Ivane Javakhishvili Tbilisi State University
Faculty of Law

Journal of Law

№1, 2020

უნივერსიტეტის
გამომცემლობა

Guram Gvinjilia*

Cyber-Attack in the context of the prohibition of the use of force – The need for Reconsideration of International Law?

With the development of modern technology, the issue of reassessment of international law is becoming more and more critical in order to enable adequate regulation of technologies by static norms of international law. The cyberspace is regarded to be one of those cases. With illegal cyber-attacks, states often violate the cyberspace of other countries. Examples of such interventions are 2007 cyber-attack on Estonia, the virus found in the computer system in Iran's nuclear power plant in 2010, and the cyber-attack on the Georgian cyberspace during the 2008 Russian-Georgian armed conflict. While currently there are no special regulations on cyberspace, the role of international law is often diminished.

The article aims to discuss the current international legal regime that applies to cyber operations. In this regard, the focus will be on the relationship between cyber operations and the United Nations Charter, the prohibition of the use of force, and the principle of non-intervention in the internal affairs of states. Analysis of the state practice shows that states perceive cyber-attacks as an independent form of use of force, and they seek legal assessment within the framework of current international law. There is also a tendency to regulate cyber-attacks with specialized norms.

Cyber-attacks require a new understanding in the terms of international law. However, this does not mean that cyber-attacks cannot fall within the framework of the current international conventional and customary law and go beyond its scope. A new understanding is needed only within the framework necessary for the incorporation of cyber-attacks into the already existing international legal framework.

Keywords: *cyber-attack, cyber operation, cyberspace, use of force, international customary law, international law of treaty, evolutionary interpretation, Tallinn Manual, intervention in domestic affairs.*

1. Introduction

The importance of technological development is rapidly increasing in the modern world. In parallel, the norms regulating it remain to be more static. Since the end of the last century, a debate began over putting cyber operations in the framework of law. The 9/11 attack on the United States of America (hereinafter "the USA") raised a concern that cyber terrorism would expand soon. States often infringe on the cyberspace of other states, subsequently, due to the lack of specific regulations, the role of international law decreases. For instance, In 2007, a massive cyber-attack caused a severe

* Doctoral Student at Ivane Javakhishvili Tbilisi State University. Invited Lecturer of Faculty of Law of Ivane Javakhishvili Tbilisi State University.

obstruction of the banking system in Estonia. In 2010, a computer virus provoked problems for the nuclear plant in Iran. The Georgian cyberspace had also become the target of hacker attacks during the Russian-Georgian armed conflict in 2008. It was the most apparent manifestation of cyber-attack in the context of armed conflict. That cyber-attack of an unprecedented scale accompanied aggression of the Russian Federation against Georgia.

The purpose of this article is to examine the instruments of international law that apply to the cyber-attacks, including the evolutionary interpretation of the United Nations (hereinafter UN) Charter to determine: Whether or not the prohibition of the use of force applies to cyber-attacks? Does international law demand new understanding in the context of cyber operations, especially the cyber-attack? Moreover, whether are there rules of international law securing states from cyber-attacks that do not amount to the use of force as given in the UN Charter?

To responding to these questions, the paper addresses state practice and particular examples for better analyzing international customary law concerning cyber-attacks and cyber operations.

It shall be emphasized that the research refers to cyber operations only in the context of *jus ad bellum*. Indications from international humanitarian law will be invoked for resolving the main issues that the article introduces.

2. Law Applicable to Cyber-Attacks

2.1. Do any Existing Treaty-based Norms Address to Cyber-Attacks?

The norms of international law are divided into two categories, first, primary norms that determine general rules for conduct of the states and secondary rules that determine the responsibility of states.[1] For this reason, answers shall be delivered for questions such as what type of norms of international law applies to the cyber-attacks? Furthermore, if there are no specific rules, then is it possible for international treaties to apply to the cyber-attacks?

Since 2000, in its resolutions, the UN General Assembly repeatedly reiterated about the interest of the international community to regulate the use of modern technologies.[2] The General Assembly drew attention to the fact that unlawful utilization of these technologies could badly impact states,[3] and it could pose a critical threat to international peace and security.[4] In 2003 and 2005, the General Assembly held two world summits in Geneva and Tunis on the matters of cyber security.[5] In 2010 in

---

1 *See e.g. Cassese A. (ed.),* The Oxford Companion to International Criminal Justice, Oxford University Press, 2009, 19-20.

2 *See e.g.* United Nations General Assembly (UNGA) Resolutions 55/28 of 20 November 2000; 56/19 of 29 November 2001; 59/61 of 3 December 2004; 60/45 of 8 December 2005; 61/54 of 6 December 2006; 62/17 of 5 December 2007; 63/37 of 2 December 2008; 64/25 of 2 December 2009; 65/41 of 8 December 2010; 66/24 of 2 December 2011; 67/27 of 3 December 2012.

3 UNGA Resolutions 55/63 of 4 December 2000; 56/121 of 19 December 2001, Preamble.

4 UNGA Resolutions 58/32 of 8 December 2003; 59/61 of 3 December 2004; 60/45 of 8 December 2005; 61/54 of 6 December 2006; 62/17 of 5 December 2007; 63/37 of 2 December 2008; 64/25 of 2 December 2009; 65/41 of 8 December 2010; 66/24 of 2 December 2011; 67/27 of 3 December 2012.

5 *Roscini M*., Cyber Operations and the Use of Force in International Law, Oxford University Press*,* 2014, 3-4.

Astana, the memorial declaration of the OSCE acknowledged cyber operations as ”increasing transnational threat”.[6] In November of the same year, NATO stated that cyber-attacks could reach such level that may endanger the security and stability of the alliance.[7] In 2011, China, the Russian Federation, Tajikistan, and Uzbekistan, jointly initiated a project of resolution on the international code of informational security.[8] However, the initiative was unsuccessful.

The abovementioned is a manifestation of the rising concern of the international community towards cyber operations and a sign of the approaching universal and specific document on this issue. There have already been such efforts on the regional level, such as the Convention of Cybercrime of the Council of Europe.[9] Also, in 2001 the Dakar summit passed the Additional Protocol to the Convention of the Organization of African Unity on the Prevention and Combating of Terrorism, referring to the cyber-attacks as well.[10] Nevertheless, specific binding document on cyber operations still does not exist.

2.2. Evolutionary Interpretation of International Treaties: Does Current Legal Regime Apply to the Cyber Operations?

Absence of specific treaty norms in cyberspace raises a logical question - does the current international legal regime cover cyber operations? It is not a matter of dispute that international humanitarian law, known as *jus in bello*, in particular, Geneva Conventions of 1949 and its Additional Protocols of 1977 apply to the cyber-attacks as it applies to all of the means and methods of warfare.[11] This approach is supported by the International Court of Justice (hereinafter "ICJ") in its advisory opinion in the *Legality of the Threat or Use of Nuclear Weapons*, stating that the Martens Clause “has proved to be an effective means of addressing the rapid evolution of military technology.”[12] The question arises, whether it is possible to apply UN Charter and other international legal documents to the cyber operations through evolutionary interpretation? A positive answer to this question is essential for having any further discussion.

