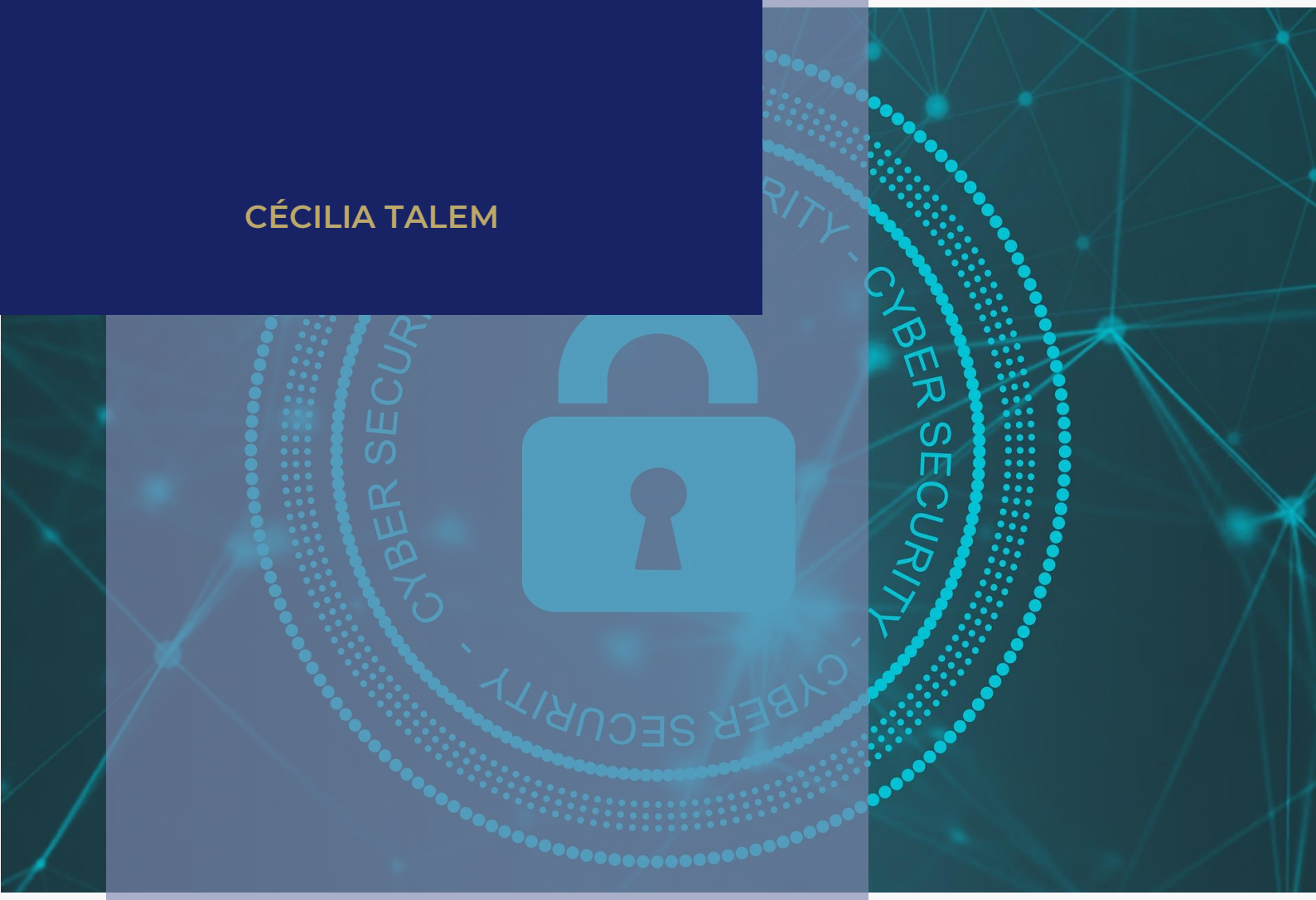
PAPER
DECEMBER 2020

INTERNATIONAL LAW IN CYBERSPACE: CYBER ATTACKS AS USE OF FORCE

CÉCILIA TALEM



UNIVERSITÀ DEGLI STUDI FIRENZE

Center for Cyber Security and International Relations Studies

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,

Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell'Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.

