopted within the Tallinn Manual in cases of cyber-attacks.[114] For instance, if a group or individual conducts a cyber-attack by using the cyber infrastructure or computer system that belongs to or is located in the territory of a state, that state will be in breach of the due diligence principle, if it does not take 'necessary or reasonable' steps to prevent such an attack.[115]

4. Remedies in Cyber Warfare

The legal status of a wrongful act does not change, even if that action cannot be attributed to a state.[116] In cases of a wrongful act against a state, the remedy or at least an access to a remedy becomes a necessity. The wrongful act may lead to a dispute among states where the acts cannot be easily attributed to a state or a state does not consider an act to be wrongful. These disputes between state parties may involve legal and political issues. The states are obligated by the UN Charter to settle their disputes peacefully.[117] The PCIJ in *Mavrommatis Palestine Concessions (Jurisdiction)* case has defined dispute among states as "a disagreement over a point of law or fact, a conflict of legal views or of interests between two persons".[118] The state parties may choose a way of peaceful settlement of a dispute, or the UN Security Council may call upon the state parties to settle a dispute peacefully.[119] The methods for the peaceful settlement of disputes include negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, and resort to regional agencies or arrangements.[120] All the methods available to settle disputes peacefully are operative only upon the consent of the particular states.[121] The grounds of a dispute include legal and political matters. The methods of negotiations, mediations, good offices and conciliation deal with the settlement of disputes by using diplomatic offices. The adjudicative methods including arbitration, judicial settlement and to an extent enquiry deals with the disputes in both legal and political perspectives. According to Jennings, "the adjudicative process can serve not only to resolve classical legal disputes, but it can also serve as an important tool of preventive diplomacy in more complex situations".[122] A matter involving transnational cyber-attacks and actions involving cyberspace can be settled through using diplomatic offices, where the issue does not involve complicated factual and legal problems. However, as discussed earlier,

[113] *Corfu Channel Case* (*UK v. Albania*) Judgment, 9 April 1949, ICJ Reports 1949, p. 22.
[114] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd ed, 2017, Commentary to Rule 6 and 7.
[115] *Roscini*, above n. 15, p. 40.
[116] *Whetham and Lucas,* above n. 88, p. 166.
[117] UN Charter, Article 2(3) and Article 33. See also GA Res 2625 (XXV). See also the Manila Declaration on the Peaceful Settlement of International Disputes, GA Resolution 37/590; GA Resolutions 2627 (XXV); 2734 (XXV); 40/9; The Declaration on the Prevention and Removal of Disputes and Situations which may threaten International Peace and Security, GA Resolution 43/51 and the Declaration on Fact-finding, GA Resolution 46/59.
[118] PCIJ, Series A, No. 2, 1924, p. 11.
[119] Ibid.
[120] Ibid.
[121] With the exception of binding Security Council resolutions: see, for example, *Shaw, M.* International Law. 6th Edition, 2008, chapter 22, p. 1241.
[122] *Peck, C. and Lee, R. S.* (eds.). Increasing the Effectiveness of the International Court of Justice. London: Martinus Nijhoff, 1997, p. 79.

the technological development and increasing reliance on technology by state actors makes the actions within cyberspace more technical and difficult to understand. The peaceful settlement of these disputes among state actors would require procedures of enquiry and arbitration or judicial settlement.

In cases of differences of opinion on factual matters, a commission is made for an inquiry to be conducted by reputable observers and specialists to ascertain the facts in contention.[123] The ICJ under its statute has power under Article 51 to entrust "any individual, body, bureau, commission, or other organization that it may select, with the task of carrying out an enquiry or giving an expert opinion". The procedure of inquiry has been used numerous times for the ascertainment of the factual realities.[124] In contemporary issues, according to Malcolm Shaw, inquiry has fallen out of favour as a separate mechanism.[125] The inquiry procedure may nevertheless be instrumental in arbitration between state parties. Perhaps in some circumstances the inquiry has been used more as an arbitration procedure and less as a fact-finding inquiry.[126] In cases of complex issues within cyberspace, the attribution of actions to the state parties would require fact finding inquiries.