International law of treaties frequently faces issues of evolutionary interpretation of various treaties. Because of technological advances and other factors, treaties often lose adequacy to modern challenges. Annulment or replacement of these treaties is associated with difficulties and lengthy

---

6 OSCE, Astana Commemorative Declaration – Towards a Security Community, SUM.DOC/ 1/10/Corr.1, 3 December 2010, § 9, <http://www.osce.org/cio/74985?download=true> [16.05.2020].

7 NATO, Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation, November 2010, §§ 7, 12, <http://www.nato.int /lisbon2010/strategic-concept-2010-eng.pdf> [26.05.2020].

8 UN Doc A/66/359, 14 September 2011.

9 Convention on Cybercrime, Council of Europe, ETS No185, (opening of the treaty to sign: 23.11.2001; entry into force: 01.07.2004).

10 *Salinas de Frias A. M., et al. (ed.),* Counter-Terrorism: International Law and Practice, Oxford University Press, 2012, 1005-1006.

11 For further reading *See*: *Scmitt, M. N.,* Wired Warfare: Computer Network Attack and Jus in Bello, International Review of the Red Cross, Vol 84, Issue 846, 2002, 365-399.

12 *Legality of the Threat or Use of Nuclear Weapons,* ICJ, Advisory Opinion, 8 July 1996, §78.

procedures. In such situations, a primary consideration is given to the contemporary interpretation of the problem, labeled by legal academics as evolutionary interpretation.[13] In *Dispute Regarding Navigational and Related Rights*, ICJ highlighted that the parties to the treaty were conscious of the fact that in time, the interpretation of the treaty would evolve, and hence the treaty was open-ended, there was a presumption that it's terms had evolutionary character.[14] This is one of the remarkable examples of evolutionary interpretation of the treaty.[15] Noteworthy, except for the ICJ, the doctrine of evolutionary interpretation is often used by the European Court of Human Rights as well, indicating that the European Convention on Human Rights is "a living instrument that must be interpreted according to present-day conditions."[16]

Therefore, the evolutionary interpretation of international treaties performs a vital function in the development and codification of international law. Though, it shall be noted that such an interpretation of the law is strongly interlinked with judicial bodies. ICJ or any other international court or tribunal has not yet delivered a judgment on the cyber-operations. Nevertheless, the UN Charter and international legal system still apply to it if interpreted through the virtue of evolutionary theory, in particular with regard to the prohibition of the use of force that corresponds to cyber-attacks.

2.3. Does Customary International Law Apply to Cyber-Attacks?

The positive answer on the problem of evolutionary theory leads us to the next question, notably whether or not we could find any general or particular rule in customary international law that applies to the cyber-operations. Or moreover, whether or not we are facing the process of emerging new rules of customary international law.

Article 38 of the Statute of ICJ defines customary international law "as evidence of a general practice accepted as law."[17] Customary international law, that is mainly represented in a verbal form,[18] consists of two cumulative elements. These elements are State practice and cognitive element or *opinio juris ac necessitates,* that is defined as „evidence of belief that the [State] practice has a binding character and is reinforced by the appropriate rule of law."[19]

---

13 *Cannizzaro E, (ed.),* The Law of Treaties Beyond the Vienna Convention, Oxford University Press, 2011, 125.

14 *Dispute Regarding Navigational and Related Rights (Costa Rica v. Nicaragua),* ICJ, Judgment, 13 July 2009, §§ 49-52, 66.

15 *Bjorge E*., The Evolutionary Interpretation of Treaties, Oxford University Press, 2014, 1-22.

16 *See e.g. Rasmussen v Denmark,* ECtHR, Judgment, 28 November 1984, Series A, No. 87, § 40; *Guzzardi v Italy,* ECtHR, Judgment, 6 November 1980, Series A, No. 39, §95; *Rees v the United Kingdom,* ECtHR, Judgment, 17 October 1986, Series A, No. 106, § 47; *Ireland v United Kingdom,* ECtHR, Judgment, 18 January 1978, Series A, No. 25, § 239.

17 The Statute of the International Court of Justice, Article 38.

18 Though, there are many conventions that itself represent customary international rules. For example, the Vienna Convention on the Law of Treaty, 1907 Hague Convention, or four 1949 Geneva Conventions.

19 *North Sea Continental Shelf* (Germany v. Denmark/The Netherlands), ICJ, Judgment of 20 February 1969, §77; *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. US), Merits, ICJ, Judgment of 27 June 1986, § 183.

First and foremost, the existence of cyber specific norms in customary international law shall be determined. The Tallinn Manual is essential in this regard. The introduction of the Tallinn Manual suggests – "because State cyber practice and publicly available expressions of *opinio juris* are sparse, it is sometimes difficult to conclude that any cyber specific customary international law norm exists."[20]

Despite above-mentioned, it is not proper to contend that current customary international law does not apply to cyber operations since the existence of cyber specific rules is under doubt.[21] As Dinstein rightly argues, "State practice shall not necessarily evolve separately towards each weapon."[22] Furthermore, there is an increased number of States whose military manuals consider utilization of cyber forces as a precondition for the application of the right to self-defense. The importance of military manuals in the determination of the customary rule was acknowledged in the *Tadic Case* by the International Tribunal for the Former Yugoslavia.[23] Even though the number of such documents is not impressive, the formation of a customary rule does not require a clear demonstration of support by every State. ICJ reasoned in the *Fisheries Case* that by not protesting on the existing customary rule of straight lines, the United Kingdom had recognized the customary character of the rule.[24] States and international organizations that acknowledge cyber-attacks as a prerequisite for the right to self-defense are following: USA, China, Australia, Cuba, Hungary, Italy, Iran, Mali, Netherlands, Qatar, the Russian Federation, the United Kingdom and European Union.[25] Remarkably, any protest is missing that could obstruct the emergence of a customary rule that deems cyber-attacks to be covered by the prohibition of the use of force or conceiving it as a prerequisite for the right to self-defense.

Hence, emerging state practice is evident and as it is illustrated by more and more states, by including cyber-operations into their military manuals. Also, concrete cases show states invoking the right to self-defense in response or for the prevention of cyber-attacks. As for the second element of customary law, the *opinion juris* is not evident in our case. However, the lack of protest of states leads us to consider that silence as an expression of acceptance. This may be a starting point for emerging customary rule. "The soft law" could also play a crucial role in this process, and it will be reviewed in the next chapter. Before that, in conclusion, it shall be stated that current customary international law applies to cyber operations.

---

20 *Schmitt M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 5;

21 *Roscini M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 3-4, 25-26.

22 *Dinstein Y.*, Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference, International Law Studies, Vol. 89, 2013, 280.

23 *The Prosecutor v. Dusko Tadic,* ICTY, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Case IT-94-1, 2 October 1995, § 99.

24 *Fisheries Case (United Kingdom v. Norway)*, ICJ, Judgment, 18 December 1951.

25 *Roscini M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 21-23.

2.4. 2009 Tallinn Manual as a Soft Law

In response to the 2007 massive cyber-attack on Estonia,[26] NATO established the Cooperative Cyber Defense Center of Excellence. In 2009, NATO invited 20 distinguished international law experts to draft guiding principles based on international law that would apply to cyber operations both in the situations of *jus ad bellum* and *jus in bello*. As a result, the Tallinn Manual on the International Law Applicable to Cyber Operations was prepared.

