STATE SOVEREIGNTY AND SELF-DEFENCE IN CYBERSPACE

PALLAVI KHANNA,

High Court of Delhi (New Delhi, India)

DOI: 10.21684/2412-2343-2018-5-4-139-154

Given the increasing role and use of cyberspace in our daily lives, it is important to consider the large-scale dynamics of the cyber forum. Shifting the focus from individuals to nation states as participants that engage in activities in cyberspace raises doubts over the status of nations in this domain. Do they continue to remain sovereign entities on such a platform? Do they have the right to defend themselves against attacks from other nations? These questions have been subject to a lot of debate in the context of international law. The aim of this paper is to study the implications of the principle of state sovereignty and self-defence in cyberspace. The paper focuses on two prime considerations of sovereignty and self-defence in the context of cyberspace and its link to international law. Thus the scope is limited to concepts such as territorial jurisdiction, sovereignty, attribution and self-defence. While doing so, the researcher seeks to answer questions such as, Is international law applicable to cyberspace? Can cyberspace be called a sovereign domain? Do principles of territorial jurisdiction apply to cyberspace? How does the attribution mechanism work in cyberspace? Under what circumstances are states permitted to exercise the right of self-defence against cyber attacks? and What are the deficiencies in international law governing cyberspace?

Keywords: sovereignty; self-defence; jurisdiction; cyberspace; cyber attack; attribution; international law.

Recommended citation: Pallavi Khanna, *State Sovereignty and Self-Defence in Cyberspace*, 5(4) BRICS Law Journal 139–154 (2018).

Introduction

"Here be lions," an expression used by ancient cartographers to describe unexplored territories and dangers, would suit cyberspace if it was not merely a virtual domain.[1] Cyberspace is characterised as being something more than the internet. It is a vast field which affects a variety of human conduct. It is transnational in nature, having no central authority and few points of control. It is largely facilitated via third parties. Given the ubiquity of information and computer technology, the increasing dependence on cyberspace is perceived as a security concern. Thus, states seek to preserve their access and safeguard their dependence on cyberspace, and this often entails a departure from set norms.

It has become a trend to classify cyberspace as a novel aspect of warfare, insulated from international law and capable of being abused. Malicious governments and institutions tend to exploit the cyber domain to attack global infrastructure and critical cyber assets. The results of these operations range from the disruption of governmental functions and financial loss to the physical destruction of property, strategic defence equipment, etc., and deaths as well.[2]

Cyberspace is not disjoined from state sovereignty. It requires physical infrastructure to function and an entity to monitor its development. Since the potential to cause harm is very real in cyberspace, it cannot be left ungoverned. Cyberspace is also capable of challenging state sovereignty, since it can question the state's ability to regulate movement across borders. An individual in a given state can freely enter another state through cyberspace and engage in harmful activities in the latter. In furtherance of their commitment to protect cyber borders, nation states can take robust measures to regulate the information technology infrastructure that operates within their domestic territory.[3]

However, the prospect of monitoring cyberspace has been the subject of controversy and has not received general acceptance given its tendency to compromise on potential human rights obligations.[4]

Through the course of this paper, the researcher seeks to understand the principles of international law which govern the conduct of states in cyberspace by analysing aspects of state sovereignty, response mechanisms and problems of attribution. The

---

1 Marco Roscini, *World Wide Warfare – Jus ad bellum and the Use of Cyber Force*, 14 Max Plank Yearbook of United Nations Law 85, 86 (2010).

2 Michael N. Schmitt, *Cyberspace and International Law: The Penumbral Mist of Uncertainty*, Harvard Law Review Forum, 5 April 2013 (Nov. 10, 2018), available at http://harvardlawreview.org/2013/04/cyberspace-and-international-law-the-penumbral-mist-of-uncertainty/.

3 Andrew Liaropoulos, *Power and Security in Cyberspace: Implications for the Westphalian State System* in *Panorama of Global Security Environment* 541, 545–546 (M. Majer et al. (eds.), Bratislava: Centre for European and North Atlantic Affairs, 2011).

4 Eric T. Jensen, *Cyber Sovereignty: The Way Ahead*, 50(2) Texas International Law Journal 275, 297 (2015).

first part undertakes to establish a connection between the norms of international law and their applicability to cyberspace. The second part is a discussion on the territoriality and jurisdiction of states over the cyber domain. This extends in the third part into the issue of state sovereignty in the context of internet regulation. The fourth part studies the measures that may be employed by states to counter cyber attacks and unauthorised entry to servers. In the final part, the question of attribution of responsibility for cyber operations is analysed.

