The Legality of Cyberwar from Revolution to Evolution

Metodi HADJI-JANEV
Military academy "General Mihailo Apostolski", Skopje, University "Goce Delcev", Shtip, Macedonia
Ira A. Fulton School of Engineering, Arizona State University, ASU, U.S.A.
metodi.hadzi-janev@ugd.edu.mk, hadzijanev@gmail.com

Abstract: Information and communication technologies have caused an enormous effect on international security. State and non-state actors, among others, are using these technologies to achieve strategic objectives, and thus have spurred the changing character of war. Applicability of international law in the future cyberwar have dominated the legal and operational academic environment for quite a while. This article assumes that cyberwar is possible. The main subject of analysis throughout the article is the evolution of the applicability of international law to cyberwar. The article also provides a brief overview of the existing challenges in this context.
Keywords: International law, Cyber war, Changing character of war, Ius ad bellum, Ius in bello

INTRODUCTION

The development of information and communications technologies (ICT), the changes in international relations and the need of the military to cope with these changes have influenced the "changing character of war". States' interests, threat perceptions and the requirements of the sovereign (the states' authorities) to protect under the changed security reality among others have also contributed to the "changing character of war". At the same time, these dynamics and processes in the globalized world have urged the global power redistribution which caused states to lose the monopoly of power. Non-state actors (violent groups and individuals, NGO's and private corporates) emerged as power consumers and power employers and thus, have started to feed the "fog of war" along with the state actors. Like never before, non-state actors and some states can lunch operations through cyberspace and emerge as a peer adversary to the mightier military asymmetrically and unconventionally. The ability to exploit cyberspace in a way that is impossible to exploit physical space has affected the ability to distinguish between peace and war.

Changes in the concept of warfighting in the age of ICT have stimulated (along with additional factors) a discourse of political perception of the meanings "the use of military" and "the use of force". At the same time in pursuit of their interest (duty to protect and to influence international community) states are trying to apply existing international principles and standards that regulate peace and wartime behavior, rights and obligations of states.

Questions about the relevance of the existing principles and standards of international law in the future cyberwar have dominated the legal and operational academic environment for quite a while. The article explores the evolution of stats' approach over the applicability of international law to cyberwar. The main assumption during the debate and research was that cyberwar is a possible option in the stats' pursuit to accomplish their political objectives and is driven by states' interest and threat perception. Consequently, the argument is that states' position over the applicability of international principles and standards of

international law to cyberwar has evolved as the state's interest (i.e. necessity, ability and duty to protect and influence) and threat perception (from the domain of opportunity to domain of vulnerability) have evolved. Therefore, the article first analyzes how in the age of ICT the character of war has changed. Then, drawing on these conclusions it briefly explores how states' positions over the applicability of international law to cyberwar evolved. A short analysis of some of the reasons for the differences that have aroused is also presented. Finally, it surmises some of the existing challenges in the applicability of international law to cyberwar. Eventually, these changes affected the ability for power projection, where military or use of force and ability for and actual warfighting is an instrument of national power. Put in the words of the operational wisdom's thinkers while the nature of war remained the same, technology affected its character and caused the change.

TECHNOLOGY, POLICY AND CHANGING CHARACTER OF WAR IN THE NEW "DIGITAL" SECURITY REALITY

Technology has always been a key in the revolution of military warfighting and "changing character of war". The entire development of historical warfare has coincided and evolved parallel to the technological developments that serve to make warfare possible in increasingly efficient ways.(Ryan, 1995) Fuller (1946), like many others, have observed that technology changes society and consequently, this affects warfare. Similarly, Toffler (1995), asserted that "*since the force of technology transforms our economy and society, it will transform war as well*". Even though, the ultimate goal of warfighting remained the same over time, i.e. use of force to coerce and impose political will to the opponents, technology proved to be the game-changer in terms of how opponents fought, where they fought and with what they fought (Townshend, 2000). Precisely, throughout history technological development affected the methods of warfighting (strategy, doctrine, and tactics), actors in warfighting (the distinction between combatants, non-combatants, illegal combatants) and means of warfighting (i.e. weapons and ammunition) (ICRC, July, 2004).

The rise of the ICT affects the time and space driven operational environment and have arguably caused a revolution in warfighting. Interconnectivity and accessibility (i.e. the ability of civilians and non-state actors to possess them and have access) to these technologies have started to transform the essential military functioning. On one hand, the ICT and interconnectivity multiply the capacities (and thus are a force multiplier). On the other, these same technologies opened vulnerabilities. Unpredictability and accessibility have become the top priority concerns of these technologies. The commodity of predictability for which Machiavelli wrote, *….an army must move in an orderly manner, and you will, therefore, be able to draw up your forces*" (Machiavelli, 1965), is gone. The element of surprise thus changes everything in terms of planning and preparedness. Furthermore, unlike conventional and traditional threats states no longer have the luxury to know the origin of the attack – i.e. cyber-attacks. This revolutionary shift spurred by technology has militarized the internet (Deibert, 2003).

