Torun International Studies

2016, No. 1 (9), pp. 79–86

Published online February, 2017

DOI: http://dx.doi.org/10.12775/TIS.2016.007

Konrad Węgliński*

CYBERWARFARE AND RESPONSIBILITY OF STATES

ABSTRACT

The aim of this paper is to provide a general insight into the questionable nascence of the international custom in the context of cybersecurity and the most relevant attempt to draft a document regarding the subject matter from the Western perspective, taking into account the lack of any widely accepted international convention regarding the cyber security. Moreover, the paper analyzes legal requirements for finding a state responsible for a cyber attack by means of Article 2 of the ILC's Articles on Responsibility of States for Internationally Wrongful Acts. Specifically, it analyzes legal requirements necessary to attribute a certain conduct to a state. Also, it considers if cyber attacks in general can be treated as the use of force within the meaning of article 2.4 of the UN Charter. Moreover, it examines whether the doctrine of due diligence can be used while accusing a state for a breach of its international obligations.

Keywords: cyber attack, cybersecurity, states' responsibility, use of force, due diligence

1. INTRODUCTION

> "Global interconnectedness brought about through linked digital information networks brings immense benefits, but it also places a new set of offensive weapons in the hands of states and non-state actors, including terrorist groups" (Waxman, 2011, p. 422).

It was only in the late 1990s, when the issue of cyber attacks became a subject of concern for the international legal and academic community. The first decade of 21st century witnessed spectacular and afflictive cyber attacks including these against Estonia in 2007 as well as against Georgia, during the war with the Russian Federation, in 2008 and the so-called "Sony Pictures Entertainment hack" in 2014.

* The John Paul II Catholic University of Lublin, koonrad.w@gmail.com

Cyber attacks against Estonia began on April 27, 2007 and were aimed at, inter alia, websites of Estonian organizations, including Estonian parliament, banks, ministries, newspapers and broadcasters. Notably, they took place during the disagreement with Russia concerning relocation of "the Bronze Solider of Tallinn – a Soviet-era grave maker (Shackelford, 2009). Even though the Estonian Foreign Minister Urmas Paet accused the Kremlin of direct involvement in the cyberattacks, he admitted that there was no evidence linking cyber attacks to Russian authorities. Interestingly, Colonel Anatoly Tsyganok – the of Russian Military Forecasting Center – confirmed that Russia is technically able to carry out such an attack, however, in any event it would not violate the international law.

Furthermore, the attacks against Georgia occurred in August 2008 and affected Georgian governmental web resources, mass-media, forums as well as plenty of Georgian domains. They resulted in significant disruptions of communication as well as financial losses. The Russian government denied the allegations that it was behind the attacks, asserting that it was infeasible that individuals in Russia or anywhere would be able to start the attacks.

As to the "Sony Pictures Entertainment hack", on November 24, 2014, the group of hackers called the Guardian of Peace Group (hereinafter: "the GOP") leaked a release of classified data from the Sony Pictures Entertainment film studio. In December 2014, the GOP demanded the Sony Pictures Entertainment to abstain from releasing its film "The Interview" – a comedy about the leader of North Korea, Kim Jong-un - and threatened terrorist attacks at cinemas screening the film. United States intelligence officials alleged that the attack was controlled by North Korea. Unsurprisingly, North Korea has expressly denied all responsibility.

States' attention has been drawn to the problem of security in the cyberspace for good. Professor Michael N. Schmitt, one of the most influential authors on the subject matter, emphasized that "the scope and manner of international law's applicability to cyber operations, whether in offence or defense, has remained unsettled since their advent" (Schmitt, 2013, p. 3). Indeed, experts and scholars indicated that there is an urgent need to create a new and congeneric legal regime at local as well as international levels to address the cyberwarfare efficaciously (Hathaway et al., 2012, p. 4).

So far, however, international consensus regarding cybersecurity has not been reached. For the sake of illustration, suffice it to remark that even defining the term "cyber attack" is the lay of land for international lawmakers, since standpoints of the most powerful and affluential states such as the USA, China or Russia in regard to global cybersecurity diverge significantly. Thus, the actual meaning and scope of this notion is subject to substantial dissensions. There is every indication that the international community will not come up with a widely accepted convention regulating cyberspace in the near future. In a similar vein, an international custom concerning cyber attacks has not yet crystalized.