1. International Law and Cyberspace

The application of customary international law to cyberspace is not a new question and it has garnered a lot of attention. The classification of cyberspace as a novel avenue to which international law is not applicable is disappointing, and it is believed that demands for new international law solely governing cyberspace is not justified since states, in principle, agree to the application of customary international law to cyberspace though sometimes a consensual adaptation may be required.[5]

The President of the United States of America, at the International Strategy for Cyberspace, has also observed that there is no need to develop or reinvent norms of customary international law for regulating state conduct in cyberspace, as traditional international norms will guide the behaviour of states even in cyberspace. However, in doing so, governments must work together in consensus.[6]

There are unavoidable hurdles that one encounters in applying the customs of international law to cyberspace since a majority of those rules originated before the advent of this new domain. Those opposing the application of international law to cyberspace argue that cyber attacks are inherently distinct from traditional warfare which involves the actual use of instruments of war and hence cyberspace requires new systems of regulation. However, others believe that this is a flawed assumption and that the rules of war can be reconciled with this new domain since the effect of both these kinds of attacks is similar even though the means employed are not the same.[7]

It has often been debated whether or not cyber operations are attributable to a state on account of the law of state responsibility. States thus have started considering how current international law regulates cyberspace. Restrictions on the cyber world further limit the freedom of states to act in cyberspace. Nevertheless, these problems can be overcome if the states exercise due diligence and undertake

---

[5] Wolff Heintschel von Heinegg, *Legal Implications of Territorial Sovereignty in Cyberspace* in *4th International Conference on Cyber Conflict* 7, 8 (C. Czosseck et al. (eds.), Tallinn: NATO CCD COE Publications, 2012).

[6] *Id.* at 10.

[7] Ella Shoshan, *Applicability of International Law on Cyber Espionage Intrusions*, Thesis (Faculty of Law, Stockholm University, 2014), at 32 (Nov. 10, 2018), available at http://www.diva-portal.org/smash/get/diva2:799485/FULLTEXT01.

to initiate measures ensuring that their territories are not forums for cyber operations put to the detriment of other states.[8]

2. Territorial Jurisdiction

Cyber-libertarians propound the belief that the cyber world is only subject to an internal means of governance, and there are those who echo the sentiment of cyberspace being an independent area free from the rules of other spheres of human activity.[9] The early users of cyberspace strongly believed in the idea of cyberspace being a *terra nullius*, i.e. a space free from any kind of government regulation.[10] This view translates into the idea that no state has cyber territory and hence the question of extra-territorial intervention by states does not arise.[11]

The *supra* territoriality of cyberspace makes it hard to locate cyber actions territorially. This gives rise to more instances where multiple territories experience consequences at the same time. Hence, allocating jurisdiction to a specific state is not merely a technical question but also one that entails making distributional and political choices as well.[12]

Though it has been suggested that the emerging sovereignty of cyberspace extends beyond the judicial sovereignty of countries, this view is open to challenge since no country has expressly recognised the independent sovereignty of cyberspace, which is deemed to be dependent on the sovereignty of states.[13] The non-territoriality of cyberspace imposes no embargo on states from partially territorialising it by instituting surveillance mechanisms to secure information flowing across their borders.[14]

For instance, in the *Yahoo!* case a French court had ordered Yahoo! to suspend the auctioning of Nazi memorabilia. The site refused to comply by arguing that it is an "American" company and not a French one, and that it operates in cyberspace and not within the territory of France. In its legal defence, Yahoo! also proposed that not only would the ordered action be impossible, but that there was the risk of the government's being unreasonable and exercising indiscriminate tyranny. However, the High Court of Paris rejected these claims since evidence shown indicated that

---

8 Michael N. Schmitt, *In Defence of Due Diligence in Cyberspace*, 125(1) Yale Law Journal Forum 68 (2015).

9 Shoshan, *supra* note 7, at 35.

10 *Id*.

11 *Id*.

12 Joel Trachtman, *Cyberspace, Sovereignty, Jurisdiction and Modernism*, 5(2) Indiana Journal of Global Legal Studies 561, 569 (1998).

13 Alireza Hojatzadeh & Afshin Jafari, *Cyber-attacks and Jus Ad Bellum*, 1(2) International Journal of Humanities and Social Sciences 76, 79 (2014).

