*Journal of Learning and Teaching in Digital Age, 2017, **2**(2),* 46-53

Prohibition of Use of Force and Cyber Operations as "Force"

Huseyin Kuru
Gazi University
yigit.cagatay04@gmail.com

ABSTRACT

Technology have become core element of the critical infrastructures that maintain communities' vital services. While this situation facilitates the daily life of the societies, systems running online are exposed to risks from vulnerabilities based on internet and systems. Increasing cyber-attacks, especially between countries in governmental level, created a new term "cyber warfare". As in all the evolutions of the war, the concept of cyber warfare also needs original rules due to its unique characteristics. International society has divided into two groups. First group claims that existing conflict rules should apply this new battle field and the other group says the situation requires a new consensus. The purpose of this study is to examine the scope of the prohibition and to explain exceptions, by examining the developed approaches for establishing the conditions for the use of force in cyber operations, highlighting the most appropriate evaluation criteria with emphasizing existing limitations. In the light of the data collected, the literature was searched exhaustively to achieve this aim. What characteristics cyber-operations should have and objective approaches that we can use for the assessment and we can suppose as use of force will be also discussed.

Keywords: *Cyber warfare, cyber operation, prohibition of use of force, right to self-defense, law of armed conflict*

INTRODUCTION

Modern western societies are more wired and established in terms of their vital services like hospitals, banks, factories and even nuclear plants on systems dependent on internet. If computer nets have become nervous systems of civil and military infrastructures, neutralizing them would paralyze all the country (The White House, 2003). Dependency of military capacity and capabilities have transferred warfare to the cyber domain as well as land, sea, air and space (US Department of Defence, 2006). In accordance with the technological developments that have taken place in the world, new legal regulations were made and the rules of the game were rebuilt (Saint Petersburg Declaration, 1868). With the cyber space becoming a new field for international conflicts, the question of how *the jus ad bellum* that is regulating the use of force in international relations will be implemented for cyber operations (Roscini, 2010).

In this study, the prohibition of use of force and exceptions were explained, by examining the developed approaches for establishing the conditions for the use of force in cyber operations, mandatory criteria for the evaluation of cyber operations as use of force and effective evaluation criteria are emphasized in the light of obtained data.

METHOD

Notion of cyber warfare are generally misused with metaphors like war on sugar, war on cigarette, war on cancer etc. For this purpose, books, articles, decisions and advisory opinions of International Justice Court, declarations and decisions of the United Nations General Assembly and the Security Council, the views and recommendations of NATO and other official bodies and statements of government officials were examined deeply.

Questions of the Study

This study made an afford to answer the questions mentioned below:

- Can the existing law of armed Conflict be used in cyber operations?
- What is the unique characteristics of cyber operations as "force"?

***Correspondence to*:** *Huseyin Kuru, Department of Forensic Computing, Institute of Information, Gazi University, Ankara, Turkey, E-mail: yigit.cagatay04@gmail.com*

- Which approach is the objective way to recognize the cyber operations as "force"?

USE OF FORCE IN INTERNATIONAL RELATIONS

International Humanitarian Law (IHL) and *Law of Armed Conflict (LOAC)* are regulations and customary international law emerged from the view that even subject is war, conflict, damage or causality, there must be some rules sought to be in line with by taking lessons from the state conflicts taken place for many years. Although there are many articles on law of war that the states have agreed on, but as we will see in the next chapters, there are some topics that states have disagreement. When the subject is a cyber-environment, even the compromised subjects need new arrangements and improvements. For many years, many writers, academics, cyber space specialists and military leaders from different fields studied on cyber warfare and rules of cyber warfare and the limits of behaviours in that environment are not clear in this sense.

Prohibition of the Use of Force

Law of Armed Conflict (LOAC) has been binding rules for states to establish open regulations on war and conflicts which have been going on for centuries. Official documents, agreements, rules of conduct and decisions made by international courts constitute the main framework of international conflict rules. While reducing the effects of war, Law of Armed Conflict is seeking a balance between allowing war and regulating its implementations at the same time (May, 2015).

