THE CENTRE FOR internet & society

The Potential for the Normative Regulation of Cyberspace: Implications for India

BY
Arindrajit Basu

EDITED BY
Elonnai Hickok, Sunil Abraham, Udbhav Tiwari

RESEARCH ASSISTANCE
Tejas Bharadwaj

The Centre for Internet and Society, India

Designed by **Saumyaa Naidu**

Acknowledgements

The author would like to thank Tim Maurer of the Carnegie Endowment for International Peace for his comprehensive and insightful comments on this report. All errors and inaccuracies remain my own.

Contents

Executive Summary

The standards of international law combined with strategic considerations drive a nation's approach to any norms formulation process. With the cyber norms formulation efforts in a state of flux,India needs to advocate a coherent position that is in sync with the standards of international law while also furthering India's strategic agenda as a key player in the international arena.

This report seeks to draw on the works of scholars and practitioners, both in the field of cybersecurity and International Law to articulate a set of coherent positions on the four issues identified in this report. It also attempts to incorporate, where possible, state practice on thorny issues of International Law. The amount of state practice that may be cited differs with each state in question.

The report provides a bird's eye-view of the available literature and applicable International Law in each of the briefs and identifies areas for further research, which would be useful for the norms process and in particular for policy-makers in India.Historically, India had used the standards of International Law to inform it's positions on various global regimes-such as UNCLOS and legitimize its position as a leader of alliances such as the Non-Aligned Movement and AALCO. However, of late, India has used international law far less in its approach to International Relations. This Report therefore explores how various debates on international law may be utilised by policy-makers when framing their position on various issues. Rather than creating original academic content,the aim of this report is to inform policy-makers and academics of the discourse on cyber norms.In order to make it easier to follow, each Brief is followed by a short summary highlighting the key aspects discussed in order to allow the reader to access the portion of the brief that he/she feels would be of most relevance. It does not advocate for specific stances but highlights the considerations that should be borne in mind when framing a stance.

The report focuses on four issues which may be of specific relevance for Indian policy-makers. The first brief, focuses on the Inherent Right of Self-Defense in cyberspace and its value for crafting a stable cyber deterrence regime. The second brief looks at the technical limits of attributability of cyber-attacks and hints at some of the legal and political solutions to these technical hurdles. The third brief looks at the non-proliferation of cyber weapons and the existing global governance framework which india could consider when framing its own strategy. The final brief looks at the legal regime on counter-measures and outlines the various grey zones in legal scholarship in this field. It also maps possible future areas of cooperation with the cyber sector on issues such as Active Cyber Defense and the legal framework that might be required if such cooperation were to become a reality.Each brief covers a broad array of literature and jurisprudence and attempts to explore various debates that exist both among international legal academics and the strategic community.

The ongoing global stalemate over cyber norms casts a grim shadow over the future of cyber-security. However, as seen with the emergence of the nuclear non-proliferation regime, it is not impossible for consensus to emerge in times of global tension. For India, in particular, this stalemate presents an opportunity to pick up the pieces and carve a leadership position for itself as a key norm entrepreneur in cyberspace.

Introduction

Information Communication Technologies (ICTs) are intricately woven into every aspect of routine existence worldwide. The increasing global links created through cyberspace has spurred concerted attempts to create norms that regulate its use and guarantee its security. Yet, the normative push to secure cyberspace has faced backlash from alliances of states that view norm-creation as a political strategy that further entrenches the leverage occupied by the economically and militarily powerful states.[1] This report seeks to articulate the areas of convergence in normative discourse, highlight the positions of key-stakeholders and in doing so, outline a set of strategies that India could adopt to contribute to the norms high table in cyberspace.

There have been multiple gambits to secure the governance of cyberspace through the universal acceptance of 'cyber norms' that stem from accepted standards in International Law. The United Nations Group of Governmental Experts (UN-GGE)[2] Reports, the Global Commission for Stability in Cyberspace (GCSC)[3] the Tallinn Manual[4] and the initiative of the Carnegie Endowment for International Peace towards a norm protecting financial stability[5] are cases in point. Other normative efforts include efforts in specific interest areas[6] or among groups of like-minded states, such as regional organisations.[7]

According to noted International Affairs scholars Martha Finnemore and Duncan Hollis, these projects thus far share a common Achilles Heel.[8] They view norms as products and focus on what norms should say rather than how they will play out given the varying socio-economic realities across states. This deracinated approach to the norms formulation process has possibly been responsible for two major fetters to the formation of an effective normative regime for the regulation of cyberspace.[9]

First, there has been insufficient attention paid to the global social, economic and cultural contexts in which norms evolve, which could be responsible for a lack of universal consensus on the substantive content of norms, as was exemplified by the recent breakdown of talks in the fifth UN-GGE in 2017.[10] Like other existing technological infrastructure, the internet is a

1 Michael Schmitt and Liis Vihul, "International Law Politicized: The UN GGE's failiure to advance cyber norms," Just Security, Jun 30 2017, accessed Nov 18,2017, at <https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/> [hereinafter 'Schmitt Just Security']

2 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, paras. 9–15,UN Doc. A/70/174 (July 22, 2015) [hereinafter 2015 GGE Report].

3 Global Commission on stability of cyberspace, accessed July, 12, 2018, https://cyberstability.org/

4 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, paras. 9–15,UN Doc. A/70/174 (July 22, 2015) [hereinafter 2015 GGE Report].

5 Protecting Financial Stability, Carnegie Endowment for International Peace, accessed July 10, 2018, at <http://carnegieendowment.org/specialprojects/ProtectingFinancialStability>

6 For example, see Wassenaar Arrangement, at <http://www.wassenaar.org> (export controls regarding intrusion software and IP network surveillance systems);

7 As an example, the Shanghai Cooperation Organization (SCO) has published two international codes for cybersecurity

8 Martha Finnemore and Duncan Hollis, " Constructing norms for global cybersecurity", 110 American Journal of International Law 3 (2016),425-479,at 427 [hereinafter 'Finnemore and Hollis']

9 Ibid, at 427

10 Schmitt Just Security, (supra 1); Arun Mohan Sukumar," The UN-GGE failed: Is International Law in cyberspace doomed?",Lawfare, July 4,2017, accessed Nov, 18, 2017, https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well [hereinafter Arun Mohan, cyberspace doomed?]

product of contested social action and shapes social behaviour by crafting goals aligned with the stakeholders who define it.[11] Therefore, internet governance could easily be condemned to a hegemonic pursuit by the most powerful players in the technological space-that necessitates a more realistic approach to cyber norms formation and internet governance. Second, even if there may be universal consensus on substantive norms, they become ineffective as tools that could enforce the regulation of cyberspace and further cybersecurity, if created without keeping the process in mind. As Finnemore and Hollis argue further, norm cultivation occurs out of specific contexts following a period of concerted interaction among the key actors involved.[12] While these briefs largely tackle the substantive aspects of cyber norms, it is also crucial that the international community works towards improving the process underpinning norm proliferation by considering prior analogous regimes while considering the unique nature of cyberspace.[13]

Primer on Normative Development at the United Nations

As Lucas Kello has authoritatively demonstrated in *The Virtual Weapon*[14], cyberspace has uprooted conventional models of thinking on the International System, which recognize states as the protagonists in a global 'ordering system'[15] with 'constitutional normative principles.'[16] He identifies three orders of cyber-revolution. Third-order revolution or systemic disruption results in drastic changes within the confines of the existing state structure.[17] The drastic changes happen in both the material ingredients of power which are, in in this case, defined by (1) A change in the physical architecture that defines power at the international level and (2) A change in the norms and rules which govern interactions between states. He then identifies second-order cyber revolution, which is brought about when a state or a group of states reject the shared purpose of the existing units, (systems revision) which may be exemplified by North Korea's weaponization of cyberspace.[18] Finally, first-order cyber revolution sees a change in the relative arrangement of building blocks of the international system which has resulted due to the increased proliferation of non-state actors in the cyber arena.[19] (systems change)

The possibility of a cyber- attack caused Russia in 1998 to propose a treaty at the United Nations that would regulate and restrict the utilization of cyber-attacks and cyber weapons.[20]

---

11 Claudia Aradau, " Security that matters: Critical infrastructure and objects of protection" 41 Security Dialogue 5 (2010), 491–514; Tim Stevens, " Cyberweapons: Power and governance of the invisible" International Politics (2017)

12 Finnemore and Hollis, (supra 8) at 428

13 Elonnai Hickok and Arindrajit Basu,"Conceptualizing an International Security Regime for Cyberspace" (Briefings of the Research and Advisory Group, Bratislava, May 2018) at <https://cyberstability.org/wp-content/uploads/2018/06/GCSC-Research-Advisory-Group-Issue-Brief-2-Bratislava-1.pdf> 37-73,63-73 for a set of recommendations

14 Lucas Kello The Virtual Weapon and International order, (YUP 2017) 82 [hereinafter The Virtual Weapon].

15 Kenneth Waltz, Theory of International Politics (New York,McGraw-Hill,1979) For Wlt, the organising principle is the absence of centralised government, therefore leaving sovereign states as the supreme organising units.

16 Hedley Bull, The Anarchical Society: A study of Order in World Politics (London, Macmillan, 1995),67-68.

17 The Virtual Weapon, (supra 14) at 86.

18 Ibid, at 90.

19 Ibid,at 92.

20 James Andrew Lewis, " Revitalizing Progress on International Negotiations in Cybersecurity" in Osler Hampson and Michael Sulmeyer, Getting Beyond Norms:New approaches to cybersecurity challenges (Centre for Governance and Innovation, 2017), 13

The initial proposal was based on norm proliferation in the fields of arms control and disarmament.[21] At the time, this proposal was opposed by the United States and found little support. Academic literature on the development of an international cyber security convention was also discarded as impractical and failed to gain traction within the United Nations.[22]

Further research on non-binding norms and confidence building measures as alternatives to the development of a full-fledged treaty regime lead to the international community pivoting towards this approach.[23] They attempted to follow the norms-driven approach set up through regimes such as the Missile Technology Control Regime (MTCR).[24] This resulted in the birth of the UN-GGE process. The GGE was set up in 2004 and comprised of independent experts from 15 states.[25] This group designed to advise the UN on promoting peace and stability in cyberspace. Even though the first UN-GGE was unable to agree upon a report, the second GGE was able to garner more consensus and released a report in 2010. The third GGE presented its report in 2013 and agreed on a set of founding norms for the governance of cyberspace.[26] The document expressed that international law, state sovereignty and human rights were applicable to the governance of cyberspace. Further, the report also stated that states must not use non-state proxies to commit cyber- attacks on other states or allow non-state actors to use their territory for the launching of cyber-attacks.[27]

The 2015 report of the fourth UN-GGE elaborated on these concepts and laid down a comprehensive framework for further discussion on cyber norm evolution.

Section III of the report lays down several norms, rules and principles for responsible state behaviour in cyberspace.[28] These include

- Not knowingly allowing their territory to be used for the commission of internationally wrongful acts using Information Communication Technologies (ICTs);
- To cooperate for the exchange of information using ICTs
- Refraining 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
- To not knowingly supporting ICT activity contrary to the principles of international law.

Failure of 2017 GGE

Drawing from what appeared to be universal consensus on the norms process a fifth GGE was instituted by the United Nations “to study, with a view to promoting common understandings,

21 Ibid

22 Ibid

23 Ibid

24 Arms Control Association,”The Missile Technology Control Regime at a glance” (July 2017) , https://www.armscontrol.org/factsheets/mtcr

25 Elonnai Hickok and Arindrajit Basu,”Conceptualizing an International Security Regime for Cyberspace” (Briefings of the Research and Advisory Group, Bratislava, May 2018) at <https://cyberstability.org/wp-content/uploads/2018/06/GCSC-Research-Advisory-Group-Issue-Brief-2-Bratislava-1.pdf> 59

26 David Fidler, “The GGE on Cybersecurity: How International Law Applies to Cyberspace, “NET POLITICS Apr. 14, 2015, accessed July 1, 2018, at <http://blogs.cfr.org/cyber/2015/04/14/the-un-gge-on-cyber-issues-how-international-law-applies-to-cyberspace/>.

27 See Tim Maurer, Cyber Mercenaries: The State,Hackers and Power (Cambridge University Press, 2018)

28 2015 GGE Report, para 12 (Supra 2)

... how international law applies to the use of information and communications technologies by States, as well as norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building...." [29] However, due to what cyber security and International Law expert and chair of the Tallinn Manual Process, Prof. Michael Schmitt terms the 'politicization of cyber norms,'[30] the UN-GGE was not able to arrive at consensus due to stonewalling by Cuba and reportedly China and Russia. Gauging from Cuba's publicly available statement[31], the UN-GGE disagreed on three fundamental questions. It appears from their statement that they believe that applying the traditional rules of international law to the cybersphere would convert it into a 'theatre of military action' and legitimize unilateral punitive sanction. Mike Schmitt criticizes this position -claiming that it has no validity in international law and is being utilised by states to gain an asymmetric strategic advantage. The states engaging in the stonewalling are rarely the victims of unlawful cyber attacks.[32] Further, as stated by Arun Mohan Sukumar, the dissenting states did not want the rules of the game to be dictated by militarily advanced states.[33] Sukumar goes on to criticise this approach, even in terms of its strategic validity as predictability in cyberspace is an end that all states should desire. De-legitimizing the progress made by the 2016-17 GGE through an excessive focus on International Law was thus possibly a flawed approach.[34]

The only two publicly available statements made by state representatives to the GGE are those of Cuba and the United States. It appears therefore that the GGE broke down due to a lack of consensus on

1. Response to internationally wrongful acts (countermeasures in cyberspace), (Will be discussed in Brief 4)
2. Self-Defence in cyberspace, (Will be discussed in Brief 1)
3. The applicability of International Humanitarian Law to cyberspace.

The Core Divide Among State Parties Since the Commencement of the GGE Process

A crucial fissure in the norms formation process revolves around the question of sovereignty.[35] The Sino-Russian view suggests that sovereignty in international law is absolute and no entity other than the sovereign state itself can limit the exercise of this power.[36] Consequently, both Russia and China believe that each country should have the right

29 Schmitt Just Security (Supra 1)

30 It may be argued that the process was always 'political' but the disagreements have become more intense.

31 Declaration by Miguel Rodriguez, Representative of Cuba, At the final session of group of governmental experts on developments in the field of information and telecommunications in the context of international security (June 23 2017), at <https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf> [hereinafter Cuban Declaration]

32 Schmitt Just Security (Supra 1)

33 Arun Mohan, cyberspace doomed? (supra 10)

34 Ibid

35 Eneken Tikk and Mika Kerttunen, The Alleged Demise of the UN-GGE: An autopsy and eulogy (Cyber PolicyInstitute,2017), at 17, at <http://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf>, accessed January 6 2018. [hereinafter 'Tikk and Kerttunen']

36 Report of UN Secretary General, Developments in the Field of Information and Telecommunications in the Context of International Security UN Doc A/61/161 (July 18, 2006); Jinghan Zeng, Yaru Chen and Tim Stevens, "China's solution to global cyber governance: Unpacking the Domestic Discourse on 'Internet Sovereignty' 45 Politics and Policy 3 (2017), 432-464[hereinafter 'Zeng, Chen and Stevens']

to manage and define its 'network frontiers'[37] through domestic legislation or state policy. According to this view, each country has the right to patrol information at its cyber borders- a view which has been a principled stand in accordance with their long-time reading of International Law.[38] They believe that ICTs come laden with foreign influence and can disrupt the sovereign authority of the concerned state[39], which is directly at odds with the desire of the US and like-minded states to preserve the free-flow of information.The Russian chair of the 2004/2005 GGE stated that issues of 'international informations security' must be discussed and understood in light of the global information revolution.[40]

The UK and US have repeatedly stated that the use of the term in this fashion indicates that information itself is a security threat which must be guarded against.[41] As per their position, excessive focus on 'information security' could potentially spiral a shift towards a position where the internet no longer serves as a platform for the rapid exchange of discourse and ideas but as domains of excessive sovereign regulation.[42] On May 23rd, 2018, the United Kingdom's Attorney General Jeremy Wright gave a speech at Chatham House on the role of international law in cyberspace[43], which was the first official proclamation of UK's broad view on this topic. He argued that it is crucial for states to clearly articulate their understanding of international law, especially in cyberspace. Dynamic and rapidly evolving norms makes the framing of clear rules challenging.[44] He further proclaimed that states have a responsibility to be clear about how international laws bind them- a responsibility that extends to cyberspace. he also affirmed the conclusions of the UN Expert Group 2015 Report and made several other observations, which will be discussed in the relevant brief.