Since the Tallinn Manual is the only specific and codified document on cyber warfare, it is necessary to determine its nature. In particular, whether it is a mere opinion of scholars and, therefore, a secondary source of international law according to Article 38(1)(d) of the ICJ Statute or a "soft law" that could be considered as a preliminary stage for the formation of a customary international law.

The term "soft law" was first introduced by Lord MaCnair to describe indirectly binding documents.[27] Soft law is primarily associated with international governmental organizations and resolutions or recommendations they pass. A soft law itself could be categorized as follows: non-binding documents of international organizations such as resolutions, non-binding agreements between states,[28] and non-binding parts of interstate binding conventions.[29]

Soft law is often discussed in the light of *lex feranda*, which is preferably a direction towards which international law should develop.[30] Besides that, soft law is characterized by different traits. Notably, it may be considered to be a mean of reinforcement for traditional sources of international law.[31] Especially interesting seems to be its correlation with customary international law. For instance, in international environmental law, it plays an essential role since it carries *de facto* binding effect[32] and, at the same time, accelerates the formation of a customary rule. Notably, such an approach is not limited only by environmental law. The existence and mandatory character of soft law were recognized as well by the ICJ in the *Oil Platforms Case*. In the *Oil Platforms Case*, Iran based its *compromis* on the 1955 bilateral agreement with the USA that highlighted the necessity of peace and cooperation among the parties. The point is that this agreement did not constitute an international treaty as it represented soft law; however, ICJ considered it and stressed that the agreement should have been applied for interpretation and examination of the conduct of the state parties.[33]

---

26 See below section 3.1.

27 *Thurer D.,* Soft Law. Max Planck Encyclopedia of Public International Law, Oxford University Press, 2009, §5. *Roscini M.*, Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 45.

28 For example, the 1975 Helsinki Final Act represents soft law by its nature. See Final Act, Conference On Security and Co-Operation in Europe, 1975.

29 *Thurer D.*, Soft Law, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2009, §§ 9, 15.

30 *Thirlway H.*, The Sources of International Law, Oxford University Press, 2014, 165.

31 Ibid.

32 *Beyerlin U., Stoutenburg J. G.*, International Protection of Environment, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2015, §§ 2, 8, 21, 30.

33 *Oil Platforms case (Iran v. USA)*, ICJ, Judgment, 6 November 2003, §52; Also See: *Thirlway H.*, The Sources of International Law, Oxford University Press, 2014, 167.

The reasoning, as mentioned above, is essential for determining the legal nature of the Tallinn Manual. At a glance, this document is a work of universally acknowledged scholars, but the crucial fact is that it uses normative language. Furthermore, the manual was prepared under the auspices of the NATO, and international (intergovernmental) organization - a fully-fledged subject of international law. The Tallinn Manual is more than just mere paperwork of scholars. At least, the manual shall be considered as a subsidiary means for interpretation of international law and placed in the list suggested by Article 38 of the ICJ Statute. It must be highlighted here, that some scholars advocate against formal hierarchy among sources of international law.[34] Besides, the Tallinn Manual could be regarded as a part of soft law that demonstrates the emergence of customary law. Historical facts also support this proposal. For example, the San Remo Manual on International Law Applicable to Armed Conflicts at Sea[35] was prepared by the International Committee of the Red Cross as a part of soft law, however today, that manual is actively exploited by states as customary international law.[36]

3. Inter-State Cyber-Attacks in Practice

3.1. Estonia 2007

In spring of 2007, the Estonian Government announced that the statue of the "Russian Soldier" would be removed to the new location in the suburb of Tallinn. The statue was erected in memorial of soviet soldiers who fell during the war against the Nazi regime. But according to the government statement, now the statue became a symbol of occupation. The ethnic Russian population disapproved the decision of Estonia, and soon the dissatisfaction converted into demonstrations. The cyber-attacks, accompanying violent manifestations, targeted on Government and private sector (such as the media and banking system). There had been launched DDoS (Distributed Denial of Service) type hacker attacks, meaning that websites received excessive requests of information, leading them to slow down or entirely stop functioning. As a result, legitimate customers are distracted from using websites. In the beginning, the DDoS was clumsy and easy to avoid,[37] but soon it upgraded and became difficult to detect. The Botnet had also been exploited. The Botnet is a computer web that is used without permission of the owner. In the Estonian case, 85 000 computers were manipulated to send requests of information to the government websites. Estonian websites could not withstand such a flow and were ultimately crushed.[38] Cyber-attacks continued for three weeks (from April 26 to May 19), although the Government of the Russian Federation denied any link with them. The involvement of the Russian Government was not approved; however, Estonia still seeks Russian Federation responsible.[39]

---

34 *Thirlway H.,* The Sources of International Law, Oxford University Press, 2014 117-128.

35 San Remo Manual on International Law Applicable to Armed Conflicts at Sea, 12 June 1994, ICRC. <https://www.icrc.org/ihl/INTRO/560?OpenDocument> [25.05.2020].

36 *Roscini M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 32-33.

37 *Tikk E., Kasha K., Vihul L.,* International Cyber Incidents: Legal Considerations, Cooperative Cyber Defence Centre of Excellence, 2010, 19.

38 *Steed D.,* The Strategic Implications of Cyber Warfare, Cyber Warfare: A Multidisciplinary Analysis, *Green J. A.*, Routledge, 2015, 78.

39 Russia Accused of Unleashing Cyberwar to Disable Estonia. The Guardian (17 May 2007) <https://www.theguardian.com/world/2007/may/17/topstories3.russia#maincontent> [09.05.2020].

The question was raised in the media and academics whether the DDoS type cyber-attack could be considered as unjustified use of force. Uniquely, those attacks caused severe damage to Estonia. In May 2007, Estonian Parliament Speaker compared effects of the cyber-attacks to the effects of the use of nuclear weapons and stated that cyber-attacks do not cause bloodshed; however, they destroy everything and everyone.[40]

3.2. Russian Cyber-Attacks Against Georgia During the 2008 War under International Law and Tagliavini Report

2008 was remarkable not only because of the aggression against Georgia but because of the massive, unprecedented cyber-attack that the Russian Federation carried out against the public and private sector of Georgia as well.

The first wave of attacks shut down government websites and replaced the information with fake notifications. Lots of disinformation was disseminated, aiming to sow fear among the citizens.[41] Georgian Government even announced that the Russian Federation was carrying out cyber war.[42]

The second wave of attacks targeted at blocking of civil and private websites. For some time, the population had been prevented from access to broadband. Public panic and feeling of helplessness raised, respectively.

