Challenges of State Sovereignty and the Right of State to Self-defense: The Case of Cyber Attacks

Joel Niyobuhungiro
Faculty of Law, Universitas Airlangga, Surabaya, Indonesia

Keywords: Cyber-Attack, Right to Self-Defence, Sovereignty of State.

Abstract: Sovereign states enjoy right of freedom from threat or use of force albeit this freedom is jeopardized in the realm of cyber warfare. Cyber threats continue to pose challenges to state sovereignty and attributing responsibility is difficult in cyber warfare because of sophisticated technology, anonymity and rapidity rendering it difficult to discern the source of the attacks. Some countries retaliate under the auspices or umbrella of inherent right of self-defence embedded in UN Charter. However, the legality of this self-defence is controversial. This research aims to know whether cyber-attack constitutes use of force or not. It ascertains if a state can invoke its right of self-defence in response to a cyber-attack presenting the same effects as those of armed attacks. Do cyber-attacks against state amount to use of force? With normative legal research this article analyzes the use of force, right of states to self-defense as state sovereignty is threatened in cyber-attacks which leave potential challenges.

1 INTRODUCTION

Although it is a significant life facility, cyber carries negative effects detrimental to both natural and legal person such as states, companies etc. Some cyber users maliciously target unsuspecting individuals, companies, banks, military and government agencies with malicious code to alter computer code, logic or data, resulting in disruptive consequences compromising data and lead to cyber-crime such as information and identity thef (Hathaway & Croot of 2012, p.12). Although states enjoy the freedom of threat or use of force under international law, with the development of technology, this freedom is jeopardized in the realm of cyber warfare.

Cyber-attacks directed against states violate state sovereignty in which those are one of the determining factors of statehood. To relate between state responsibility and cyber-attacks is a difficult thing due to sophisticated technology used. Ascertaining the actual source of cyber-attack and technical attribution is difficulty whereas it is not the issue in conventional international armed conflicts where state forces distinguish their weapons and personnel with clear markings identifying their provenance (Margulies2013, pp 7-8).

Although some states exert retaliatory means as inherent right to self-defence, its legality remains perplexing as to whether cyber-attack constitutes use of force or a state can invoke its right to self-defence in cyber-attacks recognized under international law. As far as materials and methods are concerned, the idea of this paper was conceived after reading various international legal instruments especially United Nations Charter articles 2(4) and 51 which were of paramount source. However, books, published articles, other documents and Internet hugely contributed to this research. This paper discusses the state sovereignty in cyber-attacks, right of state to self-defence under International Law, and the challenges of attributing state responsibility in cyber-attacks.

2 STATE SOVEREIGNTY UNDER INTERNATIONAL LAW

Concept of sovereignty is not odd in Public international law. State sovereignty is one of the determining factors of statehood (Montevideo Convention, 1933). In the spirit of Montevideo Convention, state is defined by four elements: a permanent population, a defined territory, a

Niyobuhungiro, J.
Challenges of State Sovereignty and the Right of State to Self-defense: The Case of Cyber Attacks.
DOI: 10.5220/0007549206680671
In *Proceedings of the 2nd International Conference Postgraduate School (ICPS 2018)*, pages 668-671
ISBN: 978-989-758-348-3

government and capacity to enter into relations with other States (Article 1-2). However, even before international recognition, a state has right to defend its integrity and its independence (Montevideo Convention1933, article 3). A sovereign state is a nonphysical juridical entity represented by one centralised government that has sovereignty over a geographic area and is neither dependent nor subjected to any other power or state (JSTOR, no date).

Sovereign states enjoy rights and duties such as freedom from threat or use of force directed against them by any state as result of being sovereign (UN Charter, 1945). Sovereign states enjoy many prerogatives in international law including, inter alia, establishing the breadth of its territorial sea up to a limit not exceeding 12 nautical miles (UN Convention on Law of the Sea 1982, article 3). Impliedly, sovereignty of State is not limited to land territory, it extends to territorial sea.

3 RIGHT OF STATE TO SELF-DEFENCE UNDER INTERNATIONAL LAW

In principle, an act of use of force against a sovereign state infringes on fundamental rights of states as regulated in article 2 of UN Charter. However, it will be lawful as it is pursuant to the requirements set forth in the UN Charter i.e. self-defence if an armed attack occurs against a member of UN and by exercising this right of self-defence, it shall be reported immediately to Security Council (UN Charter 1945, article 51). The rationale behind this provision is to preclude wrongfulness of use of force in self-defence. Nevertheless, one may wonder if the content of the article 51 definitely excludes the possibility of anticipatory self-defence referred to as the ability to foresee consequences of some future action and take measures aimed at checking or countering those consequences (Leo Van den hole 2003, pp. 97-98). It is not always prerequisite to conduct self-defence after the occurrence of an attack (International Court of Justice, Nicaragua v. USA 1986)

Anticipatory self-defence is possible though subjected to some preconditions such as: “necessity”, “proportionality" and "immediacy” (Leo Van den hole, 2003, pp. 97-98). Right to self-defence embedded in UN Charter existed even before as international customary law. However, right to self-defence in customary perspective did not allow anticipatory actions as reasons of self-defence albeit it seems to have been legitimated as written laws take prevalence over customary rules (Brownlie1963, p.230).