The process of arbitration has been instrumental in settlement disputes between states.[127] The decision of an arbitration tribunal is binding upon the states.[128] It is a simple process, whereby the arbitrators are selected by the states, lay down the rules of procedure and laws applicable to the case. There are multiple regional and international dispute settlement bodies for specific purposes. The Permanent Court of Arbitration (PCA) was established in 1899 for the settlement of disputes among states through arbitration procedure.[129] This organ facilitates the states to settle their disputes with any legal issues. There are tribunals with specific scope and expertise, for instance, The International Centre for Settlement of Investment Disputes (ICSID) was established under the auspices of the World Bank by the Convention on the Settlement of Investment Disputes between States and the Nationals of Other States, 1965 and administers *ad hoc*

[123] Inquiry as a specific procedure under consideration here is to be distinguished from the general process of inquiry or fact finding as part of other mechanisms for dispute settlement, such as through the UN or other institutions. See *Lillich, R. B.* (ed.). Fact-Finding Before International Tribunals. London: Brill, 1992.

[124] See, for instance, Bar-Yaacov, *N.* The Handling of International Disputes by Means of Inquiry. 1975, chapter 3; See also *Merrills, J. G.* International Dispute Settlement. 2011, p. 47; and *Scott, J. B.* The Hague Court Reports, 1916, p. 403.

[125] *Shaw*, above n. 121, p. 1022.

[126] *Merrills*, above n. 124, p. 56.

[127] In recent years, states have relied upon the arbitration procedure for peaceful settlements of disputes, the Eritrea – Yemen arbitration 114 ILR, p. 1 and 119 ILR, p. 417; Eritrea – Ethiopia Arbitration see 129 ILR, p. 1; See also *Shaw, M.* Title, Control and Closure? The Experience of the Eritrea–Ethiopia Boundary Commission. *International and Comparative Law Quarterly*, No. 56, 2007, p. 755; See also *the Guyana v. Suriname Maritime Delimitation Case,* award of 17 September 2007.

[128] See the Nottebohm Case (*Liechtenstein v. Guatemala*); Second Phase, International Court of Justice (ICJ), 6 April 1955, 111, 119; See also Arbitration Commission on Yugoslavia, Interlocutory Decision of 4 July 1992, 92 ILR, pp. 194, 197.

[129] *Hudson, M. O.* The Permanent Court of International Justice 1920–1942 (1943), p. 11; *Hamilton, P.* et al. (eds.). The Permanent Court of Arbitration: International Arbitration and Dispute Settlement. 1999; *Allain, J.* A Century of International Adjudication: The Rule of Law and its Limits. 2000, chapter 1; and *Jonkman, J.* The Role of the Permanent Court of Arbitration in International Dispute Resolution, in addresses on 6 and 27 July 1999 at the Hague Academy of International Law, Peace Palace, The Hague, on the Occasion of the Centennial Celebration of the Permanent Court of Arbitration, Vol. 279, 1999, p. 9.

arbitrations.[130] The jurisdiction of the centre extends to "any legal dispute arising directly out of an investment, between a contracting state [..] and a national of another contracting state, which the parties to the dispute consent in writing to submit to the Centre".[131] There are various bilateral and multilateral treaties giving jurisdiction to the ICSID in cases of disputes among the parties.[132] Other arbitration tribunals exist for specific purposes, for instance, the Court of Arbitration for the International Chamber of Commerce.[133] Hence, there are numerous dispute settlement bodies with specific powers, functions and jurisdiction. The common feature of these bodies is that they mostly work with a specific expertise and defined laws to apply in specific cases and adopt rules to carry on the procedure swiftly. There is no dispute settlement body for disputes related to cyberspace. The option for states with disputes related with cyberspace is to refer the matters to the PCA, however, the issues involving enquiries and more technical questions will require cyberspace specialists along with legal experts to deal with the disputes.