The 2009 Tagliavini Report that was prepared by the fact-finding mission on the 2008 war has found: „If these attacks were directed by a government or governments, it is likely that this form of warfare was used for the first time in an inter-state armed conflict.“[43]

Reports on cyber-attacks are one of the distinct specifications of the 2008 Russian-Georgian war.[44] Beyond doubt, cyber-attacks were being executed during the armed conflict. In the first days of the war, Georgian governmental and information websites had been damaged or became inaccessible. Later, some websites had been moved to American, Estonian, and Polish servers.[45] Some experts suggest that these attacks could have weakened the decision-making ability of Georgia, as well as communications with its allies, ultimately leading to a decline in the operational mobility of Georgian forces. The most exciting events that effected the sustainability of the state and where Russian Federation invaded into sovereign rights of Georgia were the followings:[46]

---

40 *Ergma E.,* Speaker of the Estonian Parliament, cited in *Davis J.,* Hackers Take Down the Most Wired Country in Europe, Wired Magazine (21 August 2007) <https://www.wired.com/2007/08/ff-estonia/> [23.05.2020].

41 *Markoff J.,* "Before the Gunfire, Cyberattacks", The New York Times*,* 2008. <http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0> [17.05.2020].

42 *Swaine J.,* "Georgia: Russia 'Conducting Cyber War'", The Telegraph, 2008. <http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html> [17.05.2020].

43 Report of the Independent Fact-Finding Mission on the Conflict in Georgia, Vol. II, September 2009, 217–219.

44 *Korns S. W., Kastenberg J. E.,* Georgia's Cyber Left Hook, Small Wars Journal Parameter, Winter Edition, 2008-2009.

45 For example, Polish Server, <www.president.pl>.

46 Georgian government blamed the Russian Federation for instigating "the virtual fire". RFERL 12.08.2008. <http://www.rferl.org/content/Georgian_Government_Accuses_Russia_Of_Cyberwar/1190477.html>; <http://georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.html> [25.05.2020].

- On July 20, website of President of Georgia was shut down for 24 hours;
- On August 7, several Georgian servers and the Internet traffic were seized and placed under external control;
- On August 8, large-scale cyber-attacks against sites in Georgia began. The source of the cyber-attacks was uncertain. Some reports attributed them to an organization called the "Russian Business Network."[47]
- At this time, it was reported that all Georgian Government websites were unobtainable from the US, UK, and European cyberspace. The Turkish AS9121 TTNet server, one of the routing points for traffic into the Caucasus, was blocked, reportedly via COMSTAR;
- On August 9, the Georgian Ministry of Foreign Affairs website was defaced by hackers, who replaced it with offensive photographs. Other Georgian websites that also suffered cyber or hacker attacks included those of the Ministry of Internal Affairs, the Ministry of Defence, and the website of Sanakoyev's pro-Georgian Interim Administration of South Ossetia. Besides, reportedly the National Bank of Georgia was defaced, and Georgian news portals were affected by DDoS (distributed denial of service) attacks.
- By August 12, website of the President of Georgia and a popular Georgian TV website were transferred to Tulip Systems. Tulip was then also attacked;
- On 12-13 August, websites of Ministry of Internal Affairs and the Ministry of Defence experienced extensive cyber-attacks and two periods of downtime.

At the same time, more limited attacks have been launched against Russian sites as well (Web-site of Ria Novosti (РИА Новости) went offline for 10 hours).

With high probability, cyber-attacks against Georgia were directed by the Russian Government. If that is true, then the 2008 war was the first case ever where cyber-attacks had been carried out in the context of warfare. It must be noted that such attacks are easy to undertake, though challenging to prevent or track origins.

As mentioned in the Article, while considering cyber-attack as a use of force, attention should be drawn to the scale of the attack and the damage it caused. Tagliavini's suggestion that the Russian Government could have managed cyber-operations sheds light on many things.

Absolute blocking of broadband, dissemination of disinformation, and purposeful spreading of fear among the population is nothing but an attempt to cause disturbance and inability to maintain order in the State. Such circumstances threatened the lives of hundreds of thousands of persons whose houses had already been bombed by the Russian air forces. Russian forces had also paralyzed the highway connecting East and West Georgia as they locked Georgian town, Gori. As a result of cyber-attacks, communications between Georgians were obstructed. Indeed, such damage is still unprecedented in the world. Even the attacks on Estonia are not close to the scale of strikes against Georgia.

Thus, the course of Russian cyber-attacks in the 2008 Russian-Georgian war represents yet another case of aggression and unjustified use of force.

[47] Report of the Independent Fact-Finding Mission on the Conflict in Georgia, Vol. II, September 2009, 218.

3.3. Iran 2010

In July 2010, the Government of Iran discovered a virus, later called Stuxnet, installed on its computers. The virus was explored on numerous computer systems of Iran, with epicenter in the Natanz Nuclear Power Plant.

Used for the enrichment of uranium, Natanz is Iran's most advanced nuclear power plant. The Government of Iran claimed that the aim of their program was peaceful, in particular - the production of atomic energy. Though, the international community still has doubts about the possible use of that nuclear energy for the creation of the weapon of mass destruction.[48]

Enrichment of uranium requires thorough perseverance of specific conditions. Firstly, uranium shall be freed of extra admixtures. Then, placed in the centrifuges, it spins with constant speed under certain pressure and temperature.

Stuxnet virus started to change the speed of centrifuges; however, devices did not indicate any malfunction.[49]

The Government of Iran did not disclose details of the virus effects. The Head of the Atomic Energy Organization of Iran announced about detecting the virus before it penetrated the apparatus.[50] On the contrary, according to the statement of the President of Iran, the virus inflicted severe problems on several centrifuges and proper functioning of the software.[51]

Other reports claim that the damage was much more large-scale than the government representatives of Iran declared. The Institute for Science and International Security insisted[52] on alleged damage of not only uranium but of the centrifuges too. According to the evidence of the International Atomic Energy Agency, Iran replaced 1 000 centrifuges in 2009 and 2010 - seemingly as a result of the Stuxnet virus.[53]

Considering that Article 2(4) of the UN Charter is a result-based prohibition, those attacks on Iran could hardly be evaluated as unjustified use of force since, during the attacks, the virus had not been identified and revealed. As the President of Iran declared, intrusion induced malfunction of centrifuges by which enrichment of uranium had been obstructed. This type of attack does not count as unlawful use of force since the material property had not been impaired.[54] On the contrary, if the suggestion of the International Atomic Energy Agency about the breaking down of centrifuges is real, then such kind of harm could constitute a violation of Article 2(4) of the UN Charter.

---

48 United Nations Security Council (UNSC) Resolution 1696, 31 July 2006.

49 *Shakarian P.*, Stuxnet: Cyberwar Revolution in Military Affairs. Small Wars Journal, Vol. 7, 2011, 1.

50 "Iran Briefly Halted Enrichment", Aljazeera (23 November 2010), <http://www.aljazeera.com/news/middleeast/2010/11/201011231936673748.html> [11.05.2020].

51 "Iran says Cyber Foes Caused Centrifuge Problems" Reuters (29 November 2010). <http://www.reuters.com/article/iran-ahmadinejad-computers-idAFLDE6AS1L120101129> [24.05.2020].

52 *Albright D., Brannan P., Walrond C.,* Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?, Institute for Science and International Security, 2010, <http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf> [22.05.2020].

53 *Katz Y.,* Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years. Jerusalem Post (Jerusalem, 15 December 2010), <http://www.jpost.com/IranianThreat/News/Article.aspx?id=199475> [26.05.2020].

