Journal of Naval Science and Engineering
2017, Vol. 13, No.1, pp.60-72
Savunma Bilimleri/Defence Sciences

PROHIBITION AGAINST THE USE OF FORCE AND THE COERCIVE USES OF THE CYBERSPACE

Hakan Selim CANCA[1]

Social Sciences Department
National Defense University, Turkish Naval Academy, Tuzla, Istanbul
hcanca@dho.edu.tr

Date of Receive: 01.02.2017 **Date of Acceptance: 19.03.2017**

ABSTRACT

The use of force is resorted by States as a form of dispute settlement generally as a last resort. But Article 2(3) of the United Nations (UN) Charter states that all members shall settle their international disputes by peaceful means. Article 2(4) bans the unilateral use or threat of force by States. In the customary international law, Article 2(4) is interpreted as a prohibition against the use of force focusing on restricting the use of military instruments. This instrument-based interpretation of the use of force causes the responsibility of States which deploys cyber instruments to cause physical damage in the target States' critical infrastructures, remain outside the scope of Article 2(4).

There are doctrinal difficulties in examining current international law on use of force and self-defense in cyberspace, while the legal frameworks for defining the parameters of operations in cyberspace are not clear. As being unforseen until this age of information and cyber technology, the prohibition of the use of force interpreted from Article 2(4) should be evolved to cover coercive uses of cyber instruments being used to have destructive effects in the enemy's physical infrastructures such as telecommunications, transportation, power systems, finance and emergency services.

Categorizing the cyber attacks as having physical effects to critical infrastructure and not having any physical effects can be the first step to solve the problem of evolving the article to cover cyber attacks within the concept of use of force. Then the efforts may be concentrated on the cyber attacks having physical effects on the enemy's infrastructures to be considered as a use of force. The main problem is that there would be an unwillingness of the powerful States which are

[1] Assistant Professor of Law, Commander (Navy), Head of Social Sciences Department, National Defense University, Turkish Naval Academy-Istanbul, hakancanca@gmail.com. All the opinions, considerations, proposals and mistakes in this text belong to the writer and do not reflect any opinion, consideration, proposal or policy of any institution. All the informations in this text are provided from unclassified sources. While every effort has been made to ensure that the information contained in this text correct, neither the author nor the publisher can accept any responsibility for any errors or omissions or for any consequences arising therefrom.

likely to use the opportunities of cyberspace in Inter-State coercion to evolve the interpretation of the article, while the technology-dependent or powerless States would have a volition to evolve the Article.

ÖZ

Kuvvet kullanımına, devletler tarafından anlaşmazlıkların çözümünde genellikle son çare olarak başvurulmaktadır. Ancak Birleşmiş Milletler Şartının 2(3) maddesinde, tüm taraf devletlerin uluslararası anlaşmazlıklarını barışçı yollarla çözmesi gerektiği ifade edilmektedir. Madde 2(4), devletler tarafından tek taraflı kuvvet kullanımı ya da kuvvet kullanma tehdidinde bulunulmasını yasaklamaktadır. Uluslararası örf adet hukukunda Madde 2(4), askeri araçların kullanımını kısıtlamaya odaklanan bir kuvvet kullanımı yasağı olarak yorumlanmaktadır. Kuvvet kullanımı yasağına ilişkin söz konusu araç-temelli yorum, hedef devletlerin kritik tesisleri üzerinde fiziksel hasara neden olacak şekilde siber araçları kullanan devletlerin sorumluluklarının Madde 2(4)'ün kapsamı dışında kalmasına neden olmaktadır.

Siber uzayda kuvvet kullanımı ve meşru müdafaaya ilişkin mevcut uluslararası hukukun incelenmesinde doktrinsel güçlükler olmakla birlikte, siber uzayda yürütülen harekatların parametrelerinin tanımlanmasına ilişkin hukuki çerçeveler de açık değildir. Günümüz bilgi ve siber teknoloji çağına kadar göz önüne alınmamış olmakla beraber, Madde 2(4)'te söz konusu kuvvet kullanma yasağı, siber araçların, düşmanın telekomünikasyon, ulaştırma, güç sistemleri, finans ve acil durum servisleri gibi fiziki altyapısına yıkıcı etkiler meydana getirecek şekilde cebri kullanımını da kapsayacak şekilde yeniden düzenlenmelidir.