In addition to the arbitration procedures, the states may approach the International Court of Justice (ICJ) in cyberspace issues. In cases where violation of the UN Charter is in contention or the issue of non-intervention is involved, the ICJ may be consulted for reparations. The quantification of losses occurred due to the alleged attacks will be difficult; the collection of data from multiple institutions in multiple states would be a daunting task for the ICJ.[134] The jurisdiction of the ICJ is also limited, with compulsory jurisdiction in very few cases where states themselves have agreed to provide jurisdiction in similar cases. Moreover, it may issue advisory opinions on request under Article 96 of the UN Charter. Although the opinions are non-binding, they still are instrumental in the development of international law.[135] However, the opinions of the ICJ do not provide any appropriate remedy to the state parties.

In cases of the failure of the peaceful settlement of disputes, the state parties may, under Article 37(1) of the UN Charter, refer the matter to the Security Council, if the matter may endanger the maintenance of peace and security. Under the Chapter VII of the UN Charter, the Security Council has the authority to determine the existence of any threat to peace, breach of peace, or act of aggression.[136] The cases of an "unfriendly act" or an "ordinary breach of international law,"[137] do not come within the prohibition of a "threat or use of force", as that

[130] See *Lowenfeld, A. F.* International Economic Law. Oxford: Oxford University Press, 2008, p. 536; *Dolzer, R. and Schreuer, C.* Principles of International Investment Law. Oxford: Oxford University Press, 2008, p. 222; *Schreuer, C.* The ICSID Convention: A Commentary (2001); *Broches*, The Convention on the Settlement of Investment Disputes. *Columbia Journal of Transnational Law*, No. 3, 1966, p. 263; *Wetter, J. G.* (ed.). The International Arbitral Process: Public and Private. London: Oceana Publishers, 1979, p. 139; and *Muchlinski, P.* Multinational Enterprises and the Law. Oxford: Oxford University Press, 1995, p. 540.

[131] Article 25(1), The Convention on the Settlement of Investment Disputes.

[132] See *Pogany, I.* The Regulation of Foreign Investment in Hungary. 4 ICSID Review – *Foreign Investment Law Journal*, 1989, pp. 39, 51. See also *The Case of Asian Agricultural Products v. Sri Lanka*, 30 ILM, 1991, p. 577. See e.g. article 1120 of the NAFTA Treaty, 1992 and *Metalclad Corporation v. United Mexican States*, 119 ILR, p. 615. See also Article 26(4) of the European Energy Charter, 1995.

[133] See *Wetter*, above n. 130, p. 145.

[134] See *Roscini*, above n. 27, 111.

[135] See, for example, *Conforti, B.* The Law and Practice of the United Nations. Leiden: Martinus Nijhoff, 2005, p. 276.

[136] UN Charter, Art. 39.

[137] *Dinstein*, above n. 73.

term is used in Article 2(4) of the United Nations Charter. As discussed earlier in this article, an "inherent" right of self-defence is only triggered when "an armed attack occurs against a member of the United Nations."[138] The classification of a cyber-attack into an armed attack is contentious and open to interpretation from different perspectives. The lack of amicable remedies available to states against any cyber-attack will create more confusion with regard to the issues at hand and make the situation more complicated. It will present a serious threat to international peace and security, keeping in mind the growing importance of technological advances. Henceforth, a timely, efficient and relevant remedy must be provided to cover different aspects of the cyber-attacks.