14 Liaropoulos 2011.

there were adequate links to France to vest the country with the jurisdiction to hear the complaint. The fact that the auctions were open to bidders from France, and that the display of these objects was forbidden under French criminal law and amounted to public nuisance, and the fact that Yahoo! was aware that French residents were accessing the auction site since the site displayed advertisements in the French language when accessed by users from France, etc., further established the territorial jurisdiction of the French court.[15]

Cyberspace, though an abstract entity, has physical manifestations through its servers which are subject to state jurisdiction akin to being actors existing in cyberspace, and this shows that cyberspace does not operate within a vacuum, and that the infrastructure and actors as part of this domain are subject to the jurisdiction of the state.[16]

For instance, it is believed that cyber espionage constitutes intrusiveness violating the sovereignty and territorial jurisdiction of states since unauthorised entry to servers located in a state violates the right of states to sovereignty and territorial jurisdiction. Moreover, cyber espionage does not fall within the ambit of Article 2(4) of the U.N. Charter[17] since it does not involve the use of force. Since data is stored on servers which are part of cyber infrastructure, intrusion into such data located within the territory of the target state empowers the target state to exercise sovereign prerogatives with respect to such data. In recognition of this the Tallinn Manual acknowledges that states have the exclusive right to exercise jurisdiction over cyber infrastructure and activities that fall within their sovereign territory.[18] Thus the territorial sovereignty and physical location of the cyber infrastructure creates a right to control the same in favour of the state.[19]

3. Sovereignty

Respect for the territorial sovereignty of independent states is a significant basis of international relations, confirmed in the ruling of the International Court of Justice

---

15 LICRA v. Yahoo! (*Ligue contre le racisme et l'antisémitisme et Union des étudiants juifs de France c. Yahoo! Inc. et Société Yahoo! France*), decided by the High Court of Paris (*Tribunal de grande instance*) in 2000. Also *see* Jon Henley, *Yahoo! Cleared in Nazi Case*, The Guardian, 13 February 2003 (Nov. 10, 2018), available at http://www.theguardian.com/technology/2003/feb/12/newmedia.media.

16 Catherine Lotrionte, *State Sovereignty and Self-defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, 26(1) Emory International Law Review 825, 829 (2012).

17 Article 2(4) of the Charter of the United Nations: "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."

18 Rule 1 – Sovereignty, Tallinn Manual, at 15–17 (Nov. 10, 2018), available at http://insct.syr.edu/wp-content/uploads/2015/06/Tallinn-Manual-Sovereignty.pdf.

19 Shoshan, *supra* note 7, at 34.

in the *Nicaragua* case.[20] Hence, hostile cyber operations aimed against the cyber infrastructure on another state's territory involves a violation of the sovereignty of the target state even if it does not result in any harm or injury since it amounts to an unlawful intervention by the exercise of jurisdiction by the other state.[21]

The effects-based approach qualifies a cyber attack as an armed attack if its effect is similar to destruction by physical weapons. However, it ignores the damage caused by non-physical consequences, and the denial of the right of self-defence prevents states from instituting any methods of deterrence.[22]

The realist assumption is founded on the idea that laws based on geography seem logical when the government exercises control over the physical domain and the people or things located within that jurisdiction are the ones that are affected.[23] However, given the fact that the internet operates throughout multiple jurisdictions and that effects are not concentrated in a single geographical location, imposing exclusive jurisdiction does not always seem reasonable.[24]

The sovereignty of states has been a common theme across discussions, given the borderless world of the internet. Concerns for state sovereignty have instigated several regulatory initiatives. China's attempts to preserve its informational sovereignty by insulating its internet from Western websites are a clear example of how anxiety over sovereignty has been responsible for restrictions. Restrictions on the regulation of the internet have often been based on arguments of state sovereignty, which primarily raise the issue that regulating the internet activities arising in other states amounts to illegitimate encroachment on their sovereignty.[25]

States often rely on the realist conception of sovereignty, which believes that states are the principal actors in the international legal system, to justify regulation of the internet by asserting jurisdiction on the basis of the principles of territoriality and the effects doctrine. The territorial principle translates into the states having authority to regulate the transmission of information across their borders and the use of such information by the people within their territory. This is reflected in China's filtering of possibly harmful information. The territorial principle is also invoked by states to monitor the hardware and software used in internet communications within the state.[26]

---

20 Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25(2) Stanford Law & Policy Review 275 (2014).

