internet
democracy
project

Dr Anja Kovacs

Addressing India's Global Cybersecurity Concerns:

Norm Development, Regulatory Challenges, Alternative Approaches

August 2015

Introduction

Over the past few years, India has repeatedly argued that the UN should play a greater role in the formulation of international Internet-related public policies. Since the country has formally endorsed multistakeholder approaches to Internet governance in June 2015, that demand may have waned or changed form, but it certainly has not altogether disappeared. In particular, India has continued to ask for a greater role for the multilateral system where issues relating to cybersecurity are concerned.

Such requests take a variety of forms. Quite consistent, and justifiably so, are an emphasis on international cooperation and calls for confidence-building measures. Also frequently mentioned is the need to develop a common understanding of the applicability of rights, norms and even rules of conduct in cyberspace. References such as these can be found, most recently, in, for example, India's oral statement at the First Preparatory Meeting of the Member States for the WSIS+10 Review in New York, 1 July 2015[1] and in the Ufa Declaration of the 7th Seventh BRICS Summit[2].

At times India goes even further, however. In its first written contribution into the WSIS+10 Review process, India noted that it 'favours a global framework, such as an International Convention for Legal Cooperation on Cybercrime, which would harmonize effective international cooperation between member states in tackling cybercrime'[3]. This echoed India's statement at the 18th session of the UN Commission on Science and Technology for Development (CSTD) earlier this year, in May 2015, where India had called for the development of an 'international legal framework for online privacy and data protection, including issues like human rights, trade standardization and security perspectives'[4]. Even earlier, in April 2014 at the NETmundial, too, India had called for a 'new cyber jurisprudence' to 'ensure security of the cyberspace and institutionalise safeguards against misuse of the protection of Internet users and at the same time also ensure the free flow and access to information'[5].

India is certainly right to argue that with the arrival of cyberspace, a whole new host of security and other challenges have arisen which are not always adequately tackled. The term cyber denotes not only the Internet of networked computers but also intranets, cellular technologies, fiber-optic cables, and space-based communications (Nye 2011). Cybercrime and cyberattacks have consequences for users' safety, for economic and commercial activity, and for military effectiveness. As the barriers to entry in the cyber domain are low and participation can come cheaply (Nye 2011), they involve a large and varied number of actors: from criminal hackers over terrorist networks to nation states, which may be involved in cyber espionage for commercial or military reasons or in the disruption of critical infrastructure.

The complexity of the cybersecurity landscape is further increased as new technologies reshape warfare, aiding both the development of new methods of employing lethal force and the rise of modern forms of hybrid warfare. 'Where wars traditionally have regular and irregular components in different areas of operation, modern hybrid war has the tendency to combine these aspects' (Deep 2015) as well as terrorist acts and, some have argued, criminal behaviour – deploying them, often simultaneously, with synchronous effects in the physical and psychological dimensions of conflict *across* operating environments (see also Hoffman 2009). New technology has played an important role in making this simultaneous compression of the levels of war and of convergence of modes a possibility. Not only are many technologically advanced weapons systems now available at relatively low cost, pre-existing commercial technology, such as mobile phones and the Internet, too, is increasingly used to support war efforts – be it to communicate, to influence public opinion, to learn new techniques of war, to gather intelligence or to engage in cyberattacks (for examples, see Deep 2015; Hoffman 2009; Maurer and Janz 2014; NATO StratCom Centre of Excellence 2014)[6]. Precisely because the changing landscape brings such a wide range of challenges with it, India's more ambitious proposals for solutions, however legitimate they may be, are also, however, far more complex to realise: if the treaty negotiations necessary to develop new international legal frameworks are always complicated, in this particular case the challenges are even bigger due to the nature of cyberspace.

What exactly are India's proposals up against, and what might be more feasible to achieve in the shorter term? In the remainder of this paper, I will try to shed some light on this issue by first analysing existing and proposed efforts within the multilateral system regarding norm development, both through the application of existing law and the potential creation of new law. I will then examine three broad, cross-cutting regulatory challenges that these processes, as well as more ambitious attempts to develop legal frameworks, in particular have to contend with. I will finally briefly discuss three complementary approaches that largely avoid these pitfalls and might provide a more productive place to start international collaboration in this area and for India to take a leadership role in the shorter term. As will become evident, India's current appreciation of the value that multistakeholder approaches can bring to a range of Internet governance issues make it particularly well-placed to do so.