Center for Cyber Security and International Relations Studies

INTERNATIONAL LAW IN CYBERSPACE: CYBER ATTACKS AS USE OF FORCE

Cécilia Talem

UNIVERSITÀ DEGLI STUDI FIRENZE

Paper

December 2020

ABOUT THE AUTHOR

Cécilia Talem is a Master student in Public International and European Law at Paris-Saclay University. She also attended the course of ICT Policy and Cyber Security at School of Political Science “Cesare Alfieri” (University of Florence) through Erasmus exchange programme. Her research interests include public international law, diplomacy, and defence related to the emergence of cyber issue, negotiation and crisis management.

INTERNATIONAL LAW IN CYBERSPACE: CYBER ATTACKS AS USE OF FORCE

Introduction

Modern technologies have become the core of our existence. Indeed, they permit us to do almost everything from the simplest task like send an email or write a paper to the most complex and skilled things like coding. However, those technologies being more and more innovative and performing, we rely increasingly on them and thus a lot of our personal and sensitive information are nowadays at the palm of our hands. More and more people are getting skilled in the area of computer science, while some actors are taking advantage of the new cyber domain to conduct malicious activities.

Because of our immense reliance on those technologies we are more exposed and vulnerable than ever. In 2020, cyber attacks and other malicious activities have become more frequent and global, reaching all of the strata of society from the average person to international organizations like the WHO (World Health Organization 2020) especially with the spread of COVID-19 (Check Point Software 2020). Cyberspace became the new war arena of the 21st century. Indeed, many states and non-state actors have been the target of numerous cyber attacks, which had disastrous effects due to their dependency on computers, networks, and the Internet.

In the light of above, a distinction has to be made here between national and international level. Indeed, cybercrimes aimed at the private sector, such as espionage or fraud, and they are governed by national legislation. However, cyber attacks could aim at states and, according to several scholars and practitioners, when perpetrated by states they are governed by international law and *jus ad bellum*, regulating the use of armed force at international level (Roscini 2010, 90; Remus 2013, 179).

Today, there is no international legal framework ruling the cyber domain and especially with regard to the use of force which is the subject of this paper. Indeed, in general an attack that constitutes the use of force or armed aggression is illegal under international law according to Article 2.4 of the UN Charter.

Thus, we can wonder whether existing international law (IL) ruling the use of force is enough complete and can be adaptable to the cyber domain. Answering this question will permit to determine whether cyber operations can be considered as use of force. At first sight, existing international rules with regard to use of force cannot be used to rule cyber domain and more precisely cyber attacks. Indeed, the cyber domain has some specificities which make it different from the physical domain and thus make the already existing international law obsolete to what can be considered as new facts or a new situation.

In order to verify this hypothesis, we start first with *a contrario* assumption determining why some states consider (and, as showed in the following pages, especially the Western countries) that it is possible to apply existing international law. Then we will determine why this application has limits because of the lacunas of existing international law and of the peculiarities of cyberspace.

The possibility to apply existing international law in cyberspace concerning the use of force: The Western view

We focus first on the existing international law with regard to the use of force and determine if it is possible to apply those rules in the cyberspace.

An existing text ruling the use of force in international law

In international law, there is already existing law ruling the use of force. Indeed, a general prohibition ruling the use of force is Article 2.4 of the UN Charter which declares that "all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations." This provision prohibits the use of force or the use of threats to use force and is considered as customary international law binding upon all the states.

Because this prohibition is customary, the relationship between the treaty norm and the customary norm is a difficult issue. Indeed, states often try to find derogations through the customary norm because it can be derogated from by the means of a treaty or other arrangements between states (UN International Law Commission, 2010). Moreover, Article 3.1.5.3 of the Guide to Practice on Reservations to Treaties states that that "the fact that a treaty provision reflects a rule of customary

international law does not in itself constitute an obstacle to the formulation of a reservation to that provision."

This is why the prohibition is also a peremptory norm of international law meaning that it could not be derogated from, and it is not possible to derogate from it with a treaty, as the treaty will be invalid. This prohibition has *erga omnes* effects and a state is obliged to comply with this prohibition *vis à vis* other states. If a state does not comply, there will be serious consequences concerning the state responsibility. As a peremptory norm, all countries can react to that violation, even the countries not injured.