21 *Id.*

22 Sheng Li, *When Does Internet Denial Trigger the Right of Armed Self-Defense?*, 38(1) Yale Journal of International Law 179, 187 (2013).

23 *Cyberspace Regulation and the Discourse of State Sovereignty*, 112 Harvard Law Review 1680, 1685 (1999) (Nov. 10, 2018), also available at http://cyber.law.harvard.edu/property00/jurisdiction/hlr.html.

24 *Id.*

25 *Id.* at 1681.

26 *Id.* at 1684.

Application of the principle of territorial sovereignty to cyberspace translates into vesting the territorial state with the right to exercise jurisdiction over its cyber infrastructure and cyber activities. This means that the cyber facilities located within the territory of a state are subject to a wide array of state enforcement, regulation and prohibitions which extends into the global cyber domain, and thus states are not prevented from applying their domestic laws over cyber activities. The effects doctrine is an interesting manifestation of territorial jurisdiction. As per this doctrine, the state has jurisdiction not only over actions taking place within their domestic territory, but also over those actions that generate harm in that territory though the actions causing this effect did not happen on the territory. In order to make use of domestic laws to regulate the out-of-state activities on the internet which cause some effects to be seen within the state, states rely on the effects principle since control over their territory implies legitimacy of state actions within that territory.[27]

Government officials also rely on the representational conception of sovereignty to support internet regulation. This is usually in circumstances where they think that the online activities undermine the sovereign state's capability to represent the populace. This stems from the belief that the ability of the internet to penetrate all borders can challenge the sovereignty of states. Hence it seeks to justify the regulations as mechanisms to protect the sovereignty of states.[28]

Consequently, we see that the principle of sovereignty is directly applicable to cyberspace. All states are on an equal plane when it comes to exercise of "cyber-sovereign" prerogatives. This implies that, irrespective of capabilities, all states have the same right to exercise sovereignty over their territory. In a similar way in which states exercise their sovereign rights, states are entitled to do the same in cyberspace as well, but they are required to accept the obligations that correspond to such rights. By virtue of the right of sovereignty, states are authorised to develop cyber infrastructure as they wish. However, this comes with the proviso that states are to peacefully settle cyber conflicts that threaten international peace and security, and that in the exercise of cyber activities states must have due regard for the rights of other states, and not intrude into the domestic cyber affairs of other states except through mutual agreement.[29]

4. Response Mechanisms

As per the territoriality rule, cyber infrastructure falls within the jurisdiction of the flag state and is also subject to that state's sovereign prerogatives. The principle of sovereignty read with the idea of non-intervention adds to the responsibility of the state to secure its networks.[30]

---

27 Heinegg 2012, at 14.

28 *Cyberspace Regulation*, *supra* note 23, at 1687.

29 Jensen 2015, at 285–288.

30 Liaropoulos 2011, at 546.

Though states exercise sovereignty over their cyberspace, sometimes there are reasons for them to take steps in the cyber domain of foreign countries in the form of legitimate countermeasures or illegitimate probes or even armed attacks. However, some attacks which may not constitute the use of force may amount to illegal interference as well.[31] The principle of non-intervention is applicable to cyberspace also; yet, there is debate as to whether damage caused is crucial for classifying an act as an illegal intrusion and thus violative of territorial sovereignty.[32]

The U.S. International Strategy for Cyberspace also espouses a broad interpretation of the idea of territorial sovereignty since it seeks to assert its right to respond to these kinds of acts by all necessary means, including employing force if needed.[33]

Cyberspace is enmeshed in a web of international law which outlaws malevolent cyber operations and also permits states to respond robustly to the same. Pursuant to customary international law and Article 51 of the U.N. Charter, if the armed attack threshold is exceeded by the cyber operations, target states can defend themselves through the use of force. The increasing use of the cyber domain for attacks has strengthened the belief that cyber attacks constitute use of force and hence defending against them is legitimate as per Article 51.[34] However, others feel that Article 51 is applicable only when the intensity and consequences of such attacks are along the same lines as a physical armed attack.[35]

There is continuing debate over what meets the threshold of use of force. Non-destructive cyber operations may also amount to use of force. For instance, supplying malware to rebels which they then misuse to cause destruction can be called use of force. Yet, it must be noted that all unfriendly acts do not rise to the level of use of force. The International Group of Experts has devised a list of factors that influence how states use cyber operations as use of force, and acts of economic coercion have been excluded from the ambit of use of force.[36] These last include aspects such as severity, directness, immediacy, invasiveness, military character, measurability, presumptive legality and

---

31 Pål Wrange, *Intervention in National and Private Cyber Space and International Law*, Fourth Biennial Conference of the Asian Society of International Law, New Delhi, 14–16 November 2013 (Nov. 10, 2018), available at http://www.diva-portal.org/smash/get/diva2:682092/FULLTEXT02.