54 *Woltag J. C.,* Computer Network Operations below the Level of Armed Force, European Society of International Law Conference Paper Series, 2011, 1. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1967593> [26.05.2020].

4. The Lawfulness of Cyber-Attacks under the UN Charter

4.1. Examination under Article 2(4) of the UN Charter

Article 2(4) of the UN Charter[55] was referred as a cornerstone of the Charter by ICJ in *Nicaragua Case*.[56] This norm, being part of customary international law,[57] represents a *jus cogens* norm as well.[58] As mentioned in the previous chapter, evolutionary interpretation may apply to the international treaties and among them the UN Charter. Though, in this chapter, the following questions shall be answered - whether or not the UN Charter prohibits cyber-attacks? Does cyber-attack amount to the use of force? Furthermore, if so, then what types of cyber-attacks could constitute the use of force, and how shall be determined whether or not a specific cyber-attack meets the criteria of the use of force?

Experts of the Tallinn Manual suggest that *jus ad bellum* also applies to the particular categories of cyber-attacks.[59] This reasoning stems from the assessment by ICJ in the *Nuclear Weapons Case*, indicating that right to self-defence "apply to any use of force, regardless of the weapons employed".[60] Since the invocation of the right to self-defense correlates with Article 2(4) of the UN Charter and "any weapon" may also imply both the electric means and cyber-attacks, it is evident that *jus ad bellum* in the modern era also spreads over cyber operations. While taking actions in cyberspace, conducting cyber-attack by one State against another one should be perceived as an conduct, while electronic means is the instrument for performing such conduct.

Noteworthy, commentaries to the UN Charter do not oppose the estimation of computer attack, having a similar effect to the weapon, to constitute use of force in the light of Article 2(4) of the Charter.[61] Moreover, in certain circumstances, it may amount to the armed attack, triggering Article 51 of the Charter.[62]

Cyber-attack constitutes the use of force if three prerequisites are met: a) The attack shall be carried out by a State; b) Cyber operation must be perceived as a threat or use of force; c) Threat or use of force shall be undertaken in the context of international relations between states.[63]

---

55 "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."

56 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, §§ 188–190.

57 Ibid*,* §§187-190.

58 *Roscini M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 44.

59 *Weller M. (ed.),* The Oxford Handbook of the Use of Force in International Law, Oxford University Press, 2015, 1112.

60 *Legality of the Threat or Use of Nuclear Weapons,* ICJ, Advisory Opinion, 8 July 1996, §39.

61 *Simma B., et al (eds.),* The Charter of the United Nations: A Commentary, Vol. I (3rd ed.), Oxford University Press, 2012, 210.

62 Ibid*.*

63 *Roscini M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 44.

As for the first criteria, it may entail not only official or *de jure*,[64] but *de facto* organs of state aw well,[65] including non-state actors who remain under the effective control of a state.[66]

Concerning the threat or use of force, the Tallinn Manual declares that this precondition is satisfied whenever the results and effects of cyber operation could be compared to the damage caused by the conventional weapon, which would be enough to assess the action as the use of force.[67]

On the one hand, the prohibition of the threat or use of force under Article 2(4) may apply to cyber operations. However, a clear definition of what may constitute a threat or use of force does not exist. In situations like that, the 1969 Vienna Convention, reflecting customary international law, acknowledges interpretations based on contextual analysis. It must be highlighted that the term "force" is also given in the preamble of the UN Charter as well as in Articles 41, 44 and 46. In all of these cases, the word "force" is preceded by the word "armed", while Article 44, in general, refers to the use of armed forces. Such a distribution causes a diversity of opinion. On the one hand, it could be assumed that Article 2(4) also relates "use of force" to the armed context, similar to other articles of the Charter. Likewise, it is arguable that Article 2(4) purposefully omitted the term "armed" because its scope is broader than other norms. The latter argument is supported by the spirit of the Charter too, since the Charter aims to protect future generations from the cruelty of the war.[68] Even if the argument for the narrow scope of Article 2(4) wins, cyber-attacks would still fall into its ambit as they obviously may constitute an armed attack. The only remaining question here addresses the degree of a scale that a cyber-attack shall have so that it could amount to the "armed attack" for the UN Charter. In this regard, legal doctrine uses three distinct factors: assessment of the means of attack, assessment of the target, and assessment of the effects of the act. In scholarship, more dominant is the latter approach that draws attention to the assessment of the direct and devastating effects on property and humans.[69]

4.2. Factors Established by the Tallinn Manual

Group of international experts agrees that when determining whether cyber-attack constitutes use of force or not, states shall pay attention to the following factors: severity; immediacy, directness; invasiveness; measurability of effects; military character; state involvement; and presumptive legality.[70]

---

64 Articles on State Responsibility for Internationally Wrongful Acts, International Law Commission, 2001, art. 4.

65 Articles on State Responsibility for Internationally Wrongful Acts, International Law Commission, 2001, art. 8, It shall be emphasized that the ICJ confirmed customary character of both Article 4 and 8. *See*.: *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, ICJ, Judgment, 26 February 2007, §§ 385, 398.

66 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986.

67 *Schmitt M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, art. 11, 45.

68 *Roscini M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 45.

69 Ibid*,* 47.

70 *Schmitt M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, წესი 11, § 9(a-t), 54-55.

Severity is the most important of all the factors listed above. Indeed, a cyber-attack followed by the destruction or death of humans falls within the scope of use of force. Whenever such a material loss is absent, cyber-attack may still fall in the ambit of Article 2(4) considering its scale, length, intensity, etc.[71] Immediacy is determined by the period between the beginning of an attack and the emergence of its effects. Directness reflects the causality between the attack and damage inflicted. Invasiveness is given whenever incursion into another state's cyberspace occurs without approval. The measurability of effects deals with the ability to measure the damage inflicted. Unlike other factors, presumptive legality shall be absent. For example, the economic pressure of one State on another falls within the presumptive legality and therefore does not violate international law, nothing to say about Article 2(4) of the UN Charter. In the end, a cyber-attack must carry the military character. However, this should not be perceived as just an attack on military facilities.[72]

It shall be noted that, cyber-attacks on Estonia in 2007 can be freely assessed as the use of force in the light of Article 2(4) of the UN Charter. But the problem is the lack of evidence that the Russian Government had planned or organized the above-mentioned cyber-attack.

4.3. Principle of Non-Intervention as an Alternate to Prohibition of Use of Force for Low-Intensity Cyber-Attacks

In particular cases, cyber operations may not reach the threshold required for qualifying it as the use of force, even though such acts remain within the margins of international law.

Those cases would constitute interference in the internal affairs of a state, a prohibited act under international law that infringes state sovereignty[73] and the customary law principle of non-intervention.[74]

Whenever the primary rules of international law are violated, the secondary rules trigger and establish responsibility. Obviously, in case the threshold of threat or use of force is not reached, a military response could not be justified. However, the matter is regulated by alternative means. In this respect, 2001 Articles on State Responsibility for Internationally Wrongful Acts[75] plays a significant role as it reflects customary international law and establishes state responsibility.

