Cyber Space Regulation and the International Humanitarian Law

Author

Zahra Niazi

Abstract

Over the period of two decades, the threat landscape of state, global and human security has substantially modified, becoming ever-more dangerous. In this context, the cyber revolution has played a marked role in altering the threat landscape. However, the world is yet unprepared to deal with the consequences of the most dreadful outcome of a cyber-attack-a nuclear war while the domain of cyber space remains largely unregulated. This research will attempt to investigate the differing positions of states hindering the achievement of a global consensus for the regulation of cyberspace and argue whether International Humanitarian Law is applicable to cyber-attacks and if its applicability is sufficient to address the threat of cyber-attacks. The impact of the research includes being able to come up with certain recommendations.

Keywords: Cyber Space, Cyber Attacks, International Humanitarian Law

Introduction

Today, while the world is witnessing the spread of coronavirus and a resultant social disruption, the hacktivists are successfully exploiting the situation to either further their malicious agendas or test their cyber skills in the absence of a regulatory framework. The enormity of the exploitation can be ascertained from the fact that the World Health Organization has reported a five-fold increase in cyber-attacks during the current pandemic (WHO, 2020). Similarly, a 238% surge has been witnessed in cyberattacks against banks (Avantia, 2020). Besides the aforementioned, there have been numerous other reports claiming a sudden spike in cyberattacks during the period. Reports in January also claimed a cyber-attack on the United Nations that crippled 40 servers at the UN office in Vienna and the UN Office of the High Commissioner for Human rights

(McCallion, 2020). Alongside a spike, 82% of chief information officers have claimed that the techniques used by hacktivists have been advancing where weak links caused by technologies and processes in use by supply chains are being exploited besides the exploitation of human factors (Avantia, 2020).

This thus elevates fears of more frequent attacks in cyberspace of the degree of the 2007 cyberattacks on Estonia or the 2010 Stuxnet attack on Iran's nuclear centrifuges. The former included a series of attacks targeting websites of major organizations such as the parliament, ministries, banks and newspapers and thereby crippling the digitally dependent state; while the latter involved the destruction of one-fifth of Iran's nuclear centrifuges by targeting the control systems. Also, in this context, the monstrous risk of an accidental nuclear war due to the hacking of the missile command supercomputer cannot be ruled out. Moreover, the cyber warfare tools have become an easy weapon of choice for states' conduct of Hybrid warfare. However, as of yet, there is no effective regulation of cyberspace vis-a-vis the International Law. The aforementioned risks call attention to an acute need for global regulatory measures governing cyberspace for the sake of human, national and International security.

The research plays a two-fold role. Having highlighted the mounting threat of cyber-attacks, the research first gives an overview of various countries differing positions on the subject of 'information security in cyberspace' that have been hindering the achievement of a global consensus on the governance of cyberspace. Second, it argues whether the International Humanitarian law is applicable and sufficient to limit cyber-attacks until a new legal regime is constituted. Finally, the research very briefly lays down the necessary recommendations.

Various Countries positions on the subject of 'Information Security in Cyberspace'

To understand as to why the world has been unable to regulate the domain of cyberspace despite recognizing its deleterious consequences, there is a need to take account of the wider context concerning the ideological differences among the various states which had been on display at the United National Group of Governmental Experts process. Since the challenges of information and communications technology were first brought to the focus of the UN General Assembly in the late 1990s, the "UN GGE process" has been the major avenue for interstate dialogue about the international legal regulation of cyberspace. It is the forum where the Groups of Governmental

Experts" (GGE) (assisted by the UN's Office for Disarmament Affairs) set up by the UN Secretary General to study the "Developments in the Field of Information and Telecommunications in the Context of International Security" have discussed the ways of best approaching the many challenges being posed by the new technologies.

In the context of UN GGE, major areas of contention among states that have been hindering the achievement of a global consensus in the domain of information security in cyberspace include the following:

1) Applicability of International humanitarian law to cyberspace
2) The right of states to ensure their own information security
3) Adoption of a new legal regime relating to Information security
4) Application of the countermeasures and the right of self-defense in cyberspace
5) Disregard by some states for the need of disarmament and nonproliferation in connection with countering the threat being posed by information warfare

The following section will elaborate upon the differing positions of states on the subject of "information security in cyberspace" leading to a deadlock. Nevertheless, states are united by their desire to protect their critical infrastructure against cyberattacks.