Article 2(4) of the United Nations Charter

The United Nations Charter has a vital role in international relations and use of force. Charter was signed in 1945 at the end of the second world war and declared his ultimate goal in its preamble as *"…Protect next generations from the scorching effects of war..."*. The UN Charter generally prohibits member states from the threat or use of force against other countries. Article 2(4) of the United Nations Charter states that,

"All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations" (Randelzhofer, 2002).

For the common view among academicians, *"force"* in this article should be understood as *"Armed Attack"*. Harrison Dinniss from Swedish National Defense College claimed that according to the Preamble of the Charter, the aim of the United Nations is to save succeeding generations from the scourge of war. It is thus reasonable to come to the conclusion that the *"force"* definition is limited to armed forces (Dinniss, 2012). While the term *'force'* is not preceded by *'armed'*, it is widely acknowledged that 'force' refers particularly to armed force and thus excludes, for example, economic force. Some have taken a contrary position and claimed that the prohibition is wider and does indeed include other forms of force as well. For example, Hans Kelsen argues that the notion of force is meant to include any illegal action of a state that violates the interests of another, not just armed force (Kelsen, 1954).

CYBER OPERATIONS

Cyber Operations as Force

The International Court of Justice cleared in the Nuclear Weapons Advisory Opinion that Articles 2(4), 42 and 51 of the UN Charter apply to any use of force, regardless of the weapons used. For that reason, it is entirely possible for a cyber-operation to qualify as a use of force. Such a view is also supported by the Vienna Convention on the Law of Treaties, whose Article 31(3)(b) states that any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation shall be taken into account. In their statements, several countries have considered certain cyber-attacks to be a type of force (Roscini, 2010).

Unique Characteristics of Cyber Operations

When establishing rules for a weapon, characteristics of that weapon must be taken into account to come up with the effective results. So, in this case, cyber space and cyber weapons have some matchless features that no gun or field have had ever. There are several ways of describing and categorizing these characteristics. Heather Harrison Dinniss provides one example. She

identifies four characteristics of cyber operations that distinguish them from conventional attacks in terms of the framework of the use of force: indirectness, intangibility, locus and result (Dinniss, 2012).

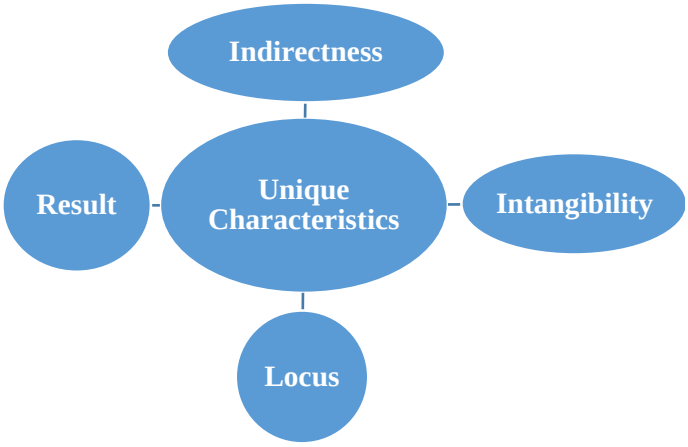

Figure 1. Unique Characteristics of Cyber Operations (Dinniss, 2012).

The Indirectness is in fact one potentially distinguishing and prominent factor, because several types of cyber operations require further action by a second actor after the initial act. Examples of such include an attack on the targeting system of a missile, or disabling air traffic control systems (Dinniss, 2012).

The Intangibility factor refers to the fact that neither the target of the attack nor the weapon used might not exist in real world. The damage might be unphysical as well, for example, as in the case of an attack on a stock exchange. Even attacks that ultimately result in physical consequences target the information resident in computers. For example, the Stuxnet attack modified the spinning frequencies of the centrifuges, which directly resulted in physical damage to them (Chien, 2010).

The locus factor takes into consideration the fact that, in some cases, it may be difficult to ascertain the origin of the attack (Schmitt, 2011). The attack may be routed through several points in different countries in order to hide the true source, or the malicious traffic may come from several countries. During the attacks on Estonia in 2007, the malicious traffic originated from 178 single countries (Tikk, Kaska & Vihul, 2010).