Siber saldırıların kritik altyapılar üzerinde fiziksel etkileri olanlar ve olmayanlar şeklinde kategorize edilmesi, söz konusu maddenin kuvvet kullanımı konsepti kapsamında siber saldırıları kapsayacak şekilde yeniden düzenlenmesi probleminin çözümü için ilk adım olabilir. Daha sonra çabalar, düşman altyapısı üzerinde fiziksel etkileri olan siber saldırıların kuvvet kullanımı olarak kabul edilmesi üzerinde yoğunlaştırılabilir. Temel sorun, teknoloji bağımlı veya güçsüz devletlerin, maddenin yeniden düzenlenmesi konusunda istekli olacak olmalarına rağmen, devletler arası zorlama yöntemi olarak siber uzay fırsatlarını kullanma ihtimali olan güçlü devletlerin, maddenin yeniden düzenlenmesi konusunda isteksiz davranacak olmalarıdır.

Keywords: *Use of Force, Self Defence, Cyberspace, Cyber Attacks, Cyberspace Operations, Act of Aggression.*

Anahtar Kelimeler: *Kuvvet Kullanımı, Kuvvet Tehdidi, Meşru Müdafaa, Siber Uzay, Siber Saldırı, Siber Uzay Harekatları, Saldırı Eylemi.*

1. Introduction

States are willing to keep the cyberspace open for the social, economic and security interests of their country and their citizens. Everyday we see that all aspects of life are getting more dependent to cyber instruments. While the use of the cyberspace is getting more comprehensive, the vulnarability of States increases because of the exploitation of the cyber instruments. It is a big question whether a State can use armed forces in self defense under a cyber attack to its critical infrastructures. There are doctrinal difficulties in examining current international law on use of force and self-defense in cyberspace, while the legal frameworks for defining the parameters of operations in cyberspace are not clear.

2. Definition of Cyberspace

Definiton of various cyber capabilities and aspects of cyberspace is important to develop policies, doctrines and responses for the use of cyber capabilities. Current U.S. Department of Defense Dictionary of Military and Associated Terms defines the term "cyberspace" as "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." The term "cybersecurity" is also defined in this doctrine as "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."[2]

The international community and all States shall clearly define the terms like cyberspace, cybersecurity and cyberattack to develop successfull strategies to handle with the gaps while securing the crucial infrastructures and the public uses of internet. Characterizing

[2] The doctrine defines the term "cyberspace operations" as "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."; U.S. Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, 8 November 2010 (As Amended Through 15 February 2016), p.57-58, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, last visited April 17, 2016.

the cyber activity will lead to determine the organizations having authority to conduct any activity, funds that may be used to pay for the resources and operations, oversight procedures applicable to the activity and approval procedures.[3]

3. The Prohibition Against the Use of Force

The question whether the *jus ad bellum* and the *jus in bello*[4] bodies of law apply to the activities in cyberspace needs to be considered very carefully. But we can say that the *jus ad bellum* as currently structured is inadequate in containing and responding to the strategic threat posed by cyber capabilities to international peace and security.[5]

Article 2(3) of the United Nations (UN) Charter states that all members shall settle their international disputes by peaceful means. But the use of force is resorted by States as a form of dispute settlement generally as a last resort. Article 2(4) bans the unilateral use or threat of force by States providing "The Organization and its members, in pursuit of the purposes stated in Article 1, shall act in accordance with the following principles: .... (4) 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."[6]

In the customary international law, Article 2(4) is interpreted as a prohibition against the use of force focusing on restricting the use of military instruments. This instrument-based interpretation of the

---

[3] Commander Todd C. Huntley, "Controlling the Use of Force in Cyberspace: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare", Naval Law Review, Vol.60, 2010, p.6.

[4] *jus in bello* are the principles designed to limit suffering and destruction once an armed conflict has begun, and *jus ad bellum* are the principles governing when a State may legitimately use force. The term *"law of armed conflict"* includes both *jus ad bellum* and *jus in bello* principles.

[5] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law*, Vol.37, 1999, p.885.

[6] Article 2(4), U.N. Charter, http://www.un.org/en/sections/un-charter/chapter-vii/, last visited April 17, 2016.

use of force causes the responsibility of States which deploys cyber instruments to cause physical damage in the target States' critical infrastructures, remain outside the scope of Article 2(4).