The alleged Russian interference in the U.S. elections through the spread of fake misinformation and 'fake news' via social media platforms has resulted in calls for the re-evaluation of this stance and assess these actions against existing international law and

---

37 Yuan Yi,. "网络空间的国界在哪 " [Where Are the National Borders of cyberspace]? 学习时报.May 19, 2016. accessed Jan 06, 2018. at <http://www.studytimes.cn/zydx/KJJS/JUNSZL/2016-05-19/5690.html> cited in Zeng, Chen and Stevens (supra 36) at 449

38 Ibid; Tikk and Kerttunen, (supra 35) at 17; Alex Grigsby, The End of Cyber Norms, 59 Survival, 6 (2017) 109-122, at 111

39 Yu Li . "如何认识与维护互联网主权" [How to Understand and Protect Internet Sovereignty]. PeoplesDaily.February 2, 2012, accessed July 11, 2018 at <http://media.people.com.cn/GB/16996575.html>

40 A/C.1/60/PV.13, page 5.;See also 2000 Information Security Doctrine of the Russian Federation that was re-adopted in 2008 and remained in force until December 2016 when a new Doctrine on Information Security of the Russian Federation was adopted. See further the Chinese contribution in 2006, whereby the free flow of information should be guaranteed under the premises that national sovereignty and security must be safeguarded and that the historical, cultural and political differences among countries be respected (Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/61/161) in Tikk and Kerttunen, (supra 35) at 18

41 United Kingdom, Submission to the United Nations General Assembly Resolution UN Doc A/68/156 (July 16, 2013), p. 15; See Tim Maurer and Robert Morgus, "Compilation of Existing Cybersecurity and Information Security Related Definition"(New America Foundation, October 2014)

42 Ibid

43 Office of ATTY GEN.Jeremy Wright, Cyber and International law in the 21st Century, Government of UK (Gov.uk) May 23, 2018, accessed July 13, 2018 at <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> [hereinafter Wright speech]

44 Isa Qasim, "United Kingdom Attorney General's Speech on International Law and Cyber" Just Security, May 23,2018, accessed July 11, 2018 at <https://www.justsecurity.org/56853/united-kingdom-atty-generals-speech-international-law-cyber-key-highlights/>

national security strategy and thus amend domestic policy accordingly.[45]

The ideological split on the nature of cyberspace has also resulted in two radically different approaches on how to regulate it. Russia's approach since the late 1990s later joined by China and SCO articulates that there should be a new treaty focusing on information security because existing international law is not sufficient to regulate it.[46] They believe that existing tenets of customary International Law cannot apply to cyberspace and the creation of a new *lex specialis* (specific law) through the drafting of a treaty that regulates cyberspace is required.[47] The United States argues existing international law applies. In addition, instead of a legally binding treaty, 'soft law' non-binding voluntary norms can address potential gaps/ activities during peacetime.[48] It has apply existing tenets of International law to cyberspace without creating a new treaty and promoting these tenets aggressively.[49]

There are pros and cons to both approaches. The US approach accepts the applicability of International Law when governing cyberspace. The absence of a detailed treaty crafting out specific obligations provides room for legal and strategic maneuvering by states through a description of the regime on cyber security using 'soft language' such as 'norms' or 'principles.' It gives them enough flexibility to interpret existing tenets of International Law in a manner that suits their national security interests through what has been appropriately termed 'Lawfare.'[50] If stability in cyberspace is to be a strategic objective, this regime might only work if it is backed by constant Confidence-Building Measures that explore the practical form these norms may take.[51] The treaty-based approach casts far stronger obligations but given that there is a fundamental divergence in how states view cyber governance, the contents of this treaty seem difficult to predict. India's approach to the norms formulation process for cyberspace should take into account the potential of its current adversaries in the South Asian region and the large extent of its vulnerabilities[52] given its rapidly digitising economy. Stability and deterrence in cyberspace should be a priority for India with a focus on Confidence Building Measures with regional allies on the safety and stability of cyberspace.

---

45 Herb Lin,Election interference as we understand it today is not a cybersecurity issue", Lawfare,Jan 5, 2018, accessed January 6, 2018, at <https://www.lawfareblog.com/election-interference-we-understand-it-today-not-cybersecurity-issue>; Ryan Goodman, " International Law and the US Response to Russian election interference," Just Security, January 5,2017, accessed Jamuary 6th 2018, at <https://www.justsecurity.org/35999/international-law-response-russian-election-interference/>

46 Dylevsky, I.N. et al, "Political and Military Aspects of the Russian Federation's State Policy on International Information Security" Military Thought 24:1 (2015)

47 Ibid

48 Martha Finnemore, 'Cultivating International Cyber Norms', in Kristin M. Lord and Travis Sharp (eds), America's Cyber Future: Security and Prosperity in the Information Age (Washington DC: Center for a New American Security, June 2011), at <https:// citizenlab.ca/cybernorms2011/cultivating.pdf>

49 Ibid

50 Charles J. Dunlap, Jr., Lawfare Today...and Tomorrow, in International Law and the Changing Character of War 315-325 (Raul A. "Pete" Pedrozo & Daria P. Wollschlaeger eds., 2011) (US Naval War College International Law Studies, Vol. 87, 2011)

51 Elana Broitman, Mailyn Fidler and .Robert Morgus, "Promoting an International Security Architecture for Cyberspace" (Briefings from the Research and Advisory Group of the Global Commission on Stability of Cyberspace, 2018) 21

52 See for example, Harish Khare " Beyond the Aadhaar security breach", The Tribune, Jan 7,2018, accessed May 23, 2018, at <http://www.tribuneindia.com/news/sunday-special/columns/beyond-the-aadhaar-security-breach/524482.html>

While bearing the strategic and pragmatic elements of these negotiations in mind, it is important for India to not lose sight of the usefulness of existing standards of International Law in the process. It is important to consider that law and norms are not conflicting or entirely congruent but interrelated processes. As Harvard Law Professor Lawrence Lessig notes-law can create, change or displace the meaning of social norms.[53] International Law provides legitimacy to the evolution of cyber norms and could influence collective expectations regarding the impropriety of actions in cyberspace.[54] International legal regimes including outer space, the deep seabed and the economic exploitation of marine resources have now lead to the fermentation of stable normative regimes that influences state practice today.[55] Both independently and through regional or multilateral mechanisms such as the Asian-African Legal Consultative Organisation (AALCO), India was an active norm entrepreneur in some of these negotiations.[56]

The Path Forward in the Formulation of India's Strategy

It is appropriate therefore for India to attempt to pick up the pieces from the 2017 GGE and craft a position on the normative regulation of cyberspace that is in consonance with its foreign policy and national security strategy. Historically, India had used the standards of International Law to inform it's positions on various global regimes-such as UNCLOS and legitimize it's position as a leader of alliances such as the Non-Aligned Movement and AALCO. However, of late, India has used international law far less in its approach to International Relations.[57] This Report therefore explores how various debates on international law may be utilised by policy-makers when framing their position on various issues.

The first step is to put forward a coherent proposal on each of the unclarified issues in the UN-GGE process that is in consonance with International Law. India has been a part of 4 out of the 5 UNGGE processes.It was left out of the 2015 GGE which made remarkable progress due to the geographical rotation rule.[58] As india had been part of the 2013 GGE process, it had to make way for another country from the same region.[59] The seat went to Pakistan. Despite that, India has demonstrated a steadfast approach to a multi-stakeholder model on internet governance that brings together a diversity of states and other entities in a bid to design this framework.[60] It won its seat back in the 2016-17 GGE.

---

53 Lawrence Lessig, "The Regulation of Social Meaning", 62 U Chicago Law Review (1995) 943.

54 Elonnai Hickok and Arindrajit Basu,"Conceptualizing an International Security Regime for Cyberspace" (Briefings of the Research and Advisory Group, Bratislava, May 2018)<https://cyberstability.org/wp-content/uploads/2018/06/GCSC-Research-Advisory-Group-Issue-Brief-2-Bratislava-1.pdf>

55 Nico Schrijver, " Managing the global commons: common good or common sink?" 7 Third World Quarterly (2016) 1252-1267;Elonnai Hickok and Arindrajit Basu,"Conceptualizing an International Security Regime for Cyberspace" (Briefings of the Research and Advisory Group, Bratislava, May 2018)<https://cyberstability.org/wp-content/uploads/2018/06/GCSC-Research-Advisory-Group-Issue-Brief-2-Bratislava-1.pdf> 37-73

56 V.S. Mani, Exclusive Economic Zone: AALCO's Tribute to the Modern Law of the Sea, in Fifty Years of AALCO : Commemorative Essays in International Law (AALCO Secretariat, New Delhi 2007), 41-61

57 Arun Mohan Sukumar,"How India lost its way in the study and use of International Law "Wire Apr 02 ,2018 accessed May 13 2018 at <https://thewire.in/diplomacy/india-is-lagging-behind-in-the-study-and-use-of-international-law>

58 Arun Mohan Sukumar, UN Reconstitutes its Top Cyber Body, This time with India at the High Table, Wire June 22 2016, accessed July 2, 2018, at <https://thewire.in/44696/un-reconstitutes-its-top-cyber-body-this-time-with-india-at-the-high-table/>

59 Ibid

60 Ibid

As reported by the Wire in September, 2017, India has formed a body under the aegis of the National Security Council Secretariat (NSCS) with Asoke Mukherji, former permanent representative to the United Nations at its helm for the purpose of studying cyber norms and articulating India's strategy on the process[61] This is a positive step and has strengthened India's image on strategic issues concerning cyber governance and has the potential to catapult it to a leadership position in the framework of norms and law governing cyberspace.

In this context, it is useful for India to consider the Tallinn Manual that was drafted by nineteen International law experts at the invitation of the NATO Cooperative Cyber Defence Centre for Excellence and considered how rules of International Law may be applicable in cyberspace.[62] Deputy National Security Advisor Dr. Arvind Gupta has acknowledged rightly that while it is an useful exercise, Tallinn Manual does not reflect the current state of International Law in cyberspace due to a lack of state practice which is a prerequisite for the formation of customary International Law.[63] Indeed, While the rules articulated in the Manual are far from being accepted by the international community, they serve as indicative guidelines on the direction the norms formulation process can take. Further, state responses to the Tallinn Manual and the reasons for disagreements with the standards put forward are essential perspectives to consider as India cements its cyber norms strategy.

Some Chinese scholarship, for example, has also offered substantive criticism of the first Tallinn Manual process.[64] Chinese scholar Chen Qi notes that the commentary features disagreement between the Experts drafting the Manual and can therefore not reflect a position of any validity in international law. He criticises it for attempting to create new norms of cyber law.'[65] For instance, he argues that the factors advocated for judging whether an attack amounts to a 'use of force' were taken from Mike-Schmitt's earlier work. Considering that Schmitt was associated with the US Naval War college, Qi dismisses the Manual as an American gambit to hegemonize the norms process.

While Qi's criticism is valid from a Chinese perspective, it is crucial that we do not dismiss the Tallinn Manual in its entirety. While the positions expressed in the Manual are that of the Group of Experts and not the international community as a whole or even that of certain states, it does offer standard guidelines that helps us navigate thorny questions on the applicability of the use of force and self-defence in cyber-space.

It is also vital for India to consider International Human Rights Law in the framing of its cyber security strategy. This body of law had its origins in the period immediately succeeding the Second World War adopted a gamut of instruments that are collectively considered the 'International Bill of Human Rights.'[66] Naturally, these instruments did not consider the contemporary challenges posed through engagement online but that does not necessarily

---

61 Anuj Srivas, After UN Talks on Cyber Norms Collapse, India Starts Chalking Out Own Strategy, Wire, September 12, 2017, accessed July 3, 2018 at <https://thewire.in/176418/un-cyber-norms-india-asoke-mukerji-nsc/>

62 Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare(Cambridge University Press ,2017) [hereinafter 'Tallinn Manual 2.0']

63 Dr. Arvind Gupta, Keynote address by Dr Arvind Gupta, Deputy national Security Advisor at the 18th Asian Security Conference on "securing Cyberspace: Asian and International Perspectives" Institute for Defence Studies and Analyses, February 10, 2016, accessed June 11, 2018, at <https://idsa.in/keyspeeches/18asc-securing-cyberspace-asian-and-international-perspectives_deputy-nsa>

64 Julian Ku, " How China's view on jus ad bellum will shape its view on cyberwarfare" Aegis Series Paper No. 1007 (2017),18

65 Chen Qi 陈颀, Wangluo Anquan, Wangluo Zhanzheng Yu Guojifa 网络安全、网络战争与国际法 [Network security,network warfare and international law], Zhengzhi Yu Falv 7《政治与法律》(2014): 147.

66 The International Bill of Rights consists of the Universal Declaration of Human Rights (1948); the International Covenant on Civil and Political Rights (1966) and the two Optional Protocols annexed thereto; and the International Covenant on Economic, Social and Cultural Rights (1966) and its Protocol

mean that Human Rights Law are rendered obsolete in the cyber realm.[67] Given the extent to which our daily lives are captured online, it is imperative that these standards serve as the edifice for the evolution of norms that genuinely safeguard human dignity online.[68]

Security should therefore be considered a positive concept-a state of feeling secure rather than the mere absence of harm.[69] Through consultation with various stakeholders in the thick internet governance ecosystem, it is important that India does not use the 'trump card' of national security to deny individuals fundamental rights-such as the Right to Privacy or Freedom of Expression as that would lead to a state of affairs where citizens feel less secure.[70]

Alternative Initiatives in the Norms Formulation Process

While it is crucial that India does not lose sight of the progress made at the UN-GGE till 2015 and does not lose sight of its bearings on that front, there are multiple other initiatives[71] that India has and could get involved with in order to articulate its strategy for norms governing cyberspace.[72] A fragmented approach to cybersecurity may not fulfill the goal of regulating cyberspace but it could be a potential catalyst for a stable international system as it would allow for some certainty in the formation of strategic alliances and in national approaches to cyberspace. Further, given the nature of contestation in cyberspace and the present lack of consensus on applicable International Law, fragmentation, through regional or strategic groupings may be the way forward in the short-run till universal minimum core markers of consensus may be found. Universal regimes, such as United Nations Convention on the Law of the Sea (UNCLOS) have flourished despite fragmentation in their initial stages.[73]

Multilateral

Starting with strategic groupings, India has endorsed the Joint Statement made by the BRICS leaders at Xiamen in September, 2017 and prioritised the equal participation of all states in cyber governance and the need to make structures that regulate cyberspace more representative and inclusive.[74] This critique applies to the GGE process where the P5 have participated in all 5 GGE processes . Estonia, Belarus, Brazil and India have participated in

67 Kubo Macak,"From cyber norms to cyber rules: Re-engaging states as lawmakers"Leiden Journal of International Law (2017),877,884; See Annex to this report documenting human rights considerations India should be looking at when framing its cyber strategy

68 UN GA, Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet, para. 1, UN Doc. A/HRC/20/L.13, (June 29, 2012); UN GA, Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet, para 1, UN Doc. A/HRC/32/L.20, (June 27 2016). GGE Report 2015 (supra 2), at 8, para. 13(e) and at 12, para. 26; Tallinn Manual 2.0 (supra 62) at 179

69 Anja Kovacs and Dixie Hawtin, "Cyber Security,Cyber Surveillance and Online Human Rights" Stolkholm Internet Forum, 2013, accessed July 2, 2018, at <https://www.gp-digital.org/wp-content/uploads/pubs/Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf>

70 Jennifer A. Chandler, "Personal Privacy versus National Security: Clarifying and Reframing the Trade-off" in Kerr, Lucock and Steeves, eds. On the Identity Trail: Anonymity, Privacy and Identity in a Networked Society, (Oxford Univ. Press, 2009) pp. 121-138.

71 Hickok & Basu, Bratislava Briefing (supra 54)

72 See compendium at Cyber Norm Index, Carnegie Endowment for International Peace, accessed July 17, 2018, at <http://carnegieendowment.org/publications/interactive/cybernorms#formal-names>

73 Dire Tladi, Ocean Governance: A regulatory Framework Regards aur la Terre [A Planet For Life], 2011,accessed July 11, 2018, at <http://regardssurlaterre.com/en/ocean-governance-fragmented-regulatory-framework>

74 BRICS Leaders Xiamen Declaration, paras 57 (September 4, 2017) at <https://www.brics2017.org/English/Documents/Summit/201709/t20170908_2021.html.>

4 while Canada, Egypt, Japan and Mexico have been a part of 3 GGE processes. Other states have been involved in two or less.[75]

The G7 utilised their strategic grouping to emphasize the applicability of the framework of International Law and the UN Charter-including self-defense, human rights law and humanitarian law through the G7 Declaration on Responsible State Behaviour in Cyber Space in April, 2017.[76] The joint endorsement of this doctrine by G7 states makes their position on the applicability of International law clear although clearer articulation providing legal reasoning and pragmatic enforcement mechanisms is needed.

On the other hand, India also endorsed the communique of the meeting of G20 Finance Ministers and Central Bank Governors in Baden-Baden,Germany in March 2017, which focused on the need for digital financial inclusion[77] and looks into the role of cybersecurity in the protection of financial services.[78] As developing economies attempt to increasingly digitize their economies to enhance economic gains, a lack of effective cyber security measures will be a major hurdle. India should look to build on existing discourse on the development dimension of cyber norms.

The NATO 2018 Communique' has identified cyber defense as a key aspect of NATO's Defense strategy and reaffirmed their commitment to act in consonance with the principles of the UN Charter, International Human Rights Law and Humanitarian Law.[79] The Communique' set out plans to establish a Cyberspace Operations Centre in Brussels[80] and identified key partners in various regions.[81]

The European Union High Representative of the Union for Foreign Affairs and Security Policy submitted a report which explicitly recognised the importance of developing a political response to cybersecurity threats as many of the threats themselves are geopolitical in nature.[82] Further, the report acknowledged that cyberspace is a domain of operations like land, air sea and space and therefore deserves priority in EU's defense strategy.[83] Russia has extended its multilateral efforts regionally at the Shanghai Cooperation Organization (SCO), which India and Pakistan were made full members of in June last year.[84] In 2009, the SCO arrived at an agreement that aimed to guarantee 'international information security'[85] In 2011, Russia and China were supported by other SCO countries in their submission of a

---

75 Australia, Ghana, Indonesia, Israel, Kenya,Malaysia and South Africa have been a part of two GGEs. Argentina, Colombia, Botswana, Cuba,Finland, Italy, Jordan, Kazakhstan,Mali, Netherlands,Pakistan, Qatar, Senegal,Serbia, Spain, South Korea, Switzerland have been involved in just 1 GGE process.

76 G7 Declaration on Responsible States Behavior In Cyberspace, April 11, 2017 at <www.mofa.go.jp/files/000246367.pdf>

77 Communiqué G20 Finance Ministers and Central Bank Governors Meeting, para 6 (March 17-18, 2017) at <http://www.g20.utoronto.ca/2017/170318-finance-en.pdf>

78 Ibid,at para 7.

79 Brussels Summit Declaration, para 20 (2018) at <https://assets.documentcloud.org/documents/4600186/2018-Nato-Communique.pdf>

80 Ibid,para 29

81 Ibid,para 30-34

82 Joint Communication To The European Parliament And The Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, para 17, at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN>,

83 Ibid, at footnotes 81.

84 Casey Michel,, It's Official: India and Pakistan Join Shanghai Cooperation Organization, The Diplomat, June 12, 2017, accessed July 13, 2018, at <https://thediplomat.com/2017/06/its-official-india-and-pakistan-join-shanghai-cooperation-organizatio/>

85 Concluded between People's Republic of China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan on July 16, 2009.

draft, which was updated in 2015. These proposals lay out the rules of the road in cyberspace governance that focuses on 'international information security' and sovereignty.[86] It is possible that Russia and China may continue to use the organisation to prolong it's pivot towards the signing of a cyber treaty and India's participation in this Organisation sets it up nicely to get involved in this process if it strategically suits its needs.