Traditionally, the principle of non-intervention in the domestic affairs was always discussed in light of the use of force.[76] However, ICJ in the *Nicaragua Case* distinguished the use of force as a

---

71 *Weller M. (ed.),* The Oxford Handbook of the Use of Force in International Law, Oxford University Press, 2015, 1114.

72 Ibid, 1115-1116.

73 For example, *See*.: GA Resolution 2131(XX) of December 21, 1965, Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty, that condemns armed and any kind of intervention in internal affairs of States. 1970 Declaration of the UN General Assembly and 1975 Helsinki Final Acts are also relevant in this context. (Final Act, Conference On Security and Co-Operation in Europe, 1975).

74 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US),* Merits, ICJ, Judgment, 27 June 1986, §202.

75 Articles on State Responsibility for Internationally Wrongful Acts, International Law Commission, 2001.

76 *Damrosch L.,* Politics Across Borders: Nonintervention and Nonforcible Influence of Domestic Affairs, American Journal of International Law, Vol. 83, 1989, 3.

"particularly obvious" form of illegitimate intervention.[77] Therefore, despite having clear margins that place the customary rules on the principle of non-intervention alongside the prohibition of the use of force, the former shall still be considered as a distinct concept.[78] According to Judge Jenning's declaration, "the principle of non-intervention stands as an autonomous rule of customary international law".[79]

The principle of non-intervention could be viewed as a beneficial legal tool for states to avoid cyber-attacks not causing material loss, but have adverse effects.

Notably, the literature mainly places cyber-attacks in the context of the use of force. Thus, a lack of examination of cyber-attacks in light of the principle of non-intervention provokes a question.

This fact may stem from the understanding of sovereignty that is a legal category, defined by the geographical borders. As ICJ ruled "the basic legal concept of State sovereignty in customary international law... extends to the internal waters and territorial sea of every State and the air space above its territory."[80]

This kind of definition of sovereignty affects the scope of the principle of non-intervention which accompanies the principle of sovereignty.[81] As for the effects of territorial understanding of the principle of sovereignty, unjustified intervention could be at hand whenever it occurs on the territory or against the territory of a state.[82]

In light of this, cyberspace is thought to be a dimension where states could not exercise their territorial control. The International Institute of Humanitarian Law observes that "the distinctive feature of cyberspace is that it is a national environment and beyond the jurisdiction of any single nation."[83]

However, the US Department of Defense advances the opposite approach, observing cyberspace as a common area, similar to high seas, air, and space.[84]

Thus, it does not come as a surprise that international law commentators avoid from arguing that intervention into the virtual space of State is an intervention against sovereignty. For instance, in the context of cyber-attacks, the intervention of one State into another's non-material area, such as electricity or radiation, could hardly be considered a breach of obligation.[85]

Nevertheless, arguably, state sovereignty is not strictly limited since customary international law is familiar with a broader interpretation of sovereignty. Sovereignty protects states from external interference, affecting their capacity of decision making and a process of internal policy development.

---

77 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, Merits, ICJ, Judgment, 27 June 1986, § 205.

78 *Jennings R., Watts A.,* Oppenheim's International Law (9th Edition): Volume 1 Peace, Oxford University Press, 2008, 429.

79 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US),* Merits, ICJ, Judgment, 27 June 1986, § 534.

80 Ibid, § 212.

81 Ibid, § 202.

82 *SS Lotus Case (France v Turkey)* [1927] PCIJ Rep Series A. No. 10, 18.

83 *International Humanitarian Law Institute,* Rules of Engagement Handbook. September 2009, 15.

84 *US Department of Defense,* The Strategy for Homeland Defense and Civil Support, June 2005, 12.

85 *Kanuck, S.,* Recent Development: Information Warfare: New Challenges for Public International Law, Harvard International Law Journal, Vol. 37, 1996, 288.

ICJ has established an approach in favor of the broad interpretation of sovereignty. While determining the customary status and its margins for the principle of non-intervention, the Court declared in the *Nicaragua Case* that:

"A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty to decide freely. One of these is the choice of a political, economic, social, and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention…"[86]

Accordingly, prohibited intervention comprises coercive actions that fall within the scope of the non-intervention principle. In this regard, the exact scenario would be a state intervention aiming to coerce another state to change its policy.[87] Still, coercion solely is not enough. *Nicaragua Case* defines that the coercion shall relate to an affair in which State has complete discretion. This element is also highlighted in the literature.[88] Observing these elements is essential for the prevention of all forms of intervention to become unlawful, since, through their practice, states may change the cause of the evolution of customary international law. For example, in *Nicaragua Case,* ICJ discussed the possibility of such a customary rule that would allow states to intervene directly or indirectly, with or without using force whenever moral or political reasons justified this.[89] Nevertheless, ICJ stated that there is no such right to intervene in modern international law.[90] This approach is essential since there is always a chance of modification of the principle of nonintervention in case of appropriate state practice and *opinion juris*.

The purpose of this paper is not to define the scope of the principle of non-intervention, but to demonstrate that this principle applies to cyber-attacks whenever the later probably amounts to the use of force. For that, based on the above-mentioned analysis, it is vital to establish a) whether or not the intervention targets to coerce a state to change its policy and b) if the coercion is used. Provided that the conclusion is affirmative, as the next step, it should be assess whether such intervention affects those issues that are at the discretion of the targeted State. Deciding the first issue necessitates an assessment of the effects on the targeted State. The second issue deals with the purpose of the intervention.

Considering this, it is interesting whether the 2007 attacks on Estonia represent prohibited intervention. To explain that, first, we should determine whether those attacks aimed to modify the policy of the Estonian Government. Here we need to estimate the scale of damage done by cyber-

---

86 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US),* Merits, ICJ, Judgment, 27 June 1986, § 205.

87 *Jamnejad M., Wood M.,* The Principle of Non-Intervention, Leiden Journal of International Law, Vol. 22, 2009, 348.

88 *Damrosch L.,* Politics Across Borders: Nonintervention and Non-forcible Influence of Domestic Affairs. American Journal of International Law, Vol. 83, 1989, 2.

89 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US),* Merits, ICJ, Judgment, 27 June 1986, § 206.

90 Ibid, § 207.

attacks. In 2007, having had the most prominent web in Europe, Estonia was called "the information society".[91] Government, citizens, and private sector were highly dependent on internet services. In 2007, 95% of banking operations had been enforced through the internet.[92] That is why the cyber-attacks on the banking system damaged the economic activities.

Media stations also became the target of attacks. Mostly, the population had been accessing media through the internet as well. Due to this, the disconnection of primary information websites prevented the population from understanding the scale and results of the cyber-attacks. Additionally, after discovering the foreign origin of the attacks, the incoming internet traffic had been disconnected, and thus, Estonia had been cut off from the world.

Attacks had a substantial adverse effect on the public sector too. Websites of the Prime-Minister and its political party, apparatus of the President, Parliamentary and State Audit's sites also became targets. These sites went dysfunctional, unable to update information, or maintain communication via e-mail.[93]

Finally, it is noteworthy that the attacks on Estonia lasted for the whole three weeks. Taking into consideration this amount of time alongside the intensity, arguably, those attacks bear elements of coercion, attempting to change the Estonian Government's decision on relocation of the statue of the soldier.