Needless to say, nowadays the world is highly dependent upon information technologies and this is an upward trend. Consequently, international relations – political, economic or military – have become perilously vulnerable to cyber attacks. The vagueness of the subject matter, the lack of both domestic and international legal regimes regulating cyberspace as well as an international custom seems to constitute insurmountable obstacles to find a certain state responsible for a cyber attack. Therefore, such operations have been, and still can be, carried out by states against other states in order to achieve certain goals on political, business

or martial fields and simultaneously remain untouchable when it comes to facing legal consequences on the international level.

The aim of this paper is to provide a general insight into the questionable nascence of the international custom in the context of cybersecurity and the most relevant attempt to draft a document regarding the subject matter from the Western perspective. Moreover, the paper analyzes legal requirements for finding a state responsible for a cyber attack by means of Article 2 of the ILC's Articles on Responsibility of States for Internationally Wrongful Acts. This article is structured in a following way. Firstly, the issue of international custom in the context of cybersecurity is briefly discussed. Due account is given to the Tallinn Manual. Secondly, the problem of finding a state responsible for a cyber attack is elaborated upon. Specifically, the trouble to attribute a cyber attack to a state by means of Article 2 of the Articles on Responsibility of States for Internationally Wrongful Acts is analyzed. Furthermore, it is considered whether cyber attacks in general can be treated as the use of force within the meaning of the article 2.4 of the UN Charter as well as whether the doctrine of due diligence under the international law can be used while accusing a state for a breach of its international obligations. Finally, the paper summarizes the foregoing analysis.

2. ITERNATIONAL CUSTOM AND CYBER SECURITY

Article 38 of the ICJ Statute enumerates custom as a source of international law. Given the wording of the article, customary international law may be defined as international law which has been derived from "general practice, accepted as law" (Schlutter, 2010, p.9). Hence, there are two elements which determine the existence of international custom, namely opinio juris and state practice (Schlutter, 2010, p. 13) The former is the subjective element used to assess whether the practice of a state stems from a belief that it is legally obliged to act or otherwise in a particular way (Bederman, 2001, p. 15–16). The latter is the objective element which refers to actual, settled practice of a state (*The North Sea Continental Shelf Case,* 1969, para. 27).

For the purpose of this paper it is worth stressing that customary international norms regarding the cyber warfare have not yet developed (Kilovaty, 2014, p. 108). There is lack of global and undisputed consensus in the context of cybersecurity. Suffice it to say that states including, for instance, Russia as well as China perceive the concept of applicability of international law to cyber security in an utterly declinable way (Giles & Monaghan, 2014, p. 1).

In 2009, however, at the invitation of the NATO Cooperative Cyber Defense Centre of Excellence located in Tallinn, Estonia, the group of experts chosen from NATO member countries drafted the Tallinn Manual[1], i.e. a non-binding document examining applying existing law to cyber warfare (Schmitt, 2013, p. 1). It established ninety-five "black-letter rules" governing cyber warfare (Schmitt, 2013, p. 1). No matter how laudable, landmark and professional, this document merely reflects the point of view of a bunch of Western experts and by no means cannot be regarded as reflection of internationally accepted opinio juris or state practice.

[1] Available at: https://ccdcoe.org/research.html.

3. RESPONSIBILITY OF STATES FOR CYBER ATTACKS

Articles on Responsibility of States for Internationally Wrongful Acts set forth two cumulative criteria for finding a state responsible for an internationally wrongful act. Firstly, a certain conduct must be attributable to a state. Secondly, the conduct of a state shall constitute a breach of an international legal obligation in force for that state at that time (*Phosphates in Morocco,* 1939, p. 10; *United States Diplomatic and Consular Staff in Tehran,* 1980, p. 3).

Turning to the first criteria, attribution can be regarded as a normative operation (Condorelli & Kress, 2010, p. 225) used in order to establish a connection between an act, a physical author thereof and a state through application of rules determining if there is a sufficiently close link between a certain conduct and a state so as to ascribe that conduct to the state (Ortega, 2015, p. 4). Importantly, the very essence of attribution is to "make a state answer for, or face the consequences of, deeds of persons or entities that belong to its organization or function under its control" (Nollkaemper, 2005, p. 140).