India should also look to engage more actively with regional norms formulation processes such as ASEAN.[87] Despite these being entrenched structural disparity in capacity between the ten states, they have tried to adopt a common vision of digital adoption and information. The e-ASEAN Framework agreement in 2000 set out the framework for e-commerce in the region. In 2016, at the ASEAN Ministerial Meeting on Cybersecurity (AMMC), Dr. Yaacob Ibrahim validly re-asserted the need for a regional approach to the global norms formulation process that took into account the unique socio-political environment in this region.[88]

However, ASEAN is yet to release a Joint Declaration on international law should apply. However, it has pledged to work towards a common framework for co-operation on national security.[89] The ASEAN ICT Masterplan which was adopted in 2016, for example notes[90]:

Initiative 8.1*: Strengthen Information Security in ASEAN, create a trusted ASEAN digital economy", which lays the stress on data protection and critical information infrastructure;*

Initiative 8.2*: Strengthen Information Security Preparedness in ASEAN, improve cyber emergency responses and collaboration*

Starting with technical co-operation as a gateway for developing robust cyber norms may be an appropriate strategy for the region. Cooperation on technical matters through incremental advancements such as tangible sector-specific issues and exchanges leading to capacity-building could aid the norms formulation process by building trust between and increasing engagement between actors in the region.[91] Being involved in such confidence-building measures should be a priority for India.

Bilateral

In addition to the independent multilateral initiatives ,there have also been several bilateral and trilateral initiatives seeking to articulate common understandings on cyber norms[92] These understandings could be useful for the purpose of building economic or diplomatic relationships with states although to be of any normative or legal significance, clearer legal reasoning would be needed. For example, the Joint Statement following the Australia-India

86 UN GA, Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc A/69/723 (January 13 2015) at <https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf>

87 See Candice Tran Dai & Miguel Alberto Gomez "Challenges and opportunities for cyber norms in ASEAN, Journal of Cyber Policy (2018)

88 Yaacob Ibrahim,"Opening Speech by Dr Yaacob Ibrahim, Minister for Communications and Information" and Minister-In-Charge of Cybersecurity, at the Asean Ministerial Conference On Cybersecurity, Cybersecurity agency of Singapore (CSA.gov.sg), November 10 2017, accessed June 11, 2018, at <https://www.csa.gov.sg/news/speeches/minister-yaacob-speech-for-amcc-2016>

89 Tran Dai & Gomez (supra 87) at 8

90 ASEAN. 2016. 16th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings, Bandar Seri Begawan, Brunei Darussalam, Joint Media Statement, November, 26 2016, accessed July 13, 2018, at <http://asean.org/storage/2012/05/TELMIN-16-JMS-Final-cleared.pdf.>

91 Elana Broitman, Mailyn Fidler and .Robert Morgus, "Promoting an International Security Architecture for Cyberspace" (Briefings from the Research and Advisory Group of the Global Commission on Stability of Cyberspace, 2018) 21

92 See compendium (supra 72) at <http://carnegieendowment.org/publications/interactive/cybernorms#formal-names>

Cyber Policy Dialogue re-enforces the importance of an 'open and free cyberspace' and the accepted principles of the 2015 GGE, but does not make reference to any of the thorny issues in the 2017 GGE.[93] The document outlining the US-India cyber relationship does much the same without exploring the points of disagreement in the 2017 GGE.[94]

Apart from the state-oriented initiatives, India also has the opportunity to play a crucial role in shaping discourse that is developing in symbiosis with the private sector. Microsoft, for example has released its own set of norms in 2014 and 2016 seeking to apply norms of International Humanitarian law to cyberspace-terming the final treaty a Digital Geneva Convention.[95] Scholars have approved this idea and even considered the prospects of a Red Cross for cyberspace.[96] Another fruitful endeavour is being coordinated by the Global Commission on the Stability of Cyberspace (GCSC) which engages the full range of stakeholders involved in Internet Governance in order to arrive at and promote shared understandings.[97] CIS has contributed to the Research and Advisory Group of this initiative. The future of a stable universal regime lies in such extensive engagement from all stakeholders.

93 Joint Statement, Australia-India Cyber Policy Dialogue (July 13, 2017) at <http://dfat.gov.au/international-relations/themes/cyber-affairs/Pages/australia-india-cyber-policy-dialogue.aspx>

94 Framework for the U.S.-India Cyber Relationship, accessed July 13, 2018, at <https://in.usembassy.gov/framework-u-s-india-cyber-relationship/>

95 Brad Smith[President Microsoft], The need for a Digital Geneva Convention, Microsoft, February 14, 2017, accessed July 13, 2018 at <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>

96 Tim Maurer and Duncan Hollis, 'A Red Cross for Cyberspace', Time, February 18, 2015, accessed July 7, 2018, at <http://time.com/3713226/ red-cross-cyberspace/>

97 Global Commission on Stability of Cyberspace at < https://cyberstability.org/>

Summary and Key Takeaways for Policy-Makers

- There have been multiple gambits to secure the governance of cyberspace through the universal acceptance of 'cyber norms' that stem from accepted standards in International Law. The United Nations Group of Governmental Experts (UN-GGE) Reports, the Global Commission for Stability in Cyberspace (GCSC) the Tallinn Manual and the initiative of the Carnegie Endowment for International Peace towards a norm protecting financial stability are cases in point. Other normative efforts include efforts in specific interest areas or among groups of like-minded states, such as regional organisations.
- Key fetters plaguing the UN efforts has been a deracinated approach to the norms formulation process, which has divorced the normative standards of International Law from the strategic considerations that guide state policy. The fourth UN-GGE in 2015 released a report acknowledging the applicability of international law to cyberspace but the fifth 2017 GGE broke down due to disagreement over the applicability of self-defense, countermeasures and the standards of International Humanitarian Law.
- While these briefs largely tackle the substantive aspects of cyber norms, it is also crucial that the international community works towards improving the process underpinning norm proliferation by considering prior analogous regimes while considering the unique nature of cyberspace.
- A crucial fissure in the norms formation process revolves around the question of sovereignty. The Sino-Russian view suggests that sovereignty in international law is absolute and no entity other than the sovereign state itself can limit the exercise of this power,which is directly at odds with the desire of the US and like-minded states to preserve the free-flow of information.
- While it is crucial that India does not lose sight of the progress made at the UN-GGE till 2015 and does not lose sight of its bearings on that front, there are multiple other initiative that India has and could get involved with in order to articulate its strategy for norms governing cyberspace.
- A fragmented approach to cybersecurity may not fulfill the goal of regulating cyberspace but it could be a potential catalyst for a stable international system as it would allow for some certainty in the formation of strategic alliances and in national approaches to cyberspace.
- The first step is to put forward a coherent proposal on each of the unclarified issues in the UN-GGE process that is in consonance with International Law. India has been a part of 4 out of the 5 UNGGE processes. In this context, it is useful for India to consider the Tallinn Manual that was drafted by nineteen International law experts at the invitation of the NATO Cooperative Cyber Defence Centre for Excellence and considered how rules of International Law may be applicable in cyberspace.
- In addition the state-oriented initiatives, India also has the opportunity to play a crucial role in shaping discourse that is developing in symbiosis with the private sector. Microsoft, for example has released its own set of norms in 2014 and 2016 seeking to apply norms of International Humanitarian law to cyberspace-terming the final treaty a Digital Geneva Convention. India's future strategy should involve an amalgamation of participation in and inputs from all the covered processes.

Brief 1: Inherent Right of Self-Defense in Cyberspace

Introduction

A cyber-attack against critical infrastructure or military establishments could severely limit the economic or military operations in a state's territory. The recent spate of cyber attacks [98]worldwide in the past half-decade has lead to increasing efforts by various states to build robust cyber-defense mechanisms that can repel or deter these attacks. The asymmetric advantages certain states gain through the possibility of using offensive cyber capabilities without the fear of lawful retaliation offer a potential strategic advantage. While these concerns are valid and must be taken into account when considering the cyber norms regime holistically, the substantive import of the standards of International Law must not be confused with the politics of consensus in its realization as a universal norm. They exist as two distinct stages in the norms formulation process and therefore must be evaluated separately.

This brief limits itself to the International Law on self-defense and its applicability to cyberspace. It considers first the reasons for the breakdown in the GGE talks in 2017 and goes on to answer four crucial questions on the international law of self-defense and its applicability to cyberspace.

Breakdown in GGE

The normative applicability of the right to self-defense was also contested at the 2014-15 GGE. As reported by Mike Schmitt, in a bid to compromise between the insistence of Western States to explicitly refer to the availability of self-defense measures in response to cyber-armed attacks and objection from other states, the final report simply stated that ' the Charter applies in its entirety'[99]- which could be considered an implicit endorsement of Article 51.

While the fifth UN-GGE was tasked with the role of building upon the normative progress at the 2015 GGE, obstruction from Cuba and reportedly Russia and China prevented the presentation of the final report. The only publicly available justification for this is the statement by the delegation of Cuba.[100] The statement appears to be skeptical of the false equivalence between the malicious use of ICTs and the notion of 'armed attack' which could spiral into the utilization of cyberspace as a "theater of military operations and to legitimize, in that context, unilateral punitive force actions, including the application of sanctions and even military action by States claiming to be victims of illicit uses of ICTs."

Michael Markoff, US representative to the GGE was critical of this position and released a statement claiming that "*A report that discusses the peaceful settlement of disputes and related concepts but omits a discussion of the lawful options States have to respond to malicious cyber activity they face would not only fail to deter States from potentially*

98 Florence De Marignan, Cyberattack: major cyber attacks over the past 10 years, Phys Org, May 13, 2017, accessed June 18, 2018, at <https://phys.org/news/2017-05-cyberattack-major-cyber-years.html>

99 Schmitt Just Security, June 30 2017, accessed November 18,2017,(supra 1) at <https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/>

100 Miguel Cuban Declaration (Supra 31) at <https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf>

destabilizing activity, but also fail to send a stabilizing message to the broader community of States that their responses to such malicious cyber activity are constrained by international law." [101]

Mike Schmitt, who was Chairman of the International Group of Experts (IGE) drafting the Tallin Manual was also scathing in his criticism of this stance and dismissed Cuba's statement as 'legal soft-balls.'[102] He criticised this position by citing the Advisory Opinion in the *Nuclear Weapons* case, which states that the right applies to "any use of force, regardless of the weapons employed."[103] While the threshold of an armed-attack is difficult to judge, it is possible to devise parameters for such an assessment. Further, the practical obstacles to making such an assessment should not prevent the application of traditional tenets of international law to evolving global realities.

India should take note of both Schmitt and Markoff's criticism. Clearly stating its position on self-defense in cyberspace would lead to more certainty for other states and entities when considering India's strategic capabilities. The potential adversary needs to be made aware of India's intent to act through legitimate retaliatory options against violations of its digital security. This perception would only be fostered if India articulates a coherent interpretation on the norm itself.

To do so, it must answer two crucial questions:

1. What is the threshold for the 'use of force' as per Article 2(4) in cyber space?
2. What are the conditions required for an act that qualifies as 'use of force' to also qualify as an 'armed attack' in cyber space?

Two further questions have been considered.The treatment of these questions are far more contested even within the realm of traditional International Law and are therefore addressed separately even though articulation of India's position on these questions as well would be useful.

3. Is there a right to anticipatory self-defence in cyberspace?
4. Is there a right to self-defence against non-state actors operating extraterritorially in cyberspace?

Threshold of 'Use of Force'

The extreme variety of cyber operations makes this classification a challenging exercise**.** Oona Hathaway offers a useful summary of the various kinds of cyber-attacks and the terminology used to classify them.[104]

The first crucial distinction is between a cyber-crime and a cyber-attack.[105] While there is no universally accepted definition of 'cyber-crime'- or 'cyber-attack', it is broadly recognized as any crime that is facilitated using a computer network or hardware device and as such

101 Michele Markoff [U.S. Expert to the GGE] Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, United States mission to the United Nations (usun.state.gov), June 23, 2017, accessed July 18, 2018, at <https://usun.state.gov/remarks/7880> [hereinafter Markoff]

102 Schmitt Just Security (supra 1)

103 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226, International Court of Justice (ICJ), 8 July 1996, para 39.

104 Oona Hathaway, " The Law of Cyber Attack" 100 California Review (2012), 833.

105 Ibid.

encompasses a broad range of illicit activities.[106] Unlike cyber-attacks, however, they need not necessarily undermine the target computer network. Therefore, fraudulent practices on the internet, online piracy and the sharing of child pornography all qualify as cyber-crimes, which are largely dealt with by municipal legislation and does not, as such need to be considered by the norms formulation process. For a cyber-crime to also qualify as a cyber-attack, it must have the objective of undermining a computer network, either through theft of information or a Distributed Denial-of-Service (DDoS) attack or through the injection of malware or through the planting of inaccurate information. Most of them would usually have a larger political or national security motive, such as the 'Sony Hack' of 2014 which was conducted in a bid to prevent Sony from releasing a comedy concerning the plot to assassinate the dictator of North Korea.[107]

Cyber attacks that meet the threshold of 'use of force' in Article 2(4) are then colloquially classified as 'cyber-warfare.'

The Tallinn Manual states that 'acts that injure or kill persons or damage or destroy objects are unambiguously uses of force'.[108] This means that a cyber attack which has the same impact as a kinetic attack would fall within the ambit of Article 2(4). This would include attacks that cause damage to electricity grids, water facilities or air traffic signals and therefore pose a threat to human life.[109]

On the other hand, non-destructive cyber operations that aim solely to disrupt the daily economic functioning of a nation in most cases would not qualify as 'use of force'. Thus, it is unclear whether the alleged Russian interference in US elections amounts to use of force according to other tenets of international law such as the law against non-intervention.[110]
All cyber-attacks that fall within the range of the two ends of the spectrum could be judged on the basis of eight non-exhaustive criteria-namely: severity, immediacy, directness, invasiveness, measurability, military character and presumptive legality. These criteria can be expressed in the form of questions[111]:

***Severity**: How many people were killed? How large an area was attacked? How much damage was done within this area?*

***Immediacy**: How soon were the effects of the cyber operation felt? How quickly did its effects abate?*

***Directness**: Was the action the proximate cause of the effects? Were there contributing causes giving rise to those effects?*

***Invasiveness:** Did the action involve penetrating a cyber network intended to be secure? Was the locus of the action within the target country?*

***Measurability:** How can the effects of the action be quantified? Are the effects of the action distinct from the results of parallel or competing actions? How certain is the calculation of the effects?*

***Military character:** Did the military conduct the cyber operation? Were the armed forces the*

106 Ibid

107 Paul Szoldra, A hacker explains why you shouldn't believe North Korea was behind the massive Sony hack, Business Insider UK, June 10, 2016, accessed July 10, 2018, at <http://uk.businessinsider.com/north-korea-sony-hack-2016-6?r=US&IR=T>

108 Tallinn Manual 2.0, (supra 62) at 333.

109 Arindrajit Basu, India Needs a Credible Deterrence Strategy for Cyberspace, The Wire, September 23, 2017, accessed July 8, 2018, at < https://thewire.in/179682/india-needs-credible-deterrence-strategy-cyberspace/> [hereinafter Basu India Deterrence]

110 Ohlin, Jens David, "Did Russian Cyber Interference in the 2016 Election Violate International Law?," 95 Texas Law Review 1579 (2017)

111 Tallinn Manual 2.0, (supra 62) at 336.

target of the cyber operation? State involvement: Is the State directly or indirectly involved in the act in question? But for the acting State's sake, would the action have occurred?

Presumptive legality: *Has this category of action been generally characterised as a use of force, or characterised as one that is not? Are the means qualitatively similar to others presumed legitimate under international law?*

While these criteria are illustrative in nature, they could be used as tools to decide whether an attack amounts to the use of force in International Law by using them in conjunction with national policy. An attack on India's Aadhaar database[112] combined with the leaking of sensitive biometric information contained within the database may amount to the 'use of force' given the recognition of UIDAI's Central Identities Data Repository (CIDR) as a 'protected system' under Section 70 of the IT Act.[113]

For the U.S. Government, the physical impacts of a cyber-attack are the key to making this determination. Harold Koh, Legal Advisor to the State Department asserted that "[c]yber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force."[114] For him, it is a 'matter of common sense': " if the physical consequences of a cyber- attack work the kind of physical damages that dropping a bomb or firing a missile would, that cyber- attack should equally be considered a use of force." He further suggested that "[i]n assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors: including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues." [115] The UK Attorney-General has stated that cyber operations which result in an 'equivalent scale' of death and destruction as an armed attack would give rise to a Right to Self-Defense under Article 51. As per him, example sof these attacks include interference with nuclear reactors resulting in a widespread los of life, disabling air traffic control towers causing planes to crash or targetting of essential medical services (which seems to be an implicit reference to the WannaCry attack)

While other states are yet to put forward a cohesive legal position on the threshold for the use of force, these could serve as potential guidelines for India when cementing its own strategy for answering this question.

Threshold of Armed Attack

Traditional international law is yet to answer the crucial question of when the 'use of force' amounts to an armed attack and therefore triggers an inherent right to self-defense.

Article 51 of the UN Charter which enshrines the Right to Self-Defence reads:

Nothing in the present Charter shall impair the inherent right of individual or collective self-Council has taken measures necessary to maintain international peace and security...