We can ask ourselves whether the prohibition extends to the use of economic and political force; but it is clear that this article refers exclusively to the use or threat of armed force. However, this does not mean that the use of a disproportionate amount of economic force does not violate other treaties and conventions.

This prohibition is not absolute because two exceptions with regard to self-defence exists: self-defence and the use of force authorized by the Security Council in the context of the security system. In this vein, Article 51 states as follows:

> Nothing in the present charter shall impar 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 the measures necessary to maintain international peace and security. Measures taken by members in the exercise of this right of self-defence shall be reported immediately 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 at any time such action as it deems necessary in order to maintain or restore international peace and security.

In this article self-defence means self-defence against another armed attack, and any other form of attack would not justify an armed response. Only an armed attack or aggression authorizes an armed response - which is self-defence as first reaction so that the Security Council has time to take over. Since state often tries to resort to the exception to the prohibition to the use of force, there was a need to put requirements and procedural obligations to self-defence. First, there are two fundamental requirements for self-defence: immediacy, i.e. the armed response must be carried out in the immediate aftermath of the attack; necessity, i.e. an armed response is necessary when, for

instance, it is not possible to achieve the result of stopping the attack or averting the attack by resorting to non-forcible options; and proportionality to the actual attack the state suffered from, meaning that the response to an armed attack must be equivalent in terms of scope, nature and gravity of the attack itself (ICJ 1984). Of course, a state actor needs proof that the attack is (or was) a military attack to justify, as a matter of international law, the resort to force to restore the *ex-ante* situation (Berman 2006, 9-14).

Secondly, the procedural obligations concern the involvement of the Security Council. Indeed, only the Security Council can authorize the use of force and decide to take military action[1]. Thus, there is an obligation to immediately report any situation of self-defence. It is crucial for the functioning of the system and it is provided by Chapter VII of the UN Charter, which ideally transfers the monopoly of the use of force to the Security Council.

The more exceptions you make to this principle, the higher the risk is that that states will abuse or take advantage of that. In this view, it could be very difficult to restrain state's actions (Ratner and Lobel 2002). A corollary is that the states which resort to force, particularly states generally attached to international law, have to be very careful and strict. If they go too far, this could be backfired and used by other states to justify their actions.

The possibility and the need to apply international law to cyberspace

Since there are existing rules regulating the use of force in international law, the question remains whether it is possible to apply those principles to cyberspace. On one hand, we can affirm that it is possible to apply the principles of international law (Koh 2012, 3). Indeed, the position of the international community suggests that international law should be applied to cyberspace. The International Court of Justice (ICJ) stated in the Nuclear Weapons Advisory Opinion that the Article 2.4 of the UN Charter should apply to any use of force regardless of the nature of the weapon employed (ICJ 1996). Consequently, in the same way as the use of classical forces, chemical ones or biological ones, the use of

[1] Chapter VII of the UN Charter, Article 51 stated: "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 at any time such action as it deems necessary in order to maintain or restore international peace and security."

cyber forces shall fall within the scope of application of Article 2.4 of the UN Charter.

This same position is taken with regard to *jus in bello*, i.e. the law concerning the conduct of hostilities, more precisely in the so-called "Martens Clause", formulated for the first time in the preamble of the 1899 Hague Convention II and stated again in a more modern form in 1977 in Article 1.2 of the Additional Protocol I to the Geneva Conventions [2] which assert: "in cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience."

The International Court of Justice also referred the Nuclear Weapons Advisory Opinion and more precisely to a clause stating that it has proved to be an effective means of addressing the rapid evolution of military technology (ICJ 1996).

This position is also taken by some states and especially in the Western hemisphere, led by the United States which in their first comprehensive strategy for cyberspace stated that existing international law does apply in cyberspace in times of peace and of conflict, but it also recognized the need for additional clarifications and maybe additional rules because of some unique aspects of cyber operations (Obama 2011, 14). The US also stated that it will respond to hostile acts in cyberspace as to any other threat. This shows that the US does not make distinctions between cyber threat or physical threat, applying for both the existing international law rules regarding threats and use of force. As opposite, other countries like China believe that since cyberspace is a new man-made domain, not all the concepts and rules of international law can be applied. In the Chinese view, in order to apply existing international law to cyberspace, there is a need of revision and clarification of those rules or even of creation of new rules (Zhang 2012, 804).