In a sense, states might be understood as abstract entities that act through physical persons (*Certain Questions Relating to Settlers of German Origin in the Territory Ceded by Germany to Poland, Advisory Opinion,* 1923, p. 22). Any state may be liable for actions of their organs as well as for the actions of private persons, acting on their behalf or order (Kulesza, 2009, p. 148). For the purpose of attributing a certain conduct to a state it is therefore vital to demonstrate that perpetrators acted under direction or control of a state. So far, two possible tests to examine a level of a state's control over perpetrators of certain acts have been applied in the international law, namely the "effective control" as well as the "overall control" tests (Green, 2015, p. 113). Moreover, the third approach of "virtual control" test has recently been suggested (Margulies, 2015, p. 19).

Firstly, the effective control test will be discussed. According to the ICJ's ruling in the Nicaragua Case, in order to attach responsibility to a state, it must be demonstrated that it possessed the effective control of the military or paramilitary operations which led to certain violations (*Case Concerning Military and Paramilitary Activities In and Against Nicaragua,* 1986, para. 65). The effective control test, which was subsequently applied by the ICJ in the Bosnian Genocide case, requires that the state has specific, practical control over the actor concerned before that actor's actions can be attributable to it. Providing evidence of control over specific operations of a group involves proving the instructions, command or particular instances of State control over the acts in question (Ortega, 2015, p. 11).

Let us now turn to the overall control test. It was in 1999, when the ICTY applied this test in the Tadić Case. However, the overall control test is regarded to be wider than the effective control test (Green, 2015, p. 113). Nonetheless, in its judgment in the Bosnian Genocide case, the ICJ reasoned that this test is unpersuasive since the overall control test overly broadens the scope of state responsibility and applied the effective control test (The *Bosnian Genocide Case,* 1996, para. 406). The overall control requires a general level of control going beyond mere support or provision of funds (*The Tadić Case,* 1999, paras 116–145). As reasoned by the ICTY, a state has the overall control if it has a role in organizing, coordinating as well as providing support for a group.

Recently, the virtual control test has been suggested (Margulies, 2015, p. 19). The test is supposed to be wider than the aforementioned approaches (Green, 2015, p. 113). Under the virtual control test the mere provision of finances or support by a state would amount to

sufficient control over perpetrators (Green, 2015, p. 113). However, currently there is little basis in law for the aforementioned test. Additionally, so far it has never been applied by any court.

Bearing in mind the above-discussed tests, it is legitimate to assert that they are hardly useful in the context of cyber attacks. To illustrate, the mere fact that the malware used in the cyber attack had been traced to a certain computer infrastructures located in the territory of a certain state does not constitute a compelling argument to find it responsible for the attack. Firstly, experts stress that networks are complex, data paths may go through many systems in many countries or may be controlled by many different administrative domains (Wheeler & Larsen, 2003, p. 19). Moreover, computer network environments are not designed to support attribution of attackers (Wheeler & Larsen, 2003, p. 19). Furthermore, such an infrastructure might have come under the control of non-State actors who use that infrastructure to conduct cyber operations.

It is worth emphasizing that the attribution is a necessary criteria in order to find a state responsible for a certain conduct. Apparently, the international law does not keep up with the rapidly developing information technologies and the efficaciousness of up-to-date acquis of international lawmakers, jurisprudence and scholars is highly doubtful.

4. THE BREACH OF STAES' INTERNATIONAL OBLIGATIONS

The second criteria contained in Article 2 of the Articles on Responsibility of States for Internationally Wrongful Acts sets forth that a certain conduct of a state shall constitute a breach of an international legal obligation in force for that state at a given time to find the state responsible for the conduct.

This articles considers only two possible aspects of the issue. First, it analyzes if a cyber attack could be regarded as a use of force within the meaning prescribed by the article 2.4 of the UN Charter. Secondly, the obligation of states to exercise due diligence in the context of cyber attacks is discussed.

4.1. CYBER ATTACKS AS THE USE OF FORCE

Article 2(4) of the UN Charter contains the prohibition of the use of force, which reflects customary international law (Geiger, 2011, p. 677). However, there is no legal definition of the term "use of force" contained therein and therefore its scope and content is "a subject of fundamental disagreement" (Gray, 2008, p. 114).