As for the question - whether or not the attacks related to the matter that should have been freely decided by a state - it goes without saying that a state does not possess the right to interfere with another state's decision regarding relocation of statue of utmost importance and particular interest. In other words, this is a field where the principle of non-intervention unconditionally protects a state.

In conclusion, 2007 cyber-attacks are a manifest violation of the principle of non-intervention and sovereignty of Estonia. This determination is critical for suppression of unlawful acts, prevention of their repetition, and whenever possible, claiming of reparations.[94] Besides, customary international law allows states to take countermeasures in case the unjustified acts are enduring.[95] Such countermeasures shall satisfy the criteria of necessity and proportionality.[96]

All that being said, the principle of non-intervention creates a legal framework securing states from cyber-attacks when cyber-attack does not constitute use of force but is characterized by coercion of other states with regards to the matters that fall entirely in their domestic discretion.

---

91 *Tikk E., Kasha K., Vihul L.,* International Cyber Incidents: Legal Considerations, Cooperative Cyber Defence Centre of Excellence, 2010, 16.

92 Ibid. 17.

93 *Woltag J. C.,* Computer Network Operations below the Level of Armed Force, European Society of International Law Conference Paper Series, 2011, 5.

94 Articles on State Responsibility for Internationally Wrongful Acts, International Law Commission, 2001, Art. 30-31.

95 Ibid, Art 49.

96 Ibid, Art 51.

5. Conclusion

In the footsteps of technological advancements, reassessment of the conservative approach towards international law becomes more and more relevant. One of the main reasons for the initiation of such a process lies in the need for regulation of cyber-attacks that are undertaken on an international level. Cyber security is strengthening its position in state security matters.

With regards to the questions raised in the introduction of this paper, based on the presented analysis, could be summed up as follows:

1) Cyber-attacks shall be thought to be within the scope of Article 2(4) of the UN Charter since:

- Conduct is considered to be a use of force according to its results. If cyber-attacks would cause effects similar to the armed attacks, then according to the cyber equivalence approach, they would constitute a use of force;
- The concept of the use of force is not as strictly limited with the "armed" criteria. For example, as "armed attack" defined in Article 51 of the UN Charter;
- Article 2(4) is a contractual clause opening the way for evolutionary interpretation - the purpose of this rule was to forbid actions in international relations bearing coercive elements. It was impossible in the drafting process of the UN Charter to foresee the appearance of cyber operations. Evolutionary interpretation is essential for both the security of the intention of the rule and the filling of its gap. Accordingly, whenever certain criteria (scale, intensity, gravity, etc.) are met, cyber-attacks could constitute prohibited conduct under Article 2(4) of the UN Charter.

2) On the other hand, a cyber-attack not reaching the threshold of the use of force would still fall within the scope of international law, in particular the principle of non-intervention. To benefit from such protection, it is necessary that:

- The purpose of the intervention is coercion of a state to modify or change its policy;
- Coercion shall be related to the matters that may be freely decided by the targeted State.

3) In light of this, there is a trend of regulating the cyber-attacks by specialized legal norms. A good demonstration of this is the Tallinn Manual that was advanced by an international organization such as NATO. The involvement of NATO in the drafting of that document raises its authority. Moreover, the authority of the Tallinn Manual as a source of soft law increases because it was drafted by the most qualified scholars and using normative language.

4) Furthermore, state practice and their cognitive attitude towards cyber-attacks play an essential role as well. Examination of military manuals and growing state practice demonstrates that cyber-attacks are perceived as a distinct form of use of force, and their assessment is undertaken through the current state of international law.

5) Cases of Georgia, Estonia, and Iran indicate the scale of damage that may be inflicted by the intervention into cyberspace. In this view, we may assume that soon a new branch of law, namely international law of cyber operations, would emerge, focusing on the means of response and state responsibility.

6) ICJ has established an *obiter dictum* that the interpretation of the contractual clause may evolve from time to time. This allows the application of current legal rules on cyber-attacks. Such an approach implies a novel understanding of international law regarding cyber operations.

In conclusion, to answer the question posed by the article, it can be submitted that cyber-attacks require a new approach in the context of international law; however, it does not mean that such an attack stays beyond the scope of current international conventional and customary law (prohibition of the use of force and principle of non-intervention). A new understanding is decisive concerning the incorporation of cyber-attacks into the current system of international law.

Bibliography:

1. United Nations Charter (Date of adoption: 26.06.1945; Entry into Force: 24.10.1945).
2. Statute of the International Court of Justice, Article 38.
3. Convention on Cybercrime, Council of Europe, ETS No. 185, (Date of adoption: 23.11.2001; Entry into Force 01.07.2004).
4. RFERL, Georgian Government accuses Russia of Waging "CyberWarfare" 12.08.2008, <http://www.rferl.org/content/Georgian_Government_Accuses_Russia_Of_Cyberwar/1190477.html> [25.05.2020].
5. United Nations General Assembly Resolution 2131(XX) of 21 December 1965.
6. United Nations General Assembly Resolution 2625(XXV) of 24 October 1970.
7. United Nations General Assembly Resolution 55/28 of 20 November 2000.
8. United Nations General Assembly Resolution 56/19 of 29 November 2001.
9. United Nations General Assembly Resolution 59/61 of 3 December 2004.
10. United Nations General Assembly Resolution 60/45 of 8 December 2005.
11. United Nations General Assembly Resolution 61/54 of 6 December 2006.
12. United Nations General Assembly Resolution 62/17 of 5 December 2007.
13. United Nations General Assembly Resolution 63/37 of 2 December 2008.
14. United Nations General Assembly Resolution 64/25 of 2 December 2009.
15. United Nations General Assembly Resolution 65/41 of 8 December 2010.
16. United Nations General Assembly Resolution 66/24 of 2 December 2011.
17. United Nations General Assembly Resolution 67/27 of 3 December 2012.
18. United Nations General Assembly Resolution 55/63 of 4 December 2000.
19. United Nations General Assembly Resolution 56/121 of 19 December 2001.
20. United Nations General Assembly Resolution 58/32 of 8 December 2003.
21. United Nations General Assembly Resolution 59/61 of 3 December 2004.
22. United Nations General Assembly Resolution 60/45 of 8 December 2005.
23. United Nations General Assembly Resolution 61/54 of 6 December 2006.
24. United Nations General Assembly Resolution 62/17 of 5 December 2007.
25. United Nations General Assembly Resolution 63/37 of 2 December 2008.
26. United Nations General Assembly Resolution 64/25 of 2 December 2009.
27. United Nations General Assembly Resolution 65/41 of 8 December 2010.
28. United Nations General Assembly Resolution 66/24 of 2 December 2011.