In the *Oil Platforms*[116] and *Nicaragua*[117] cases, the International Court of Justice held that the gravest uses of force qualify as an 'armed attack, thereby galvanizing a right of self-defence

112 Basu, India Deterrence (supra 109) "https://thewire.in/179682/india-needs-credible-deterrence-strategy-cyberspace/

113 Notification, Ministry of Communications and Information Technology (India) (December 11, 2015) at <http://meity.gov.in/writereaddata/files/UIDAI%20CII%20notification%20Dec15.pdf>

114 Harold Hongju Koh, Legal Advisor of the Dep't of State, International Law in Cyberspace, Address to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), at <http://www.state.gov/s/l/releases/remarks/197924.htm.>

115 Ibid

116 Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America, International Court of Justice (ICJ), 6 November 2003

117 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

as per Article 51.[118] This interpretation may be endorsed by a teleological reading of the UN Charter as the prohibition in Article 2(4) uses the phrase 'use of force' while Article 51 uses the phrase 'armed attacks.' Critics of this position include former U.S. State Department Legal Advisor William H. Taft who believes that two distinct thresholds would encourage states to engage in a series of less severe attacks without a threat of unilateral response from the other state.[119] Tarcisio Gazzini further argues that distinction would mean 'unacceptable risks' for states and believes that the limits on the use of self-defense measures do provide enough of a safeguard.[120] Further, Christine Gray notes that there is a lack of state practice which could support that distinction.[121] In a separate opinion in the *Oil Platforms* case, Judge Bruno Simma argues that there are two levels of attacks-the level of 'armed attacks' used in Article 51 and a lower level of 'hostile military action."[122] According to his opinion, the right to self-defense may exist against the lower level of acts as well but with a stricter assessment of necessity and proportionality.

Drawing from the *Nicaragua* judgment, The Tallinn Manual focuses on the 'scale and effects' test.[123] It argues that the scale and effects required for an act to be characterised as an armed attack necessarily exceed those qualifying the act as a use of force and must be the most grave forms of the use of force. It goes on to provide some useful examples. It states, for instance, that, acts of cyber intelligence gathering and cyber theft, as well as cyber operations that involve brief or periodic interruption of non-essential cyber services, do not qualify as armed attacks.[124] However, a cyber operation that seriously injures or kills a number of persons or that causes significant damage to, or destruction of, property would satisfy the threshold

Another key question on the threshold of an armed attack is the treatment of 'pin-prick' attack-attacks that may not individually amount to an armed attack but could constitute an armed attack when aggregated.[125] Another key question on the threshold of an armed attack is the treatment of 'pin-prick' attacks. These are attacks that may not individually amount to an armed attack but could constitute an armed attack when aggregated. The analogy refers to the pricking of the skin using a pin. Each prick might not be painful individually but might pain the victim if taken cumulatively[126] While the ICJ is yet to answer this question conclusively in the context of kinetic attacks, there is sufficient judicial posturing that recognises this possibility.[127]

There is also some explicit state practice advocating for the acceptance of this concept in International Law.[128] The Tallinn Manual addresses this concern in the context of cyberspace and provides that the determinative factors must be: (1) Whether the same originator(s) had carried out similar small scale incidents; (2) The incidents are related; (3) Together they must

---

118 Janne Valo, Cyber attacks and the use of force in International Law (Helsinki,2014)

119 William H. Taft, 'Self-Defense and the Oil Platforms Decision'. 29 YJIL (2004) 295–306.

120 Tarcisio Gazzini, The Changing Rules on the Use of Force in International Law (Manchester University Press, 2005).

121 Christine Gray, International Law and the Use of Force (3rd Edn., Oxford University Press, 2008).

122 Oil Platforms, Separate Opinion of Judge Simma at paras 12–13 (supra 116)

123 Tallinn Manual 2.0, (supra 62) at 341

124 Ibid, at 342

125 Abhimanyu George Jain, "Rationalising International Law Rules on Self-Defense: The Pin Prick Doctrine" Chicago-Kent Journal of International and Competition Law (2014)

126 Ibid

127 Ibid, at 27

128 Ibid

measure up to the standards of the 'scale and effects' test and (4) There must be conclusive evidence of the first three points.[129]

There is some clear state practice recognising the applicability of self-defense norms to cyberspace. Apart from the United States, the United Kingdom has explicitly endorsed the applicability of Article 51 to cyberspace. In a submission to the General Assembly earlier this year, the United Kingdom *"re-affirmed that the UN Charter applies in its entirety to state actions in cyberspace, including the prohibition of the use of force (Article 2(4)), the peaceful settlement of disputes (Article 33), and the inherent right of states to act in self-defence in response to an armed attack (Article 51). The law of state responsibility applies to cyber operations in peacetime, including the availability of the doctrine of countermeasures in response to internationally wrongful acts."*[130] The UK Attorney-General has stated that cyber operations which result in an 'equivalent scale' of death and destruction as an armed attack would give rise to a Right to Self-Defense under Article 51.[131] As per him, examples of these attacks include interference with nuclear reactors resulting in a widespread loss of life, disabling air traffic control towers causing planes to crash or targetting of essential medical services (which seems to be an implicit reference to the WannaCry attack[132])

The European Union is set to launch a framework that allows states to treat cyber-attacks as an 'act of war' and take measures in self-defence.[133] Further, states who are victims of such attacks may be entitled to seek assistance from other EU governments under Article 42(7) of the EU Treaty.

Further Issue 1: Self-Defense Against Non-State Actors in Cyberspace

There exists no consensus on whether the right enshrined in Article 51 applies against non-state actors.[134] A teleological reading of Article 51 would imply that such a right is in fact available, as it uses the phrase 'any armed attack' without specifying that such armed attack must emanate from a state. However, the ICJ in the *Palestine Wall Advisory Opinion* [135]moves away from this argument and focused on the requirement of attribution of an armed attack

129 Tallinn Manual 2.0, (supra 62) at 341.

130 Foreign & Commonwealth Office (United Kingdom), Response to General Assembly resolution 71/28 "Developments in the field of information and telecommunications in the context of international Security" (July 2017) at <https://s3.amazonaws.com/unoda-web/wp-content/uploads/2017/09/UK-ES-and-full.pdf>

131 Wright Speech (supra 43) at <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>

132 Josh Fruhlinger, "What is WannaCry Ransomware, How does it infect and who was responsible" CSO, September 27, 2017, accessed July 18, 2018 at <https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html> ("WannaCry is a ransomware worm that spread rapidly through across a number of computer networks in May of 2017. After infecting a Windows computers, it encrypts files on the PC's hard drive, making them impossible for users to access, then demands a ransom payment in bitcoin in order to decrypt them.")

133 Bradley Barth " New EU framework allows members to consider cyber attacks acts of war" SC Media October 31, 2017, accessed July 14, 2018, at <https://www.scmagazineuk.com/new-eu-framework-allows-members-to-consider-cyber-attacks-acts-of-war/article/703965/>

134 Marko Milanovic , " Self-Defense against Non-State Actors and the jus ad bellum", EJIL Talk, February 21, 2010, accessed July 15, 2018, at <https://www.ejiltalk.org/self-defense-and-non-state-actors-indeterminacy-and-the-jus-ad-bellum/>

135 Advisory Opinion Concerning Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, International Court of Justice (ICJ), 9 July 2004

to a state for the right of self-defense to be applicable. This position has been vociferously disputed by several publicists on the grounds that such a legal position is untenable in today's day and age when a significant proportion of armed attacks are carried out by transnational actors that cannot be considered agents or organs of any state.[136] Judge Kooijmans in his separate opinion in the *Armed Activities* case, endorsed a right to self-defense even in the absence of state attribution."[137]

Ongoing operations against ISIL in Iraq has seen a revival of discussion of the 'unwilling or unable doctrine.' [138]A growing number of States now argue that use of force in self-defense against a non-state actor operating from the territory of a third state may be lawful provided that the territorial state is 'unwilling or unable to prevent such action. Thus far 10 states have explicitly objected to the applicability of this doctrine while 4 states have explicitly objected.[139]

Applying this doctrine to cyber operations, The Tallinn Manual concluded that the principle of sovereignty must be carefully considered in such cases.[140] It argued that actions in self-defence may be taken on the territory of a third state as long as it is not violating its sovereignty. While the experts were divided on the characterisation of non-consensual action, the majority concluded that self-defence against a cyber armed attack may be permissible only if it complies with the principle of necessity which means that it should be the only available means of repelling the armed attack.[141]

Further Issue II: Anticipatory Self-Defense in Cyberspace

A further question India needs to consider is the applicability of anticipatory self-defense in cyberspace.Most experts agree that states do not need to wait for the actual attack to commence, even though the UN Charter uses the phrase 'if an armed attack occurs."[142] There is also universal acknowledgment of the three prongs of the *Caroline* test, which are now regarded as customary international law : namely the necessity for the use of self-defence ("instant, overwhelming leaving no choice of means and no moment for deliberation"), proportionality (the attack must not.involve anything unreasonable or excessive) and imminence of the attack itself. Divergence between experts lies in the extent of imminence or how imminent an attack must be.[143]

The Tallinn Manual focuses on whether the responding state has a 'window of opportunity' to prevent the attack from materialising.[144] It creates a distinction between the placement of a logic bomb and the placement of remotely activated malware. The point of departure

136 Michael N. Schmitt, Sean Watts; Beyond State-Centrism: International Law and Non-state Actors in Cyberspace, 21 Journal of Conflict and Security Law 3, (December 1, 2016) 595–611; Hakimi, Monica. "Defensive Force against Non-State Actors: The State of Play." Int'l L. Stud. 91 (2015): 1-31.

137 Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda); Request for the Indication of Provisional Measures, International Court of Justice (ICJ), 1 July 200

138 Elena Chachko & Ashley Deeks, Who is on Board with "Unwilling or Unable"? Lawfare, October 10, 2016, accessed July 4, 2018, at < https://www.lawfareblog.com/who-board-unwilling-or-unable>

139 Ibid

140 Tallin Manual 2.0, (supra 62) at 344

141 Ibid

142 Christine Gray, International Law and the Use of Force (3rd Edition, Oxford University Press, 2008) 114

143 Ibid at 114.

144 Tallinn Manual 2.0, (supra 62) at 352

between these two mechanisms lies in the fact that the logic bomb goes off after the occurence of likely pre-determined factors whereas the malware requires external activation.

A 'Cold Start for Cyberspace': Identifying Cyber Readiness and Existing Vulnerabilities

India's war doctrine permits the launch of pre-emptive operations if continuing provocations cumulatively amount to an 'armed attack."[145] Extending this doctrine to cyberspace could prove to be useful.

Modern Indian military strategy sees its origins in the immediate aftermath of the 2001 Parliament Attacks. While there are many interpretations of the greatly politicised 'Cold Start Doctrine[146], this strategy essentially entails rapid responses to any form of external threats through the stationing of more streamlined integrated units near the border.[147] The extension of this doctrine to cyberspace could be crucial in signalling to potential rivals that India's cyber defences are robust enough to deny gains from the mounting of any attack. That can only happen through (i)Construction of streamlined cyber response units that work together to thwart cyber attacks and (ii) An honest appraisal of vulnerabilities in the digital infrastructure which might be attacked by cyber security specialists.

As of now, there exists no national level organisation in the military that is responsible for cyber defense.[148] even though there are some non-military bodies that specialise in elements of cyber security and cyber defense. The Indian Computer Emergency Response Team, for example was formed in 2004 under the Ministry of Electronics and Information Technology and acts as the main body for cyber incident response in non-critical sectors although it is tasked with other responsibilities such as facilitating cross-sector cyber co-operation[149] and maintaining records.[150] For all sectors defined as Critical Information Infrastructure, [151] the National Critical Information Infrastructure Protection Centre (NCIIPC) has been responsible since its creation in 2014 through a Gazette Notification of the Central Government. It has broadly identified five core CII areas-namely Power and Energy, Banking, Financial Institutions and Insurance,Information and Communication Technology, Transportation and E-governance.[152] Through a more coherent approach to cyber defense, the NCIIPC has taken great strides towards identifying vulnerabilities in sectors that may be victims of cyber

145 Ali Ahmed, "India's Conflict Strategy: The Legal Angle" 4 Journal of Defense Studies 3 (2010) at <https://idsa.in/system/files/jds_4_3_aahmed.pdf >

146 Shashank Joshi &Vipin Narang, Future Challenges for the Indian Army 2030, Observer Research Foundation February 22, 2017, accessed June 29, 2018, at <,http://www.orfonline.org/expert-speaks/future-challenges-for-the-army-2030/>

147 M.F.What is India's "Cold Start" military doctrine?,, The Economist, January 31, 2017, accessed July 3, 2018, at <https://www.economist.com/blogs/economist-explains/2017/02/economist-explains>

148 Basu India Deterrence (supra 109) at https://thewire.in/179682/india-needs-credible-deterrence-strategy-cyberspace/

149 India Computer Emergency Response Team, at <http://cert-in.org.in/>

150 Saikat Datta "The NCIIPC and its Evolving Framework" Digital Frontiers, Observer Research Foundation November 3 2016, accessed June 29, 2018, at <http://www.orfonline.org/expert-speaks/nciipc-its-evolving-framework/> [hereinafter Saikat NCIIPC]

151 Amendment to Section 70 of the IT Act defines 'Critical Information Infrastructure' (CII) as "those facilities, systems or functions whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation."

152 National Critical Information Infrastructure Protection Centre, Sectors in NCIIPC, accessed January 14, 2018, at <https://nciipc.gov.in/?p=sector>

attacks.[153] However, the NCIIPC does not quite focus on offensive cyber techniques, something that might be a crucial component of India's deterrence arsenal.

The National Technical Research Organisation (NTRO) – established in 2004, on the other hand – is a specialised technical research organisation modelled under the National Security Agency of the United States unit and specialises largely in intelligence gathering.[154] Sukumar and Sharma have emphasized the need for a National Cyber Security Agency which reports to the Prime Minister's Office.[155] This organization would consist of a Policy and Advanced research wing to study trends in cyber security and identify vulnerabilities while the Operations Wing headed by an Army Personnel would be in charge of offensive techniques.

While cyber-space could not serve as an exclusive domain of warfare given the low costs of mounting an attack and the even lower odds of attribution, protecting India's critical infrastructure is a boon in itself and could enable the cultivation of best practices and Confidence Building Measures among regional allies. Further research would need to focus on vulnerability identification and its potential impact on a regional cyber-deterrence regime.

Conclusion

There exists enough state practice to justify the strategic use of a norm of self-defense in cyberspace. Faced with cyber-threats from adversaries, it may be useful for India to publicly endorse this norm in order to strengthen its cyber deterrence strategy. As argued by Martin Libicki of the RAND Corporation cyberspace could be one in a rung of retaliatory options in order of belligerency – diplomatic, economic, cyber, physical force and finally, nuclear force.[156] So, the strategic use of cyber warfare could seek to serve the goal of deterrence by creating a credible threat of punishment provided India also looks to identify and clearly plug the vulnerabilities in critical infrastructure.[157] Thus, cyber deterrence, if articulated through clear public posturing and a reference to the standards of International Law could become a part of a legitimate and cohesive strategy looking to deter hostile acts.

153 Saikat NCIIPC (supra 150) at <http://www.orfonline.org/expert-speaks/nciipc-its-evolving-framework>

154 Melissa Hathaway, Chris Demchak, Jason Kerben & Jennifer McArdle, Francesca Spidalieri, INDIA CYBER READINESS AT A GLANCE (Potomac Institute for Policy Studies, December 2016) at <http://www.potomacinstitute.org/images/CRI/CRI_India_Profile.pdf>

155 Arun Mohan Sukumar & Col. R.K. Sharma, The Cyber Command: Upgrading India's National Security Architecture, Observer Research Foundation, Special Report (March 2016) at <http://cf.orfonline.org/wp-content/uploads/2016/03/SR_9_Arun-Mohan-Sukumar-and-RK-sharma.pdf>

156 Martin Libicki, Cyber Deterrence and Cyberwar (RAND Corporation,2009) https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

157 "Basu India Deterrence (supra 109) at <https://thewire.in/179682/india-needs-credible-deterrence-strategy-cyberspace/>

Summary and Key Takeaways for Policy-Makers

- The normative applicability of the right to self-defense was also contested at the 2014-15 GGE. The final report simply stated that ' the Charter applies in its entirety'- which could be considered an implicit endorsement of Article 51.
- While the fifth UN-GGE was tasked with the role of building upon the normative progress at the 2015 GGE, obstruction from Cuba and reportedly Russia and China prevented the presentation of the final report. The only publicly available justification for this is the statement by the delegation of Cuba.
- To do so, it must answer two crucial questions:
    1. What is the threshold for the 'use of force' as per Article 2(4) in cyber space?
    2. What are the conditions required for an act that qualifies as 'use of force' to also qualify as an 'armed attack' in cyber space?

  Two further questions have been considered. The treatment of these questions are far more contested even within the realm of traditional International Law and are therefore addressed separately even though articulation of India's position on these questions as well would be useful.
    1. Is there a right to anticipatory self-defence in cyberspace?
    2. Is there a right to self-defence against non-state actors operating extraterritorially in cyberspace?
- India's war doctrine permits the launch of pre-emptive operations if continuing provocations cumulatively amount to an 'armed attack.' Extending this doctrine to cyberspace could prove to be useful.
- There exists enough state practice to justify the strategic use of a norm of self-defense in cyberspace. Faced with cyber-threats from adversaries, it may be useful for India to publicly endorse this norm in order to strengthen its cyber deterrence strategy.

Brief II: Attribution of Cyber Attacks

Introduction

Technical constraints on attributability have compelled discourse on the evidentiary and legal standards that enable the attribution of a cyber-attack to a certain state. Uncertainty of attribution limits the options available to a victim state-both in terms of opting for defensive measures and garnering support from multilateral fora. It also acts an incentive for states to opt for offensive measures in cyberspace as there are reduced possibilities of punishment in the absence of attribution. Lack of proper publicly declared parameters for attribution by states therefore fetters the creation of a cyber deterrence regime [158] and thus fosters greater instability in cyberspace. India has yet to publicly attribute a cyber attack to a state or non-state entity with reference to existing tenets of International Law.

This brief considers first the traditional legal regime on attribution and engages in a survey of relevant case law and scholarly opinion. It then goes into recent suggestions of an alternate legal regime that has been suggested for the attribution of cyber attacks. It then embarks on a survey of inter-disciplinary policy proposals on enhancing attributability and focuses on the possibility of a global consortium that could carry out investigations into cyber attribution.