The results of cyber operations include a wide range of consequences spanning from only inconvenience to physical destruction. The indefiniteness and variety of the results spanning from inconvenience to physical damage is arguably the most difficult factor in categorizing the rules on the use of force to cyber-attacks (Moore & Roberts, 2013). *The results* might, in some cases, also be more unpredictable than in the case of kinetic force. A common example of such a case is a cyber-attack on a stock exchange or a single bank (Schmitt, 1999).

Cyber Operations as Use of Force

Studies to determine whether cyber operations are within the scope of use of force have led to the emergence of three different approaches: effects-based, target-based, and instrument-based views. The instrument-based approach uses the weapon used as the decisive factor: a cyber-operation may be identified as force if the weapon used sufficiently resembles the traditional ones. The target-based approach deems any action targeting critical infrastructure as an armed attack. The effects-based approach uses the impact and scope of all results of the operation as a determining factor (Hollis, 2007).

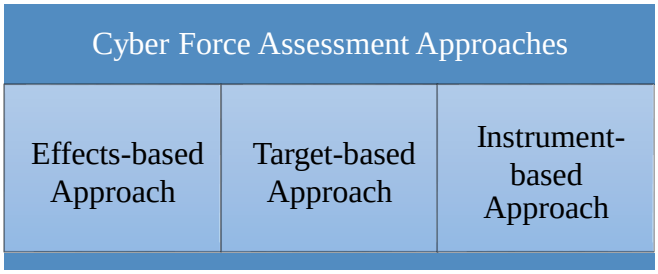

Figure 2. Cyber Force Assessment Approaches (Hollis, 2007).

All of these approaches have a sense in their field, but most accepted and easy to implement way is probably effects-based approach. This view has also been used by international group of experts which have established the *Talinn Manual* (Silver, 2002). The Manual refers to the 'scale and effects' assessment used by the International Court of Justice in Nicaragua. The ICJ stated that the sending of armed bands by a state to another state may classify as an armed attack if the scale and effects of the attack are such that it would have constituted an armed attack, if it were carried out

© 2017, *Journal of Learning and Teaching in Digital Age*, ***2****(2)*, 46-53

by regular armed forces (International Court of Justice,1986).

Effects-based Approach

The group behind the *Tallinn Manual* agreed that acts that injure or kill persons or damage or destroy objects are unambiguously uses of force. Towards the other end of the spectrum, the Manual states that non-destructive, psychological cyber operations intended solely to undermine confidence in a government or economy do not qualify as uses of force. As regards other, more unclear events, the Manual non-exhaustively lists eight factors which are considered to be influential when states assess whether a cyber-operation constitutes a use of force (Schmitt, 1999).

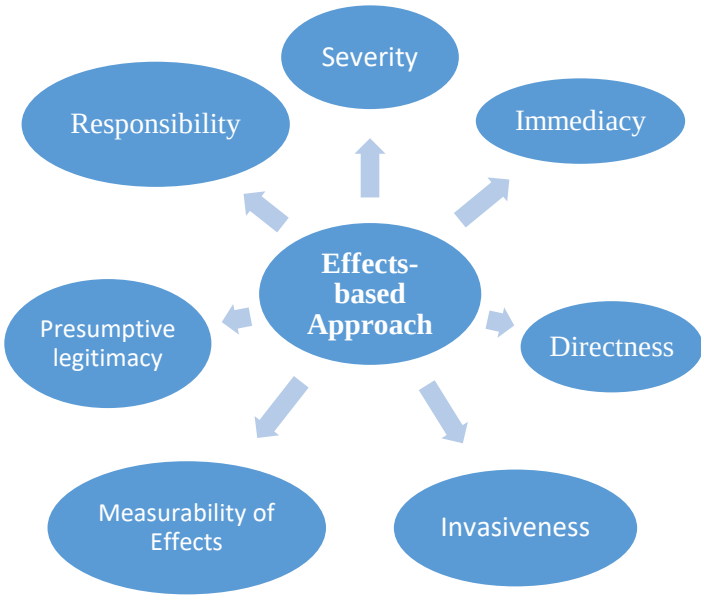

Figure 3. Sub-criteria used in measuring effect of cyber operations (Shmitt Criteria) (Schmitt, 1999).