1. Norm development

a. Applying existing international law

As in the physical domain, a considerable role can be foreseen for the multilateral system in determining the norms and rules that govern offensive state action in the cyber domain. In fact, with the changing circumstances further complicating the application of existing internationally agreed frameworks from so many different vantage points, as explained above, there is a clear and urgent need for greater clarity and consensus on this count. Where India argues for the need for greater clarity on the applicability of norms and rules, it, too, thus calls for more effort to be put into such initiatives.

Over the past few years, two have been of particular importance. The first one is the work done by consecutive Groups of Governmental Experts (GGEs) established under the auspices of the UN General Assembly[7]. Though progress initially was slow, the third GGE provided a breakthrough when, in its report, it concluded unanimously that international law, including the Law of Armed Conflict and the UN Charter, is applicable in cyberspace. This report is widely seen as indicative of an emerging consensus on the validity of applying existing international rules to cyberspace. Experts from fifteen different countries, including from India, participated in this GGE. The mandate of the fourth GGE, of which India was not a member, was extended to explicitly include consideration of how international law applies to cybersecurity questions[8]. Its report, which made incremental progress, was released in June 2015 and will be presented to the First Committee of the General Assembly in October 2015.

The latter question has also been the focus of the second major initiative in this field, a three year effort that led to the Tallinn Manual on the International Law Applicable to Cyber Warfare. The Manual was created by a group of international law and cybersecurity experts brought together by the North Atlantic Treaty Organisation's Cooperative Cyber Defence Centre of Excellence, based in Tallinn. In particular, the experts considered *jus ad bellum* (the set of rules to be consulted before engaging in war) and *jus in bello* (the law of armed conflict or international humanitarian law), including cyberespionage (Azzopardi 2013).

Despite its nonbinding status, the Manual is considered an important attempt to 'delineate the threshold dividing cyber war from cybercrime and formalize international rules of engagement in cyberspace' (Fleck 2013). However, this work has not been without its critics. For example, it has been noted that a considerable number of important unresolved issues remain, such as the question as to where exactly the threshold of a serious damage (rather than inconvenience) lies.

Though both the GGE report and the Tallinn Manual have broken important ground, considerable work on norm development, thus, remains to be done regarding offensive state action in the cyber domain, including on issues such as cyberespionage by states and state responsibility for actions emanating from their territory. India's calls to continue such work certainly make imminent sense.

b. Norm development and the creation of new international law

In addition, however, the question continues to be raised whether existing international laws are indeed *sufficient* to deal with cyberthreats, even if they are *applicable*. Proponents of a new treaty have been found both among states and scholars, and though the details of the new international legal framework that India is hoping for aren't yet fully clear, its statements at recent Internet governance events, as explained above, indicate that it, too, would be a proponent of this where the criminal use of ICTs is concerned. What have others argued in this regard?

The Russian Federation first proposed in 1998 that UN Member States agree to a treaty that would govern cyberweapons in much the same way as those that for nuclear, chemical and biological weapons. They found little enthusiasm for this approach, in part because cyberweapons raise a very different set of issues. For example, any proposed verification of 'disarmament', while a central tenant for existing arms control agreements, would sit at great odds with the principle of anonymity (Hollis 2011).

Scholars such as Oona Hathaway and Rebecca Crootof (2012) have argued in favour of a treaty of a more comprehensive kind. By agreeing on definitions of cybercrime, cyberattacks, and cyberwarfare, at the global level, they argue, the way is paved for harmonisation of domestic criminal legislation on these issues and for greater international collaboration in evidence collection and criminal prosecution of individuals involved in transnational cyberattacks of all kinds.

In many ways, the approach taken by Hathaway and Crootof reflects that of existing regional efforts to address cybercrime in particular. In 2001, Western states negotiated a treaty, the Convention on Cybercrime (also known as the Budapest Convention), which 'requires parties to adjust their domestic criminal law to proscribe certain commonly defined offenses […]. It also requires a certain amount of cooperation in investigating and prosecuting such crimes through preservation and production of digital evidence, extradition, and mutual legal assistance' (Hollis 2011: 392). While the Budapest Convention makes cybercrime one of the few cybersecurity related areas in which multilateral cooperation has been formalised, its scale is limited and a global multilateral treaty that addresses these challenges remains absent. Some of India's proposals seem to be aimed at addressing this gap. Proposals such as that by Hathaway and Crootof, too, do so at least in part, as well as extending the approach used to threats that are cyberattacks too, whether or not they amount to cyberwarfare.