Traditional Legal Regime on Attribution

State responsibility is fundamentally premised on two elements: (1) the act or omission that leads to a breach of an international obligation and (2) attribution of that act or omission to the state in question. Generally, acts of private persons or groups are not attributable to the state.[159]

There are however, certain exceptions. The first exception relates to the acts/omissions of de jure or de facto state organizations. This would include entities that are not formally recognized as stage organs in municipal law but must be deemed so as they are completely dependent on the state.[160] This is a widely accepted rule of international law and is captured by Articles 4-6 of the Articles on State Responsibility. The second exception imputes state responsibility " if the conduct of a non-state actor is "acting under the instructions of or under the direction and control of the state carrying out the said conduct."[161] This test, known as the the 'effective control' test was laid down by the International Court of Justice in *Nicaragua*[162] and imported by the ILC into Article 8. The test essentially requires a state to "exercise such a degree of control in all fields, as to justify the non-state actors on its behalf." [163] It implies that the state must have directed each allegedly wrongful act in order to attract international responsibility. This test has been criticized by several scholars as being too high a threshold and therefore limiting greatly the scope of state responsibility.[164]

---

158 Jonathan Solomon. "Cyberdeterrence between Nation-State Plausible Strategy or a Pipe Dream?" Strategic Studies Quarterly, (2011)

159 International Law Commission, Articles on the Responsibility of States for Internationally Wrongful Acts, Report of the International Law Commission on the Work of its 53rd session, A/56/10, August 2001, UN GAOR, 56th Sess Supp No 10, UN Doc A/56/10(SUPP) (2001), art. 4(1) ("Articles on State Responsibility").

160 Articles on State Responsibility, Arts. 4-6.

161 Ibid, Art.8

162 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, at para 86.

163 Ibid, at 62-64,65

164 Antonio Cassese; The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia, 18 European Journal of International Law 4, (2007)Pages 649–66

Thirteen years later, in 1999, an alternate test, known as the 'overall control test' was put forward by the Appeals Chamber of the United Nations International Criminal Tribunal for the Former Yugoslavia in its oft-cited *Tadic*' opinion.[165] It is key to note that this test was evolved in a different legal context as it was not to hold a state responsible in international law but to classify the armed conflict as one between two states as per the standards of International Humanitarian Law. Under the overall control test, the state in question need only have control over the group generally and not have directed each specific internationally wrongful act.

The ICJ re-endorsed the effective control test in 2007 in the case concerning the *Application of the Convention on the Prevention and Punishment of the Crime of Genocid*e.[166] The Court criticized the ICTY's 'overall control' test as exceeding its jurisdiction.

There has been further state practice endorsing imputed state responsibility for states who harbour or provide material support to those who cause harm in another state.[167] The US attributed the 9/11 attacks to Al Queda and this was accepted by the global community at the time. The 'safe harbour principle' differs from the effective and overall control tests because it refers to another doctrine of international law-which is the duty to prevent transboundary harm and the 'due diligence' principle that was first articulated in the 1941 *Trail Smelter* arbitration[168] of the PCIJ and then endorsed in the ICJ's *Corfu Channel*[169], *Nuclear Weapons*[170] and *Gabcikovo-Nagymaros*[171] judgments. Simply put, the due diligence obligation is basically an obligation that requires states to minimize the risk of harm occurring, given the capacity at its disposal.[172] It is well established that due diligence is an obligation of conduct, not result. Therefore, it only imposes responsibility on states for its own actions rather than imputed state responsibility for the acts of non-state actors.[173]The degree to which a state must exercise 'due diligence' remains largely a contextual question.[174]

The Tallinn Manual also endorsed the 'effective' control test.[175] Although the International Group of Experts (IGE) drafting the manual recognised the tension between the 'effective' and 'overall' control tests in the first Tallinn manual, they seem to have done away with the overall control test altogether in the revised Tallinn Manual 2.0. Rule 17 of the Tallinn Manual 2.0 reflects clearly Article 8 of the Articles on State Responsibility and states that cyber operations conducted by a non-state actor may be attributable to a state only when it is engaged in pursuant to its instruction or under its direction and control. The IGE clarifies that instructions in this context "refers most typically to situations in which a non-state actor functions as a State's auxiliary."[176] Effective control includes the ability to ensure that a specific activity occurs and also the ability to make it cease through explicit instructions.[177]

---

165 Prosecutor v. Tadić, Case No. IT-94-1-I, Appeal Judgment, ¶ 120 (Jul. 15, 1999) ("Tadić").

166 Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime ofGenocide (Bosn. & Herz. v. Serb. & Mont.), 2007 I.C.J. Rep 43 at 210 (Feb. 26) ("Bosnia Genocide").

167 See Kimberley Trapp, State Responsibility for International Terrorism (OUP, 2011), 54

168 Trail Smelter (U.S. v. Can.), 3 R.I.A.A. 1905, 1965 (1941).

169 Corfu Channel Case (U.K. v. Alb.), 1949 I.C.J. 4, 35 (Apr. 3).

170 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 29 (July 8)

171 Gabčíkovo-Nagymaros Project (Hung. V. Slovk.), 1997 I.C.J. 7, 53 (Sept. 25).

172 UN ILC, 'Draft Principles on the Allocation of Loss in the Case of Transboundary Harm Arising out of Hazardous Activities (with Commentaries)' (2006) GAOR 61st Session Supp 10, 106

173 Ibid

174 See Timo Kouruva, "Due Diligence," Oxford Public Intenational Law (2017) , at <http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1034>

175 Tallinn Manual 2.0, (supra 62), Rule 17, at 94.

176 Tallinn Manual (supra 62), at 95

177 See Tim Maurer, 'Proxies and Cyberspace' 21 JCSL 3 (2016),383-403, (Useful table on page 401 capturing the varying degrees of control a state can exercise over proxies

Schmitt and Vihul have argued that the relatively high levels of support needed before a state can be held responsible for the actions of proxies essentially creates a normative 'safe zone for them."[178] Essentially, the standards of effective control enshrined in Article 8 of the Articles on State Responsibility set too high a threshold for implementation in the modern context of cyber attacks.

Shift Towards a New Test of State Responsibility for Attributing Cyber Attacks

At the 9th International Conference on Cyber Conflict held in 2017, Peter Stockburger put forward a new test known as the 'control and capabilities' test which would be *the lex specialis* (specific law) governing international responsibility in the case of attributing cyber attacks.[179] This approach veers away from the rigid focus on 'control' embodied in the 'effective control' test and focuses on multiple indicative factors that could serve as a guide to effective attribution. Stockburger proposes a set of non-exhaustive factors that may be utilised for this purpose, which includes :(1)Relationship between non-state actor and state, (2) The influence the state exerts over the non-state actor; (3)Methods employed by the non-state actor; (4) Motivations of the parties involved ; (5)whether they use similar code; (6) Technical capabilities of the non-state group and (7) geographic location.[180]

Stockburger also highlights recent state practice that may support a move towards this new test. These cases include:

Estonia-2007[181]: After Estonia was struck by a wave of distributed denial of service ('DDoS') attacks, a large number of scholars and jurists attributed the attack to Russia as the evidence available showed that "the hackers claimed to be Russian, the tools to hack and deface were contained in Russian websites and chatroom and the attacks picked a day of significance to most Russians."

Mandiant Report, 2013[182]-Attributed APT1 attacks to the Chinese state based on geographic location of the non-state actors.

Sony Hack, 2014[183]-This was the first instance where a state publicly attributed a specific attack and provided reasons for this attribution. The parameters used by the US government to attribute the attacks to North Korea were (1) Similarities between data deletion malware used in the attacks were similar to other malware, in terms of specific lines of code, encryption, data deletion methods, that North Korean actors were known to use; (2) Overlap between the 'infrastructure' used in the cyber-attack and other infrastructure previously known to be used by North Korean actors; (3) IP addresses associated with attackers from North Korea; (4) Tools used in the attacks which were similar to those used in a prior attack carried out on South Korea in 2013.

178 Michael Schmitt and Liis Vihul, ' Proxy Wars in Cyberspace: The evolving international law of attribution" (2014) Fletcher Security Review 55,59-60

179 Peter Z.Stockburger, " Control and Capabilities Test: Toward a New Lex Specialis Governing State Responsibility for Third Party Cyber Incidents" in H. Rõigas, R. Jakschis, L. Lindström, T. Minárik (Eds.) 2017 9th International Conference on Cyber Conflict: Defending the Core (2017 NATO CCD COE Publications, Tallinn) 1

180 Ibid

181 Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia", The Guardian, May 16, 2007, accessed July 5, 2018, at < https://www.theguardian.com/world/2007/may17/topstories3.russia>

182 Exposing One of China's Cyber Espionage Units, Mandiant Apt1 at <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>

183 Michael Cieply & Brooks Barnes, "Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm",N.Y. Times December 30, 2014, accessed June 30, 2018, at <http://www.nytimes.com/2014/12/31/business/media/sony-attackfirst-a-nuisance-swiftly-grew-into-a-firestorm-.html>

Iran-2016[184]:The US Department of Justice (DOJ) again publicly attributed the operations of non-state actors to Iran by stating that they purportedly worked on behalf of the Iranian state judging from the evidence provided by the scope and capabilities of the cyber operations. They did not refer to direction and control but instead to the methods, capabilities and motivations of the actors involved.

Russian interference in U.S. elections-ongoing[185]**:** While attribution of interference in the U.S. election is an ongoing process, the Department of Homeland Security and Director of National Intelligence released a joint report highlighting that 'technical indicators prove that the non-state actors are 'likely associated' with the Russian state. The control and capabilities approach may turn out to be crucial if attribution is to be established in this case.

Wanna cry-2017[186] In the immediate aftermath of May's 'Wannacry' ransomware cyber-attacks, the United Kingdom's National Cyber Security Centre claimed speculatively that the hacker group 'Lazarus' with ties to the North Korean government were responsible for the attack.[187] In a statement released in December, 2017, the government publicly attributed the attacks to the Lazarus group concluding that the odds of them mounting this attack were 'highly likely.'[188] Following that, Thomas Bossert, assistant to the President for Homeland security penned an editorial for the Wall Street journal attributing the attacks to North Korea although he did not mention the Lazarus group by name.[189] Bossert stated that Australia,[190] Canada[191], New Zealand[192], Japan[193] and even Microsoft[194] from the private sector had all come to the conclusion that Lazarus was indeed responsible.

---

184 US Dep't of Just., "Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps - Sponsored Facilities", Press Release, March. 24, 2016 at <https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iraniansconducting-coordinated>

185 Office of Director of National Intelligence, United States of America, Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution (January 6, 2017) at <https://www.dni.gov/files/documents/ICA_2017_01.pdf>

186 Michael Schmitt and Sean Fahey, " WannaCry and the International Law of cyberspace,", Just Security, Dece,mber 22, 2017, accessed July 3, 2018, at <https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/>

187 http://www.bbc.co.uk/news/technology-40297493,

188 https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks

189 Thomas P. Bossert, It's Official: North Korea Is Behind WannaCry, The Wall Street Journal December 18, 2017, accessed July 13, 2018, at <https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537?shareToken=st2d38565d59c24132b421a4b03edb68b5&reflink=article_email_share>

190 Malcolm Turnbull, ATTRIBUTING THE 'WANNACRY' RAMSOMWARE TO NORTH KOREA, Prime Minister of Australia (PM.Gov.Au) December 20, 2017, accessed July 13, 2018, at <thttps://www.pm.gov.au/media/attributing-wannacry-ramsomware-north-korea>

191 Greta Bossenmaier(Chief), CSE Statement on the Attribution of WannaCry Malware, Communications Security Establishment (Canada) December 19, 2017, accessed July 14, 2018, at <https://www.cse-cst.gc.ca/en/media/2017-12-19>

192 New Zealand concerned at North Korean cyber activity, National Cyber Security Center (New Zealand) December 20, 2017, accessed July 5, 2018, at <https://www.ncsc.govt.nz/newsroom/new-zealand-concerned-at-north-korean-cyber-activity/>

193 Norio Maruyama, The U.S. Statement on North Korea's Cyberattacks (Statement by Press Secretary) Ministry of Foreign Affairs (Japan), December 20, 2017, accessed June 30, 2018, at <http://www.mofa.go.jp/press/release/press4e_001850.html>

194 Brad Smith (President), Microsoft and Facebook disrupt ZINC malware attack to protect customers and the internet from ongoing cyberthreats, Microsoft, December 19, 2017, accessed July 11, 2018, at <https://blogs.microsoft.com/on-the-issues/2017/12/19/microsoft-facebook-disrupt-zinc-malware-attack-protect-customers-internet-ongoing-cyberthreats/>

Technical Challenges of Attribution

Even if one were to alter the legal parameters of attributing a cyber attack, severe technical challenges remain-especially if we are to use the legal regime to foster deterrence induced stability in cyberspace. [195] Even if it can be traced back to a specific geographic area through an IP address, unless it is traced back to a state or at least to the responsible private actor, geographic tracing may be of limited value.[196]

The states with the most highly priced cyber targets are the ones most likely to invest in attribution capacity before the attack takes place.[197]The better a government's technical prowess, the larger* the pool of talent and skill at its disposal and the greater the chances of the state hiding its own covert operations and detecting others. Industrial states such as the United States have the most highly valued social,economic or military targets but also have the most advanced signals intelligence agencies to ensure their security.

Indeed,one of the primary obstacles is that the Internet was created without considering the possibility of attribution.[198] Indeed, the United States Department of Defense has stated that the explosive growth of the internet was spurred in many ways by its anonymity.[199]

Cyber-attacks are multi-stage and multi-step.[200]This complicates the attribution process a great deal. In a botnet attack, (or a Distributed Denial of Service (DDoS) attack,) a "bot-master" infiltrates a large network of vulnerable computers by creating a botnet. The bot-master subsequently directs the net of compromised computers to attack a victim network, thereby overloading the servers and causing the victim network to crash. Investigating such an attack is difficult simply because the bot-master will be removed by several degrees from the attacking machines.[201] Tracing the attack back to the bot-master would span several countries and several jurisdictions.

Other attacks are directed through multiple stages of computers set up as proxies. These innocent computers are then used to scan and compromise more machines. Once,an infrastructure of compromised machines is created (proxy-chain), the attacker uses some of these proxy machines to attack the target, others for data transit, others as "dead-drops" for the storage of temporarily exfiltrated data, and some as intermediary command and control nodes.[202] Therefore, the virtual nature of cyberspace makes tracking back a costly and challenging activity. Even if these obstacles are traced back to the geographic territory of a certain state, recovering evidence to hold a state responsible poses even more fetters.

---

195 Joshua Tromp, "Law of Armed Conflict, Attribution, and the Challenges of Deterring Cyber-attacks," Small Wars Journal, accessed July 7, 2018, at <http://smallwarsjournal.com/jrnl/art/law-of-armed-conflict-attribution-and-the-challenges-of-deterring-cyber-attacks>

196 Paul Rosenweig, Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World. (Westport, CT: Praeger Publishers, 2013.)

197 Jon R. Lindsay; Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack, 1, Journal of Cybersecurity 1 (September 1, 2015), Pages 53–67

198 Joshua Tromp, "Law of Armed Conflict, Attribution, and the Challenges of Deterring Cyber-attacks," Small Wars Journal, at <http://smallwarsjournal.com/jrnl/art/law-of-armed-conflict-attribution-and-the-challenges-of-deterring-cyber-attacks>

199 U.S. Department of Defense. Department of Defense Cyberspace Policy Report. Washington, DC: Department of Defense, (2011).

200 David Clark and Susan Landau. "Untangling Attribution." Harvard National Security Journal (Harvard University) 2 (2011).

201 Ibid, at 7

202 Benjamin Edwards, Alexander Furnas, Stephanie Forrest, and Robert Axelrod, "Strategic Aspects of Cyberattack, Attribution, and Blame, 114 " Proceedings of the National Academy of Sciences of the United States of America, 11, (March 14, 2017), pp.2825–2830. As of March 31, 2017: http://www.pnas.org/content/114/11/2825.abstract [hereinafter Edwards et al]

Way Forward: Survey of Literature Outlining Policy Proposals

Public attribution

The presence or absence of technical indicators accounts, therefore only for a part of the broader narrative.[203]Political indicators and the shaping of strategic discourse around the attribution of attacks form a crucial second part. Attribution of a certain attack is in many ways contingent on what states make of it, given what is at stake politically.[204]

Experts[205], including those at the RAND Corporation have argued that while the technical challenges of attribution in cyberspace will remain, the international community can forge a path forward by adopting a robust, integrated and multi-disciplinary approach to attribution.[206] The presence or absence of technical indicators accounts, therefore only for a part of the broader narrative.[207] Political indicators and the shaping of strategic discourse around the attribution of attacks form a crucial second part. Attribution of a certain attack is in many ways contingent on what states make of it, given what is at stake politically.[208]

Studies on attribution thus far have mainly focussed on the technical challenges of tracing an attack back to its origins.[209] In particular, the diamond model advocated by Betz and Pendergast provide a comprehensive framework discussing the strategic organisation required in response to a cyber incident but do not consider the larger geopolitical complexities involved . Bishop and Goldman argue that attribution should be based not on effects of the attack but on the capabilities of the attacker.[210] Schneier comprehensively discusses the varying levels of technical evidence required for attribution.[211] Some models have discussed the strategic angle in terms of game theory but not extended the scope to geopolitical tensions that may underpin said strategy.[212]

Lucas Kello has extended this analysis to attribution in cyberspace and has accounted for the systemic upheaval that the 'cyber revolution' is responsible for.[213] He cites Robert Axelrod's path-breaking analysis on international co-operation which argued that patterns can evolve under conditions of uncertainty if players engage in iterated 'tit-for-tat' games, where they

---

203 Thomas Rid & Ben Buchanan " Attributing Cyber Attacks," Journal of Strategic Studies, 38 (2015) 1-2, 4-37

204 Edwards et al (supra 202)

205 As per Rid and Buchanan, analysts actively opposed ideas of a linear checklist for attribution

206 Davis, John S., Benjamin Adam Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern and Michael S. Chase. Stateless Attribution: Toward International Accountability in Cyberspace. Santa Monica, CA: RAND Corporation, (2017). At <https://www.rand.org/pubs/research_reports/RR2081.html.> [hereinafter 'RAND Corporation']

207 RAND Corporation, (supra 206) at 9.

208 Ibid

209 Wheeler and Larsen, Techniques for Cyber Attack Attribution (Institute for Defense Analysis, Alexandria, VA 2003)

210 M. Bishop and E. Goldman, "The strategy and tactics of information warfare. "Contemp Security Policy 24(1):113–139 (2003)

211 Bruce Schneier," We still don't know who hacked Sony'. The Atlantic., January 15,2016, accessed November 18, 2017, at <https://www.theatlantic.com/international/archive/2015/01/we-still-dont-know-who-hacked-sony-north-korea/384198/>

212 Edwards B, Furnas A, Forrest S, et al. Strategic aspects of cyberattack, attribution, and blame. Proceedings of the National Academy of Sciences of the United States of America 114(11): (2017) 2825–2830

213 The Virtual Weapon (supra 14)

can develop a scheme of mutual reward and punishment. [214]This scenario can only develop if the players know each other's identities and value stability over the next few encounters enough to not deviate from the agreed upon terms that foster stability.[215] Relative obscurity in cyberspace, however reduces the incentive for compliance with the set standards but even partial attribution standards and the looming prospect of an insecure and unstable cyberspace may lead to a tacit understanding among as per Axelrod's theory even if International Law cannot bring about formal codification.