32 *Id.* at 7.

33 Heinegg 2012, at 12.

34 Article 51 of the Charter of the United Nations: "Nothing in the present Charter shall impair the inherent right of collective or individual 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 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."

35 Hojatzadeh & Jafari 2014, at 81.

36 Schmitt 2014, at 281.

state involvement. This is not an exhaustive list and additional factors such as the political environment, the nexus between cyber operations and the military, the identity of the perpetrator, the nature of the target, etc., are also considered to be relevant. Over time, the meaning of use of force will be subject to different interpretations. For instance, states may start characterising operations that non-destructively harm crucial infrastructure as use of force, and data destruction which disrupts societal functions may also be characterised as being an example of use of force.[37]

Experts on the Tallinn Manual acknowledge that states must refrain from knowingly allowing the cyber infrastructure within their territory or under the government's control to be used for otherwise unlawful acts which may be detrimental to the interests of other states. If the state fails to meet this obligation, the victim state should be at liberty to adopt countermeasures.[38]

Contemporary discussion does not focus on the proximity of the prospective attacks to the defensive actions but on the opportunity of self-defence which is qualified by three prerequisites. In order to react by use of armed attack in the form of self-defence against a cyber attack, the conditions of necessity, immediacy and proportionality must be met. Necessity implies that force is being used as a last resort and that all other mechanisms have failed. Thus identification of source, the unfeasibility of alternate means of retaliation and the intentional nature of the cyber attack must be clearly established before one avails oneself of this right. Nevertheless, the most crucial condition which needs to be fulfilled by states exercising the right to self-defence is the proportionality rule. This rule seeks to restrict the force to what is in proportion to the aggression it seeks to end. It should also meet the object of exercising self-defence, which usually is to restore the status quo. Hence, states must carefully evaluate the damage that may be caused if they intend a forceful response.[39]

The "unwillingness test" enables balancing the right of self-defence against the sovereignty of the host state since it allows self-defence involving violation of the sovereignty of the host state only if the host state is unwilling or incapable of preventing armed attacks launched from within its territory. This is a corollary of the necessity principle which allows self-defence as a legitimate action only when other alternatives to using force have been exhausted.[40]

Any forced defence action in cyberspace easily qualifies in respect of the conditions of necessity and immediacy. This is because any such action in the form of cyberspace warfare is likely to occur only as a response to armed attack warranting recourse to force as a last resort. Moreover, all cyber attacks require immediacy in

---

37 Schmitt 2014, at 281.

38 Schmitt 2015.

39 Jay P. Kesan & Carol Hayes, *Self Defense in Cyberspace: Law and Policy*, Illinois Public Law and Legal Theory Research Paper Series No. 11–16 (2011), at 12.

40 Li 2013, at 205.

countermeasures in order to mitigate or prevent the destructive potential of a cyber attack.[41]

The law regarding self-defence suffers from uncertainty in two respects. Firstly, it is a subject of controversy as to whether activities which do not cause any physical disruption are armed attacks. The international group of experts clarified that the use of force which injures or destroys people or property is an armed attack and states can resort to using force for purposes of self-defence in these situations.[42] While a narrow view of the same limits the law to physical effects, an alternative approach is not to focus on the nature of the effect but on the severity of the consequences.[43]

Secondly, while it is imperative to define a standard of armed attack, it has yet to be done. Merely characterising a cyber operation as being a wrongful use of force only seeks to label the state as contravening international law. Though countermeasures are limited to non-forceful means, armed attack allows states the right to respond by their own use of force. Hence the chances that cyber operations launched by a state may be miscalculated by the target state as having grave consequences are quite high.[44]

Some interpret the right of self-defence as extending to those states that are unable or disinclined to prevent their territory from being used for cyber operations. States harbouring such operations may not have the technical capacity to detect or take measures to stop attacks. There may be occasions when the quick escalation of the attack prevents a state from notifying the target state about the operations underway and thus precludes their ability to take remedial action. Thus target states will have to face situations where they are left with no choice but to take immediate action against such attacks.[45]