Cyberwar and the operations in the cyberspace span not just throughout the military phases (NATO, 2016), but also through the diplomatic concepts (conflict prevention (UN Secretary General Report 1992), conflict management (Borisoff & Viktor, 1989), conflict resolution (Yasuaki, 2017) and transit from conflict to peace processes (The Secretary General of the United Nations, 2009). As

a result, the lines between peace and war status are blurred. Consequently, the cyberwar type of activities blend the existing legal construct that separate peace and war. This is understandable since cyberspace does not recognize geographical and physical boundaries. Activities in cyberspace can be launched from everywhere, at any time, and can be easily hidden. A cyber-attack can remotely affect critical infrastructure and cause cascade effects, scale and effects (mass casualties and material damage) equal to the effects of war. Furthermore, information sent via cyberspace can be altered, manipulated and can undermine the trust among the allies and any diplomatic attempt for peaceful settlement of disputes. As a result, some have even tried to propose that in the ICT world the "nature" not just the character of war has changed (Wooding, September 1, 2019).

The Oxford-based Changing Character of War Centre (CCW)'s research concluded that in the changed environment states are no longer the sole actors that matter in conflict (CCW, 2015-2017). Addressing the shift in the power balance they asserted that the ambiguity (their approach to Clausewitz's "fog of war" (Clausewitz, 1989)) is comprised of violent non-state groups, hybridity, urban, peripheral and maritime space and the information age (CCW, 2015-2017). Others have also addressed the ambiguity emphasizing blurring lines between peace and war where interconnectivity and ICT were prescribed as the drivers of the "changing character of war", (Sussman, Dec 27, 2019; Joseph, 1992).

Regardless of the different approaches and debates on the issue, the change in the character of war under the pressure of cyberwar type activities is evident and it raises many legal concerns in the context of the possibility to wage cyberwar. Questions about the relevance of the existing principles and standards of international law in the future cyberwar have dominated the legal and operational academic environment for quite a while. The evolution of this approach, however, is in the core interest.

INTERNATIONAL LEGAL ASPECTS OF CYBER WARFARE: THE EVOLUTION OF THE APPROACH AND THE CHALLENGES TO IT

The idea of international law in most general view is to regulate the relations and behavior of states as international actors. It consists of a set of rules, norms, and standards generally accepted in relations between states. It establishes normative guidelines and a common conceptual framework to guide states across a broad range of domains, including war, diplomacy, trade, and human rights.There is a general tendency that the law reflects the reality and applies even when a change in international relations is evident. However, when new technologies are developed, they often present challenges for the application of existing bodies of law. The same applies to the changed security environment and as a result, the threat perceptions and the proper response by states to the security challenges. Although states drive the process of the change (including by interest and perceptions, (Slomanson, 2011, pp 4-5)) and adaption of the law, (as a result of the change we have addressed above) non-governmental advocacy groups, international organizations, international tribunals, domestic constituencies, political action groups, religious leaders, etc. stimulate this change (Michael, 2013).

[1] *Ius contra bellum* - part of the international law that contains principles and standards for peaceful settlement of disputes, *Ius ad bellum* refers to a set of criteria that are to be consulted before engaging in war in order to determine whether entering into war is permissible. *Ius in bello* represent a set of criteria principles and standards (body of law)) that governs the way in which warfare is conducted; *ius post bellum* - principles and standards after the conflict resolutions

The article 38 of the Statute of the International Court of Justice regulates the sources of international law (Statute of the International Court of Justice, 1945, art.38). In this line, Schmidt observed that broadly, "*international law represents a consensus among states as to the rules of the game that govern their interactions. They consent thereto either by opting into treaty regimes or by engaging in practices out of a sense of legal obligation (opinio juris) that, combined with similar practice by other states, eventually crystallizes into customary international law*" (Schmitt, 2014, pp. 273). States have interests and consent, but also obligations that more or less drive the development of international law and are thus, the engine of normative evolution (Schmitt, 2014, pp. 273).

The same conclusions resonate with the applicability of international principles and standards to cyberwar and cyber operations. In general, states' approach to the issue as in other similar cases is driven by their threat perceptions which shape the interest (ranging from protecting economic interests, through effective governance up to existential threats from cyberspace). Technical advancement and interconnectivity are just another reason that feeds the state's interest. The more technologically developed the state is the more vulnerable to cyber threats is Bures, (Oldrich, 2010). Legal position over the applicability of international law to cyberwar thus, consequently, reflects the states' interest (their threat perception and technical development) (Rovira, 2014, p765-793. It is important of course to emphasizes that good practices and the core values based behavior is also something that shapes states› interest in contributing to the practice of law and thus, contributes toward law development. Therefore, it is quite normal that states that have an interest are stimulating debates and are trying to shape the interpretation of international law or to stimulate change that will serve in their best interest (Schmitt, 2014).