Rid and Buchanan adopt a more holistic approach and argue that attribution is as much an art as it is a science. No technical routine can fully solve the problem of attribution in cyberspace.[216] Quality attribution depends not only on the effective use of skills and tools but also on a positive organisational culture, well run teams and cooperation across sectors.[217] In this context, public communication regarding the attribution process become very important as it can foster public discourse on accountability standards and be a tool for cyber deterrence.

There are three crucial ways in which public declaration of attribution standards could foster the creation of a more robust attribution regime.

1. **Publication after a thorough investigation into the roots of the attack furthers public credibility in the attribution process**. Easily communicated and accessible evidence enables civil society or states to galvanize momentum against the state or non-state entity responsible for the attack. It further cements public confidence in cyber security, which enables them to put more faith into utilising the Internet of Things more frequently.
2. **Publication can lead to better quality of attribution**. One of the major bureaucratic hurdles to technical attribution is fragmentation between researchers and lack of a shared knowledge base across national boundaries.[218] For example, Kaspersky Lab found that analysis done by BAE and Anomali on the connection between the North Korean–associated Lazarus Group and the Bangladesh bank heist focussed on similar methodology-using the wiper tool code.[219] Publication of attribution standards could facilitate discourse on best practices in the arena. Further, publication allows civil society to get involved in the process and question the evidentiary standards used, which could cascade into a more thorough investigation and therefore, ultimately, a higher quality of attribution.
3. **Publication can contribute to deterrence.** Publication of information could signal to the adversary and future adversaries that the state is galvanizing its machinery for retaliation against the attack.[220] It could also enable third-party states to garner public support for imposing sanctions on the offending state depending on the manner in which the attribution finding is communicated.

Importantly, however, publically stated attribution must fulfill standards of accountability and transparency. Attribution findings need to be honest about their limitations.[221] The

214 Ibid, at 132.

215 Robert Axelrod, The Evolution of Cooperation (New York, Basic Books, 1984)

216 Rid and Buchanan, (supra 203) at 14.

217 See Kim Zetter, Countdown to Zero Day (New York: Crown, 2014)

218 Rand Corporation, (supra 206) at 20

219 Ibid

220 Rand Corporation, (supra 206) at 21

221 Sherman Kent, 'Estimates and Influence', Studies in Intelligence 12/3 (1968), 11–21.in Rid and Buchanan, (supra 203) at 30

more honest a public finding is about the uncertainty of its estimate, the more credible the findings become. It is crucial that best practices for attribution standards converge across sectors-both public and private, beyond national boundaries and across various disciplines. This form of convergence could result in the global consortium for attribution as was conceived by the RAND Corporation.

Global Consortium for Attribution

The RAND Corporation explored the nature of an international organization, which it named the Global Cyber Attribution Consortium.[222] The goal was to bring together a broad team of international experts to conduct an independent investigation into major cyber incidents for the purposes of attribution. It would work with victims upon request and publish its methodologies and findings for review. The international community could then use the Consortium's findings to bolster cyber defences and institute follow-on enforcement actions to hold the perpetrators accountable. They were certain of the need for the organisation to be independent of states in its entirety, which would distinguish from analogous investigative organizations such as the International Atomic Energy Agency, for three reasons. First, states' attribution claims are based on evidence-based intelligence that they are often unwilling to share. Second, states would want to shape the findings in order to serve their strategic interests. Third, they would influence the incidents that the Consortium investigates. In its report, the RAND Corporation further explores formal triggering condition standards; the Evidence-Collection Process; Evidence-Assessment Framework; Attribution Confidence Standards; Notification and Public Statement Procedures and Severity and Sophisticated Assessment Procedures.

An extension of the RAND Corporation model that could be explored in further research is the possibility of it undertaking regular inspections to ensure cyber hygiene in all nations and ensure they are undertaking their due diligence obligations to prevent the use of their infrastructure for harbouring future attacks.

Conclusion

A lack of global standards on attribution and the existence of very few publicly conducted attributions remain one of the core fetters to a stable cyber-security regime. The absence of a concrete regime on attribution allows both state and non-state actors to treat cyberspace like the 'Wild West' as they need not fear legal or military sanction for carrying out cyber-attacks. India is yet to articulate clear standards on attributability. This brief explored why the existing legal standards on attribution in the Law of State Responsibility might not be sufficient for carrying out a public attribution. Therefore a new 'control and capabilities' test proposed by peter Stockburger that looks at an intersection of geo-political and technical factors may be more useful for making this determination. It then went on to consider the political and legal advantages of publishing the evidence that underscored an attribution, which might include the sharing of best practices and contribute to deterrence by enabling the adversary to know the capabilities of the state in question. Finally, India might consider how a global consortium on attribution might look like and seek to playa leadership role in the creation of this body by ensuring that a diverse, multi-stakeholder approach to this issue is indeed taken.

222 RAND Corporation, (supra 206) at 35

Summary and Key Takeaways for Policy-Makers

- Technical constraints on attributability have compelled discourse on the evidentiary and legal standards that enable the attribution of a cyber-attack to a certain state.
- Uncertainty of attribution limits the options available to a victim state-both in terms of opting for defensive measures and garnering support from multilateral fora. It also acts an incentive for states to opt for offensive measures in cyberspace as there are reduced possibilities of punishment in the absence of attribution.
- Lack of proper publicly declared parameters for attribution by states therefore fetters the creation of a cyber deterrence regime and thus fosters greater instability in cyberspace.
- India has yet to publicly attribute a cyber attack to a state or non-state entity with reference to existing tenets of International Law
- The traditional legal regime on attribution stems from the legal regime on state responsibility-which has been articulated in the Articles on State Responsibility. State responsibility is fundamentally premised on two elements: (1) the act or omission that leads to a breach of an international obligation and (2) attribution of that act or omission to the state in question. Generally, acts of private persons or groups are not attributable to the state.
- There are however, certain exceptions. The first exception relates to the acts/ omissions of de jure or de facto state organizations. The second exception imputes state responsibility " if the conduct of a non-state actor is "acting under the instructions of or under the direction and control of the state carrying out the said conduct."
- At the 9th International Conference on Cyber Conflict held in 2017, Peter Stockburger put forward a new test known as the 'control and capabilities' test which would be the *lex specialis* (specific law) governing international responsibility in the case of attributing cyber attacks. This approach veers away from the rigid focus on 'control' embodied in the 'effective control' test and focuses on multiple indicative factors that could serve as a guide to effective attribution.
- Stockburger proposes a set of non-exhaustive factors that may be utilised for this purpose, which includes: (1)Relationship between non-state actor and state, (2) The influence the state exerts over the non-state actor; (3) Methods employed by the non-state actor; (4) Motivations of the parties involved ; (5) whether they use similar code; (6) Technical capabilities of the non-state group and (7) geographic location.
- There are three crucial ways in which public declaration of attribution standards could foster the creation of a more robust attribution regime: (1) Publication after a thorough investigation into the roots of the attack furthers public credibility in the attribution process; (2) Publication can lead to better quality of attribution; (3) Publication can contribute to deterrence.

- The RAND Corporation explored the nature of an international organization, which it named the Global Cyber Attribution Consortium. The goal was to bring together a broad team of international experts to conduct an independent investigation into major cyber incidents for the purposes of attribution.
- Even though it is yet to do so,India should develop technical standards for attribution and also look to cement a politically viable process for attribution of cyber attacks.

Brief III: Prevention of Development of Cyber Weapons

Introduction

While malicious software with offensive capabilities have existed and been used as a covert military and intelligence tool, the Stuxnet attack[223] illustrated how computer code may be utilised for the purpose of generating political impact. Therefore, it lead to the re-visiting of older debates on how the acquisition or use of cyber weapons could be regulated or prohibited through 'cyber arms control' regimes.[224]

This brief surveys positions on how the architecture of global governance may be utilised for the purpose of regulating the development and proliferation of cyber weapons. It first highlights concrete perspectives that define a 'cyber-weapon.' It moves on to summarising the clusters of literature on the matter. Then, it considers three international legal regimes that have emerged in the global governance architecture and focuses on India's involvement in them. Finally, it considers perspectives on the possibility of a new treaty regulating the development of cyber weapons and contrasts it with the use of the existing regimes.

Definition of Cyber Weapon

International law is yet to officially define the term 'cyber-weapon,' which now encapsulates within its ambit a broad range of malicious software, possessing a variety of offensive capabilities. Gary Brown's review of existing definitions of cyber weapons argues that the definition of a cyber weapon should be usable by cyber operators and be linked to objects whose primary purpose is to be used as a weapon. [225]Rid and Mcurnby attempted to define it as "computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings."[226] This approach is in line with that of other experts who have identified cyber weapons broadly as having offensive capabilities that cause harm. [227]Stevens validly points out that weapons are a hybrid conglomeration of both human and non-human entities and therefore the weaponization of a specific entity is dependent on the human agent controlling it.[228] Summer and Brown add crucially that these cyber weapons may be used as 'force multipliers' to damage caused through kinetic attacks.[229] Smeets focusses his analysis on the transitoriness of cyber weapons.For him, this refers to the "short-lived or temporary ability to effectively

223 Stuxnet was a malicious computer worm first uncovered in 2010 but believed to be in development since 2005. It targeted Supervisory Control and Data Acquisition (SCADA) systems and while no one claimed responsibility, it was believed to be a joint US-Israeli effort. See Josh Fruhlinger, "What is Stuxnet, who created it and how does it work" (August 22, 2017) at <https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html>

224 Tim Stevens," Cyber Weapons: An emerging global governance architecture," Palgrave Communications, (January 10, 2017).

225 Gary Brown and Andrew Metcalf, " Easier said than done: Legal review of cyber weapons" 7 Journal of National Security Law and Policy (2014)115, 138

226 T. Rid and P.McBurney," Cyber-weapons". The RUSI Journal; 157 (1): 6–13.

227 Boothby B (2016) Cyber weapons: Oxymoron or a real world phenomenon to be regulated? In: Friis K and Ringsmose J (eds). Conflict in Cyberspace: Theoretical, Strategic and Legal Perspectives. Routledge: Abingdon, UK; New York, pp 165–174. Bourne M (2012) Guns

228 Stevens, (supra 224) at 1

229 Sommer and Brown "OECD/IFP Project on Future Global Shocks – Reducing Systemic Cybersecurity Risk, (2011), p. 6

cause harm or damage" by accessing a computer network.[230] Transitoriness is a matter of degree and can be clarified by three important caveats which he highlights. First,cyber weapons that attack software vulnerabilities are more transitory than those that attack hardware due to the greater possibility of finding the software defect nd developing a patch for the intrusion.Second, cyber-weapons attacking closed access systems are more likely to be transitory than those attacking open access ones as open access systems have multiple entry points. This leaves them open to a larger number of attack vectors and makes the cyber attack more difficult to trace and halt. A cyber weapon that causes a larger amount of visible damage is more likely to be transitory as such weapons are more likely to be detected fast.

Statements[231] made by representatives of states at various forums cite a variety of harms including mass/massive psychological manipulation with a view to destabilize society/ state,[232] overthrowing governments or uprooting the social order[233] or causing confusion or disadvantage.[234]

Weapons that are 'inherently indiscriminate' are prohibited under instruments of International Humanitarian Law.[235] The US Department of Defense Law of War Manual states "inherently indiscriminate weapons" are "weapons that are incapable of being used in accordance with the principles of distinction and proportionality"[236] Landau, Lin and Bellovin put forward two criteria which may render a weapon discriminate- (1) It must be capable of being directed against explicitly designated targets and (2) Must be able to minimise the creation of significantly negative effects on entities that is not being targeted.[237]

Literature on Cyber Weapons and Global Governance

In the trajectory to limit inherently discriminate weapons, Stuxnet was widely perceived to be a 'game-changer' in the manner in pushing the international community to develop mechanisms that could regulate the proliferation of cyber weapons.[238] Early authors on global governance in this field advocated the use of criminal law to regulate its use by non-state actors and International Humanitarian Law to do the same with state use of cyber weapons.[239] Subsequent scholarship was divided into two broad strands- the first strand advocated arms control regimes modelled on experiences with chemical, biological and

230 Max Smeets " A matter of time: On the transitory nature of cyber weapons", Journal of Strategic Studies, (2017) , at 7.

231 Tim Maurer & Robert Morgus, Compilation of Existing Cybersecurity and Information Security Related Definitions, NewAmerica (October 2014) at <https://na-production.s3.amazonaws.com/documents/compilation-of-existing-cybersecurity-and-information-security-related-definitions.pdf>

232 Russia, Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space (Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве), 2011

233 Cuba, Submission to the United Nations General Assembly Resolution A/58/373, p. 5 State > Other (In paragraph)

234 Report of UN Secretary General, Developments in the field of information and telecommunications in the context of international security, Submission of Philippines to the United Nations General Assembly Resolution UN Doc A/56/164 (July 3 ,2001) p. 4

235 The ICRC has stated this in Rule 71 of their Rules on Customary International Humanitarian Law, at <https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule71>

236 Office of General Counsel Department of Defense. Weapons. In Law of War Manual. Washington, DC: United States Department of Defense (2015) 340

237 Collateral damage in terms of jus in bello/IHL

238 Farwell JP & Rohozinski R ("Stuxnet and the future of cyber war" Survival; 53 (1): 23–40 (2011)

239 Sofaer AD & Goodman SE" A Proposal for an International Convention on Cyber Crime and Terrorism." Working paper. Stanford University: Stanford, CA (2000).

nuclear weapons as a possible framework.[240] The second broad cluster of scholarship looks at the criminalization of the use of cyber-weapons through regimes such as the Budapest Convention.[241] Both these schools of thought rely on a centrally binding legal authority and a hierarchical bureaucratic structure.

Josepph Nye has tried to bridge the gap between the two schools by considering the nuclear arms control regime cautiously when seeking to regulate the development of cyber weapons.[242]He discusses how strategic prudence in the non-use of nuclear weapons developed into a norm. The norm of non-use did have a preventive effect on leaders of most major nations, although this is currently being tested with the rise of leaders such as Donald Trump[243] and states such as North Korea. Nye argues that the entanglement of benefits received from the internet would prevent attacks on the Domain name System. [244]Further, the fact that cyber war is relatively new with relatively unforeseen consequences might trigger a norm preventing the use of cyber-weapons. He draws an analogy with the 1925 Geneva Protocol which prohibited the use but not possession of chemical and biological weapons- a norm that developed mainly through a fear of retaliation.[245] He further acknowledges that the difference between a computer program which is a weapon and a non-weapon is simply intent and therefore banning the possession of programs would not be possible.[246]Therefore, he argues that the normative taboo might work by prohibiting attacks against certain targets, rather than trying to ban weapons outright.[247]

Stevens takes this one step forward and considers how analysis of the regime should be done through the lens of global governance by considering how global governance architecture[248] may influence politics in this space. [249] This architecture explores and analyzes spaces where interactions between the concerned actors and regimes may intersect with each other and urges a focus on the institutional and procedural paths by which these various components may come together. This approach may be useful when analysing the

240 Louis Arimatsu, "A treaty for governing cyber-weapons: potential benefits and practical limitations" in Czosseck C, Ottis R and Ziolkowski K (eds). Proceedings of the 4th International Conference on Cyber Conflict, Tallinn, Estonia, 5–8 June. CCD COE Publications: Tallinn, pp 91–109; Maybaum M and Tölle J (2016) "Arms control in cyberspace: architecture for a trust-based implementation framework based on conventional arms control methods" in: Pissanidis N, Rõigas H and Veenendaal M (eds). Proceedings of the 8th International Conference on Cyber Conflict: Cyber Power, Tallinn, Estonia, (May 31- June 3). CCD COE Publications: Tallinn, pp 159–173.

241 Prunckun H 'Bogies in the wire': Is there a need for legislative control of cyber weapons? Global Crime; 9 (3): (2008) 262–272.

242 Joseph Nye, "Normative Constraints on Cyber Arms" in Osler Hampson and Michael Sulmeyer, Getting Beyond Norms:New approaches to cybersecurity challenges (Centre for Governance and Innovation, 2017), 20 [hereinafter Joseph]

243 Adam Mount, Letting It Be an Arms Race, The Atlantic, January 12, 2018, accessed June 30, 2018, at <https://www.theatlantic.com/international/archive/2018/01/trump-nuclear-posture-review/550400/>

244 Joseph (supra 242) at 20, at <https://sipa.columbia.edu/sites/default/files/Nye_Normative_Restraints_on_Cyber_Conflict_0502.pdf>

245 Ibid

246 Joseph (supra 242) at 20

247 Ibid

248 Frank Biermann, Phillip Pattberg & Harro Van Asselt,"The fragmentation of Global Governance Architectures: A Framework for Analysis " 9 Global Environmental politics 4 (2009) 14,15 (A "global governance architecture" is "the overarching system of public and private institutions, principles, norms, regulations, decision-making procedures and organizations that are valid or active in a given issue area of world politics"

249 Stevens, (supra 224) at 5

various treaty regimes and related initiatives that have emerged to secure the prevention of the development of cyber weapons.