5. Conclusion/Proposing a Dispute Resolution Mechanism

Keeping in view the discussion so far, let us consider the remedies available to the state A in a situation where the state authorities of the state B or other non-state entities working through transnational co-operation takes control of critical infrastructure of the state A through cyberspace operations. The attacks are conducted through DDoS mechanism or other available mechanisms coming under the realm of cyber-attacks; severely affecting the state A's economy. In a separate set of CNE attacks, some classified data dealing with the state A's defense mechanism is broken into, endangering the security of the state A. The economy and defense mechanism of the state A is in jeopardy because of the sudden cyber infiltrations. If the legal experts ponder over the situation in the state A in order to find legal measures of retaliation against the state B, firstly, they will have to establish that the attacks amount to armed attacks or international wrongful acts and secondly, they are attributable to the state B. The options of taking measures in self-defense can be explored after the attribution. However, as discussed above, there are difficulties in classifying such activities as armed attacks. Even if the intensity of the attacks can be used for considering them to be armed attacks, they need to be attributed to the state B. In cases where the state B officially recognizes the attack or takes responsibility, the matter becomes a bilateral issue to be solved by any available dispute resolution mechanism. In cases where the state B does not take responsibility, the issue would require an enquiry for attribution of the acts to a state. The enquiry may be carried out, if the UN Security Council passes a resolution mandating an enquiry committee, whereby a special committee would be formed on case by case basis. In cases of attribution of the acts to private entities, the cybercrimes law will apply to the criminal activities. In cases where the attacks can be attributed to a state, the options of legal remedies still remain very meagre. To be precise, there are no viable remedies for the state A in these circumstances; it has to take actions of its own cognizance. This might result in a severe danger to international peace and security. The questions related to the responsibilities of the states with regard to cyber-attacks in any form are not easy to answer. The ICRC notes that "it would appear that the answer to these questions will probably be determined in a definite manner only through future state practice."[139] In these particular cases, the states have limited options

[138] UN Charter, Art. 51.
[139] ICRC Report, above n. 41, 37.

of remedies, as the co-operation of one or more state actors is required in such transnational activities.

With such an imminent threat to the international peace and security, it is important to regulate state practice in order to come up with viable remedies available to the states. Thus, the state practice would amount to the development of law dealing with transnational cyber-attacks or cyber warfare in a broader perspective. An intermediary dispute settlement body which applies the existing principles upon the use of new technologies in cyberspace will be instrumental in regulating the state response to cyber-attacks. The customary international law will develop through the practices of this intermediary body offering a dispute resolution mechanism. There can be options of adopting specific rules for cyberspace operations, for example, a framework International Law for Information Operations (ILIO) as prescribed by Hollis.[140] It will offer and describe the cyber operations upon empirical evidence and will provide perspectives on unforeseen developments in cyberspace. This will be insufficient in cases where unseen technological equipment and methods are used in cyber-attacks.

Alternatively, the suggested dispute settlement mechanism will offer solutions based on factual circumstances of the case and develop laws through application of rules related with *jus ad bellum*. The wisdom through which international law has developed suggests that cyber warfare can be effectively regulated by the analogical approach. The rules which develop with state practice can then be devised within a framework forming a basis for customary international law. The states will be hesitant to accept any framework for cyberspace regulation because of the uneven pace of technological development of information systems. For instance, the suggestion for the formulation of new rules with regard to prohibition of new weapons within the information system was not taken positively by states.[141]

In order to deal with the transnational cyberspace issues and the limited remedies available to states, it is recommended that an Arbitration and Enquiry Tribunal for Transnational Cyberspace Operations (AETTCO) shall be formed. The states are in a situation of confusion, as far as the question of the legality of cyber-attacks is concerned. There are no specific norms regulating these situations; nor do the current norms remove the perplexities. The formation of AETTCO will help to eliminate confusion and doubt; it will develop state practice concerning this issue by providing adequate remedies and reduce the threat that cyber warfare poses to international peace and security. It is not, however, intended to offer details on the composition and working of the AETTCO, we aim to leave it for further discussion. However, we submit that it would be a viable solution in this challenging scenario.

---

[140] See *Hollis*, above n. 6.

[141] See Letter Dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations Addressed to the Secretary-General, U.N. GAOR, 53rd Session, U.N. Doc. A/C.1/53/3(1998). Available: http://daccessdds.un.org/doc/UNDOC/GEN/N98/284/58/PDF/N9828458.pdf [last viewed 07.04.2020]; The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/54/213 (Aug. 10, 1999) (of nine states submitting views, only Cuba and Belarus favored negotiations to restrict information warfare). Ultimately, the U.N. General Assembly passed Resolution 53/70, calling on Member States simply to promote consideration of existing and potential threats to information security. U.N. GAOR, 53rd Session 79th plenary meeting, at 1, U.N. Doc. A/RES/53/70 (Jan. 4, 1999).