There is general acceptance that the agreement over the applicability of international law to cyberwar types of activities among the states has evolved. If in the early 2000' only some states such as the US and to some extent the UK have vouched for the applicability of the international law to cyberwar (cyber operations) today the number of states that support this idea and have developed appropriate policies and strategies for cyber defense activities is gradually higher. The evolution of the approach over the applicability of the law to cyberwar is driven by the lex ferenda (what the law should be) interpretation context. States' approach in this line could be systematized in three aspects. First, in the tendency of the state to control the internet, or the peacetime regime (mostly driven by privacy vs. security-necessity to protect). Second, the tendency to launch massive cyber and physical military operations to protect from malicious cyber-based threats, or the *ius ad bellum* aspects of the law. Third, the tendency to apply principles and standards of international law that regulate methods of warfare, participants (or protected persons) in war and weapons and specific ammunition during the wartime, or the *ius in bello*.

When it comes to controlling the internet, liberal states' position evolved from pricing freedom during 80' and 90' to demand protection (security) in early 00' and present. For example, former US Secretary of State George P. Shultz argued in 1985 that controlling information technologies is both democratically and economically inappropriate (Kedzie, & Aragon, 2002). Similarly, former U.S. President Bill Clinton in 2000 said: "*Trying to control the Internet is like trying to nail Jell-O to the wall*" (Allen-Ebrahimian, 2016). Over time, however, as the character of the war changed under the pressure of the new

ICT liberal democracies adopted regulations that allow the development of procedures and practices intrinsic for the authoritarian regimes (Betz, & Stevens, 2012, p.67). The UK Investigatory Powers Bill, according to Woollacott's view, was a close resemblance to the legal regimes in China and Russia and thus, was struck down by the European Court of Justice as being in violation of democratic norms (Woollacott, 2016). A clear shift in the approach (from freedoms and privacy to state control in the name of security) may be the global initiative for "exceptional access" into cryptographic messengers led by the U.S., U.K. France, and Germany (Schulze, 2016). Similar measures were adopted by Russia (Szolara, 2016) and China (Geirow, 2016). Although the goals may differ, both liberal states' and authoritarian states have adopted very similar measures in the national security documents (Shafqad & Masood, 2016).

Different states' interest (in terms to protect and influence in the ICT has driven world) resulted in different suggestions of how the interpretation of existing principles and standards of law should apply to cyberwar and even how to prioritize the development of the new principles and standards. For example, during the efforts to prioritize and regulate activities in cyberspace related to cyberwar Western countries have most of the time insisted on "cybersecurity" which places the security and integrity of networks and information infrastructure as the primary area of concern (Sega, June 21, 2011). On the other hand, China and Russia have always been more focused on "information security," placing the importance on what information is protected and how it can be protected (Sega, June 21, 2011). Experts from different parts of the world have suggested that "cybersecurity" should not focus on the actor rather on the need for legal guidelines to govern all types of attacks within cyberspace that will deter state, groups or individuals from strategically mounting cyberattacks in the long term (Khan, 2011).

Legal differences among some of the leading states (in terms of capacity and ability to influence the international law) are still present including among the traditional alliance. Even though NATO has recognized the issue of a cyber threat as early as 1999, the inadequacy of NATO's activities political commitment and operational capabilities have arguably resulted to the different legal positions over some sensitive issues. Namely, the work over the Tallinn Manuals depicts the difference in the approach but also the evolution of the approach in both of the manuals (Adams, January 4, 2017). Just to be clear, the value of both documents is undisputable and it represents the convergence in the approach (the applicability of international law to cyberwar) (Jensen, 2018). The convergence of the approach among the member states (soon 30 countries-member states) is also evident in the fact that NATO has gradually advanced toward a common approach in cyber defense and has achieved more than any other international organization in this context (NATO, 2019). Nevertheless, it depicts the issue over the applicability of international law to cyberspace activities (especially in the context of cyberwar and operations) which is still present and relevant as ever.

Part of this deviation could also be attributed to the different legal traditions (the common law vs the civil-roman law tradition). In comparative law, there are many situations where the same legal term has different meanings, or where different legal terms have the same legal effect (Pajovic, 2001). Arguably this along the different state interests might be the reason why brief analysis of parts of the French declaration on International Law in Cyberspace shows, that France deviates from the U.S. and U.K. views or the Tallinn Manual 2.0 (such as the applicability of the unable-or-unwilling-test) (Roguski, September 24, 2019). Furthermore, the

European countries for example, usually take different positions due to the commitment to the European tradition of human rights, (Çalı, October 2015). During the work and preparations on the Tallinn Manual 2.0. "the Experts agreed that prescriptive nationality jurisdiction applied to a state's nationals even when overseas but did not agree on whether that individual's data was subject to extraterritorial enforcement jurisdiction of the nation's state."...(Jensen, 2018). One can argue that there is similar evidence about the evolution of the approach by analyzing the debates among the legal experts and academicians (Hadji Janev & Aleksovski, 2013).