Sources of the Global Legal Regime Regulating the Development of Cyber Weapons

There are three broad legal regimes that could apply to cyber weapons-although they are not mutually exclusive and operate together: (1) International Humanitarian Law (IHL), (2) International Cyber Crime regime and (3) Export control regimes[250]

International Humanitarian Law

The first crucial source of the global legal regime is international humanitarian law (jus in bello) There is yet to be international consensus on the extent of applicability of IHL to the use of cyber-weapons The Tallinn Manual addresses cyber-weapons within its framework and draws from existing principles of IHL-namely distinction, military necessity and proportionality. It declares clearly that cyber weapons are prohibited from causing 'unnecessary suffering' to combatants unless they are furthering a military objective, which means that this obligation must be written into the way in which cyber weapons are designed.[251]

The GGE process, however, was fraught right from its inception, with a lack of consensus on the applicability of IHL to cyberspace. In the build up to the 2015 Report, the Russian and Chinese delegates explicitly objected to the use of the term in the final report.[252] Thus it only broadly referred to "humanity, necessity, proportionality and distinction." [253] The applicability of IHL to this field was also one of the factors responsible for the gridlock in the present GGE as the publically released statement by Cuba made it very clear that the applicability of IHL would legitimize military action through the use of ICTs.[254] Russia and China were also reportedly on board with Cuba. On the other hand, the United Kingdom and USA have confirmed these principles in their war doctrines.[255]

International regime on cybercrimes

The next major regime that could apply to the development of cyber-weapons[256] is The Budapest Convention.[257]The objective of the convention is to harmonize the standards of

250 Ibid

251 Michael Schmitt (ed)(2013) Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press: Cambridge, UK; 143.

252 Stefan Soesanto & Fosca D'Incau, The UNGGE is dead: Time to fall forward on cyber governance" European Council on Foreign Relations, August 15, 2017,accessed November 18 2017, at <www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance>

253 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ,UN Doc. A/70/174 (July 22, 2015) [hereinafter 2015 GGE Report].

254 71 UNGA: Cuba at the final session of Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security. Cuba's Representative Office Abroad, June 23, 2017, accessed December 13, 2017, at <http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information> [hereinafter Cuba Representative office]

255 Ministry of Defence. (2013) Cyber Primer. Ministry of Defence: London; Office of General Counsel Department of Defense. Weapons. In Law of War Manual. Washington, DC: United States Department of Defense, (2015), 340

256 Steven, (supra 224) at 4; Jakobi AP "From prohibition to regulation? The global governance of illegal markets". Paper presented at the Comparing the Global Governance of Illegal Markets workshop, October, Bielefeld, Germany (2015).

257 Council of Europe Convention on Cybercrime, ETS 185 November 23, 2001, accessed November 21 2017 at <http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf>

national crime legislation and further global policing. While it was originally a Council of Europe initiative, several non-European states, including Canada, Japan, Australia and the United States have opted into the process. Brazil and India have not signed it as they did not play a role in drafting the treaty[258], and Russia argues that this form of transnational policing violates its sovereignty.[259] Alexander Segel, the Executive Secretary of the Convention noted in his remarks at CyFy 2016 that India would gain from joining the Convention as it would be able to contribute to the Convention as a party in the future and be a priority nation for capacity building.[260] On the other hand, China and Russia have suggested that the Shanghai Cooperation Organization is their preferred forum for cybercrime cooperation.[261] While there is no explicit mention of cyber-weapons in the text of the Convention, Article 4.1 mandates that states refrain from intentional actions via computer systems that result in the "damaging, deletion, deterioration, alteration or suppression of computer data without right". As per Article 4.2, state parties have the right to require that such acts must result in serious harm. While this would presumably cast an obligation on states to not use indiscriminate cyber weapons, participation in the component market remains a legal ambiguity that may need to be addressed.[262] According to Steven, this framework could criminalize the use and proliferation of cyber weapons and thereby possibly play a role in disrupting the supply chains of cyber weapons.[263]

Export Control Regimes

The newest source of cyber weapons regulations is the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (1996)[264]. It was initially applicable to the conventional arms and dual-use weapons used for the production of weapons of mass destruction (WMD).[265] It was expanded in 1998 to include controls against strong encryption software and in 2013 evolved to also include surveillance and intelligence gathering software by controlling the creation and use of hardware and software associated with intrusion software[266] Intrusion software was defined in the Wassenaar Arrangement as "software specially designed or modified to avoid detection by monitoring tools, or to defeat protective countermeasures" and the extracted data from a computer or network device modified "standard execution path" of a program to allow "the execution of externally provided instructions."[267]

EU member states incorporated these rules into domestic legislation.[268] While the United

---

258 F. Calderoni The European legal framework on cybercrime: striving for an effective implementation. Crime, Law & Social Change; 54 (5)(2010): 339–357.

259 Ibid

260 Alexander Seger,(Executive Secretary Cybercrime Convention Committee, Council of Europe) " India and Budapest Convention: Why not?", accessed November 21 2017, at <https://rm.coe.int/16806a6698>

261 Ibid

262 MJ Wolf and N Fresco , "Ethics of the software vulnerabilities and exploits market." The Information Society: An International Journal; 32 (4):269–279.

263 Steven, (supra 224) at 4.

264 The Wassenaar Arrangement- On Export Controls for Conventional Arms and Dual-Use Goods and Technologies accessed November 18 2017, at <http://www.wassenaar.org/about-us/>

265 Ibid

266 "classes of hardware and software "specially designed or modified for the generation, operation or delivery of, or communication with 'intrusion software'"

267 Garrett Hinck, Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research, Lawfare, January 5, 2018, accessed July 1, 2018, at <https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research> [hereinafter Hinck]

268 Alan Cohn, " Export Controls the next frontier in cybersecurity" Microsoft, April 23 2016, accessed November 18 2017 at <https://blogs.microsoft.com/eupolicy/2017/04/13/export-controls-the-next-frontier-in-cybersecurity/>

States initially displayed similar posturing,a public consultation in 2016 revealed significant opprobrium. [269]The principal objection was that the arrangement would criminalize researchers seeking to improve security product using malware systems.This harks back to the dual-nature of malware, which can be used both for defensive purposes and offensive deployment.

At the December 2017 meeting of the Wassenaar Arrangement,the United States successfully managed to negotiate exceptions based on research use to the existing export controls regime.[270]

The list of amendments to the Wassenaar regime include[271]:

(a) With regard to the description of controlled software,replacement of the term 'specially designed' to operate or communicate with intrusion software with the term 'command and control' intrusion software

(b) The addition of an exception for software which creates updates authorized by the operator or owner of the computer system

(c) Addition of exemptions for controls that is involved in the development of intrusion software or in the development of software which operates, controls or delivers intrusion software

(d) An addition of a clarification note, which does not diminish the right of national authorities to ascertain the extent of compliance with the existing control regime.

While these amendments act as a major boost for the cyber-security community,the definition of 'intrusion software' still remains relatively broad.[272]The security community will be waiting for the submission of the Trump's administration's list of controls to the Wassenaar Control List , which are due by March and will be negotiated later this year[273]

The future of the Wassenaar Regime certainly depends on balancing the control of export of illegitimate cyber weapons with the incentivising of genuine security research. [274]This task is further complicated by weak enforcement mechanisms under the arrangement that vary considerably from one jurisdiction to another.[275] Despite that, both USA and Russia remain a part of this 41-nation-club which is a positive sign for the future of the regime. By enabling the amendments in December,2017, the regime has shown that it is flexible enough to balance the needs of the various nation states who are members of the Arrangement and through this flexibility, also keep the non-state lobbying groups such as the cyber-security community satisfied.

After a concerted bid to become a part of the Wassenaar arrangement,[276] India became the

269 "Major Business and Tech Groups Call on Administration Officials to Renegotiate Wassenaar Arrangement to Strengthen"Cybersecurity, ITIC accessed November 21, 2017 at <https://www.itic.org/news-events/news-releases/major-business-and-tech-groups-call-on-administration-officials-to-renegotiate-wassenaar-arrangement-to-strengthen-cybersecurity>,

270 Shaun Waterman, The Wassenaar Arrangement's latest language is making security researchers very happy, Cyberscoop, December 20, 2017, accessed July 13, 2018, at <https://www.cyberscoop.com/wassenaar-arrangement-cybersecurity-katie-moussouris/>

271 Hinck (supra 267)

272 Ibid

273 Ibid

274 Fabian Bohnenberger, "The Proliferation of Cyber-surveillance technologies: Challenges and Prospects for Strengthened arms control" 3 Strategic Trade Review 4 (2017) 81-102

275 Stewart Baker, Wassenaar, Cybersecurity, and Why European Officials Get Better Lunches than Americans, Lawfare, November 5, 2017, accessed January 4, 2018, at <https://lawfareblog.com/wassenaar-cybersecurity-and-why-european-officials-get-better-lunches-americans>

276 "Nuclear Power: India trying to join Wassenaar Arrangement, Australia Group, Livemint, July 9, 2017, accessed June 4, 2018, at <http://www.livemint.com/Industry/H0yXPv8NcmpTz3adZYOfOI/Nuclear-Power-India-trying-to-join-Wassenaar-Arrangement-A.html> [India Wassenaar]

42nd member of the Wassenaar Arrangement in December, 2017.[277]India has satisfied all elements needed to be a part of the regime-most recently by approving SCOMET (Special Chemicals, Organisms, Materials, Equipment, and Technologies) items.[278] Being a part of the Wassenaar arrangement brings with it two main benefits for India.[279] First, it cements the global reputation of India as a 'responsible nuclear power'[280] that is willing to abide by the rules of the road. Second,as a supplier state, India would have more discretion both in terms of shaping its own exports and having a say in the crafting of the regime itself. This could be crucial for improving the credibility India has among the international community in terms of meeting its nonproliferation obligations and pave a way for its entry into other mechanisms such as the Nuclear Suppliers Group.[281]

Global Treaty for the Regulation of Cyber Weapons

Recently, there has been academic discourse on whether cyber weapons should be regulated through informal means utilising the global governance architecture or through a more formal treaty regime. The benefits of a treaty regime seem obvious-for the solidification of cyber norms and ensuring compliance at the domestic level.[282]The challenges of putting together a treaty regime are obvious given the differing interests of states in cyberspace and common calls for sovereignty. As Slack observes, "the fundamental conception of cyberspace, the lack of a common terminology, the issue of verification, and the dual-use, asymmetric, fast-paced and non state-centric nature of the domain … ultimately render a treaty approach unfeasible". [283]

One such issue area is certainly cyber weapons governance. A 'one-size' fits all approach may ignore the various contextual and strategic concerns that are essential in any norms formulation process and therefore working on the existing global governance mechanisms may bear more fruit.

Conclusion

There is no doubt that International Law prohibits the use and by implication, the development of inherently indiscriminate cyber weapons, such as NotPetya[284] and

277 Rakesh Sood, Joining Wassenaar is India's latest step in the quest for the 'responsible nuclear power' tag Observer Research Foundation, December 15, 2017, accessed July 8, 2018, at <http://www.orfonline.org/research/joining-wassenaar-is-indias-latest-step-in-the-quest-for-the-responsible-nuclear-power-tag/> [hereinafter Rakesh]

278 India Wassenaar (supra 275)

279 Rajeswari Pillai Rajagopalan and Arka Biswas, "Wassenaar Arrangement: The case for India's membership" ORF Occasional Paper 92 (2016)

280 Rakesh (supra 277)

281 Rajeshwari Pillai Rajagopalan and Arka Biswas, " India's Membership to the Nuclear Suppliers Group" ORF Issue Brief No. 141 (2016)

282 Mette Eilstrup-Sangiovanni, " Why the world needs an International Cyberwar Convention," Philosophy and Technology (2017), 1-29

283 C.Slack Wired yet disconnected: the governance of international cyber relations. Global Policy; 7 (1): 69–78.

284 Josh Fruhlinger, "Petya ransomware and NotPetya malware: What you need to know now" (CSO, October 17, 2017) at <https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html> ("Petya and NotPetya are two related pieces of malware that affected thousands of computers worldwide in 2016 and 2017. Both Petya and NotPetya aim to encrypt the hard drive of infected computers, and there are enough common features between the two that NotPetya was originally seen as just a variation on a theme. But NotPetya has many more potential tools to help it spread and infect computers, and while Petya is a standard piece of ransomware that aims to make few quick Bitcoin from victims, NotPetya is widely viewed as a state-sponsored Russian cyberattack masquerading as ransomware.")

WannaCry.[285] Achieving a normative framework of commitments that enforces this rule is a challenging task given varied strategic interest and legal perspectives across the international community. In this context, the negotiation of an all-encompassing treaty may be too idealistic a goal. Therefore, as argued by Stevens, utilising the emerging systems to foster a cohesive global governance architecture that encourage compliance with existing standards may be a more realistic and inclusive process. There are three inter-linked regimes that form a part of this architecture-IHL, international cybercrimes convention and the export-control regime. India has already signalled an intent to play a greater role in the existing architecture and could utilise this increased participation to further its strategic interest and international reputation. Considering and solidifying positions on the questions outlined in this paper could help India engage in the existing architecture.

285 Josh Fruhlinger, "What is WannaCry Ransomware, How does it infect and who was responsible" (CSO, September 27, 2017) at <https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html>("WannaCry is a ransomware worm that spread rapidly through across a number of computer networks in May of 2017. After infecting a Windows computers, it encrypts files on the PC's hard drive, making them impossible for users to access, then demands a ransom payment in bitcoin in order to decrypt them.")

Summary and Key Takeaways for Policy-Makers

- International law is yet to officially define the term 'cyber-weapon,' which now encapsulates within its ambit a broad range of malicious software, possessing a variety of offensive capabilities.
- Weapons that are 'inherently indiscriminate' are prohibited under instruments of International Humanitarian Law.
- It is crucial to consider how the global governance architecture may impact politics in the space of cyber weapons proliferation. This architecture explores and analyzes spaces where interactions between the concerned actors and regimes may intersect with each other and urges a focus on the institutional and procedural paths by which these various components may come together. This approach may be useful when analysing the various treaty regimes and related initiatives that have emerged to secure the prevention of the development of cyber weapons.
- There are three broad legal regimes that could apply to cyber weapons-although they are not mutually exclusive and operate together: (1) International Humanitarian Law (IHL), (2) International Cyber Crime regime and (3) Export control regimes.
- After a concerted bid to become a part of the Wassenaar arrangement, India became the 42nd member of the Wassenaar Arrangement in December, 2017. India has satisfied all elements needed to be a part of the regime-most recently by approving SCOMET (Special Chemicals, Organisms, Materials, Equipment, and Technologies) items. Being a part of the Wassenaar arrangement brings with it two main benefits for India.
- First, it cements the global reputation of India as a 'responsible nuclear power' that is willing to abide by the rules of the road. Second,as a supplier state, India would have more discretion both in terms of shaping its own exports and having a say in the crafting of the regime itself. This could be crucial for improving the credibility India has among the international community in terms of meeting its nonproliferation obligations and pave a way for its entry into other mechanisms such as the Nuclear Suppliers Group
- Recently, there has been academic discourse on whether cyber weapons should be regulated through informal means utilising the global governance architecture or through a more formal treaty regime.India should not adopt a 'one-size' fits all approach as doing so may ignore the various contextual and strategic concerns that are essential in any norms formulation process and therefore working on the existing global governance mechanisms may bear more fruit.

Brief IV: Countermeasures and the Extent of Force

Introduction

In international law, countermeasures are a crucial feature of a decentralised state system that allow injured states to enforce their rights and restore the legal relationship which the state indulging in the internationally wrongful act has ruptured.[286] Simply put, the law of countermeasures allows the victim state of an internationally wrongful act attributable to another State, to take otherwise unlawful measures against the responsible State, subject to specific conditions, which this brief will discuss.[287] For cyber operations that fall below the threshold of 'armed attack,' invoking the legal regime on countermeasures may enable states to prevent, mitigate or cease the ongoing injury caused to their infrastructure by cyber operations. This brief will trace the legal regime on countermeasures, as it may be applicable to cyberspace and then go on to consider recent state practice on the use of countermeasures.

Legal Regime on Countermeasures

The customary international law doctrine of countermeasures has been codified in Articles 49-54 of the Articles on State responsibility. Article 49 specifies three crucial conditions limiting the use of countermeasures. (1) As a threshold, countermeasures are only available when there is malicious cyber activity attributable to a state. (2) They are temporary or provisional in character and therefore their aim would be a restoration of legality between the two states. They are a form of inducement to comply with legal obligations, not punishment. (3) They should as far as possible choose countermeasures that are reversible.[288] Paragraph 1 of Article 50 further specifies that countermeasures should not affect : (a) The obligation to refrain from the threat or use of force as embodied in Article 2(4) of The UN Charter; (b) Obligations for the protection of fundamental human rights. The Commentary clarifies that most human rights treaties clarify certain fundamental human rights cannot be derogated from even in times of war or public emergencies.[289] (c) Obligations of a humanitarian character prohibiting reprisals against different classes of protected persons. These reprisals are codified in the Geneva Conventions and are widely accepted in the international community.[290](d) They must uphold the peremptory norms of international law known as jus cogens.[291] Countermeasures must also be proportionate to the injury suffered, considering both the gravity of the injury suffered and the rights involved. The Commentary on the Draft Articles takes us back to the purpose required by Article 49, which highlights that each countermeasure must have a clearly defined purpose, linked to ensuring the wrongful act ceases and not be unnecessarily punitive. States are not allowed to deploy 'shock and awe' tactics to intimidate states into compliance.[292]

---

286 International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, November 2001, Supplement No. 10 (A/56/10), chp.IV.E.1,

287 Brian J. Egan, "International Law and Stability in Cyberspace", 35 Berkeley J. Int'l Law. 169 (2017).

288 Gabčikovo-Nagymaros Project, Hungary v Slovakia, Order, , [1997] ICJ Rep 3, Para 88

289 Article 4 of International Covenant on Civil and Political Rights, Article 15 of the European Convention on Human Rights and Article 27 of the American Convention on Human Rights

290 Matthias Rufert, " Reprisals," Oxford Public International Law, at <http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1771>

291 Jus Cogens, Legal Information Institute, accessed July 1, 2018, at <https://www.law.cornell.edu/wex/jus_cogens>

292 Brian J. Egan, "International Law and Stability in Cyberspace", 35 Berkeley J. Int'l Law. 169 (2017).

The doctrine of counter-measures stipulates that the injured state must attempt to negotiate with the erring state and notify it of its intent to take counter-measures. Further, the counter-measure must be ceased once the wrongful act has ceased to take place. Counter-measures may be taken in cyberspace in response to a wrongful act. According to Brian Egan, former Legal Advisor to the U.S. State Department, countermeasures may take the form of cyber-based countermeasures or non-cyber-based countermeasures. This is a decision that lies at the discretion of the state involved.[293]

The Tallinn Manual, which is a report of a Group of independent Experts and not an incantation of official policy, makes clear that countermeasures are not available in response to a cyber operation carried out by a non-state actor unless it is attributable to a state.[294] It uses the example of a hacktivist group located in one state exploiting a buffer overflow vulnerability in a SCADA (Supervisory Control and Data Acquisition)[295] that is situated in another state. A take-down operation may only be mounted if the group's activities are attributable to the state or the state has violated its obligations under the due diligence principle to maintain cyber hygiene.[296]

As per the commentary to the Articles on State Responsibility, assessment of damage is not limited to the damage sustained by the victim State. As was explained in the *Air Services litigation*[297], the implications on broader community interests may be considered. In that case the economic impact was considered not only with respect to effects felt in the injured state but also impacts on air traffic safety as a whole. According to Egan, this could be of potential significance in a cyber context if cyber terrorism is recognised as a crime that may be prosecuted under the doctrine of universal jurisdiction as that could justify countermeasures.[298]

Gaps in Scholarly Literature and State Practice

The international law literature has very little material on countermeasures as a lawful response to cyber-attacks. [299]The scholars at the Chatham House Conference on Cyber Security and International Law surmised that this is so because legal scholars working in the cyber security field tends to be divided among experts on issues of municipal law such as internet governance or experts on the use of force.[300] General scholars on public international law are yet to enter this field.[301]As counter-measures and the law of state responsibility is an issue of general international law, there is yet to be focussed academic discourse in this realm.