When a state undertakes a harmful cyber act it is seen as an internationally wrongful act, and hence it opens the door to countermeasures by the injured state. Countermeasures refer to acts that, otherwise unlawful, are justified when taken in response to a wrongful act of another state. Consequently, countermeasures can take the form of steps that are in violation of the sovereignty of a state by affecting its government's cyber infrastructure. Countermeasures are not necessarily cyber in nature and may take the form of sanctions. Moreover, they may be directed against governments and private entities alike.[46]

International law governing the extent of self-defence permissible must not be so wide that it may be invoked as an excuse for aggression. However, the guidelines

---

41 Dimitrios Delibasis, *State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century*, 8 Peace Conflict and Development: An Interdisciplinary Journal 13 (2006).

42 Schmitt 2014, at 282.

43 *Id.* at 283.

44 Schmitt 2014, at 284.

45 *Id.* at 288.

46 Schmitt 2015.

regarding self-defence must also not be extremely restrictive, since restraining states from responding lawfully with force against acts of aggression would encourage aggressors. Moreover, while international law in respect of countermeasures limits the right to respond to attacks only to states that have been injured, the self-defence system does not suffer from such a drawback, as the U.N. Charter recognises the collective right of self-defence, and thus allows states to defend allies who have suffered armed attacks.[47]

5. Attribution

It is difficult to respond to cyber attacks because unlike traditional battles cyber attacks are invisible by nature. The anonymity of the attacker creates further hindrances to legitimate defence. Attribution and ascertaining intent are crucial factors because they prevent states from retaliating against innocent countries. Moreover, the laws governing response mechanisms differ for state and non-state perpetrators. The ban in respect of the use of force under Article 2(4) of the U.N. Charter extends to states and not to private individuals. Thus, international law bars states from employing force against other states, but actions by individuals are subject to prosecution under national criminal law.[48]

If taking countermeasures against actions aimed abroad is impractical, failure on the part of the state to do so does not imply that there is a breach of its obligation of due diligence. The legal standard expected is subject to the capabilities of the state.[49] While constructive knowledge will be assessed on the standard of due care, the dissimilar capabilities of states to attribute or locate harmful cyber operations makes due care also subjective. However, states may attempt to evade their duty by giving false information about their capabilities.[50]

States have a duty to prevent cyber attacks originating from their territory and inflicting harm on other states. Such an obligation presumes active knowledge of such acts by the state when a cyber attack is traced to that state by the state organs themselves or by the target state.[51]

Cyber attacks when attributable to a state constitute a transgression of the custom of non-intervention on matters which the state by virtue of the principle of sovereignty can decide freely.[52]

---

47 Li 2013, at 211–212.

48 Hojatzadeh & Jafari 2014, at 80.

49 Schmitt 2015.

50 Schmitt 2014, at 278.

51 Heinegg 2012, at 16.

52 Roscini 2010, at 103.

For lawfully exercising self-defence against states which are the source of cyber attacks, there must be confident identification of the state as the regional origin of the cyber attack and also as being responsible for the attack.[53] Since countermeasures are usually permitted only for state actions, it is uncertain how target states can react to the cyber operations of non-state actors.[54] Though the stance with respect to state-sponsored cyber attacks is firm, states usually resort to the plea of necessity to base their response against non-state actors whose actions cannot be attributed to a state, and this plea is also raised in support of operations whose author is unknown and only the technological source is identified. If despite best efforts a state is unable to restrain the harmful cyber actions, the state being so affected may retaliate by doing all that is needed to end such operations even if it extends to affecting the non-cyber activities of the other state. However, the threshold of the plea of necessity is hard to define in strict terms.[55] It is also said that there is no requirement to attribute the attacks to a specific person: it is sufficient to identify the jurisdiction to which the operator/networks belong in order to give rise to acting in collective self-defence, as the level of hostilities will be the decisive factor.[56]

Moreover, non-state actors sometimes act in ways such that the target state can trace their actions to a state and thus respond with force against the non-state actor as well as the state to which their actions can be attributed. Cyberspace provides fertile ground within which to acquire the means and opportunity to undertake operations at the level of armed attacks in order to attack states. This would lead states to resist relying solely on law enforcement mechanisms to fight serious attacks by non-state actors; failure to take prompt and forceful action against destructive attacks by non-state actors would be politically dire and unsound in practical terms. Given the hidden and instant nature of cyber operations which are difficult to attribute and which may have dire consequences, in addition to the ease of acquiring cyber capabilities, it is illogical to seek adherence to a temporal standard. If the right of exercising self-defence is to be effective, states must be allowed to act forcefully in order to avert any armed attack the moment they learn that a cyber operation is going to be mounted, and they will lose the opportunity to defend themselves effectively if they delay or hesitate in responding urgently.[57]