Even though most of the international community, as we have seen, determined that it was possible to apply international law in cyberspace, however, as China stated (Zhang 2012, 804), there are too many lacunas due to the specificities of cyberspace with regard to international law.

[2] Protocol Additional to the Geneva Conventions of August 12, 1949 and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977.

The lacunas of existing international law with regard to the use of force in cyberspace

Because of the fact that cyberspace is a new domain, it is not possible in my opinion to apply existing international law, which was designed for the other classical domains, to this new domain which is cyberspace. It is like applying old rules to new facts. There are some grey areas that are not covered.

An issue to determine the notion of "force"

The first challenge concerns the notion of force *per se*. Even if the UN Charter prohibits the threat or the use of force, there is no clear definition of what constitutes force. However, the International Court of Justice, in the Nicaragua case, looked in depth at this notion, determining 3 categories of possible illegal acts, i.e. armed attacks, use of force and interventions, where Article 2.4 covers the first two categories (McCoubrey and White 1992, 62). Like the UN Charter, the Court did not define these different categories. Nevertheless, it is widely accepted, e.g., in the Tallinn Manual (Schmitt 2017, 415) that the attack must produce physical damage to be considered as an unlawful use of force.

Indeed, a cyber attack can cause physical damage and therefore constitute an illegal use of force under Article 2.4. Thus, if a cyber attack can be considered as use of force, then international law and specifically the UN Charter could be applied.

But, even if the international community generally agrees on the application of international law and thus of Article 2.4, it is difficult to determine what kind of cyber operation falls under the category of use of force or the threat of use of force. Cyber operations are a very complex and heterogeneous group and thus setting up precise and absolute rules to determine which kinds of cyber operations do constitute force is impossible. For example, if we focus on cyber attacks specifically, many cyber attacks could not manifest physical damages.

This is why, there is a general assumption, which is that Article 2.4 applies on a cyber attack that basically have the same effects as a kinetic attack (Eisenstein Bar-On, n.d). There, a transposition is made between kinetic attacks and the cyber attacks. If the effects caused by the cyber attack looks like it could have been made by a kinetic one, then the use of force applies and thus self-defence would be legal (Sofaer, Clark and

Diffie 2010). A similar view proposed by Michael Schmitt is about whether a cyber attack constitutes force depends on multiple factors deriving from what made military force special in international law: severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy (Schmitt 1999, 914-915; Robertson 2002, 140). Other policy experts have similar conclusions, emphasizing that in order to respond militarily appropriately to a cyber attack, we have to focus on the effects or consequences of it (Clarke and Knake 2010, 178; Lewis 2010, 16). This view was also adopted by the Tallinn Manual.

However, this assumption creates a legal lacuna, because it does not consider cyber attacks that do not have the same effects as a kinetic one like the attacks aimed at hospital data, banking systems or state authority networks as use of force especially since they have implications exclusively or mostly in the cyber domain or, they impact other classical domains could be considered only indirectly.

It is as if we consider the cyber domain as a physical domain, thus limiting the damages that it can cause to physical and tangible one. However, the cyber domain is a man-made layer, an artificial domain able to include and affect all the classical and natural domains and thus it can also have intangible effects. This is not because an effect is intangible that it does not make damages. In this vein, for instance, states like France have an extensive interpretation of the notion of "attack" (French Ministry of the Army 2009, 13).

In the light of above, if we only consider this analogy between the effects of a cyber attack and the effects of a kinetic one, the existing rules of international law seem not to be sufficient with regard to cyberspace. As consequence of this effect-approach, several attacks do not amount to use of force and thus the right of self-defence does not apply often. There is a grey area, where the threshold to determine what is considered as use of force or not is quite narrowed. This is why there may be the need to provide a new legal framework adapted to the specificities of cyberspace with new specific rules.

This need is also the of view of Eastern countries and Russia, who claims that more regulations is needed regarding the application of international law in cyberspace, with the aim of exercising more sovereignty over the Internet. In this vein, the NotPetya campaign illustrated the complexity of applying international law to ambiguous cyber scenarios. It did not cause death or any physical injuries and thus

the right of self-defence did not apply. However, it was aimed at "causing economic losses, sowing chaos, or perhaps testing attack capabilities or showing own power" (CCDCOE 2017). Since most of today's economy of the globalized world relies on technology, we can wonder if non-destructive cyber operations, such as NotPetya causing wide-spread economic destabilization, should amount to uses of force (Schmitt and Biller 2017). In June 2017, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) researchers wrote that "NotPetya and WannaCry call for a joint response from international community" (CCDCOE 2017).