The most important point of contention has been the disagreement over the applicability of IHL to cyber space. In the 2012/2013 GGE, the Chinese blocked any attempt to explicitly mention humanitarian law principles in the group's report on the basis that an endorsement of their applicability would legitimize armed conflict in cyberspace (Henriksen, 2019). Hence, the 2012/2013 report concluded that "the application of norms derived from existing international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability" (UNIDR, 2013). but failed to reference International Humanitarian law. Although the 2014/2015 consensus report was a step forward in that the report referred to the international legal principles of necessity, humanity, distinction and proportionality that are the principles of IHL or the Law of Armed Conflict (UNIDR, 2015), but these principles were not referred to in the context of the IHL. Prior to the drafting of the final report, the Chinese and the Russian delegation objected to the direct mentioning of the pertinence of IHL in the document and hence the final report could only make a reference to the aforementioned principles. The US has

interpreted it as endorsing the applicability of these IHL principles in cyberspace but the Chinese and Russians have avoided doing so. Given the lack of consensus particularly on how the IHL applies on the use of communication and Information technologies, the GGE failed to submit a final report of its recommendations to the UN General Assembly in the year 2017 (Henriksen, 2019). The major reason being the reluctance on the part of China and Cuba was to concede to the applicability of IHL to cyberspace. The Cuban delegation viewed an endorsement of its applicability as leading to the legitimization of the scenario of war and military actions in the context of ICT. This view was also backed by the Chinese delegation.

Similar to this is the disagreement over the utilization of the right of self-defense and countermeasures in cyberspace. China has maintained that any allusion to Article 51-the right to self-defense-would send an erroneous notification to the international community suggesting the authorization of cyber warfare (Korzak, 2017). Moreover, it was during the 2017 GGE that the Cuban delegation also opposed the use of the right of self-defense and countermeasures in cyberspace.

Another area of disagreement is the question of Information Communication Technology and the free flow of information or to be more specific over the term, Information Security, itself. The East Bloc considers certain ICTs and free flow of information itself as a threat (Tikk & Kerttunen, 2017). However, according to the US, the application of information security must not have a bearing on the privilege of any individual to seek, acquire and transmit ideas and information through any media such as the electronic media regardless of the boundaries. Moreover, the UK does not concede to the validity of the term “information security” when employed in this context on the premise that this would legitimize further controls on freedom of expression.

Countries including Russia, China, Belarus and Brazil since the GGE in 2004 have been promoting the right of states to ensure their own information security. These states and in particular Russia and China have maintained that every country has the entitlement to control its own cyberspace in conformity with the domestic legislative prescriptions. However, the US and other like-minded states have opposed this on the premise that this could hinder the free flow of information.

Further, the US and the European countries have rejected any reference to disarmament in any of the reports whereas some states have wanted to consider the issue in connection with countering the threat of information warfare.

The Cuban, Russian and Chinese delegations have propelled for the establishment of a completely newly created set of international laws for ensuring information security in cyberspace. To put it alternatively, they have sought *lex specialis* (Tikk & Kerttunen, 2019). On the other hand, the United States and other like-minded states have been opposing the establishment of a new legal regime governing cyberspace. This concern can be interpreted in light of the United States' cyber dominance since a new regime would limit its cyber capabilities. As a result of this deadlock, states including India and Switzerland have suggested the creation of a cyber committee of the General Assembly. Similarly, Brazil has suggested the consideration over a new legal framework that could prohibit the offensive use of cyber operations and the compromising of the information security of other states.

In November 2018, the United Nations General Assembly adopted two competing resolutions in order to address cyber threats. The Russian-sponsored resolution called for the creation of an open-ending working group of the General Assembly that studies the existing UN GGE norms and identifies new cyber norms (Grigsby, 2018). On the other hand, the US-sponsored resolution called for the creation of a new group of governmental experts that deals with the applicability of international law to state actions in cyberspace and identify mechanisms to ensure states' compliance with these norms (Grigsby, 2018). Both the resolutions emerged as the victors leading to the establishment of two parallel processes including an open-ending working group for 2019/2020 and the UN Group of Governmental Experts for 2019/2021. However, the creation of the two parallel bodies has neither been able to ensure a consensual agreement on the governance of cyberspace, nor accelerated the process.

The following sections explore if and how IHL applies to cyber operations which is a highly contested subject and whether it is sufficient to regulate state behavior in the said domain until a new legal regime is constituted.

Applicability of International Humanitarian Law in cyberspace

There is no provision of IHL that individually manages the conduct of hostilities or protects the sufferers of a cyber-attack; nor is there explicit evidence of normative customary international law in the aforementioned context be it in the shape of *opinio juris* or state practice. The following section will elaborate upon the possible link between international humanitarian law and attacks conducted via cyberspace.

Armed Attacks via Cyberspace

According to ICRC, the International humanitarian law would apply to cyber operations that occur during an armed conflict. This makes the applicability of IHL in cases of cyberattacks occurring during peacetime rather dubious.