The evolution toward more general acceptance of the applicability of international law to cyberwar types of activities is evident and it will continue to follow the general need of the states as they become ever more dependent on cyber activities. However, there are still open legal issues that urged attention and required valuable solutions.

A BRIEF OVERVIEW OF THE EXISTING CHALLENGES THAT STEM FROM STATES PERCEPTIONS TO THE APPLICABILITY OF INTERNATIONAL LAW TO CYBERWAR

To have a better understanding of the disagreement over the applicability of international regulations to cyberspace briefly we will follow the above explained systematic approach of international legal principles and standards. The analyses will thus address the challenges in peacetime (or as we have approaches the *ius contra bellum*), *ius ad bellum*, *ius in bello* and the *ius post bellum*. Giving that regulations, principles, and standards in post bellum (transition from war to peace-in diplomatic – policy terms) reflects the law of occupation or the mandate (if the authority for military intervention comes from the UN SC Mandate, which more or less is the same as the so-called peacetime regime (*ius contra bellum*) principles and standards we will systematize the challenges in this three groups. It must be noted though that giving the space and the scope of the article the analyses that follow will just touch on some of the most emphasized challenges that gravitate over the issue.

A BRIEF OVERVIEW OF THE PEACETIME CHALLENGES OVER THE APPLICABILITY OF INTERNATIONAL LAW TO CYBERWAR

States mostly agree that the general principles and standards of international law during peacetime apply to cyberspace. As in the physical domain, these standards and principles do not forbid states to acquire technology, hardware and software, training and all they need to effectively defend and deter potential adversaries. International principles and standards follow this logic (for example states are permitted to use force in self-defense regardless of the general rule for the prohibition of the use of force-we will address this later). A good source and overview of how these principles and standards apply in peacetime are the NATO supported project led by Dr. Ziolkowski (December, 2013) and published as the edition titled: "Peacetime Regime for State Activities in Cyberspace." The driving principles of international law in the context of our interest are the principle of sovereign equality and non-interventions. These principles, however, have evolved and their application has sparked many legal debates (Kelsen, March 1944).

Accordingly, states should regulate all cyber activities taking place on their territory, control the use of any cyber infrastructure located there, and exercise legal jurisdiction over such

activities (Schmitt, 2014, p. 274). States disagree not just in the essence of the effects that these technologies can accomplish, but also in the approach of how to prevent the proliferation of malicious cyber weapons and technology. Schmitt (2014, p.275) reports that even NATO members disagree on the issues that stem from the approach of legal obligations under the principle of sovereignty. He explains that: "*The International Group of Experts could achieve no consensus as to whether such activities amounted to sovereignty violations. Arguably, the distinction between cyber operations resulting in physical damage or injury and those that do not is overly formalistic. Although physical violation was contemplated, as reflected in the derivative principle of territorial integrity, physicality was not the norm's exclusive focus. The prohibition on intervention, which requires coercive intent but not physical damage or injury, illustrates, it would seem, the lack of an all-encompassing requirement for physical effects. Nonetheless, the disagreement remains unsettled.*"

Regulation of cyberspace to prevent or to prepare a nation to sustain in the massive cyber-attacks that may amount to an act of war has been undergoing in many nations. The approach to peacetime regulation among the states differ (Raboin,2011), straddling the boundaries of espionage, human rights and privacy concerns (Gellman & Poitras, 2013) (even among the traditional Allies) (Bimbaun, June 2010, 2013) to limitation of the cyberweapons (as suggested by Russia) (Malawer, February , 2010) up to a suggestion that an international treaty should be formed to prevent the outbreak of such a war (AFP, January 30, 2010). The issues and challenges between the states about what the law should be (*lex ferenda*) to support more robust cyber defense rather than how existing law (*lex lata*) should be applied to categorized cyber threats produce further challenges in the *ad bellum* context.

IUS AD BELLUM CHALLENGES TO APPLICABILITY OF THE EXISTING INTERNATIONAL LAW APPLICABLE TO CYBERWAR

As we have already noticed one of the greatest challenges of the applicability of International law to cyberwar is the "threshold" to trigger the principles and standards of war (i.e. International law of armed conflict, or International humanitarian law). States and scholars have a different opinion when an act in cyberspace becomes a "use of force", under international law (Roscini, 2010). Schmitt, reports that the same issue crated frustration among the experts drafting the Tallinn Manual 2.0. which resulted in the development of "*a nonexclusive list of factors that would likely influence the characterization of cyber operations by states as uses of force: severity, immediacy, directness, invasiveness, measurability, military character, state involvement, and presumptive legality*" (Schmitt, 2014, p. 281).