The current attribution scheme puts the focus on the level and kind of support extended by the state in respect of the non-state actor. If there is a close nexus between the state and cyber actions, other states are more likely to perceive those actions as the use of force by the source state. The greater the support, the higher

---

53 Li 2013, at 203.

54 Schmitt, *supra* note 2.

55 Schmitt 2015.

56 Kesan & Hayes 2011, at 11.

57 Schmitt 2014, at 286–288.

the chances are that the state will be held responsible for the acts of the non-state actor. Moreover, the fact that cyber attacks can be located almost anywhere, and not necessarily in the target or attacking state, creates evidentiary problems in finding the attackers who may also try to deceive everyone into believing that the attack is being launched from inside or by a country other than the real country of origin. Thus, the anonymity of location raises hurdles in assigning responsibility except when the attack by a non-state actor was manifestly undertaken in order to promote the territorial ambitions of a particular state. The increasing involvement of non-state actors in armed conflicts and cyber attacks also raises concerns about the attribution issues that are prevalent in cyber conflicts. While devising rules of state responsibility, states should be conscious of the difficulty in identifying the perpetrators of cyber attacks. The ease of launching and financing cyber warfare must also be acted upon.[58]

Conclusion

As a new forum, cyberspace contains many uncertainties, but this does not preclude international law from being applicable to cyberspace. In the perspective of international law, the discussion on cyberspace has focused on the use of force. Cyber attacks that are not designated as use of force or violative of Article 2(4) of the U.N. Charter have often been considered to be unproblematic, although they often constitute illegal intrusion into the sovereignty of other states. Nevertheless, it is not absolutely clear as to how the principles of international law operate in this field. States have not been very proactive in clarifying these issues, nor have they shown any initiative to frame a new set of legal instruments for the same, and hence the lack of *opinio juris* coupled with the lack of state practices to rely on create problems for a comprehensive understanding of this field.[59]

Since some states are perceived as being cyber sanctuaries, i.e. they are breeding grounds for cyber operations into other territories, these states mostly interpret their duty to end harmful cyber activities as undertaking preventive measures alone. This may be justified on the grounds that extensive monitoring of cyber infrastructure will raise concerns surrounding privacy and policy matters.[60]

However, it is unlikely that such a laissez-faire approach is sustainable. Given the lack of conclusive state practices and the infancy of the law of self-defence, non-destructive cyber operations have not risen to the level at which they would be regarded as armed attacks. However, states over time will start treating such cyber operations as armed attacks to which they may respond forcefully when the

---

58 Collin S. Allan, *Attribution Issues in Cyberspace*, 13(2) Kent Journal of International and Comparative Law 78 (2013).

59 Kesan & Hayes 2011, at 18.

60 Schmitt 2014, at 277.

consequences are grave. The dangerous potential of cyber operations will raise such threats to security that the evolution of the law of self-defence will become inevitable. As cyber activities become crucial to the functioning of societies, the law will adapt by allowing them enhanced protection. The law will require states to act as responsible inhabitants of the cyber domain and lower the threshold at which cyber operations are said to violate the prohibition on the use of force, empowering states to respond forcefully and increase protection of cyber activities during armed conflicts. These transitions will not be free of cost and will encounter obstacles such as privacy concerns, etc., but states will eventually realise that it is in their interest to take measures to safeguard access to cyberspace.[61]

In order to attribute responsibility, target states will need to discover ways in which to improve the level of knowledge of the states which are the bases for launching cyber operations. Apart from preventing trans-boundaries harm, states are also obligated to cooperate with victim states that face adverse cyber effects on infrastructure either located in their territory or under their governments' control if the effects pose a threat to international peace.[62] All states should pass strict criminal laws and conduct vigorous investigations and prosecution of attackers, and also cooperate with the victim states in order to discourage non-state actors.