The prevailing view in the United States and among its major allies has long been that the Article 2(4) prohibition of force is only applicable to military attacks or armed violence (Farer , 1985, p. 405; Waxman, 2011, p. 427). However, as reasonably noted, authors of the UN Charter could not have foreseen the emergence of cyber attacks (Waxman, 2011, p. 428). Other interpretations concerning the meaning of "force" described it as coercion (Schachter , 1986, p. 113) as well as interference. However, the most important aspect is the article 2(4) addresses only states (Dinstein, 2001, p. 87). It means that unless a conduct of physical persons is attributable to a state, the prohibition anchored in article 2(4) does not apply (Dinstein, 2001, p. 87–88).

As such, it seems that such a construction of the article 2.4 makes it technically infeasible to attribute a certain conduct to a state. The problem of attribution has already been duly elaborated upon and does not need further clarification.

4.2. DUE DILIGENCE IN THE CONTEXT OF CYBER ATTACKS

The notion of due diligence, formulated in the 17th century by Grotius (Hessbruegge, 2003–2004, p. 283) and stemming from the very principle of sovereignty (Schmitt , 2015, p. 71), is not used in Articles on Responsibility of States for Internationally Wrongful Acts. Notwithstanding the fact that the ICJ has never addressed the due diligence requirements in the context of cybersecurity, the cases discussing it generally can serve as a beacon for States while adapting cyber-security policies.

Importantly, in Corfu Channel Case, the International Court of Justice stressed that every state is obliged not to allow knowingly its territory to be used for acts contrary to the rights of other states (*The Corfu Channel Case,* 1949, para. 22). Moreover, in the Bosnian Genocide case the Court reasoned that the due diligence refers to undertaken actions and not results thereof. Nonetheless, it is worth underlying that the doctrine of due diligence is violated only if a state had possessed knowledge about a forthcoming cyber attack before they took place.

In the view of the foregoing, it is legitimate to cast a substantial doubt on the actual effectivity of the due diligence doctrine while arguing that a certain state has violated its international obligations and therefore it may be found responsible in accordance with the Article 2 of the Articles of Responsibility of States for Internationally Wrongful Acts. Specifically, the indispensable requirement that a state shall possess knowledge about attacks before they occur conjures up a crucial query about the practical use of such an argument and most importantly the ability to duly substantiate it in persuasive manner during proceedings before an international tribunal.

5. CONCLUSION

Cyber threats and attacks are becoming more common, sophisticated and damaging. Without a shadow of a doubt, there is an urgent need to find the solution of this stalemate situation. Since the world today's is highly dependent upon information technologies, the cybersecurity shall be regarded as one of the highest priorities of international community to contribute to the stability and peace in the world. Even though experts and scholars are well aware of the need to address this issue in a new and congeneric way (Hathaway et al., p. 2), the up-to-date attempts to do so shall be regarded as a peak of an iceberg, rather than useful, technical and concrete blueprint to contend the problem of impunity of states in cyber warfare.

Available legal mechanisms do not keep up with the rapidly developing information technologies. Requirements set forth by Article 2 of the Articles on Responsibility of States for Internationally Wrongful Acts can easily be avoided by states and, consequently, cyber attacks can be used as a powerful weapon to pursue certain political, economic or martial strategies. NATO is well-aware of the rapidly escalating danger, and it recognizes the need to be prepared to defend its networks and operations against the growing sophistication of the cyber threats and attacks it faces.

It is therefore my view that the international community shall undertake any reasonable and effective endeavor to quash the unbearable lightness of conducting cyber attacks. It is, however, unattainable without reaching the international consensus regarding fundamental and very basic issues regarding cybersecurity, such as the exact definition of the term "cyber attack". There is also urgent need to deliver at efficient and innovative legal regime which would provide tools to bring offensive states to justice on the international level. The risk as well as potential harm which might be caused by another cyber attacks is tremendous. And so is the temptation to use them with impunity.

REFERENCES

BOOKS AND ARTICLES

Ortega A. E. L. Álvarez (2015). The rules of attribution: general considerations, Barcelona: Revista para el Análisis del Derecho, 1.

Bederman D. J. (2001) *International law frameworks*, New York: Foundation Press.

Condorelli L., Kress C. (2010) The Law of International Responsibility. In Crawford J., Pellet A., Olleson S. (eds.), *The Law of International Responsibility*, Oxford/New York: Oxford University Press.

Dinstein Y. (2001). *War, Aggression and Self-defence*, Cambridge: Cambridge University Press.

Farer T. J. (1985) Political and Economic Coercion in Contemporary International Law, American Journal of International Law, 79.