Once that the threshold under the ad bellum context is met states have the right to use force as an exception by the general prohibition (Art. 2(4) of the UN Charter, to use force in self-defense under Article 51 of the UN Charter (1945, art.2). The challenge that exists in the ongoing debates among the states and legal community is whether or not cyber activities that do not cause material damage or loss of lives can trigger the right to Self-defense. The challenge that the so-calledd Stuxnet attack caused (Richardson, July 22, 2011), i.e. the ability to hide the effects that cyber-attack can cause or to prolong the manifestation and severity of a cyber-attack urge international community to seriously reconsider this problem and prevent unilateral last resort reaction that could establish a dangerous practice.

IN BELLO CHALLENGES TO APPLICABILITY OF INTERNATIONAL LAW TO CYBERWAR

Once when the threshold to use force in self-defense is met, or there is a UN SC Resolution - a mandate to use force, the law of armed conflict (also widely known as international humanitarian law) applies. Many of the challenges explained in the above analyses of the changing character of war loom lights in the context of *in bello* applicability of international principles and standards to cyberwar. Although it seems that at least in the Euro-Atlantic community the applicability of *in bello* principles and standards are widely accepted debates over the applicability based on the analogy stubbornly oppose these feelings (Sinks, 2008).

International principles and standards that regulate armed conflict are clear and apply when there is an armed conflict between two or more states, and when those states resort to armed force in settling the disputes (ICTY, 1995). Case law has also established the practice that *ius in bello* principles and standards apply in a situation when non-state organized armed group uses armed force as the group is acting under the overall control of another state (ICTY, 1999). According to the ICRC "*Any difference arising between two States and leading to the intervention of armed forces is an armed conflict*". For the ICRC time and scale and effects are irrelevant (ICRC, 1952). The challenges in this line in the context of cyber operations are three folded.

First, not all cyber operations may qualify as operations equal to armed conflict-cyberwar. A good example of this represents the Dutch government's position as Schmitt reported. Accordingly, *A cyber-attack that impacts civil or military computer systems and only results in the modification or destruction of non-essential data would not rise to the threshold of armed conflict. Even if an attack has clear political, financial or economic consequences, such as the DDoS attack on Estonia in 2007, it would not be sufficient to breach the threshold of armed conflict. Acts that have such consequences in the physical world are not subject to international humanitarian law either. However, if an organized cyber-attack (or series of attacks) leads to the destruction of or substantial or long-lasting damage to computer systems managing critical military or civil infrastructure, it could conceivably be considered an armed conflict and international humanitarian law would apply. The same is true of a cyber-attack that seriously damages the state's ability to perform essential tasks, causing serious and lasting harm to the economic or financial stability of that state and its people. An example would be a coordinated and organized attack on the entire computer network of the financial system (or a major part of it) leading to prolonged and large-scale disruption and instability that cannot easily be averted or alleviated by normal computer security systems.* (Scmitt, 2014, pp.290)"

Second, challenges stem from the applicability of the principles and standards for non-international armed conflict scenarios. Unlike most of the European states (Roguski, September 24, 2019) that have pro-liberal approach the U.S. (Wittes, April 8, 2016), for example, have different opinions and will consider cyber-attacks as an armed attack regardless of whether or not these attacks *are attributable to another State (i.e. because they were conducted pursuant to the instructions or direction or control of that State)*" (Schmitt, September 16, 2019). In practice, it is well established that sporadic cyber incidents, including those that directly cause physical damage or injury, do not constitute a non-international armed conflict."(Tallinn Manual, 2013). This means that for principles and standards of international armed conflict to apply to operations and activities of non-state actors they have to be organized and coordinated (ICRC, 1987).

Third, challenges come from the applicability of the well-established principles of distinction, proportionality, military necessity, and humanity. In the digital age applicability of these principles is very subjective. The danger stems from the many "unknown" (something that we discussed above the attribution and predictability of the cascade effects). Hence the line between humanity and military necessity on one hand and the distinction and proportionality on the other is blurred more than ever. Furthermore, the interpretation of proportionality (relevant in terms of use of deadly force) i.e. in the law-enforcement context and the military context reflects the challenges from the ad bellum debate. Regardless of the legal skepticism to cyberwar these and other relevant legal concerns represent a serious challenge for the states and international organizations and urge a greater will and efforts to resolve potentially destructive interpretation and application of the international law to cyberwar and states activities in the cyberspace.