It is only after an attack via cyberspace rises to the extent of an armed attack that the provisions of the IHL can be activated. The question then is to what extent do the cyber-attacks constitute the use of armed force. According to the Charter of the UN, such circumstances involve the existence of troops and the employment of traditional military weapons within the boundaries of another state's territory. However, it remains silent on such forms of coercion and subversion that fail to cross the threshold of a perceived threat of armed force. However, it is possible for the attacks via cyberspace to be included within the domain of armed attacks that violate the legal principles upholding non-intervention and sovereignty. Information warfare is an expansive category of military activities including physical attacks on information systems by traditional military means, psychological operations, military deception, and electronic warfare operations such as jamming and hence can possibly fall under the IHL framework (Macros, 2009). The point of contention makes an appearance in the case of a pure information (computer network) attack as being a category of information warfare that includes the employment of electronic methods to attain access to information or otherwise to change it and hence, does not damage the physical components. Such attacks would not trigger the IHL provisions. However, such Information (computer network) attacks if directed towards causing harm to humans and property can be characterized as the threat or use of force and hence, may fall under the category of an armed attack (Macros, 2009).

The Issue of Attribution

Further, even if an attack via cyberspace reaches to the extent of an armed attack, it is the speed as well as the anonymity of the cyber-attacks that complicate the distinction among actions taken by the terrorist groups, criminals or the nation states. Article 2 of the 1949 Geneva convention relating to the International Armed Conflicts provides that it applies to all instances of proclaimed war or of any other armed conflict which may happen to occur between two or more of the 'High Contracting Parties' (Rulac, 2019). Hence, this definition automatically limits this type of armed conflicts to those between states rather than the ones between states and non-state actors or criminals. Hence, before triggering the IHL provisions, the contentious issue is to determine the perpetrators of the cyber-attack. Further, the operations conducted by military forces are presumed to be under the control of national governments. However, no such presumptions govern the actors participating in cyber conflict. The laws of war require states attacking another state to identify themselves. However, in case of a cyber-attack, it is extremely hard to attribute an attack conducted by specific individuals to a government.

According to Macros (2009), in the wake of the Estonian cyber-attack, the critical issue of attribution arose given that the hackers disguised their origins by routing their actions to faraway localities. Although the Estonian officials claimed they had proof that some of the earliest salvoes originated from Russian government computing centers or by the affiliated centers run by Nashi su and other similar organizations. However, determining the exact locale from where these attacks originated was exceedingly hard since a number of them originated from undetectable private computers around the globe. But given the fact that the alleged hackers according to Estonian suspicions were Russian, Estonia submitted a plea for bilateral inquiry under the Mutual Legal Assistance Treaty between Russia and Estonia. Although Russia initially promised to probe into the matter, the promise was later abandoned. A month following the attack, the private sector and the US government conducted several assessments which partly substantiated the origin of cyber-attacks to certain politically motivated hackers such as the Nashi Su rather than the security agencies themselves. Nevertheless, a Russian hacker SpORaw views these efficient attacks on Estonia to have certainly been carried out with the assistance of the Russian authorities. Hence, it was not determined whether the attack was a cybercrime with Russian Nashi hackers aiming at regime change, or a cyberwarfare supervised by the Russian intelligence operatives.

Similarly, in case of the Stuxnet, the attack was only allegedly traced back to United States and Israel given the sophistications of its traits and the fact that the attack followed the explosion of Iranian gas pipelines and assassination of Iran's leading nuclear scientists (Gibney, 2016). This ultimately created an impression that a state entity was attempting to sabotage the Iranian nuclear program. However, a definitive source of attack could not be determined.

Applying International Humanitarian Law Norms to Cyberattacks

The case of Cyber Warfare calls attention to the following three provisions of International Humanitarian law:

(1) The distinction between combatants and non-combatants

(2) The distinction between civilian and military infrastructure

(3) The prohibition of a perfidious action

As for the cyber-attack, one cannot distinguish between the non-combatants and combatants given the fact that the cyber attackers do not identify themselves as combatants. According to the Hague Conventions, it is only the regular armed forces of a country who have the right to employ force against the enemy. However, the use of force needs to be in accordance with the rules of war but failing to do so would not deprive them of this status. However, according to Protocol I, Article 44, soldiers who do not identify themselves as combatants either by carrying the arms or wearing the uniform would be deprived of their combatant privilege. And this brings us to the question as to whether the Hague conventions could be applicable to the captured cyber attackers. However, given the fact that cyber attackers disguise their attacks as innocent requests for information, those accused can be prosecuted under Protocol I, Article 37 of the Geneva Conventions which prohibits an act of perfidy(treachery) under which a soldier faking a civilian status would be prosecuted (Lin, 2019).