2. Regulatory Challenges

If a range of proposals have been made already so far, by India and others, why has more progress not been achieved as yet? Any attempt to create new law in the cybersecurity area will require policy makers to find greater clarity and make progress on three major, difficult underlying issues.

a. Reach: Which actors to address

The Convention on Cybercrime focuses specifically on 'identifying and deterring particular perpetrators without regard to motives, so long as they are private actors' (Hollis 2011: 392). Domestic cybercrime laws, too, focus on private actors, generally without making a distinction as to motives. Where a cyberattack or exploit originates from a state, different sets of rules are thus supposed to apply, drawing on, but perhaps extending, existing international law. Whether it is wise, or even feasible, to address such a wide range of issues in a singly treaty at the global level remains a first question policy makers will need to address (and some of the issues I will examine below further complicate the answer to that question).

Hathaway and Crootof (2012: 821) make a further distinction. As they have defined cyberattacks as all actions 'taken to undermine the function of a computer network for a *political or national security purpose*' [emphasis mine], they additionally foresee regulation of, on the one hand, state-led attacks that do not amount to cyberwarfare, and on the other hand, private actor-led attacks that are believed to be not merely criminal, but political in nature. With this, their approach would, thus, importantly, open the door to delineating cyberterrorism as a category to be dealt with *separately* under international law.

Certainly cyberterrorism is an issue on the agenda of the Indian and many other governments. But in its initial report, in 2009, the UN Working Group on Countering the Use of the Internet for Terrorist Purposes, set up to investigate such issues, came to the conclusion that 'there is not yet an obvious terrorist threat in the area' and that 'it is not obvious that it is a matter for action within the counter-terrorism remit of the United Nations'. In a subsequent report, in 2011, the Working Group recommended domestic implementation of existing regional and international instruments addressing cybercrime and transnational organised crime, rather than the creation of new legislation specifically to address cyberterrorism (Maurer 2011).

Indeed, and perhaps somewhat surprisingly to the lay person, while the use of the Internet for terrorist purposes may have become commonplace, the extent to which private actors would be able to inflict severe damage through a cyberattack, presently or in the future, remains a matter of intense debate. More generally, the use of the term 'cyberterrorism' remains deeply controversial (see also Macdonald et al 2013).

The question of whether a treaty should be extended to address cyberterrorism separately, or merely as a cybercrime though with possible consequences for issues around state responsibility, too, thus remains an open question.

b. Applicability: The problem of attribution

If different rules are put in place to address different cyberthreats inflicted by different actors, it becomes essential to be able to attribute each act, as this will determine which set of rules will need to apply. But attributing cyberthreats is often extremely difficult. Identities can be easily concealed. Governments may rely on private companies for attribution where they lack expertise themselves, but this may be controversial, especially in cases where the interests of the two are seen as being closely aligned. And even where the source of an attack can be identified, this does not always provide sufficient information to determine who, or which country is responsible (Raymond, Shull and Bradshaw Forthcoming).

At the same time, however, if governments are too careful to attribute once technical and legal criteria have been satisfied – and thus to hold those using cyber means for unlawful purposes accountable – this may lead to the development of a culture of permissiveness, even impunity.

The question of what rules will govern when and how states publicly attribute cyberattacks and, especially, assign state responsibility is, thus, an important one for policy makes to ask themselves. Progress on this count has so far, however, remained quite limited.

c. Scope: Cybersecurity and human rights

A third set of issues concerns the relationship between cybersecurity and human rights. Russia and its allies in the Shanghai Cooperation Organisation (the accession process to which India formally started in July 2015) defend an information security doctrine that extends the concept of cybersecurity to control over content. For many Western governments, this is not acceptable. Observers have for long regarded this difference in perspective as a major hurdle in the development of a cybersecurity treaty.