Severity: The consequences describing acts of physical harm to individuals or goods does merely mean use of force. Those generating only minor inconvenience or irritation will never do such an effect. Between the extremes, the more consequences impinge on critical national interests, the more they will contribute to the depiction of a cyber-operation as a use of force. In this regard, the scale, scope, and duration of the consequences will have great bearing on the appraisal of their severity. Severity is self-evidently the most significant factor in the analysis.

Immediacy: The sooner consequences manifest, the less opportunity states have to seek peaceful accommodation of a dispute or to otherwise forestall their harmful effects. Therefore, states harbour a greater concern about immediate consequences than those that are delayed or build slowly over time.

Directness: The greater the attenuation between the initial act and the resulting consequences, the less likely states will be to deem the actor responsible for violating the prohibition on the use of force. Whereas the immediacy factor focused on the temporal aspect of the consequences in question, directness examines the chain of causation. For instance, the eventual consequences of economic coercion are determined by market forces, access to markets, and so forth. The causal connection between the initial acts and their effects tends to be indirect. In armed actions, by contrast, cause and effect are closely related—an explosion, for example, directly harms people or objects.

Invasiveness: The more secure a targeted system, the greater the concern as to its penetration. By way of illustration, economic coercion may involve no intrusion at all (trade with the target state is simply cut off), whereas, in combat, the forces of one state cross into another in violation of its sovereignty. The former is undeniably not a use of force, whereas the latter always qualifies as such (absent legal justification, such as evacuation of nationals abroad during times of unrest). In the cyber context, this factor must be cautiously applied. In particular, cyber exploitation is a pervasive tool of modern espionage. Although highly invasive, espionage does not constitute a use of force (or armed attack) under international law absent a nonconsensual physical penetration of the target state's territory, as in the case of a warship or military aircraft which collects intelligence from within its territorial sea or airspace. Thus, actions such as disabling cyber security mechanisms to monitor keystrokes would, despite their invasiveness, be unlikely to be seen as a use of force.

Measurability: The more quantifiable and identifiable a set of consequences, the more a state's interest will be deemed to have been affected. On the one hand, international law does not view economic coercion as a use of force even though it may cause significant suffering. On the other, a military attack that causes only a limited

degree of destruction clearly qualifies. It is difficult to identify or quantify the harm caused by the former while doing so is straightforward in the latter.

Presumptive legitimacy: At the risk of oversimplification, international law is generally prohibitory in nature. In other words, acts which are not forbidden are permitted; absent an express prohibition, an act is presumptively legitimate. For instance, it is well accepted that the international law governing the use of force does not prohibit propaganda, psychological warfare, or espionage. To the extent such activities are conducted through cyber operations, they are presumptively legitimate.

Responsibility: The law of state responsibility come in to use when a state will be responsible for cyber operations. But, it must be understood that responsibility lies along a continuum from operations conducted by a state itself to those in which it is merely involved in some fashion. The closer the nexus between a state and the operations, the more likely other states will be inclined to characterize them as uses of force, because of greater risk posed to international stability.

The Tallinn Manual clearly declares that the presented criteria are meant to be factors influencing the use of force assessments by states and not binding legal criteria. In this issue, Martti Koskenniemi argued that exact rules and their automatic application is problematic, because of their over and under inclusiveness (Koskenniemi, 2002). The extreme variety of possible cyber operations and the uncertainty regarding the whole field emphasizes this point even further. While the criteria of the Tallinn Manual – sometimes also referred to as the Schmitt criteria – do offer a basis for the evaluation of an operation, the determination seems to in many cases boil down to the severity criterion and a seemingly simple result, if a cyber-operation results in physical damage to human or property comparable to that produced by a kinetic attack, the operation counts as force. Katharina Ziolkowski approaches the issue from a similar viewpoint and argues that there is no need for special criteria beyond focusing on the effects (Ziolkowski, 2012).