We can safely pronounce the issues which the AETTCO can address in current situation. It has been discussed in detail that the attribution issues in cases of cyber-attacks can be a main hurdle in attaching responsibility. As we have no specific international body working on cyberspace-related transnational issues, the matter of investigation becomes solely states' own burden with limited co-operation. It is thereby suggested that the AETTCO should address the main issue of enquiry by independent and neutral investigators, the member states being under an obligation to co-operate in such enquiries. In cases where an act may be attributed to non-state actors, the issue can be resolved by the arbitration tribunal which should come up with a solution acceptable to all state parties. Moreover, in the current situation it will take years for the law related to cyber warfare to develop, creating a state of confusion for all actors. Thus, it will be difficult for states to forecast the outcome of any attacks against them or the legality of cyber operations they are involved in.

The current system offers no mechanism for investigating the cyber-attacks. The cyber espionage, for instance, introduces a new dimension to the covert operations previously committed by states. With perpetrators residing in different locations and hiding their identity, there is a far greater apprehension of state sovereignty being compromised. Hence, the AETTCO will provide a defense against such interventions through enquiry and arbitration by cyberspace and international law experts. The alternative to AETTCO may be to come up with a framework allowing states to intervene in their territories in cases of alleged cyber-attacks from their territory.[142] A unilateral action inside the territory of another state in retaliation to cyber-attacks will not be a solution-based option. Our contention is to safeguard the principle of non-intervention and use an international body to investigate and recommend states to comply with existing international rules.

It is suggested that a specialized body with powers of enquiry and arbitration shall be made within the United Nations system; preferably, by the UN Security Council, as the increasing use of cyberspace is becoming a threat to international peace and security. The specialized body (AETTCO) should also be able, upon request, to give an expert opinion to the UN Security Council on issues where interpretation of current principles of international law is necessary. The AETTCO would be influential in drafting specific rules on regulation of cyberspace according to the developing technologies in this field. The international law dealing with cyber warfare must evolve, focusing on providing remedies and developing state practice. The suggested specialized body (AETTCO) should focus on both these elements for developing the international law and practices.

Summary

The reality of cyber operations in global perspective is undisputable. One major effect of the cyber operations is their transnational nature threatening state sovereignty and international peace and security. This threat is unconventional and unprecedented but, nevertheless, real, hence, it is pertinent to know, which forms of cyber operations imperil state sovereignty. Some actions within the cyber operations can be regulated through already established norms and international laws. In some cases, the cyber operations require further actions

[142] *Hollis*, above n. 6, p. 1055.

to avoid a future catastrophe and threats to international peace and security. It is noted that the grievance mechanism in cases of cyber operations threatening state sovereignty is unfounded. The threat looming international security because of cyber operations can be negated with a viable grievance mechanism. The proposed Arbitration and Enquiry Tribunal for the Transnational Cyberspace Operations (AETTCO) is a grievance mechanism through which a major threat to the international peace and security can be avoided.