Geiger R.H. (2011). Customary International Law In The Jurisprudence of The International Court of Justice: A Critical Appraisal. In Fastenrath U., Geiger R., Khan D-E., Paulus A., Schorlemer S. von, Vedder C. (eds.), *From Bilateralism to Community Interest. Essays In Honour Of Judge Bruno Simma,* Oxford: Oxford University Press.

Giles K., Monaghan A. (2013). *Legality in Cyberspace: An Adversary View*, Army War College Carlisle Barracks PA Strategic Studies Institute.

Gray C. (2008). *International Law and The Use of Force*, Oxford: Oxford University Press.

Green J.A. (2015). Regulation under the jus ad bellum. In Green J.A., *Cyber Warfare: a Multidisciplinary Analysis*, New York: Routledge.

Hathaway O. A., Crootof R., Levitz P., Nix H., Nowlan A., Perdue W. and Spiegel J. (2012). *The Law of Cyber-Attack*, California: California Law Review, 100.

Hessbruegge J. A. (2003-2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law, New York: New York University Journal of International Law and Politics, 36.

Kilovaty I. (2014) Cyber Warfare and The Jus Ad Bellum Challenges: Evaluation In The Light of The Tallinn Manual on The International Law Applicable to Cyber Warfare, American University National Security Law Brief, 5.

Kulesza J. (2009) States responsibility for cyber-attacks on international peace and security, Polish Yearbook of International Law.

Margulies P. (2015). Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility, Melbourne: Melbourne Journal of International Law, 14.

Nollkaemper A. (2015). Attribution of forcible acts to states: connections between the law on the use of force and the law of state responsibility. In Blokker N., Schrijver N. (eds.), *The Security Council and The Use of Force,* Leiden/Boston: Martinus Nijhoff Publishers.

Schachter O. (1986). In Defense of International Rules on the Use of Force, Chicago:The University of Chicago Law Review ,53.
Shackelford S. (2009). *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, Berkeley: Berkeley Journal of International Law, Vol 25.
Schmitt M.N., O'Donnell B.T. (eds.) (2002). Computer Network Attack and International Law, Newport, RI: Naval War College International Law Studies, 76.
Schmitt M.N. (2013) *Tallinn Manual on The International Law Applicable to Cyber Warfare*, Cambridge: Cambridge University Press.
Schmitt M.N. (2015) In Defense of Due Diligence in Cyberspace, Yale: Yale Law Journal Forum, 125.
Schlutter B. (2010). *Developments in customary international law. Theory and the Practice of the International Court of Justice and the International ad hoc Criminal Tribunals for Rwanda and Yugoslavia*, Leiden/Boston: Martinus Nijhoff Publishers.
Waxman M.C. (2011). Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), Yale: The Yale Journal of International Law, 36.
Wheeler D. A., Larsen G. N. (2003). *Techniques for Cyber Attack Attribution*, Alexandria, VA,: Institute for Defense Analyses.
M.N. Schmitt (ed.) (2013). *The Tallinn Manual on The International Law Applicable to Cyber Warfare*, Cambridge: Cambridge University Press.

CASE LAW

The North Sea Continental Shelf (Federal Republic of Germany v. Denmark; Federal Republic of Germany v. the Netherlands) , I.C.J. Reports 1969.
Phosphates in Morocco, Preliminary Objections, 1938, P.C.I.J., Series A/B, No. 74, p. 10; United States Diplomatic and Consular Staff in Tehran, I.C.J. Reports 1980.
Certain Questions Relating to Settlers of German Origin in the Territory Ceded by Germany to Poland, Advisory Opinion, 1923 PCIJ (ser. B) No. 6.
Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits, International Court of Justice (ICJ), 27 June 1986.
Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia-Herzegovina v. Yugoslavia), Judgement, 1996, IC.J.
The Tadić Case, Judgement, IT-94-1-A, 1999.

MISCELLANEOUS

United Nations, Statute of the International Court of Justice, 18 April 1946.
United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI.
Articles on Responsibility of States for Internationally Wrongful Acts, 2001, 53 UN GAOR Supp. (No. 10) at 43, U.N. Doc. A/56/83.
International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, [hereinafter: DRAFT ARS], November 2001, Supplement No. 10 (A/56/10), chp.IV.E.1.
British Institute of International and Comparative Law, State Responsibility for Cyber Operations: International Law Issues, 2014, Event Report.