This example shows the need to set up a clearer legal framework with a political consensus on what can amount to use of force, leading to new regulations.

The issue of the attribution of responsibility and of lack of sanctions

Another issue lies down in the attribution of responsibility in cyberspace. Technical attribution can be very difficult to establish in cyberspace in general, but it is even more true concerning the Internet, since anonymity takes an important place. Indeed, technologies permit to act anonymously and hide the identity within cyberspace, using, for instance, proxies and other spoofing techniques (Rowe 2009). Some malwares are even conceived to hide any mark and to destroy themselves once they infected the system, e.g., Flame malware (Zaffagni 2012). Thus, it is more and more difficult, even if not impossible, to determine the real source of the attack and the source of the use of force (Office of the Director of National Intelligence 2018, 2-3)[3].

Moreover, Internet access is not nowadays limited to the states and we saw over the last years the proliferation of non-state actors: anyone who can have access to a computer with an Internet connection or a smartphone can be the author of an attack, on the condition that he has the necessary skills. This feeds the question of whether it is possible to attribute the cyber attack to a state or not. The draft articles on state responsibility for internationally wrongful acts gives a response to that issue and more generally on the issue of state responsibility. First, Article 4 states that a cyber attack will be attributable to a state if it is attributable to one of its organs or, according to Article 5, to an entity or person which a state has authorized to exercise prerogatives of public

[3] The US Director of National Intelligence refers to primary key indicators that enable attribution: tradecraft, infrastructure, malware and intent, and indicators from external sources like open-source reports from private security firms.

(UN Commission 2001, 3). For example, some states have created specialized units in the cyber field, which can be considered as attached to the government, and thus whose actions would also be attributable to the state.

Concerning the particular issue of non-state actors, Article 8 provides that if the perpetrators of a cyber attack, which are non-state actors but act on the instructions or directives or under the control of a state, their act will be attributed to that state (UN Commission 2001, 3). This rule has been adapted in particular in the Tallinn Manual 2.0, which reiterate that cyber operations conducted by a non-state actor are attributable to a state when they are committed on the instructions or under the direction or control of this state (Schmitt 2013, 37). The problem with both those rules is that they are not binding on states. Indeed, even if they were well received, both are not binding on the international community and not everyone considers them as customs. Thus, nothing impeaches states to not respect them or to establish other special rules of responsibility like in the European Convention of Human Rights.

When the attribution of responsibility is possible, the lack of sanctions arises as additional legal and diplomatic issue within the international community. The only autonomous regime of cyber sanctions was established in the European Union as unique solution to the challenge of compliance with international law. Indeed, on 17 May, 2019, the Council established a legal framework which allows the EU to impose targeted restrictive measures to deter and respond to cyber attacks that the EU institutions or member states receives, including cyber attacks against third States or international organisations where restricted measures are considered necessary to achieve the objectives of the Common Foreign and Security Policy. It allows the EU for the first time to impose sanctions like a ban on persons travelling to the EU, and an asset freeze on persons and entities. In addition, EU persons and entities are forbidden from making funds available to those listed (Council of the European Union 2019).

This new mechanism is however not supported by all the international community, especially in its application. On 30 July, 2020, for the first time, the European Council has decided to use this sanctions regime by imposing travel bans and assets freezes against six Chinese and Russian individuals as well as assets freezes against three entities or bodies for their responsibility or involvement in cyber attacks (European External Action Service 2020). This use of the sanction mechanism aroused

strong reactions both from the Western and Eastern sides: on one hand, the United States, the United Kingdom, Australia, and Canada expressed their support and welcomed the European Union's step. The United Kingdom announced that the sanctions were in force in the UK as well, and even made a reference to their new coherent autonomous UK cyber sanctions regime, created following Brexit. On the other hand, Russia and China criticized the EU decision to impose unilateral sanctions instead of conducting a dialogue based on mutual respect, using diplomatic tools (Zlaïka 2020).