Sources

Bibliography

1. *Allain, J.* A Century of International Adjudication: The Rule of Law and its Limits. Hague: T.M.C. Asser Press, 2000.
2. *Bar-Yaacov, N.* The Handling of International Disputes by Means of Inquiry. Oxford: Oxford University Press, 1975.
3. *Beaumont P.* US Appoints First Cyber Warfare General. *The Observer*, 23 May 2010. Available: https://www.theguardian.com/world/2010/may/23/us-appoints-cyber-warfare-general [last viewed 07.04.2020].
4. British Broadcasting Corporation (BBC). US launched cyber-attack on Iran Weapons Systems, 2019. Available: https://www.bbc.com/news/world-us-canada-48735097 [last viewed 07.04.2020].
5. *Broches, A.* The Convention on the Settlement of Investment Disputes. *Columbia Journal of Transnational Law*, No. 3, 1966, p. 263.
6. *Brown, D.* A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict. *Harvard International Law Journal*, No. 47, 2006, p. 179.
7. *Bogdandy A. and Wolfrum R.* (eds.). Max Planck Yearbook of United Nations Law. Leiden: Martinus Nijhoff Publishers, 2010.
8. *Brenner, S. W.* At Light Speed: Attribution and Response to Cyber- Crime/Terrorism/Warfare. *Journal Criminal Law and Criminology*, No. 97, 2007, p. 424.
9. *Carr, J.* Inside Cyber Warfare. 2nd ed., California: O'Reilly, 2012.
10. *Chesterman, S.* The Spy Who Came in from the Cold War: Intelligence and International Law. *Michigan Journal of International Law*, No. 27, 2006, p. 1071.
11. *Clarke, R. A. and Knake R.* Cyber War: The Next Threat to National Security and What to Do About It. New York: Harper Collins, 2010.
12. *Condron, S. M.* Getting it Right: Protecting American Critical Infrastructure in Cyberspace. Harvard Journal of Law and Technology, No. 20, 2007, p. 403.
13. *Conforti, B.* The Law and Practice of the United Nations. Leiden: Martinus Nijhoff, 2005.
14. *Cox, S.* Confronting Threats through Unconventional Means: Offensive Information Warfare as a Covert Alternative to Preemptive War. *Houston Law Review*, No. 42, 2005, p. 881.
15. Cyber Security: A Pillar of our Digital World. 2019. Available: https://new.siemens.com/global/en/company/stories/research-technologies/cybersecurity.html#30yearsofcybersecurity [last viewed 07.04.2020].
16. *DiCenso, D. J.* Information Operations: An Act of War? *Air and Space Power Chronicles*, July 2000. Available: http://www.iwar.org.uk/iwar/resources/airchronicles/dicenso1.htm [last viewed 07.04.2020].
17. *Dinniss, H. H.* Cyber Warfare and the Laws of War. Cambridge: Cambridge University Publishers, 2012.
18. *Dinstein, Y.* Computer Network Attacks and Self Defense, International Law Studies No. 76, 2002, p. 99.
19. *Dörmann, K.* Applicability of the Additional Protocols to Computer Network Attacks. 2004. Available: http://www.icrc.org/eng/assets /files/other/applicabilityofihltocna.pdf [last viewed 07.04.2020].
20. *Dolzer, R. and Schreuer, C.* Principles of International Investment Law. Oxford: Oxford University Press, 2008.
21. *Doward, J.* Brittain Fends off Flood of Foreign Cyber Attacks. *The Observer*, 7 March 2010. Available: https://www.theguardian.com/technology/2010/mar/07/britain-fends-off-cyber-attacks [last viewed 07.04.2020].
22. *Ebbesson, J. et al.* (eds.). International Law and Changing Perceptions of Security. London: Brill Nijhoff, 2014.