Target-based Approach

The target-based approach is an extension of the use of force. This approach lowers the threshold of use of force and increases the risk of responding even minor attacks. Gary Sharp argues that the infiltration of another country into a country's critical computer systems that are important for his ability to defend itself is a sufficient reason for targeted county to us right of self-defence (Sharp, 1999). Such a point of view does not seem logical. Unauthorized access to a computer system may constitute a criminal offense for an individual, but even targeted systems would be critical infrastructure that cannot be identified as merely use of force.

According to Eric Talbot Jensen, the framework for the use of force and the right to legitimate defence is insufficient to combat new potential threats. For him, even a computer network attack would not constitute an armed attack under the article 51 of the UN Charter, but if it targeted critical infrastructure the old rules need to be revised to include such an attack to legitimate self-defence. As well the issue of identifying the source of the attack creates a huge gap in national defence. Therefore, the criteria for an active response must be the quality of the targeted system, not the assignation (Jensen, 2002).

Jensen's point of view is that countries can attack specific targets without revealing the source of the attack in response to the cyber-attack that they are exposed to. It is very difficult to defend such an idea, because there are some problematic points that cannot be overcome in the technological level. For example, attackers may have been able to direct attacks through other neutral and innocent countries or these attacks may have been directed from the sources within the borders of the target country. The author's approach is based on the unique qualities of computer networks and their difficulties to overcome, but ignores that the conflicts may increase and the response to be given must also be proportionate. At the same time, this view is insufficient as to what measures to take against the countries whose network was used for the attacks. Determining the responsibility of the attackers is not an obstacle, but should be seen as an unconditional requirement (Valo, 2014).

© 2017, *Journal of Learning and Teaching in Digital Age*, ***2****(2)*, 46-53

Instrument-based Approach

There are certain problems with applying instrument-based approach to cyber operations. The rules set out in this approach are inadequate against the fact that weapons that have never been identified until that day can be used in a cyber-attack (Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue & Spiegel, 2012). Because of this, it is very difficult to introduce cyber operations into this framework, because the consequences of a cyber-attack occur in a variety of environments ranging from disturbance to physical damage (Schmitt, 2013). Grouping cyber operations and classifying them according to the weapons they are using is a very difficult process, even if it is not impossible, because the results cannot be fully predicted. Dividing the cyber-attacks into smaller, more detailed groups such as cyber-attacks with physical consequences would mean applying the effects-based model that we have presented first.

RECOMMENDATIONS AND CONCLUSIONS

A Fresh Look at *Dinnis Model*

A new model has been proposed by taking the Dinnis Model as an example, which expresses the specificities separating the use of force in the cyber environment from the use of force in traditional conflict areas. In this new model, power which states have is added to *Dinnis model*. According to the power feature, countries that are strong and powerful in Cyber space also have strong limitations. For example, it is necessary to have advanced cyber weapons and advanced cyber infrastructure to apply cyber force against the rival state in the cyber environment. It is estimated that the countries that stand out in the cyber league in the world are also more likely to have cyber vulnerabilities compared to other weak countries.

In our age, hybrid warfare tactics are widely used, the weak and strong state division have become vaguer, new generation war tactics left even the most powerful states in a difficult situation, therefore advanced cyber infrastructure also means improved cyber vulnerabilities. As a result, it is estimated in the future that strong countries in the cyber space may not be willing to use this power. In Figure 4, the additional power concept to the *Dinnis model* is added to the discrete characteristics of the cyber force.