4 CYBER ATTACKS AND CHALLENGES OF ATTRIBUTABILITY OF RESPONSIBILITY UNDER INTERNATIONAL LAW

Whereas "Cyber warfare" refers to means and methods of warfare that consist of cyber operations amounting to or conducted in the context of an armed conflict within the meaning of international Humanitarian Law (International Committee for Red Cross, 2013), cyber-attacks are actions taken by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption(Clarke and Knake 2010, p.14).These actions consist of any action taken to undermine the functions of a computer network for a political or national security purpose (Hathaway and Crootof, 2012). “Cyber-attacks are subset of cyberspace operations that employ the hostile use of cyberspace capabilities, by nation-states or non-state actors acting on their behalf or not, to cause damage, destruction, or casualties in order to achieve military or political goals” (Sigholm,2013).

It is worth noting that the principle of territorial sovereignty also applies to cyberspace. Even in cyberspace, states are prohibited to interfere with the cyber infrastructure located in the territory of another state i.e. state can be responsible if the conduct inflicts severe damage on the integrity or functionality of foreign cyberInfrastructures in case responsibility is attributable (Heinegg, 2012).

State responsibility in cyber-attack however,is difficult to prove because a party asserting that a state is responsible for a cyber-attack must comply with ‘effective control’ test adopted by ICJ in Nicaragua v USA. Attributing responsibility incyber-attacks is difficult because it is preceded by a challenging technical step: discerning the actual source of the attacks and difficulty due to both the speed and anonymity of cyber attackers (Margulies, 2013). Since proving ‘effective control’ of the alleged state is difficult, states may incite or sponsor groups to commit cyber-attacks and escapes from accountability. For example Estonian officials accused Russia of perpetrating the attacks but

NATO technical experts were unable to find credible evidence (Herzog2011, p.51). Furthermore, the attempts to apply international law to cyber warfare relied on doctrine that doesn't fit cyber threats (Schmitt, 2013).

In jus in Bello perspective, armed conflicts are normally governed by Geneva conventions and its protocols (Geneva Conventions 1949, article 48). All the principles of Geneva conventions applicable to war are there to avoid unnecessary sufferings that can affect civilians and other persons who are not taking part into hostilities. However, one may wonder if it is the case for cyber-attacks since they are indiscriminate in attack as they are launched electronically even if effects may be physical depending on the nature and the purpose of the malware launched.

Although International Humanitarian Law (IHL) does not apply in cyber-attacks, states have obligation to avoid or at least minimize incidental civilian casualties and damage to civilian infrastructure because the rules and limits of wars apply just as much to the use of cyber warfare as to the use of rifles, artillery and missiles (ICRC, 2013).

Despite the suggestions of some scholars that jus in Bello principles (such as military objective, distinction, proportionality, and unnecessary suffering) should be applied within cyber-attacks, it raises question of how and against whom cyber-attacks may be lawfully conducted and by who they may be lawfully executed (Watts, 2009). It remains an issue as to how jus in Bello principles will be respected, because one may assert that cyber weapons are indiscriminate in attacks.

Although cyber operations are not conducted in a legal vacuum, cautious approach should be adoptedto avoid unnecessarily prejudge legal issues in cyber warfare (Melzer2011, p.4). Attributability of state responsibility for cyber-attacks will continue to be a challenge detrimental to states sovereignty since there is no single international treaty to regulate cyber warfare. In addition to that, cyber-attacks pose interpretative difficulties and with respect to UN Charter,it does not delineate cyber-attacks as to whether such operations constitute prohibited "force" or an "armed attack" that would justify military force in self-defence (Article 51 of UN charter).

5 CONCLUSION

Sovereign state is protected from any use of force under international law and enjoys inherent right of self-defence in case attacked as contemplated in article 51 of UN Charter. Nevertheless, the term threat or use of force contemplated in article 2(4) UN Charter creates ambiguity because it elaborates when the threat or use of force is prohibited but it failed to delineate whether use of force includes non-military force for example cyber-attacks that a state may launch against another state yet these attacks are not within the scope of the UN Charter. In this regard, the Charter should have enumerated elements that constitute "force" when it was adopted or the drafters should consider adjusting the Charter to the now cyber world. State sovereignty is jeopardized and one can assert that there is no single adopted instrument that regulates cyber warfare in international arena. Thanks to the incessant efforts made by international legal scholars and military experts whose writings such as Tallinn manual on the law applicable to cyber warfare, though non-binding, are gaining momentum in unravelling cyber warfare related issues.