The U.N. Charter also recognizes two different instances in which a State may use force:

The first instance is explained by Articles 39, 41 and 42 of the Charter. Article 39 states that "The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security."[7] Article 41 provides that "The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."[8] If the measures listed in Article 41 are inadequate or have proved to be inadequate, the Security Council, pursuant to Article 42, "may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security and such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations."[9]

The second instance where a State may also use force is to defend itself and others against an armed attack. Article 51 of the Charter states that "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take

[7] Article 39, U.N. Charter, loc.cit.

[8] Article 41, U.N. Charter, loc.cit.

[9] Article 42, U.N. Charter, loc.cit.

at any time such action as it deems necessary in order to maintain or restore international peace and security."[10] Thus, the use of force by States in individual or collective self-defense is recognized by the Charter. Article 51 limits the use of force in self-defense only if an armed attack occurs.

4. Cyber Attacks and the Prohibition Against the Use of Force

Whether a cyber attack constitutes a use of force is a complex issue. At the same time, it is very difficult to attribute cyber attacks to a specific individual, organization or State or a geographic location. Any removal or replication of valuable economic information and other forms of cyber espionage and exploitation in this area continue to remain outside the *jus ad bellum*.[11] Using the cyberspace to cyber espionage, manipulation of financial or personal data in a financial system, gain access to the control systems of critical infrastructure facilities, etc. may not reach to a level of use of force but they may cause greater damage to the security of any State or to the collective securty of the international community.

In the document named "An Assessment of International Legal Issues in Information Operations"[12] and published by the U.S. Department of Defense Office of General Councel which is dated May 1999, briefly explanations are given about "International Law Concerning the Use of Force among Nations", "Application to Computer Network Attacks" and "An "Active Defense" against Computer Network Attacks". After these explanations in this document, there is an assessment about "International Legal Regulation of the Use of Force In Peacetime" as:

> "It is far from clear the extent to which the world community will regard computer network attacks as "armed attacks" or

[10] Article 51, U.N. Charter, loc.cit.

[11] Jack M. Beard, "Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law", Vanderbilt Journal of Transnational Law, Vol.47, 2014, p.131.

[12] An Assessment of International Legal Issues in Information Operations, http://www.au.af.mil / au / awc / awcgate / dod-io-legal / dod-io-legal.pdf; last visited April 17, 2016.

> "uses of force," and how the doctrines of self-defense and countermeasures will be applied to computer network attacks. The outcome will probably depend more on the consequences of such attacks than on their mechanisms. The most likely result is an acceptance that a nation subjected to a State-sponsored computer network attack can lawfully respond in kind, and that in some circumstances it may be justified in using traditional military means in self-defense. Unless the nations decide to negotiate a treaty addressing computer network attacks, which seems unlikely anytime in the near future, international law in this area will develop through the actions of nations and through the positions the nations adopt publicly as events unfold. U.S. officials must be aware of the implications of their own actions and statements in this formative period."[13]

By this assessment it is underlined that the international community is not clear about the computer network attacks to be defined as armed attacks or use of force as prohibited by the Article 2(4) of the U.N. Charter. The U.S. officials are also noticed to be aware of the implications of their actions and statements during this period of which there is no exception in the near future about nations to negotiate a treaty addressing computer network attacks.

Commander Huntley of U.S. Navy argues that today the majority of cyber attacks conducted do not rise to a level of a use of force or an armed attack and continues: "There is a general agreement that for a cyber attack to be considered as an armed attack, the consequences of the cyber activity must be equivalent to those of a kinetic attack, that is, the activity must cause physical damage, injury or death. Such an attack would justify the use of armed force by the victim in self-defense, with the accompanying duty to abide by law of armed conflict (LOAC) in the use of that force. A State that found itself the victim of a cyber attack equivalent to a use of force, but not an armed attack, would be prohibited from using force to defend itself,

[13] An Assessment of International Legal Issues in Information Operations, http://www.au.af.mil / au / awc / awcgate / dod-io-legal / dod-io-legal.pdf; last visited April 17, 2016, p.27.

but might take diplomatic or economic measures in response to the activity."[14]

So one State under a cyber attack should consider the level of the attack and give reaction depending on the level of that attack. An entry into computer systems to obtain and observe information without causing any effect resulting destruction or modification of the system does not constitute either an armed attack or use of force, while it may constitute a violation of the territorial integrity of the State of the target computer or system.[15] So in specific circumstances in cyberspace it is very hard to determine that a cyber attack constitutes an armed attack or use of force.