CONCLUSION

Information and communication technologies have changed the character of war. States and non-states actors can use cyberspace and achieve strategic objectives like never before. Cyberwar and operations with strategic security impact challenge existing principles and standards of international law. Interpretation over the applicability of the existing principles and standards of international law to cyberwar has evolved and is shaped by states' interest and threat perceptions. While in the early days of the internet and ICT liberal democratic states have seen ICT and internet as an opportunity and vouched for less state interfering abuse of these technologies by state and non-state actors have arguably changed this approach. Many pieces of evidence confirm that both democratic and nondemocratic states have similar perceptions over the applicability of international principles and standards of international law. However, states' position differs in their approach of applicability of international law during peacetime, ability, and right to use force in self-defense and during the time of war. The analyses showed that liberal states' position over control of the internet has evolved from emphasizing the rights of privacy and individual freedoms to the duty of the state to provide protection and exercise sovereignty. The issues and challenges between the states about what the law should be (*lex ferenda*) to support more robust cyber defense rather than how existing law (*lex lata*) should be applied to categorized cyber threats in peacetime produce challenges in the *ad bellum* context. Different threat perceptions urge states to have different positions over *severity*, *immediacy*, *directness*, *invasiveness*, *measurability*, *military character*, *state involvement*, and *presumptive legality* as factors that can characterize cyber operations by states as an act of war. Furthermore, states› positions differ over the actor who can commit such acts (i.e. non-state actors vs. states). Challenges in the bello context are three folded (i.e. not all cyber operations may qualify as operations equal to cyberwar; challenges that stem from the origin of the attacker – state vs. nonstate actors; and challenges that comes from the applicability of the well-established principles of distinction, proportionality, military necessity and humanity.

The ability to abuse cyberspace to endanger international peace and security (directly through attacking critical infrastructure or causing cascade effects) is evident. The unilateral approach in the interpretation of the applicability of international law to cyberwar scenarios as a result of threat perception from such scenarios as well as an option to achieve strategic political

objectives is also indisputable. Nevertheless, regardless of their threat perceptions and interest, states and the international community must find strength and propose acceptable interpretation and appropriate development of principles and standards of international law that will balance between the states' interest and existence on one hand and the prosperity, development, and wellbeing on the other, while using these technologies.

REFERENCE LIST

Adams, M. J., "(January 4, 2017), "A Warning About Tallinn 2.0 … Whatever It Says", Lawfare, accessed at: https://www.lawfareblog.com/warning-about-tallinn-20-%E2%80%A6-whatever-it-says

AFP, (Jan. 30, 2010), "UN Chief Calls for Treaty to Prevent Cyber War", Google News, http://www.google.com/hostednews/afp/article/ALeqM5h8Uvk-jpSvCWTbqYSglWs4I4yAA

Allen-Ebrahimian, B., (2016), "The Man Who Nailed Jello to the Wall", Foreign Policy http://foreignpolicy.com/2016/06/29/the-man-who-nailed-jello-to-the-wall-lu-wei-chinainternet-czar-learns-how-to-tame-the-web/

Betz, D. J., & Stevens, T. C., (2012), Cyberspace and the State: Towards a Strategy for Cyberpower (Adelphi series) (1 ed.), New York: Routledge,

Birnbaum, M., (June 10, 2013), "Merkel, Other European Leaders Raise Concerns on U.S. Surveillance", Washington Post, accessed: http://www.washingtonpost.com/ world/merkel-other-european-leaders-raise-concerns-on-us-surveillance/2013/ 06/10/305eddda-d1da-11e2-a73e-826d299ff459_story.html.

Borisoff, D., & Victor, D. A., (1989), "Conflict management: A communication skills approach", Englewood Cliffs, NJ: Prentice-Hall

Bures, O., (2010), "Perceptions of the Terrorist Threat among EU Member States", Central European Journal of International and Security Studies

Çalı B., (October 2015), "Comparing the support of the EU and the US for international human rights law qua international human rights law: Worlds too far apart?" International Journal of Constitutional Law, Volume 13, Issue 4, Oxford, accessed at: https://academic.oup.com/icon/article/13/4/901/2450824

Check T., (2015), "Book Review: Analyzing the Effectiveness of the Tallinn Manual's Jus Ad Bellum Doctrine on Cyberconflict,: A NATO-Centric Approach", Cleveland State University Law Rev, Vol. (2015) available at https://engagedscholarship.csuohio.edu/clevstlrev/vol63/iss2/12

Changing Character of War Centre -CCW, (2015-2017), "Is the nature of war changing?", Research findings, Oxford University, Accessed at: http://www.ccw.ox.ac.uk/research

Clausewitz, C., (1989), "On War", Edited and translated by Michael Howard and Peter Paret, First paperback edition, Princeton University Press, Princeton

Deibert, R. (2003), "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace" Millennium - Journal of International Studies, 32(3), 501-530

Fuller, J.F.C., (1946), "Armament and History – A Study of the Influence of Armament on History from the Dawn of Classical Warfare to the Second World War" Eyre & Spotiswoode, London,