The unique characteristic, unpredictability and rapid evolution of cyber-attacks are posing fresh challenges which prompt some scholars and policy experts to emphasize the need for clarity in interpreting the application of article 2(4) and 51 to cyber-attacks (Maxman, 2011). To suggest, United Nations or states in general should embark on international legal experts and military experts' views to adopt a treaty regulating cyber warfare which is a new challenge that deserves a new solution**.**

REFERENCES

Brownlie I,. 1963. *International law and the use of force by states*, Oxford, Clarendon.P .230.

Clarke, R and Knake R, 2010.*Cyber war: the next threat to National Security and What to Do about it.* New York, HarperCollins Publisher. P.14

Geneva Conventions of 12 August 1949, article 48) and its Additional protocols. Available at www.icrc.org/en/war-and-law-traeties-customary-law/geneva-conventions

Hathaway, O. A., Crootof, R., 2012. *The law of cyber-attack*, Faculty Scholarship Series.*385.[*Online*]*available at:http://digitalcommons.law.yale.edu/fss_papers/3852 accessed on 24th June 2018.

Heinegg. H,2012. *Legal Implications of Territorial Sovereignty in Cyberspace*, NATO CCD COE Publications, Tallinn.P.7 [Online].Available athttps://ccdcoe.org/publications/2012proceedings/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf. Accessed on 25th June 2018

Herzog S. 2011. *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*. Journal of Strategic Security, Vol.4,no2.P.51. [Online] Available at: DOI: http://dx.doi.org/10.5038/1944-0472.4.2.3. http://scholarcommons.usf.edu/jss/vol4/iss2/4. Accessed on 25th June 2018.

International Committeeof the Red Cross (ICRC), no date. *Cyber warfare*.[Online]Available at: https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htmaccessed on 24th June 2018.

ICRC,. 2013. *Cyber warfare and international humanitarian law: the ICRC's position*. [Online]. Available at:https://www.icrc.org/eng/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdfaccessed on 24th June 2018.

International Court of Justice June in Nicaragua v. USA, June 27, 1986. General List No.70. Available at:http://www.ilsa.org/jessup/jessup08/basicmats/icjnicaragua.pdf. Accessed on 25th June 2018.

JSTOR, no date. Sovereign States. [Online]. Available at:https://www.jstor.org/topic/sovereign-states/accessed on 26th June 2018.

Leo Van den hole, 2003. *Anticipatory self-defense under International Law*, American University International Law Review, Vol. 19, no. 1(69-106). Pp 97-98. [Online].Available at:http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1160&context=auilr. Accessed on 24th June 2018.

Margulies P., 2013. *Sovereignty and cyber-attacks: Technology's challenge to the law of state responsibility*. Melbourne Journal of International Law, Vol.14, P.7-8. [Online]. Available at:http://www.austlii.edu.au/au/journals/MelbJIL/2013/16.pdf. Accessed on 26th June 2018

Melzer, N., 2011. *Cyber warfare and international law*, United Nations Institute for Disarmament Research (UNIDIR). P.4. [Online]. Available at:http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf. Accessed on 25th June 2018.

Michael N. Schmitt, 2013. *International law applicable to cyber warfare*. Cambridge University press, New York, p.25

Montevideo Convention on the Rights and Duties of States. Adopted on 26/12/1933 and entered into force 26/12/1934 Article 1-2. Retrieved from http://www.jus.uio.no/english/services/library/treaties/01/1-02/rights-duties-states.xml

Sigholm.J,. 2013. *Non-state Actors in Cyberspace Operations*, Swedish National Defense College, Vol.4. No 1. (2013).p.6 [Online] Available at: https://journal.fi/jms/article/view/7609. Accessed on 25 June 2018

United Nation Charter. Adopted on26thJune 1945 and took effect on 24 October 1945. Article2(4) and 51.

United Nations Convention on the Law of the Sea 1982. Article 3. Available at: http://www.un.org/depts/los/convention_agreements/convention_overview_convention.htm. Accessed on 24th June 2018

Watts S., 2009. *Combatant status and computer network attack*, Virginia Journal of International Law, Vol. 50, No. 2, 2010.p. 395, [Online] Available athttp://dx.doi.org/10.2139/ssrn.1460680.Accessed on 26th June 2018.

Waxman, Matthew C., 2011. *Cyber-attacks and the use of force: back to the future of Article 2(4).*YaleJournal of International Law, Vol. 36, 2011. P.11.[Online]. Available at SSRN: https://ssrn.com/abstract=1674565 or http://dx.doi.org/10.2139/ssrn.1674565 .Accessed on 26th June 2018.