Cyber threats have fundamentally different nature. In most of the cyber intrusion cases the responsible persons or organizations cannot be identified. In some cases the general geographic location from where the malicious activity eminated can be identified but one cannot be sure whether the activity had been routed through that location in an effort to shift blame or throw off investigators.[16]

Cyberspace also facilitates information operations such as psychological operations and military deception. The term "information operations" is defined in the U.S. Department of Defense Dictionary of Military and Associated Terms as "The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[17]

When a multi-week wave of cyberattacks in April to May 2007 disrupted the websites of the Estonian President and Parliament, the vast majority of Estonian ministries, three of the country's six largest

[14] Huntley, op.cit., p.43.

[15] CDR Vida M. Antolin-Jenkins, Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?", Naval Law Review, Vol.51, 2005, p.9.

[16] Huntley, op.cit., p.12.

[17] U.S. Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, 8 November 2010 (As Amended Through 15 February 2016), p.110, http://www.dtic.mil / doctrine / new_pubs / jp1_02.pdf, last visited April 18, 2016.

news organizations, and two of its major banks, the country shut down.[18]

The Stuxnet event showed us how a malware can gain control, target or destroy a critical infrastructure without using any kinetic weapons. The discovery of a malware that targeted the control systems at the Natanz nuclear facility of Iran was reported in June 2010. A malware called Stuxnet which was a 500-kilobyte computer worm had infected the software of at least 14 industrial sites in Iran, including a uranium-enrichment plant.[19] The worm attacted in three phases. In the first phase, it targeted Windows machines and networks, repeatedly replicating itself. In the second phase, it sought out Windows-based Siemens software, which is used to program industrial control systems that operate equipment such as centrifuges. In the last phase, the worm compromised the programmable logic controllers and thus, unbeknownst to the human operators at the plant, the worm's authors could spy on the industrial systems and cause the fast-spinning centrifuges to tear themselves apart.[20]

Stuxnet was designed and executed as a direct malware attack[21] targeting specific software or information technology. The other type of malware attack targets specific company or organization. Stuxnet's payload targeted specific Supervisory Control and Data Acquisition Systems (SCADA Systems).[22] Stuxnet's attack occured in diffirent approaches: a. Taking control of the centrifuge systems and begin to spin them faster and slower to crack and destroy them; b. Taking control of the nuclear fuel cascade process and begin to manipulate the process causing damage to the system; c. Deceiving

---

[18] Kelly A. Gable, "Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent", Vanderbilt Journal of Transnational Law, Vol.43, 2010, p.61.

[19] David Kushner, "The Real Story of Stuxnet; How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program"; http:// spectrum.ieee.org / telecom / security / the-real-story-of-stuxnet, erişim tarihi: 13.04.2016.

[20] loc.cit.

[21] A targeted attack is designed to attack a specific unit. A direct attack is designed to attack a single system within a specific unit.

[22] Andrew Moore, "Stuxnet and Article 2(4)'s Prohibition Against the Use of Force: Customary Law and Potential Models", Naval Law Review, Vol.64, 2015, p.2.

the engineers in the control room by sending them false data; d. Compromising digital safety systems preventing the automated systems from halting an unsafe process.[23] Thus, through the attacks of Stuxnet, the centrifuge systems and fuel cascade systems got out of control; the engineers in the control room got false data and digital safety systems compromised.

All unauthorized cyber activities are commonly referred by the terms "cyber warfare" or "cyber attack", regardless of the nature of the activity, the consequences of the activity or the person conducting the activity.[24] Current legal regimes fail to explain the legal framework to provide guidance to any State's offensive cyber operations or responses to cyber attacks. The law of armed conflict[25] do not adequately deter the States or non-State actors from using cyber attacks and intrusions to pursue their interests in a manner harmful to the national interests of another State.

The critical point is what will happen if such a complex and sophisticated malware attack would be created, tested and monitored in a well-coordinated manner by a terrorist organization or by a terror-sponsoring State? The international community shall deal with such an important issue.

All States shall investigate their cyberspace infrastructure and develop a cyber security strategy in order to prevent any attack towards critical infrastructure, networks and systems. After U.S. President Obama took office, his first acts was to order a comprehensive sixty-day review of U.S. cyberspace policy.[26]

[23] ibid, p.3.