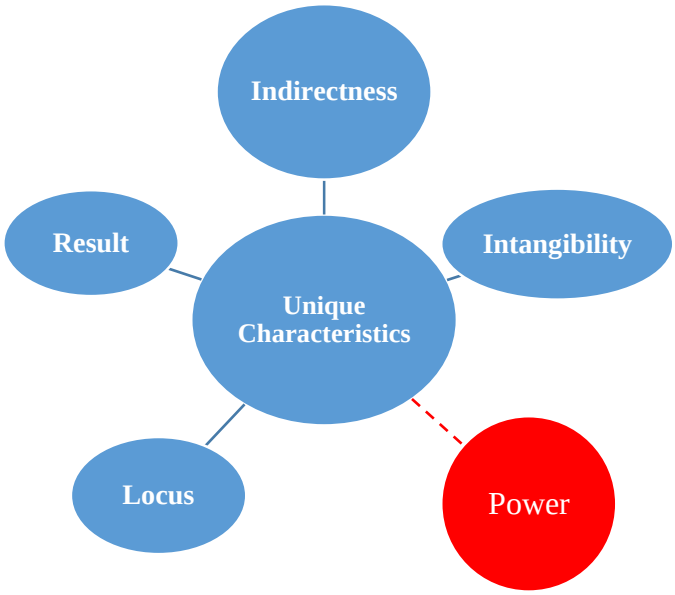

Figure 4. New proposal for cyber operation's unique characteristics

Singer and Friedman are among the writers who argue that the power in the cyber environment brings responsibility and sensitivity at the same time. According to the authors, the strongest factor preventing cyber-dominated countries from using advanced cyber weapons is their own cypher structures. This structure stems from the fact that the developed countries are connected almost vertically via the network. As former US National Security Agent Charlie Miller said "One of the biggest advantages of North Korea is that there is virtually no infrastructure linked to the internet to be targeted. On the other hand, there are countless vulnerable US have because of its networked systems that a country like North Korea can exploit. This actually creates a strange irony of cyber warfare. The more connected a country is, the more it can benefit from the internet an again the more connected a nation is, the greater the likelihood that it will be harmed by those using it for its evil purposes. İn other words, "The most talented nations at stone launching live in the largest glass houses" (Singer &Friedman, 2014).

The Need for an Effect-based Approach and *De minimis Rule*

It must be acknowledged that cyber operations are considered to be in the form of force, if they have reached a sufficient level of scope and effect. It is

stated that the evaluation of a cyber-attack force is the most reasonable and the objective way is the effect-based approach. Target-based approach seems to be a time-wasting within cyber operations. It is assessed that the concept of critical infrastructure in the target-based approach does not have clear definitions and that it gets the threshold of the use of force and especially of the armed attacks lower. Also, in Talinn Manuel effect-based approach is more accepted then target-based approach. Instrument-based approach is also over timed and difficult to implement within the cyber operations (Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue & Spiegel, 2012).

The application of the effect-focused approach to cyber operations also brings some questions. Which level is enough for a cyber-operation to pass threshold of use of force? In Talinn Manual, this question is answered clearly as cyber operations causing death, injury, damage and destruction pass the threshold of use of force (Schmitt, 2013). In this approach de minimis rule works. According to this rule, attacks with smaller and negligible consequences does not make sense. This approach may be seen as a reasonable starting point. The more difficult issue at this point is how to evaluate the cyber-attacks with less severe and destructive consequences. This issue is closely related to economic coercion measures. Article 2 (4) of the United Nations (UN) Charter did not consider economic enforcement measures as part of the use of force. However, as the economic consequences of cyber operations are far more destructive, they can reach levels that disrupt economic and political stability of a state. This keeps the debate alive about whether cyber-attacks with serious economic consequences should be considered as use of force. Grigorij Tunkin is one of the writers who think differently on this issue. According to him, for the western countries who argue that economic coercion measures should not be regarded as the use of force are more prone to cyber-attacks with devastating economic consequences (Bowett, 1958).

According to the general view, there is a difference between the use of force and the armed attack. While it is not necessary for a strike to have a wide range or excessive destructive effect for the characterization of the armed attack, the position of the armed assault is not fully specified.

In case of oil platforms, The International Court of Justice (ICJ) stated that an attack on even a single ship could be considered a weapon attack (Taft, 2004). Therefore, it is possible in this case that the cyber-attacks pass the threshold of armed attack. There is a general consensus that cyber-attacks with deadly consequences or significant destruction will also fall into the category of armed attacks. Such an assessment clearly reaffirms that activation of article 51 of the UN Charter would be legitimate action. The method used to assess the impact of an attack in this regard is again an effect-based approach. It is also important to note that as of 2017, cyber-attacks passing the level of armed attack is very exceptional.