Other than this framework, we do not find a clear international framework of sanctions with regard to use of force in cyberspace. This European framework, although demonstrating a beginning of cooperation in the imposition of sanctions, seems to be the reflection of the Western approach (in line with previous measures taken by Western countries), polarized and limited to the Western sphere.

Conclusions

Since cyberspace is a new and dynamic operating environment, always subject to evolution. In this view, we would not expect that the existing system of international law will apply to cyberspace and to specific issues like the use of force.

Indeed, cyberspace presents some peculiarities and new challenges as new issues for the international community, which are technical and political but also legal.

This is the reason why, even if in theory, by looking at several opinions, protocols and case laws of the International Court of Justice we can deduce that it is possible to apply existing international law to cyberspace, we clearly can see that in practice it is not that easy and that there is some lacunas in existing international law with regard to the use of force in cyberspace, i.e. lacunas considering the existing international law itself and lacunas linked to the peculiarities of the cyber domain that the international law rules with regard to the use of force did not. As consequence, if we do not consider that international law would not apply to cyberspace, there is a need to enact new rules and we can even push the idea to a whole new legal framework which will take into account the specificities of cyberspace, creating new provisions or even taking the existing provisions related to the use of force and adapting them to the cyber domain.

Whatever option is chosen at the international level, this framework will be binding upon the international community in order to be effective, providing political or economic sanctions in order to deter states to resort to use of force or threat to use of force.

In the meantime, a few attempts to fill those lacunas were made at international level: as reported above, the most relevant to our focus are the Tallinn Manual, the draft articles on state responsibility and the recent idea to have a Digital Geneva Convention (Guay and Rudnick 2017). The Tallinn Manual, even having a strong influence over the international community and the International Court of Justice often refers to it, it is not explicitly binding upon states. This is why in the international arena more and more state and non-state actors (e.g., Microsoft) are seeking for the elaboration of a new binding tool called the Digital Geneva Convention (Smith 2018).

References

Berman, Franklin. 2006. "The UN Charter and the Use of Force." *Singapore Year Book of International Law* 10, no. 9: 9-17.

CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence). 2017. "NotPetya and Wannacry call for a joint response of the international community." Accessed October 17, 2020. https://ccdcoe.org/notpetya-and-wannacry-call-joint-response-international-community.html.

Check Point Software. 2020. "A Perfect Storm: The Security Challenges of Coronavirus Threats and Mass Remote Working." Accessed October 17, 2020. https://blog.checkpoint.com/2020/04/07/a-perfect-storm-the-security-challenges-of-coronavirus-threats-and-mass-remote-working/.

Clarke, Richard A., and Robert K. Knake. 2010. *Cyber War. The Next Threat to National Security and What to Do About It.* New York: Harper Collins

Council of the European Union. 2019. "Cyber-attacks: Council is now able to impose sanctions." Last modified May 17, 2019. Accessed October 17, 2020. https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/.

Eisenstein Bar-On, Anat. n.d. "Cyber-attack and the Prohibition of the Use of Force: The scope of Article 2(4) in Cyberspace." Accessed October 17, 2020. https://csrcl.huji.ac.il/book/cyber-attack-and-prohibition-use-force-scope-article-24-cvberspace.

European External Action Service. 2020. "Cyber sanctions: time to act - European Commission." Last modified July 30, 2020. Accessed 17 October 2020. https://eeas.europa.eu/headquarters/headquarters-homepage/83627/cyber-sanctions-time-act_en.

French Ministry of Defense. 2009. *International Law applied to operations in cyberspace.* Paris: Délégation à l'informationet à la communication de la défense.

Guay, Joseph, and Lisa Rudnick. 2017. "What the Digital Geneva Convention means for the future of humanitarian action." UNHCR (UN High Commissioner for Refugees), June 25, 2017. Accessed October 17, 2020. https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/.

ICJ (International Court of Justice). 1996. *Advisory opinion on the Legality of the Threat or Use of Nuclear Weapons.* Accessed October 17, 2020.

https://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf.

ICJ (International Court of Justice). 1984. *Nicaragua vs. United States of America*. Accessed 17 October 2020. https://www.icj-cij.org/files/case-related/70/070-19841126-JUD-01-00-EN.pdf.