Secondly, Protocol I, Article 51 of the Geneva Convention prohibits an indiscriminate attack- the one that is not directed against a specific military target. And some instances of cyber-attacks such as the Estonian case failed to distinguish between military and civilian objects since the targets varied from banks and government services to broadcasters and air traffic control. Hence, such

indiscriminate cyber-attacks would stand in conflict to the Article 51 of Protocol I and could be covered by the aforementioned IHL prohibition (Lin, 2019).

To sum it up, the above-mentioned norms form the basis of such underlaying that should be employed with the utmost conviction to the domain of cyberspace. This clarifies that the cyber-attacks sponsored by states can trigger certain provisions of the IHL. Also, as with other methods and means of warfare, attacks involving the computer networks are deemed legal unless they do not conflict with the principles of the IHL.

Contextually, some have already recognized that in cases where the attribution for cyber-attacks has been satisfied, the attack should be addressed by the IHL framework and the cyber attackers should be held liable for war crimes (Macros, 2009). Consequently, if state launch cyber-attacks that pose large scale atrocities, they should be held accountable to war crimes by every means possible. Similarly, in case of a destructive cyber-attack aimed at destroying the group to which the victims belonged, the state should be held liable for genocide. Nonetheless, the exclusion of outer space in enumeration, the issue of an explicit determination of an armed attack in cyber space and the concern of misattribution would make the applicability of these pertinent IHL rules to any degree of cyber-attacks highly dubious.

Conclusion and Recommendations

The international community has already been undergoing situations in which cyber-attacks are being sponsored by nation-states, posing deleterious consequences for human, national and International security. It yet remains to be seen as to what extent will the Covid-19 crisis awaken the conscience of the states and pave way to a consensus on global regulatory measures in the domain of cyberspace through extensive cross-stakeholder coordination. One can only reluctantly hope that the crisis may provide a warning for states to address threats in cyberspace before it is too late. For as they say, every crisis is an opportunity in disguise. Although the aforementioned section suggests the possible applicability of IHL to attacks occurring via cyber-space, there is still a need to establish a comprehensive treaty governing cyberspace that covers the applicability of IHL along with other provisions.

A more definitive treaty should define when a computer network attack rises to the level of an armed conflict, clarify which provisions of IHL would apply to cyberattacks occurring during

armed conflicts and the ones occurring during peacetime, and provide for enforcement mechanisms. Further, it should pave the way for the establishment of a collective administrative system whereby the technological advancement of the developed nations enhances the prospects of early threat detection of malicious attacks and allows for the addressal of the critical issue of attribution through the employment of advanced Machine Learning technologies. This would ensure the shared benefit from AI in the domain of cybersecurity rather than its confinement to the technologically advanced states only. Hence, as proposed by states including China, Russia, Cuba, Belarus and Brazil, there is a need for the creation of a new legal regime governing cyberspace. This argument is further supported by the fact that given cyberspace is an International common similar to the outer space or the high seas since it is not legally owned by any single entity, it needs to be regulated by the establishment of a new legal regime. The outcome will prove conducive for the human, national and international security.

References

Alex, G. Unpacking the Competing Russian and US Cyberspace Resolutions at the United Nations. (2018) https://www.cfr.org/blog/unpacking-competing-russian-and-us-cyberspace-resolutions-united-nations Accessed 25 August 2020.

Avantia. What is Cyber Warfare. (2020). https://www.avantiacybersecurity.com/post/putting-russian-military-cyber-operations-into-context Accessed 28 September 2020.

Gibney, A. (2002). Zero Days. United States: Magnolia Pictures.

Henriksen, A. (2019). The end of the road for the UN GGE process: The future regulation of cyberspace. *Journal of Cybersecurity*, 5, 1.

Korzak, E. (2017, July 31). UN GGE on Cybersecurity.*The Diplomat.*

Lin, P. Why Cyber Attacks could be war crimes. (2019) https://www.weforum.org/agenda/2017/07/why-cyberattacks-could-be-war-crimes/ Accessed 23 August 2020.

Macros, S. (2009). From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. *Berkeley Journal of International Law*, 27.

McCallion, J. What is Cyber Warfare. (2020). https://www.itpro.co.uk/security/28170/what-is-cyber-warfare Accessed 26 September 2020.

Rulac. International Armed Conflict. (2019). http://www.rulac.org/classification/international-armed-conflict Accessed 21 August 2020.

Tikk, E., & Kerttunen, M. The Alleged Demise of the UN GGE: An Autopsy and Eulogy. (2017). https://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf Accessed 20 August 2020.

UNIDR. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (2015). https://digitallibrary.un.org/record/799853?ln=en Accessed 16 August 2020.

UNIDR. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (2013). http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf Accessed 15 August 2020.

WHO. WHO reports fivefold increase in cyber-attacks, urges vigilance. (2020). https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance Accessed 27 September 2020