[24] Huntley, op.cit., p.3-4.

[25] In the "U.S. Department of Defense Dictionary of Military and Associated Terms", the terms "law of armed conflict" and "law of war" are defined as "That part of international law that regulates the conduct of armed hostilities" and the term "rules of engagement" is defined as "Directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered. Also called ROE.", U.S. Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, 8 November 2010 (As Amended Through 15 February 2016), p.139, 207, http://www.dtic.mil / doctrine / new_pubs / jp1_02.pdf, last visited April 17, 2016.

[26] White House Press Statement, President Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review (Feb. 9, 2009)

Furthermore the U.S. Congress introduced three different bills addressing various aspects of cyber security in April 2009.[27] The developed States shall aid the technology-dependent States to counter cyber attacks and intrusions to provide collective security throughout the globe.

5. Conclusion

As being unforseen until this age of information and cyber technology, the prohibition of the use of force interpreted from Article 2(4) should be evolved to cover coercive uses of cyber instruments being used to have destructive effects in the enemy's physical infrastructures such as telecommunications, transportation, power systems, finance and emergency services. Categorizing the cyber attacks as having physical effects to critical infrastructure and not having any physical effects can be the first step to solve the problem of evolving the article to cover cyber attacks within the concept of use of force. Then the efforts may be concentrated on the cyber attacks having physical effects on the enemy's infrastructures to be considered as a use of force.

The main problem is that there would be an unwillingness of the powerful States which are likely to use the opportunities of cyberspace in Inter-State coercion to evolve the interpretation of the article, while the technology-dependent or powerless States would have a volition to evolve the Article.

The international community has much work to do in developing an international legal framework dealing with the cyber instrument threatening the security throughout the world. Cyber attacks continuously occur in daily bases not reaching to the level of use of force. States may not realize the real threat of a cyber attack until a critical situation occurs.

The international legal framework can be developed to reach to a point that enable States to use armed forces dealing with the threats

---

available at http://www.whitehouse.gov / the_press_office / advisorstoconductimmediate-cybersecurityreview/.; Huntley, op.cit., p.1.

[27] Ben Bain, Lawmakers Attack Cybersecurity on Multiple Fronts, Federal Computer Week, May 1, 2009, available at http://www.fcw.com / Articles / 2009/05/04/ news-congress-cybersecurity.aspx.; Huntley, loc.cit.

of cyber attacks, but this approach may lead to more complex situations and violent actions. Thus the mechanism to deal with the malicious uses of cyberspace should cover the operations made in the basis of cyberspace. The U.N. and other affiliated international organizations must deal with cyber warfare and develop strategies to prevent the malicious uses of the cyberspace. Very rapid mechanisms must be developed by the Security Council to react to cyber attacks intended to be used to threat the security of an individual State or the collective security of the international community.

REFERENCES

[1] Andrew Moore, "Stuxnet and Article 2(4)'s Prohibition Against the Use of Force: Customary Law and Potential Models", ***Naval Law Review***, Vol.64, 2015, p.1-25.

[2] Jack M. Beard, "Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law", ***Vanderbilt Journal of Transnational Law***, Vol.47, 2014, p.131.

[3] Kelly A. Gable, "Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent", ***Vanderbilt Journal of Transnational Law***, Vol.43, 2010, p.61.

[4] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", ***Columbia Journal of Transnational Law***, Vol.37, 1999, p.885.

[5] Todd C. Huntley, "Controllıng the Use of Force in Cyberspace: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare", ***Naval Law Review***, Vol.60, 2010, p.1-40.

[6] Vida M. Antolin-Jenkins, Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?", ***Naval Law Review***, Vol.51, 2005, p.9.

[7] An Assessment of International Legal Issues in Information Operations , http://www.au.af.mil / au / awc / awcgate / dod-io-legal / dod-io-legal.pdf; last visited April 17, 2016.

[8] David Kushner, "The Real Story of Stuxnet; How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program"; http:// spectrum.ieee.org / telecom / security / the-real-story-of-stuxnet, erişim tarihi: 13.04.2016.

[9] U.S. Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, 8 November 2010 (As Amended Through 15 February 2016), p.57-58, http://www.dtic.mil / doctrine / new_pubs / jp1_02.pdf, last visited April 17, 2016.