23. *Eshel, D.* Israel Adds Cyber-Attack to IDF. 10 February 2010. Available: www.military.com/features/ 0,15240,210486,00.html [last viewed 07.04.2020].
24. *Gjelten, T.* Seeing the Internet as an Information Weapon. 2010. Available: http://www.npr.org/templates/story/story.php?storyId=130052701 [last viewed 07.04.2020].
25. *Goetz, J.*, *Rosenbach, M. and Szandar, A.* National Defense in Cyberspace. *Spiegel Online International*, No. 2, 2009. Available: https://www.spiegel.de/international/germany/war-of-the-future-national-defense-in-cyberspace-a-606987.html [last viewed 07.04.2020].
26. *Graham, D. E.* Cyber Threats and the Law of War. Journal National Security Law and Policy, No. 4, 2010, p. 87.
27. *Green, J. A.* (ed.). Cyber Warfare: A Multidisciplinary Analysis. London: Routledge, 2015.
28. *Hamilton, P.* et al. (eds.). The Permanent Court of Arbitration: International Arbitration and Dispute Settlement, 1999.
29. *Handler, S. G.* The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare. Stanford Journal of International Law, No. 48, 2012, p. 209.
30. *Haslam, E.* Information Warfare: Technological Changes and International Law. *Journal of Conflict and Security Law*, No. 5, 2000, p. 157.
31. *Hollis, D. B.* Why States Need an International Law for Information Operations. *Lewis and Clark Law Review*, No. 11, 2007, p. 1023.
32. *Holmberg, E. J.* Armed Attacks in Cyberspace. Thesis on file at Stockholm University, 2015. Available: http://www.diva-portal.org/smash/get/diva2:854660/FULLTEXT01.pdf [last viewed 07.04.2020].
33. *Hudson, M. O.* The Permanent Court of International Justice 1920–1942. New York: McMillan, 1943.
34. *Jensen, E. T.* Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense. *Stanley Journal of International Law*, No. 38, 2002, p. 207.
35. *Jenkins, M. A.* Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places? *Naval Law Review*, No. 51, 2005, p. 132.
36. *Jochnick, C. and Normand, R.* The Legitimation of Violence: A Critical History of the Laws of War. *Harvard International Law Journal*, No. 35, 1994, p. 49.
37. *Kanuck, S. P.* Information Warfare: New Challenges for Public International Law. *Harvard International Law Journal*, No. 37, 1996, p. 272.
38. *Kington, T.* Italy Weighs Cyber-Defense Command. *Defense News*, 31 May 2010. Available: www.defensenews.com/story.php?i=4649478 [last viewed 07.04.2020].
39. *Kuehl, D. T.* Cyberspace to Cyberpower: Defining the Problem. In: Cyberpower and National Security, *Kramer, F. D., Starr, S. H., and Wentz, L.* (eds.). Washington: Potomac Books, 2009.
40. *Lillich, R. B.* (ed.). Fact-Finding Before International Tribunals. London: Brill, 1992.
41. *Markoff, J.* Before the Gunfire, Cyberattacks. *The New York Times*, 13 August 2008. Available: https://www.nytimes.com/2008/08/13/technology/13cyber.html [last viewed 07.04.2020].
42. *Lowenfeld, A. F.* International Economic Law. Oxford: Oxford University Press, 2008, p. 536.
43. *Merrills, J. G.* International Dispute Settlement. Cambridge: Cambridge University Press, 2011.
44. McAfee Report. In the Crossfire – Critical Infrastructure in the Age of Cyber War. 2010. Available: http://resources.mcafee.com/content/NACIPReport [last viewed 07.04.2020].
45. *Muchlinski, P.* Multinational Enterprises and the Law. Oxford: Oxford University Press, 1995.
46. *Nguyen, R.* Navigating Jus ad Bellum in the Age of Cyber Warfare.*California Law Review*, No. 101, 2013, p. 1079.
47. *Ohlin, J. D.*, *Govern, K.*, *and Finkelstein, C.* (eds.). Cyberwar, Law and Ethics for Virtual Conflicts. Oxford: Oxford University Press, 2015.
48. *Ophardt, J. A.* Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield. *Duke Law and Technology Review*, No. 9, 2010, p. 1.
49. *Peck, C. and Lee, R. S.* (eds.). Increasing the Effectiveness of the International Court of Justice. London: Martinus Nijhoff, 1997.
50. *Pedrozo, R. A. and Wollschlaeger, D. P.* (eds.). International Law and the Changing Character of War. Newport: U.S. Naval War College, 2011.
51. *Pogany, I.* The Regulation of Foreign Investment in Hungary, 4 ICSID Review. *Foreign Investment Law Journal*, 1989, p. 39.
52. *Rid, T.* Cyber War Will Not Take Place. *Journal of Strategic Studies*, No. 35, 2012, p. 5.
53. *Roscini, M.* Cyber Operations and the Use of Force in International Law. Oxford: Oxford University Press, 2014.
54. *Ruys, T.* Armed Attack and Article 51 of the UN Charter: Evolutions in Customary Law and Practices. Cambridge: Cambridge University Press, 2010.