Koh, Harold. 2012. "International Law in Cyberspace." *Harvard International Law Journal Online* 54 (December). Accessed October 17, 2020. https://harvardilj.org/wp-content/uploads/sites/15/2012/12/Koh-Speech-to-Publish1.pdf.

Lewis, James A. 2010. "Multilateral Agreements To Constrain Cyberconflict." *Arms Control Today* 40, no. 5 (June): 14-19.

McCoubrey, Hilaire, and Nigel D. White. 1992. *International Law and Armed Conflict*. Aldershot: Dartmouth Publishing.

Obama, Barack. 2011. *The United States International Strategy for Cyberspace – Prosperity, Security and Openness in a Networked World*. Washington DC: The White House.

Office of the Director of National Intelligence. 2018. *A Guide to Cyber Attribution*. Washington DC: Director of National Intelligence. Accessed October 17, 2020. https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

Ratner, Michael, and Jules Lobel. 2002. "The U.N. Charter and the Use of Force Against Iraq". Western States Legal Foundation, October 2, 2002. Accessed October 17, 2020. http://www.wslfweb.org/docs/Iraqstatemt.htm.

Remus, Titiriga, 2013. "Cyber-attacks and International law of armed conflicts; a "jus ad bellum" perspective." *Journal of International Commercial Law and Technology* 8, no. 3 (July): 179-189.

Robertson, Jr., Horace B. 2002. "Self-Defence Against Computer Network Attack Under International Law." *International Law Studies* 76: 121-45.

Roscini, Marco. 2010. "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force." *Max Planck Yearbook of United Nations* 14: 85-130. Accessed October 17, 2020. https://www.mpil.de/files/pdf3/mpunyb_03_roscini_141.pdf.

Rowe, Neil C. 2009. "The Ethics of Deception in Cyberspace." in *Handbook of Research on Technoethics*, edited by Rocci Luppicini and Rebecca Adell, 529-41. New York: Information Science Reference.

Schmitt. Michael N. 1999. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *Columbia Journal of Translational Law* 37: 885-937.

Schmitt, Michael N., ed. 2017. *The Tallin Manual 2.0*. *The International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.

Schmitt, Michael N., and Jeffrey Biller. 2017. "The NotPetya Cyber Operation as a Case Study of International Law." *EJIL: Talk! Blog of the European Journal of International Law*, July 11, 2017, Accessed October 17, 2020. https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/.

Smith, Brad. 2018. "The need for a Digital Geneva Convention." *Microsoft On the Issues*, February 14, 2017. Accessed October 17, 2020. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001hkfw5aob5evwum620jqwsabzv.

Sofaer, Abraham, Clark, David D., and Whitfield Diffie. 2010. "Cyber Security and International Agreements", in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, edited by National Research Council, 179-185. Whashington DC: The National Academies Press.

UN Commission. 2001. *Draft articles on state responsibility for internationally wrongful acts*. Accessed October 17, 2020. https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.

UN International Law Commission. 2010. *Guide to Practice on Reservations to treaties*. Accessed October 17, 2020. https://legal.un.org/ilc/texts/instruments/english/draft_articles/1_8_2011.pdf.

WHO (World Health Organization). 2020. "WHO reports fivefold increase in cyberattacks, urges vigilance." Last modified April 24, 2020. Accessed October 17, 2020. https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance.

Zaffagni, Marc. 2012. "Flame, un virus encore plus redoutable que Stuxnet et Duqu." *Futura*, May 30, 2012. Accessed October 17, 2020.

https://www.futura-sciences.com/tech/actualites/informatique-flame-virus-encore-plus-redoutable-stuxnet-duqu-39051/.

Zhang, Li. 2012. “A Chinese Perspective on Cyber War.” *International Review of the Red Cross* 94, no. 886 (Summer): 801-7. https://www.icrc.org/en/doc/assets/files/review/2012/irrc-886-zhang.pdf.

Zlaikha. Vered. 2020. “For the First Time, EU Sanctions in Response to Cyberattacks: Enhanced Deterrence Efforts by Western Countries?” *INSS Insight* 1364 (August). Accessed October 17, 2020. https://www.inss.org.il/publication/european-sanctions-on-cyber-activity/.

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,

Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and International Relations Studies