Geers K., (2018), "Cyberspace and the Changing Nature of Warfare-Key note speach", NATO CCDCOE, accessed at: https://ccdcoe.org/uploads/2018/10/Geers2008_CyberspaceAndTheChangingNatureOfWarfare.pdf

Gellman B. & Poitras L., (2013), "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program", The Washington Post, accessed: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Gierow, H., (2016), "China macht VPN genehmigungspflichtig, accessed: http://www.golem.de/news/internetzensur-china-macht-vpn-genehmigungspflichtig-1701125749.html

Hadji-Janev, M., & Aleksoski S., (2013), "Use of Force in Self-Defense Against Cyber-Attacks and the Shockwaves in the Legal Community: One more Reason for Holistic Legal Approach to Cyberspace", Mediterranean Journal of Social Sciences MCSER Publishing, Rome-Italy, Vol. 4, No.14;

ICTY, (1995), "Prosecutor v. Tadić, - Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction", Case No. IT-94-1-I, 70 (International Criminal Tribunal for the Former Yugoslavia Oct. 2, 1995)

ICTY (1999), "Prosecutor v. Tadić, Appeals Chamber Judgment 131-40, 145", Case No. IT-94-1-A, (International

Criminal Tribunal for the Former Yugoslavia July 15, 1999);
ICRC, (1952), "Commentary: Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the field", (Jean Pictet ed., 1952)
ICRC, (1987), "Commentary on The Additional Protocols Of 8 June 1977 to The Geneva Conventions Of 12 August 1949, (Yves Sandoz et al. eds., 1987)
ICRC, (July, 2004) "What is International Humanitarian Law?", accessed at: https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf
Jensen, E. T., (2018), "The Tallinn Manual 2.0: Highlights and Insights", Georgetown Journal of International Law, Vol. 48, accessed at: https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf;
Joseph S. N., Jr., (1992),"What New World Order?", Foreign Affairs, Spring 1992;
Katja Creutz, Tuomas Iso-Markku, Kristi Raik, and Teija Tiilikainen, The Changing Global Order and Its Implications for the EU
Khan, F. U., (2011), "States Rather Than Criminals Pose a Greater Threat to Global Cyber Security: A Critical Analysis", Strategic Studies, Vol. p. 91, accessed at: http://issi.org.pk/wp-content/uploads/2014/06/1328592265_43276030.pdf.;
Kedzie, C., & Aragon, J. (2002) "Coincident Revolutions and the Dictator's Dilemma", In: Allison J. Emmons (Ed.), Technology, Development, and Democracy: International Conflict and Cooperation in the Information Age, Albana: State University of New York Press
Woollacott, E., (2016), "UK joins Russia and China in legalizing Bulk Surveillance" Forbes. http://www.forbes.com/sites/emmawoollacott/2016/11/16/uk-joins-russia-and-china-inlegalizing-bulk-surveillance/#37d08afa65f4
Kelsen H., (March 1944), "The Principle Of Sovereign Equality Of States As A Basis For International – Organization", The Yale Law Journal, Vol.53, No 2, accessed at https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=4326&context=ylj;
Kokott J., (2011), "States, Sovereign Equality", Oxford Public International law, Max Planck Encyclopedia of Public International Law; or: Besson Samantha, (2011), "Sovereignty", Max Planck Encyclopedia Pub. International law, http://opil.ouplaw.com/home/EPIL
Machiavelli N., (1965), "The Art of War, A revised edition of the Ellis Farneworth Translation", Bobbs-Merrill Company, Inc., Indianapolis
Malawer S., (February 2010), "Cyber Warfare: Law and Policy Proposals for U.S. and Global Governance", Virginia Lawyer, International Practice Section, Vol. 58,
Michael A. S., (2008) "Cyber warfare and international law", Air Command and Staff College,
Michael J. G., (2013), "The Road Ahead: Gaps, Leaks and Drips", International Law Studies. The U.S. Naval War College, Vol. 89,
NATO (2016) "An Introduction to Operations Planning at the Operational Level", Comprehensive Operations Planning Directive (COPD), Allied Command operations, Interim V2.0 dated 4 Oct 13, accessed at: https://www.act.nato.int/images/stories/events/2016/sfpdpe/copd_v20_summary.pdf
NATO, "Cyber defense", 2019, accessed: https://www.nato.int/cps/en/natohq/topics_78170.htm
Pjovic, C., (2001), "Civil Law and Common Law: Two Different Paths Leading To The Same Goal", (2001) Vol. 32 VUWLR,
Raboin B., (2011), "Corresponding Evolution: International Law and the Emergence of Cyber Warfare", 31 J. Nat'l Ass'n Admin. L. Judiciary Iss. 2, accessed at: http://digitalcommons.pepperdine.edu/naalj/vol31/iss2/5
Richardson J. C., (July 22, 2011), " Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield", SSRN, accessed: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1892888.
Roguski P., (September 24, 2019), "France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations", Opinio Juris, accessed at: http://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/
Roscini M., (2010), "World Wide Warfare—The Jus ad Bellum and the Use of Cyber Force", 14 Max Planck Y.B. United Nations L. 85;
Rovira, M. G.-S., (2014), "The Politics of Interest in International Law", European Journal of International Law, Volume 25, Issue 3, August 2014,
Ryan, Donald E. Jr., (1995), "Implications of Information-Based Warfare", Joint Forces Quarterly, Autumn/Winter 1994-95