But concerns about the impact on human rights online in various contexts have not only been raised in the context of the Russia doctrine on information security. While the Cybercrime Convention does require conditions and safeguards under signatories' domestic law that provide for the 'adequate protection of human rights and liberties', activists fear that the clubbing together of crimes merely conducted on the Internet and crimes to which Internet infrastructure is central in that treaty arguable opens the door to content controls in countries with weak checks and balances that might otherwise have been easier to resist.

This raises questions in general about the extent to which a new cybersecurity treaty at present would be able to safeguard the human rights of people around the world. What distinguishes a legitimate cyberprotest, for example, from a cybercrime is an ongoing debate even in many established democracies. Significant guidance on human rights in the digital age has been provided by experts within the UN system in recent years. For a cybersecurity treaty to find the approval of those concerned with human rights, it is likely essential that this guidance is first translated into concrete measures and guidelines for all states to uphold – either within a cybersecurity treaty or in a separate instrument, and both in relation to substance and process aspects. Seeing that such efforts might in turn have an effect on, for example, the cyberespionage practices of states across the political spectrum, this day may be some time away. Calls such as those that India made during its statement at the First Preparatory Meeting on the WSIS+10 Review in New York, on 1 July 2015, to find an 'ideal balance between national security and internationally recognised human rights' are, however, encouraging in this regard.

3. Alternative approaches to address challenges in the area of cybersecurity

What is important to realise, however, is that treaties that proscribe the behaviour of states and other actors in cyberspace are not the only possible way forward to address challenges in the area of cybersecurity through the multilateral system. In addition to the confidence-building measures (CBMs) that India also hails, other complementary (not competing) approaches have been suggested as well.

Among the notable suggestions is a duty to assist (DTA), similar to the SOS. First proposed by Duncan Hollis (2011), such a duty would impose a requirement to assist victims facing emergent and serious harm, to avoid or at least mitigate that harm as much as possible. A DTA would, thus, avoid the challenges of attribution: the severity of the harm, rather than its origin, would determine whether or not assistance is to be provided. As agreement would need to be reached on 'which victims can call for help, when they can do so, who must provide help, and what help those assisting must give' (Hollis 2011: 378), agreement on a DTA has partially a regulating function. In addition, where effective, it also functions as a deterrence, however, as it would improve the resilience of computer networks and cause attackers to 'think twice about whether it is worth the effort to attack at all' (ibid.).

More recently, and building on the DTA, Hollis and Maurer (2015) have proposed a global cyber federation of non-governmental institutions with a commitment to provide independent, neutral and impartial assistance to the Internet and its users. Using existing Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) as building blocks, the proposed federation would thus mirror in cyberspace the Red Cross and Red Crescent movement, so as to make cyberspace a safer and more secure place. Hollis and Maurer recognise that, at present, neither an effective coordinating institution 'nor a universal set of shared values recognised and appreciated by states and non-state actors alike' exists for CERTs. The key, they believe, 'lies in generating an appreciation for the benefits of institutionalising an independent and neutral security and assistance function'. 'Recognising the existing norms that guide the CERT community and strengthening them akin to the humanitarian principles could be an important start'.

What is noteworthy about both these proposals is that they take into account the global nature of threats as well as the interdependence of actors, and the fact that actors from a *variety* of stakeholder groups are generally affected by cybercrimes and attacks: rather than privileging states in the resolution of such issues, these proposals seek to maximise the stake of all stakeholder groups – state and non-state actors alike, from whichever jurisdiction – in maintaining a safe and secure cyberspace. In other words, they respect the global nature of the Internet and the multistakeholder nature of its governance as it exists, while at the same time providing a concrete opportunity for states to take forward their nascent efforts in jointly organising against cyberthreats. With this, these proposals might well provide important stepping stones to the kind of broader agreement that might ultimately lead to a cybersecurity treaty (or several such) acceptable to all.

With India now formally acknowledging the value of multistakeholder approaches to Internet governance while at the same time also continuing to prioritise cybersecurity issues in its Internet governance policies, it is eminently placed to start taking forward such efforts, both at the national and global level. Doing so would, moreover, kill two birds with one stone. Not only would it allow India to take up the leadership mantle in Internet governance that the world has been expecting it to don for so long, it would also make it possible to start progressing immediately on the resolution of some of India's long-standing cybersecurity concerns, and this without having to give up its demands for the development of new legal frameworks in the longer term. If India only stands to gain, why wait?