55. *Schmitt, M. N.* Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, No. 54, 2014, p. 698.
56. *Schmitt, M. N.* Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, No. 37, 1999, p. 885.
57. *Schmitt, M. N.*, Legitimacy Versus Legality Redux: Arming the Syrian Rebels. *Journal of National Security, Law & Policy*, No. 7, 2014, p. 139.
58. *Schmitt, M. N.* (ed.). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press, 2013.
59. *Schmitt, M. N. and O'Donnell, B. T.* (eds.). Computer Network Attack and International Law. Newport: Naval War College, 2001.
60. *Schreuer, C.* The ICSID Convention: A Commentary. Cambridge: Cambridge University Press, 2001.
61. *Shackelford, S. J.* From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. *Berkeley Journal of International Law*, No. 27, 2009, p. 192.
62. *Shackelford, S. J.* State Responsibility for Cyber-attacks: Competing Standards for a Growing Problem. *Georgetown Journal of International Law*, No. 42, 2011, p. 971.
63. *Sharp, W. G.* Cyberspace and the Use of Force. Virginia: Aegis, 1999.
64. *Shaw, M.* Title, Control and Closure? The Experience of the Eritrea–Ethiopia Boundary Commission. *International and Comparative Law Quarterly*, No. 56, 2007, p. 755.
65. *Silver, D. B.*, Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter. *International Law Society*, No. 76, 2002, p. 73.
66. *Springer, P. J.* (ed.). Encyclopedia of Cyber Warfare. California: ABC-CLIO, 2017.
67. *Sudworth*, *J.* New "cyber attacks" hit S. Korea. *BBC News*, 9 July 2009. Available: http://news.bbc.co.uk/1/hi/world/asia- pacific/8142282.stm [last viewed 07.04.2020].
68. *Swaine, J.* Georgia: Russia Conducting Cyber War. *The Telegraph*, 11 August 2008. Available: https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html [last viewed 07.04.2020].
69. *Swanson, L.* The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict. *Loyola of Los Angeles International and Comparative Law Review*, No. 32, 2010, p. 303.
70. The United States National Security Strategy. 2010. Available: www.whitehouse.gov/sites/defsult/files/rss_viewer/national_security_strategy.pdf [last viewed 07.04.2020].
71. *Tsagourias, N.* Cyber-attacks, Self-defence and the Problem of Attribution. *Journal of Conflict and Security Law*, No. 17, 2012, p. 229.
72. *Tubbs, D. Luzwick, P. G. and Sharp*, W. G. Technology and Law: The Evolution of Digital Warfare. *International Law Society*, No. 76, 2002, p. 7.
73. *Tzu, S.* The Art of Warfare. In: *Giles, L.* (transl.), Sun Tzu on the Art of War, 2000.
74. *U. S. Department of Defense*. The National Military Strategy for Cyberspace Operations. 2006. Available: www.dod.gov/pubs/foi/ojcs/ 07-F-2105doc1.pdf [last viewed 07.04.2020].
75. United States National Military Strategy for Cyberspace Operations. 2006. Available: www. dtic.mil/doctrine/new_pubs/jp3_13.pdf [last viewed 07.04.2020].
76. *Watts, S.* Combatant Status and Computer Network Attack. *Vancouver Journal of International Law*, No. 50, 2010, p. 392.
77. *Wetter, J. G.* (ed.). The International Arbitral Process: Public and Private. London: Oceana Publishers, 1979.
78. *Wheeler, D. A. and Larsen*, *G. N.* Techniques for Cyber Attack Attribution. Institute for Defense Analysis, IDA Paper P-3792.

Case Law

1. *Asian Agricultural Products v. Sri Lanka* 30 ILM, 1991, 577.
2. *Democratic Republic of Congo v. Uganda*; 2005 I.C.J. 116, 214 (Dec. 19).
3. *Nicaragua v. United States of America*, Merits, (ICJ), 27 June 1986,
4. *Prosecutor v. Dusko Tadic* (Appeal Judgement), IT-94-1-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 15 July 1999.
5. *UK v. Albania* (Corfu Channel Case), Judgment, 9 April 1949, ICJ Reports 1949.

Other Sources

1. Draft Articles on the Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/CN.4/L.602/Rev. July 26, 2001.