Segal A., (June 21, 2011), "The Role of Cyber-Security in US-China Relations", East Asia Forum, accessed at http://www.eastasiaforum.org/2011/06/21/the-role-of-cyber-security-in-uschina-relations/

Schmitt, N. M., (2011) "Cyber Operations and the Jus ad Bellum Revisited", 56 VILL. L. REV. 569, 571-81;

Schmitt N. M., (2014), "The Law of Cyber Warfare: Quo Vadis?", Stanford Law and Policy Review, Vol. 25,

Schmitt N.M., (September 16, 2019), "France's Major Statement on International Law and Cyber: An Assessment", Just Security, accessed at: https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/

Schulze, M. (2016), "Same old story: 40 years of debating encryption". https://tresorit.com/blog/encryption-debate/

Statute of the International Court of Justice (1945), June 26, art. 38(1)

Shafqat, N., & Masood, A, (2016), "Comparative Analysis of Various National Cyber Security Strategies. International Journal of Computer Science and Information Security, 14(1), 12

Sinks, M. A. (2008) "Cyber warfare and international law", Air Command and Staff College

Slomanson, W., (2011), "Fundamental Perspectives on International Law", Boston, USA: Wadsworth,

Sussman, B., (Dec 27, 2019), " Cyber War vs. Traditional War: The Difference Is Fading", SecureWorld, accessed : https://www.secureworldexpo.com/industry-news/cyber-war-vs-traditional-war

Szoldra, P., (2016), "ISIS' favorite messaging app may be in jeopardy", Business Insider http://www.businessinsider.com/russia-anti-encryption-telegram-2016-6?IR=T

Tallinn Manual on The International Law Applicable To Cyber Warfare Cambridge University Press, (Michael N. Schmitt ed., 2013)

The Secretary General of the United Nations, (2009), "United Nations Policy for Post-Conflict Employment Creation, Geneva

The International Court of Justice, (2007), "Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro.), 2007 I.C.J. 108, 404 (Feb. 26); Prosecutor v. Lubanga, Case No. ICC-01/04-01/06, Decision on Confirmation of Charges, 211 (Jan. 29, 2007), http://www.icc-cpi.int/iccdocs/doc/doc266175.pdf.

The United Nations Charter, (1945), New York United Nations Headquarter;

Toffler, Alvin – Heidi Toffler, (1995), "War and Anti-War: Survival at the Dawn of the 21st Century", Warner Books, New York;

Townshend C., (2000), "The Oxford History Of Modern War", Oxford University Press 2000

UN Secretary General Report, 1992, "Agenda for Peace", accessed at: http://www.un-documents.net/a47-277.htm

Yasuaki, O. (2017), "Conflict Resolution (and Dispute Settlement) and International Law", In International Law in a Trans civilizational World (pp. 534-587). Cambridge: Cambridge University Press

Wittes B., (April 8, 2016), " State Department Legal Adviser Brian Egan's Speech at ASIL", Lawfare, accessed at; https://www.lawfareblog.com/state-department-legal-adviser-brian-egans-speech-asil

Wooding, C., (September 1, 2019), "The Rise of Cyber and the Changing Nature of War, Christopher", Grounded Curiosity, accessed at: https://groundedcuriosity.com/the-rise-of-cyber-and-the-changing-nature-of-war/;

Waxman, M. (2011), "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)", 26 Yale Journal of International law, 421

Ziolkowski K., (December 2013), "Peacetime Regime for State Activities in Cyberspace", NATO CCD COE Publications, available at: https://ccdcoe.org/library/publications/peacetime-regime-for-state-activities-in-cyberspace/

Metodi HADJI-JANEV

Brigadier General, (Ph.D.), is an associate professor at the Military Academy General Mihailo Apostolski"-Skopje, a unit of University "Goce Delcev" in Stip, Macedonia and Adjunct Faculty Member at Ira A. Fulton School of Engineering, Arizona State University, ASU, U.S.A. His current scholarship focuses on legal aspects of countering asymmetric, cyber, and hybrid-based threats, with emphasis on critical information infrastructure and critical infrastructure protection; on legal and strategic aspects of use of force in countering terrorism and organized crime threats, and on development of legislation and strategic documents to effectively prevent and counter cyber and hybrid threat vectors.