REFERENCES

Bowett, D. W. (1958). *Self – Defense in International Law*, New York, Praeger, 220-225.

Chien, E. (2010). Stuxnet: A Breakthrough, *Symantec Blog*, Retrieved from: <www.symantec.com/connect/blogs/stuxnet-breakthrough>. 19.02.2017

Dinniss, H. (2012). *Cyber Warfare and the Laws of War*. New York: Cambridge University Press, 265.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W. and Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, 817-885.

Hollis D. B. (2007). Why States Need an International Law for Information Operations, *Lewis & Clark Law Revie, 11,* 1023–1061.

International Court of Justice. (1986). *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America*), Judgment, I. C. J. Reports 1986, 14.

Jensen E. T. (2002). Computer Network Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense, *Stanford Journal of International Law*, 221.

Kelsen H. (1954). *Collective Security Under International Law.* U.S. Naval War College: Newport. 55, 57.

Koskenniemi M. (2002). The Lady Doth Protest too Much – Kosovo, and the Turn to Ethics in International Law, *The Modern Law Review*, 167.

May, L. (2015). The nature of war and the idea of "cyberwar.". In J. D. Ohlin, K. Govern, and C. Finkelstein (Eds.), *Cyberwar: Law and ethics for*

virtual conflicts. New York: Oxford University Press, 3-15.

Moore H. and Roberts D. (2013). AP Twitter hack causes panic on Wall Street and sends Dow plunging, *The Guardian*, Retrieved from: <www.guardian.co.uk/business/2013/apr/23/ap-tweet-hack-wall-streetfreefall>. 15.02.2017

Randelzhofer, A. (2002). Article 2(4). In B. Simma, D.-E. Khan and G. P. Nolte (Eds.), *The Charter of the United Nations: A Commentary*. New York: Oxford University Press. pp. 781-794.

Roscini, M. (2010). World Wide Warfare-'Jus Ad Bellum' and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law, 14*, 85-130.

Saint Petersburg Declaration. (December 1868). Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight.

Schmitt, M. N. (1999). Computer network attack and the use of force in international law: thoughts on a normative framework. *Columbia Journal of transnational Law, 37*, 891.

Schmitt M. N. (2011). Cyber Operations and the Jus Ad Bellum Revisited, *Villanova Law Review, 56*, 569–605.

Schmitt M. (2013). (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 10-18, 25-35, 76-105

Sharp W. G. (1999). *Cyberspace and the Use of Force*. Aegis Research Corporation: Falls Church, 129–130.

Silver D. B. (2002). Computer Network Attack as a Use of Force Under Article 2(4),*76 U.S. Naval War College International Law Studies*, 73–97.

Singer, P. and Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. New York: Oxford University Press, 160-165.

Valo, J. (2014). *Cyber Attacks and the Use of Force in International Law*. Master Thesis, University of Helsinki, Faculty of Law, Helsinki, 12.

Taft, W. H. (2004). Self-Defense and the Oil Platforms Decision. *Yale Journal of International Law, 29*, 295–306.

The White House. (2003). *The national security strategy of the United States of America*. Executive Office of the President Washington DC, 6.

Tikk, E., Kaska, K., & Vihul, L. (2010). *International cyber incidents: Legal considerations* (Vol. 112). Cooperative Cyber Defense Centre of Excellence. Tallinn, 23.

US Department of Defense. (2006). *National Military Strategy for Cyberspace Operations of the United States.* Diane Publishing, 27.

Ziolkowski K. (2012). Ius ad bellum in Cyberspace – Some Thoughts on the Schmitt-Criteria for Use of Force, in C. Czossek, R. Ottis and K. Ziolkowski (eds),*4th International Conference on Cyber Conflict Proceedings* (NATO CCD COE Publications: Tallinn, 295–309.