One notable exception is work by Oona Hathaway.Hathaway argues against an expansive countermeasures regime in cyberspace and advocates for the implementation of

293 ibid

294 Tallin Manual, Rules 15 to 17

295 Carl Gould, What is SCADA? Inductive automation, accessed July 3, 2018, at <https://inductiveautomation.com/what-is-scada>

296 Tallin Manual, (supra 62) Rules 6-7

297 Reports of international arbitral awards, Air Service Agreement of 27 March 1946 between the United States of America and France (9 December 1978) Vol. XVIII pp. 417-493, at <http://legal.un.org/riaa/cases/vol_XVIII/417-493.pdf>

298 Tallin Manual, (supra 62) Rules 6-7

299 Chatham House, " Meeting Summary: Cybersecurity and International Law," at <https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/290512summary.pdf>

300 Ibid

301 Ibid

appropriate regulatory controls.[302] First, from a legal standpoint, proponents of an expansive countermeasures regime in cyberspace usually point to Article 49 of the Articles on State Responsibility which establishes that an injured state may take countermeasures against another state responsible for an internationally wrongful act. However, Oona Hathaway validly argues that immediately succeeding Article 49 is Article 50 which deals with 'Obligations not affected by counter-measures' and includes the obligation to refrain from the threat or use of force as embodied in the Charter. She goes on to acknowledge the possibility that there may be cyber operations that do not amount to the use of force but may instead be wrongful intervention, which would trigger a right to engage in a similar cyber-attack. However, given the blurred lines between interference and the use of force, Hathaway cautions against an expansive approach. From a policy perspective, she believes that a broad right to non-interference would mean that states may be able to respond to a wide range of extra-territorial activities by other states such as government funding of NGOs. While her approach is ethically sound, adopting an excessively restrictive counter-measures regime may result in states having their hands tied and not being able to respond adequately to interference. Instead an appropriate norm for determining interference and a wrongful act must be worked towards to closely regulate actions in cyberspace, which would be a better outcome than leaving states defenseless.

This leads to legal gaps in the Literature,which should be clarified.[303] Strategically, states value ambiguity, as it enables them to carry out operations under what Michael Schmitt terms a 'mist of uncertainty.' [304] Uncertainty in the legal regime makes it less likely that its actions will be termed unlawful. Schmitt argues however that states seeking to exploit these ambiguities may find themselves victims of cyber attacks that are not clearly described as being unlawful. As an example, Schmitt cites the US response to the Russian hacking of the Democratic National Convention.[305] Due to the ambiguities in what may amount to coercion and therefore, unlawful interference in cyberspace, the US refrained from taking actions in retaliation,that may be classified as 'countermeasures.'

Available State Practice

At the GGE, Cuba[306], China and Russia actively opposed the application of the regime of state responsibility, including countermeasures to cyberspace, while the United States was disappointed with this stonewalling.[307]

The US Department of Defense is yet to refer to countermeasures or retortions[308] in detail, although it has enacted sanctions which are a form of retortion in response to cyber activity.[309] Dunlap argues that this omission is understandable as the DoD Manual is a

302 Oona Hathaway,' The drawbacks and dangers of Active Defense'(2014 6th International Conference on Cyber Conflict, NATO CCDCOE Publications) https://ccdcoe.org/cycon/2014/proceedings/d2r1s5_hathaway.pdf, accessed 23rd July 2018

303 Michael Schmitt, "Grey Zones in the International Law of Cyberspace" 42 Yale Journal of International Law 2 (2017) [hereinafter Schmitt Grey]

304 Michael Schmitt, " 'Cyberspace and International Law' : The Penumbral mist of uncertainty" 126 Harvard Law Review Forum 176 (2013)

305 Schmitt Grey (supra 303) at 2

306 Cuba Representative Office (supra 31) at <http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information>

307 Markoff (supra 101) at <https://usun.state.gov/remarks/7880>

308 See Thomas Giegerich," Retorsion," Oxford Public International Law (March 2011), at <http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e983>

309 Charles Dunlap, "Cyber Operations and the New Defense Department Law of War Manual,"Lawfare, June 15, 2015, accessed June 14, 2018, at <https://www.lawfareblog.com/cyber-operations-and-new-defense-department-law-war-manual-initial-impressions>

document that applies during war time whereas the regime on counter-measures was designed to apply during peace-time as well. [310] The UK Attorney-General has stated that states do not need to give prior notification of countermeasures taken in response to covert cyber intrusions.[311] A crucial condition to this principle is that the utilisation of secrecy must be "necessary and proportionate to the original illegality" that the countermeasure is seeking to address. This stance is not in line with the Articles on State Responsibility, which holds that prior notification must be given before taking any countermeasure.[312] However, Wright responds by saying that it would not be correct for international law to require a countermeasure to expose highly sensitive capabilities when defending the country.[313] It is unclear whether this notion applies in all cases or only if the original intrusion was covert.[314]

The most recent issue that needs to be analysed in terms of this framework is the idea of 'Active Cyber Defense.'[315] by the private sector. While the notion of active defense occurs often in national strategy documents or public debates, the contours of this concept have not been sketched in a precise definition that is available to the public.[316] The US Department of Defense describes 'active cyber defense' as " the synchronized real-time capability to deter, detect, analyze and mitigate threats and vulnerabilities" but does not specify the nature of actions that may be utilised under this concept.[317]

As of now, the private sector has not been empowered by specific domestic legislation to conduct 'hackbacks.' The authority to deploy defensive measures is still within the government domain.[318] Rep. Tom Graves and Rep. Kyrsten Sinema introduced the Active Cyber Defense Certainty Act, which would allow victims of cyber intrusions to take defensive measures that would otherwise violate US law on unauthorised access to computers. The Act includes supervision by the Federal Bureau of Investigation, which means that these measures could be attributed to the state. The compatibility of these measures with the legal rules on state responsibility is yet to be assessed.[319]

Messerschmidt has argued that private sector hackbacks are legally and practically valid , given the large nature and scale of transboundary harm caused.[320] It is justified for the state to violate its obligation of due diligence and allow private actors to effectively defend crucial cyber infrastructure. Shifting the cost of taking these measures would contribute to a more robust cyber infrastructure. Hoffman and Levite at the Carnegie Endowment endorse this

---

310 Ibid

311 Wright Speech (supra 43) at <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>

312 Articles on State Responsibility Art. 52

313 Wright Speech (supra 43)

314 Isa Qasim, "United Kingdom Attorney General's Speech on International Law and Cyber" Just Security, May 23,2018, accessed June 17, 2018 at <https://www.justsecurity.org/56853/united-kingdom-atty-generals-speech-international-law-cyber-key-highlights/>

315 Hannah Kuchler, " Cyber Insecurity: Hacking Back", The Financial Times, July 27, 2015.

316 The Virtual Weapon, (supra 14) at 231.

317 Department of Defense Strategy for Opening in Cyberspace (Washington D.C., Department of Defense, July 2011)

318 The Virtual Weapon (supra 14) at 230

319 Kristen Eichensehr, ' Would the United States be responsible for private hacking?" Just Security (Oct 17,2017) https://www.justsecurity.org/46013/united-states-responsible-private-hacking/

320 Jan E. Messerschmidt, Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm, 52 Colum. J. Transnat'l L. 275, 324 (2013)

industry-driven approach as long as there are a set of internationally recognised principles that regulate the use of hackbacks and thereby foster stability.[321]

Kello identifies both costs and benefits to a shift to active cyber defense[322] by the private sector.[323] He argues that it could positively impact national security by: (1) Improving strategic depth and flexibility in a future where private actors are the ones most threatened by cyber attacks; (2) By fostering civil-military symbiosis in a domain where technical expertise is indispensable but scarce and (3) By enabling states to engage in plausible deniability.[324] He cautions against extensive use of cyber defense by the private sector as this could attract foreign censure; harm innocent third parties and accelerate conflict leading to greater instability. Instead of inviting actors alien to the prevailing international order to undertake actions-the full consequences of which they may not comprehend or have a stake in, should remain, as Kello puts it, " a reactive enterprise."[325]

Conclusion

This brief identified that there is a lack of scholarship and state practice that merges the international legal regime on counter-measures with the practical measures states may resort to in cyberspace. States have opted for strategic ambiguity in this field as they feel that these 'grey zones' may allow them to take tactical retaliatory options even though they could find themselves victims of cyber attacks in the process. Scholarship is also limited simply because there has been little opportunity to discuss issues of International Law with reference to counter-measures that are practically opted for by states.

Analysis of the legal implications of active cyber defense may serve as the edifice for clearing the gaping holes that exist both in state practice. Without a legal or normative framework, there lies no distinction between legitimate and illegitimate action, which encourages states to exploit this ambiguity but simultaneously fall victim to other states exploiting the same. Given that most recent cyber-attacks in the recent past do not cross the use of force threshold, developing a coherent normative regime is imperative for securing the stability of cyberspace.

Therefore, with the increased need to ward off attacks that do not meet the threshold of 'use of force', India should articulate a comprehensive understanding of counter-measures,in conjunction with private sector actors. This would enable the government to work in symbiosis with the private sector to legally respond to cyber threats without compromising their position.

321 Wyatt Hoffman and Eli levite, "Private Sector Cyber Defense," (2017) at <http://carnegieendowment.org/2017/06/14/private-sector-cyber-defense-can-active-measures-help-stabilize-cyberspace-pub-71236>

322 Much of the policy documents view active cyber defense as a more proactive approach by government rather than by the private sector whereas academic literature terms actions by the private sector as

323 The Virtual Weapon, (supra 14), 237-246

324 Ibid, 237-242

325 Ibid, at 246.

Summary and Key Takeaways for Policy-Makers

- In international law, countermeasures are a crucial feature of a decentralised state system that allow injured states to enforce their rights and restore the legal relationship which the state indulging in the internationally wrongful act has ruptured. Simply put, the law of countermeasures allows the victim state of an internationally wrongful act attributable to another State, to take otherwise unlawful measures against the responsible State, subject to specific conditions, which this brief will discuss.
- For cyber operations that fall below the threshold of 'armed attack,' invoking the legal regime on countermeasures may enable states to prevent, mitigate or cease the ongoing injury caused to their infrastructure by cyber operations.
- Apart from certain notable exceptions such as the work of Oona Hathaway and Mike Schmitt, there is limited scholarly discourse on the application of countermeasures in cyberspace. Further, with the exception of the UK Attorney General's remarks in May, 2018, there is limited state practice on the matter. This lack of clarity may stem from the desire of states to maintain legal ambiguity when operating in cyberspace although this could lead to more instability in cyberspace-making states and private actors increasingly becoming the victims of cyber attacks with no legal recourse in international fora.
- Therefore, with the increased need to ward off attacks that do not meet the threshold of 'use of force', India should articulate a comprehensive understanding of counter-measures,in conjunction with private sector actors. This would enable the government to work in symbiosis with the private sector to legally respond to cyber threats without compromising their position.

Conclusion: the Road Ahead

This report sought to identify the key developments that have taken place thus far in the global bid to regulate cyberspace and explore, in particular, the roadblocks that have prevented the creation of a stable regime. It also considered how India could strategise a role for itself in clearing up the roadblocks and in doing so,gain geo-political traction. It recognised that the failings of the GGE have been rooted in an ideological deadlock, on Cold War Lines, that firmly centre around the essence of cyberspace itself. The United States and the West have opted for a 'soft' norms-based approach that recognises the extension of existing International Law to cyberspace with a focus on the free-flow of information. Russia and China, along with other members of the Shanghai Cooperation Organisation have chosen to focus on information security and sovereignty when it comes to the regulation of information in cyberspace and have rejected the application of existing norms of customary international law to cyberspace. They have suggested te carving out of a separate treaty for the regulation of cyberspace,with new laws of its own.

India will have to decide which group of states to align with or opt for a combination of the two-approaches. The report stressed on the significance of existing tenets of International Law in the norm-entrepreneurship process as a construct that can set the baseline for negotiations. At the same time, the process must not get de-railed by a deracinated approach to norms that does not consider how living entities interact with the phenomenon of cyberspace. The formation of a study group under that considers the future of the cyber norms process suggests that India is ready to take the lead in this matter and strategically steer it, given the deadlock that formed at the GGE.

The Report focussed on four key issues that would need to be addressed in the norms formulation process towards a stable cybersecurity regime. The first brief considered an inherent right to self-defense, which was the first point of diversion among the players at the GGE. Cuba and reportedly Russia and China disagreed with the application of self-defense to cyberspace, claiming that doing so would turn cyberspace into a theatre of military operations. The Brief considered questions that India would need to answer when framing its legal response to this breakdown-including the threshold of use of force, the threshold of an armed attack, self-defense against non-state actors and pre-emptive self-defense. Further, it looked at the benefits recognising an inherent right to self-defense would have in India's cyber strategy, if they simultaneously ramped up their vulnerability identification and offensive and defensive cyber capabilities.

The second brief on attribution summarised the standards of attribution in the International Law of State Responsibility. It found that both the existing tests of 'effective' and 'overall' control might be inadequate for attributing cyber attacks. Therefore, it recommended the employment of a more flexible new test employed by Peter Stockburger known as the 'control and capabilities' test. Equally relevant in the conducting of attributions would be the recognition that attribution cannot be merely a technical process given the barriers to gathering evidence in this process. Attribution of cyber attacks must necessarily weigh a range of factors-including political or financial evidence. At the same time, all evidence must be presented to the public with an acknowledgment of the limitations of the process. This form of publication would have a range of benefits, including facilitating cross-sector publication and driving the creation of globally acknowledged best practices.Finally, as suggested by the RAND Corporation,the international community might consider a global consortium for attribution, which would bring together independent experts to undertake investigations into major cyber-incidents. This might be a promising endeavour and the organisation could potentially be expanded to also conduct regular inspections of the information infrastructure in various states to ensure that each state is maintaining cyber hygiene.

The third brief looked at the prohibition on development of cyber weapons. International Law prohibits the use and by implication, the development of inherently indiscriminate cyber weapons.Achieving a normative framework of commitments that enforces this rule is a challenging task given varied strategic interest and legal perspectives across the international community. Given the difficulty in defining a 'cyber weapon, lessons from prior arms controls regimes may be limited in their use although the process that lead to normative taboo may serve as useful indicators. As stated by Joseph Nye, it is also essential that this regime focuses on targets and not weapons. While previous arms controls regimes have centred around the negotiation of treaties, an all-encompassing treaty may be too idealistic a goal. Therefore, as argued by Stevens, utilising the emerging systems to foster a cohesive global governance architecture that encourage compliance with existing standards may be a more realistic and inclusive process. There are three interlinked regimes that form a part of this architecture-IHL, international cybercrimes convention and the export-control regime. India has already begun to play a greater role in the existing architecture-demonstrated most recently with its entry into the Wassenaar Arrangement- and could utilise this increased participation to further its strategic interest and international reputation. Considering and solidifying positions on the questions outlined in this paper could help India engage in the existing architecture.

The final brief looked at the legal regime on countermeasures and identified a lack of both scholarship and state practice on the issue. A lack of scholarship may exist due to the fact that countermeasures exists within the general framework of public international law and general International Law experts are yet to enter the field of cyberspace governance. States have refrained from commenting due to the perceived benefit they gain from strategic ambiguity although this ambiguity may lead to them being targeted by cyber-attacks. An analysis of Active Cyber Defense Strategies from the perspective of countermeasures may be an ideal litmus test for the analysis of the application of the legal regime on counter-measures in cyberspace.

The cyber norms process is in flux with multiple actors stepping in and trying to broker consensus across ideological divides. India and various actors within India, including the private sector and civil society organisations have the opportunity to stake claim to a leadership role in this space and work towards the formulation of norms that take the interests of all parts of the globe into account. It is imperative that India not shy away from using and studying the standards of International Law and its applicability in this space while retaining focus on pragmatic considerations that would aid it as a world player.

Further Areas of Engagement and Research

CIS will remain actively involved in the norms formulation process over the next couple of years-both through independent research and engagement with policy-makers and private sector actors in India and the region. It hopes to also collaborate with partner organisations in other parts of the world to release output on issues including disinformation, the application of human rights and humanitarian law, the economic dimensions of cyberspace and the road ahead for the private sector. This Report will hopefully serve as a gateway into more specific avenues of research.