ENDNOTES

[1] Statement by Mr. Santosh Jha, Director General, Ministry of External Affairs, at the First Session of the Review by the UN General Assembly on the implementation of the WSIS outcomes in New York on July 1, 2015. https://www.pminewyork.org/adminpart/uploadpdf/74416WSIS%20stmnt%20on%20July%201,%202015.pdf.

[2] See para 34.3 of the UFA Declaration of the 7th BRICS Summit. http://www.brics.utoronto.ca/docs/150709-ufa-declaration_en.html

[3] India's inputs for the UNGA's Review of the Tunis Agenda for the Information Society. http://workspace.unpan.org/sites/Internet/Documents/UNPAN95026.pdf.

[4] Statement made by India at the 18th Session of the UN CSTD - Geneva, 4-8 May 2015, on Agenda Item 3 - 'Progress made in the Implementation of and follow-up to the outcomes of the WSIS at the Regional and International Levels'. http://www.pmindiaun.org/pages.php?id=1106.

[5] Government of India's initial submission to Global Multistakeholder Meeting on the Future of Internet Governance in Sao Paulo, Brazil, April 2014. http://content.netmundial.br/contribution/government-of-india-s-initial-submission-to-global-multistakeholder-meeting-on-the-future-of-internet-governance-sau-paulo-brazil-april-23-24-2014/138

[6] To what extent, for example, Russia's information campaigns in the Ukraine – an oft-cited case study of hybrid warfare – can really be understood through the lens of hybrid warfare, rather than traditional concepts of war, is a point of contention, however. For a critique, see for example Raitasalo (2015).

[7] See e.g A/RES/57/53, A/RES/62/17, A/RES/65/41, A/RES/68/243.

[8] See A/RES/68/243 and A/RES/69/28.

REFERENCES

Azzopardi, Myrna (2013). The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Brief Introduction on its Treatment of *Jus Ad Bellum* Norms. *Elsa Malta Law Review*, 3(1): 174-184.

Deep, Alex (2015). Hybrid war: Old concept, new techniques. *Small Wars Journal*, 2 March.

Fleck, Dieter (2013). Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New *Tallinn Manual*. *Journal of Conflict and Security Law*, 18(2): 331-351.

Hathaway, Oona A. and Rebecca Crootof (2012). The Law of Cyber-Attack. Yale Law School Faculty Scholarship Series. Paper 3852. http://digitalcommons.law.yale.edu/fss_papers/3852

Hoffman, Frank G. (2009). Hybrid Warfare and Challenges. *Small Wars Journal*, 52(1): 34-39.

Hollis, Duncan B. (2011). An e-SOS for Cyberspace. *Harvard International Law Journal*, 52(2): 374-432.

Hollis, Duncan and Tim Maurer (2015). A Red Cross for Cyberspace. Time, 18 February, http://time.com/3713226/red-cross-cyberspace/.

Macdonald, Stuart, Lee Jarvis, Thomas Chen and S. Lavis (2013). Cyberterrorism: A Survey of Researchers. Cyberterrorism Project Research Report (No. 1), Swansea University.

Maurer, Tim and Scott Janz (2014). The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context. *The International Relations and Security Network, Swiss Federal Institute of Technology Zurich*, 17 October, http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=184345

Maurer, Tim (2011). Cyber Norm Emergence at the United Nations: An Analysis of the UN‘s Activities Regarding Cyber-security. Belfer Center for Science and International Affairs, Harvard Kennedy School. Discussion Paper 2011-11. September.

NATO StratCom Centre of Excellence (2014). *Analysis of Russia's Information Campaign Against Ukraine*. Riga: NATA StratCom Centre of Excellence.

Nye, Joseph S. (2011). 'Nuclear Lessons for Cyber Security?' *Strategic Studies Quarterly*, 5(4): 18-38.

Raitasalo, Jyri (2015). Hybrid Warfare: Where's the Beef? *War on the Rocks*, 23 April, http://warontherocks.com/2015/04/hybrid-warfare-wheres-the-beef/.

Raymond, Mark, Aaron Shull and Samantha Bradshaw (Forthcoming). Rule-Making for State Conduct in the Attribution of Cyber-Attacks. In *Constructive Powers and Regional Security in East Asia*. http://www.academia.edu/9027635/Rule-Making_for_State_Conduct_in_the_Attribution_of_Cyber-Attacks