29. United Nations General Assembly Resolution 66/359 of 14 September 2011.
30. United Nations General Assembly Resolution 67/27 of 3 December 2012.
31. United Nations Security Council (UNSC) Resolution 1696, 31 July 2006.
32. Articles on State Responsibility for Internationally Wrongful Acts, International Law Commission, 2001.
33. OSCE, Astana Commemorative Declaration — Towards a Security Community, SUM.DOC/ 1/10/Corr.1, 3 December 2010, § 9, <http://www.osce.org/cio/74985?download=true> [16.05.2020].
34. NATO, Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation, November 2010, §§ 7, 12, <http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf> [26.05.2020].
35. San Remo Manual on International Law Applicable to Armed Conflicts at Sea, 12 June 1994, ICRC. <https://www.icrc.org/ihl/INTRO/560?OpenDocument> [25.05.2020].
36. Final Act, Conference on Security and Co-Operation in Europe, 1975.
37. International Humanitarian Law Institute, Rules of Engagement Handbook. September 2009, 15.
38. *US Department of Defense,* The Strategy for Homeland Defense and Civil Support, June 2005, 12.
39. *Albright D., Brannan, P., Walrond, C.,* Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?, Institute for Science and International Security, 2010, <http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf> [22.05.2020].
40. *Beyerlin U., Stoutenburg J. G.*, International Protection of Environment, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2015, §§ 2, 8, 21, 30.
41. *Bjorge E.*, The Evolutionary Interpretation of Treaties, Oxford University Press, 2014, 1-22.
42. *Cannizzaro E. (ed.),* The Law of Treaties Beyond the Vienna Convention, Oxford University Press, 2011, 125.
43. *Cassese A. (ed.),* The Oxford Companion to International Criminal Justice, Oxford University Press, 2009, 19-20.
44. Cyber Attacks Disable Georgian Websites, Ministry of Foreign Affairs of Georgia <http://georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.html> [25.05.2020].
45. *Damrosch L.,* Politics Across Borders: Nonintervention and Nonforcible Influence of Domestic Affairs, American Journal of International Law, Vol. 83, 1989, 2-3.
46. *Dinstein Y.*, Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference, International Law Studies, Vol. 89, 2013, 280.
47. *Ergma E.,* Speaker of the Estonian Parliament, cited: *Davis J.,* Hackers Take Down the Most Wired Country in Europe, Wired Magazine (21 August 2007) <https://www.wired.com/ 2007/08/ff-estonia/> [23.05.2020].
48. "Iran Briefly Halted Enrichment", Aljazeera (23 November 2010). <http://www.aljazeera.com/news/middleeast/2010/11/201011231936673748.html> [11.05.2020].
49. "Iran says Cyber Foes Caused Centrifuge Problems" *Reuters* (29 November 2010). <http://www.reuters.com/article/iran-ahmadinejad-computers-idAFLDE6AS1L120101129> [24.05.2020].
50. *Jamnejad M., Wood, M.,* The Principle of Non-Intervention, Leiden Journal of International Law, Vol. 22, 2009, 348.

51. *Jennings R., Watts A.,* Oppenheim's International Law, 9th ed., Vol. 1 Peace, Oxford University Press, 2008, 429.
52. *Katz Y.,* Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years. Jerusalem Post, Jerusalem, 15 December, 2010, <http://www.jpost.com/IranianThreat/News/Article.aspx?id=199475> [26.05.2020].
53. *Kanuck S.,* Recent Development: Information Warfare: New Challenges for Public International Law, Harvard International Law Journal, Vol. 37, 1996, 288.
54. *Korns S. W., Kastenberg J. E.,* Georgia's Cyber Left Hook, Small Wars Journal Parameter, Winter Edition, 2008-2009.
55. *Markoff J.,* "Before the Gunfire, Cyberattacks", The New York Times, 2008, <http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0> [17.05.2020].
56. Report of the Independent Fact-Finding Mission on the Conflict in Georgia, Vol. II, September 2009, 217–219.
57. Russia Accused of Unleashing Cyberwar to Disable Estonia. The Guardian (17 May 2007) <https://www.theguardian.com/world/2007/may/17/topstories3.russia#maincontent> [09.05.2020].
58. *Roscini M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 3-4, 21-23, 25-26, 32-33, 44-45, 47.
59. *Salinas de Frias, A. M., et al. (ed.),* Counter-Terrorism: International Law and Practice, Oxford University Press, 2012, 1005, 1006.
60. *Schmitt M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 5, 45, 54-55.
61. *Scmitt M. N.,* Wired Warfare: Computer Network Attack and Jus in Bello, International Review of the Red Cross, Vol 84, Issue 846, 2002, 365-399.
62. *Shakarian P.*, Stuxnet: Cyberwar Revolution in Military Affairs. Small Wars Journal, 2011, 1, 7.
63. *Simma B., et al (eds.),* The Charter of the United Nations: A Commentary, Vol. I, 3rd ed., Oxford University Press, 2012, 210.
64. *Steed D.,* The Strategic Implications of Cyber Warfare, Cyber Warfare: A Multidisciplinary Analysis, *Green J., A.*, Routledge, 2015, 78.
65. *Swaine J.,* "Georgia: Russia 'Conducting Cyber War'", The Telegraph, 2008. <http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html> [17.05.2020].
66. *Thurer D.,* Soft Law. Max Planck Encyclopedia of Public International Law, Oxford University Press, 2009, §§5, 9, 15.
67. *Thirlway H.*, The Sources of International Law, Oxford University Press, 2014, 117-128, 165.
68. *Tikk E., Kasha K., Vihul L.,* International Cyber Incidents: Legal Considerations, Cooperative Cyber Defence Centre of Excellence, 2010, 16-17, 19.
69. *Weller M. (ed.),* The Oxford Handbook of the Use of Force in International Law, Oxford University Press, 2015, 1112, 1114-1116.
70. *Woltag J. C.,* Computer Network Operations below the Level of Armed Force, European Society of International Law Conference Paper Series, 2011, 1, 5, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1967593> [26.05.2020].
71. *Dispute Regarding Navigational and Related Rights* (*Costa Rica v. Nicaragua*), ICJ, Judgment, 13 July 2009, §§ 49-52, 66.

72. *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, ICJ, Judgment, 26 February 2007, §§ 385, 398.
73. *Oil Platforms case (Iran v. USA)*, ICJ, Judgment, 6 November 2003, §52.
74. *Legality of the Threat or Use of Nuclear Weapons,* ICJ, Advisory Opinion, 8 July 1996, §§ 39, 78.
75. *The Prosecutor v. Dusko Tadic,* ICTY, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Case IT-94-1, 2 October 1995, § 99.
76. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, §§ 187–190, 202, 205- 207, 212, 534.
77. *Rees v the United Kingdom*, ECtHR, Judgment, 17 October 1986, Series A, No. 106, § 47.
78. *Rasmussen v Denmark*, ECtHR, Judgment, 28 November 1984, Series A, No. 87, § 40.
79. *Guzzardi v Italy*, ECtHR, Judgment, 6 November 1980, Series A, No. 39, §9.
80. *Ireland v United Kingdom*, ECtHR, Judgment, 18 January 1978, Series A, No. 25, § 239.
81. *North Sea Continental Shelf* (Germany v. Denmark/The Netherlands), ICJ, Judgment of 20 February 1969, §77.
82. *Fisheries Case (United Kingdom v. Norway)*, ICJ, Judgment, 18 December 1951.
83. *SS Lotus Case (France v Turkey)* [1927] PCIJ Rep Series A. No. 10, 18.