The claim that cyberspace is disjoined from state sovereignty can be dismissed on the basis of five principal considerations. First, in order for cyberspace to function and to even exist, there must be an entity controlling it and a physical infrastructure which is territorially grounded for providing access to users. Second, financial relationships in cyberspace require laws to govern them that are usually the laws of states, and this is proof of the fact that cyberspace is subject to state sovereignty. Third, the content transmitted through cyberspace has implications in the real world and hence is subject to the laws of the respective states since they have an interest in as well as legitimate control over cyber transactions. Fourth, states are gradually attempting to assert themselves in cyberspace for purposes of national security and, in order to prevent harm and reduce their vulnerability, they cannot afford to leave cyberspace ungoverned. Fifth, like the real world, cyberspace also requires state sovereignty for regulating, protecting and punishing various actors.[63]

As a result, to translate sovereignty in cyberspace into reality states should arrive at a consensus on the underlying norms based upon which an international regime can be founded. The right to access may be allowed to all for peaceful ends, but all should have the legitimate right to protect their sovereignty in this domain. States must assert and crystallise their interests in order to exercise more control. It is also important for states to cease being silent on issues that violate their sovereignty

61 Schmitt 2014, at 299.

62 Jensen 2015.

63 Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 Air Force Law Review 11–14 (2009).

and they must not refrain from publicly acknowledging this, as this would help in future endeavours to establish sovereignty. States would also be required to enter into agreements for creating attribution mechanisms to facilitate identification. Furthermore, they should be capable of controlling the cyber domain and responding to intrusive violations of cyber sovereignty as well.[64]

References

Allan C.S. *Attribution Issues in Cyberspace*, 13(2) Kent Journal of International and Comparative Law 78 (2013).

Delibasis D. *State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century*, 8 Peace Conflict and Development: An Interdisciplinary Journal 13 (2006).

Franzese P.W. *Sovereignty in Cyberspace: Can It Exist?*, 64 Air Force Law Review 1 (2009).

Goldsmith J.L. *The Internet and the Abiding Significance of Territorial Sovereignty*, 5(2) Indiana Journal of Global Studies 475 (1998).

Heinegg W.H.V. *Legal Implications of Territorial Sovereignty in Cyberspace* in *4th International Conference on Cyber Conflict* 7 (C. Czosseck et al. (eds.), Tallinn: NATO CCD COE Publications, 2012).

Hoisington M. *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32(2) Boston College International and Comparative Law Review 439 (2009).

Hojatzadeh A. & Jafari A. *Cyber-attacks and Jus Ad Bellum*, 1(2) International Journal of Humanities and Social Sciences 76 (2014).

Jensen E.T. *Cyber Sovereignty: The Way Ahead*, 50(2) Texas International Law Journal 275 (2015).

Kesan J.P. & Hayes C.M. *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25(2) Harvard Journal of Law & Technology 415 (2012).

Kesan J.P. & Hayes C.M. *Self Defense in Cyberspace: Law and Policy*, Illinois Public Law and Legal Theory Research Paper Series No. 11-16 (2011).

Koh H.H. *International Law in Cyberspace*, Yale Law School Faculty Scholarship Series, Paper 4854 (2012).

Lewis J.A. *A Note on the Laws of War in Cyberspace*, Center for Strategic and International Studies (April 2010).

Li S. *When Does Internet Denial Trigger the Right of Armed Self-Defense?*, 38(1) Yale Journal of International Law 179 (2013).

Lotrionte C. *State Sovereignty and Self-defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, 26(1) Emory International Law Review 825 (2012).

Perritt H.H., Jr. *Cyberspace and State Sovereignty*, 3 Journal of International Legal Studies 155 (1997).

[64] Franzese 2009, at 28–32.

Poché C.C. *This Means War! (Maybe?) – Clarifying Casus Belli in Cyberspace*, 15 Oregon Review of International Law 413 (2013).

Roscini M. *World Wide Warfare – Jus ad bellum and the Use of Cyber Force*, 14 Max Plank Yearbook of United Nations Law 85 (2010).

Schmitt M.N. *The Law of Cyber Warfare: Quo Vadis?*, 25(2) Stanford Law & Policy Review 275 (2014).

Shackelford S.J. & Andres R.B. *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42(4) Georgetown Journal of International Law 971 (2010–2011).

Tallinn Manual on the International Law Applicable to Cyber Warfare (M.N. Schmitt (ed.), Cambridge: Cambridge University Press, 2013).

Information about the author

Pallavi Khanna (New Delhi, India) – Judicial Clerk-cum-Law Researcher at the Hon'ble High Court of Delhi (B 52 Hill View Apartments, Vasant Vihar, New Delhi, 110057, India; e-mail: pallavi.nls17@gmail.com).