GLOBAL POLICY

Digital Debates 2016

Edited by Samir Saran

Digital Debates
CyFy Journal Volume 3 (2016)

Authors:

Adam Segal, Alexander Seger, Arun Mohan Sukumar, Bertrand de la Chapelle, Caitriona Heinl, Catalina Ruiz Navarro, Dennis Broeders, Isabel Skierka, Japreet Grewal, Paul Fehlinger, Paula Kift, Shaili Chopra, Saikat Datta

Editorial Team:

Arun Mohan Sukumar, Bedavyasa Mohanty, Anahita Mathai, Vinia Datinguinoo Mukherjee (ORF)

Inside Design:

Shantanu Salgaonkar

Printed by:

Mohit Enterprises, Delhi

Contents

Editor's Note
Navigating the Digital 'Trilemma'

Samir Saran

Debates around internet policy have taken centre stage in domestic politics and international relations alike. While national debates are shaped by local priorities, politics and contextual ambitions, cyber diplomacy differs from traditional diplomacy in two important respects. First, the stakeholders invested in internet policy include not just states and governments but industry and civil society as well. Second, the norms that define conduct over cyberspace remain diverse, divergent and fluid. Creating a universal set of norms to guide policymaking on digital spaces is further complicated as individual sovereign assessments are significantly implicated by regional and strategic tensions unique to them.

Concurrently, the world is also witnessing two parallel sets of conversations on digital policy. One is largely focused on translating rights from the offline world to the online world. This conversation is premised on a clear understanding of what the rights entail in the offline world; the central task that remains is focussed on demarcating the contours of those rights online. The other, related, conversation attempts to negotiate the very nature of, and need for, these rights. For instance, the European Union holds data protection in the highest regard, enshrining it within the European Charter of Fundamental Rights. At the same time, India, the largest democracy in the world, is yet to explicitly recognise a right to privacy within its constitution. The difference in these approaches transcends legal regimes. The social contract in Europe, a product of legal, cultural and political factors, pried access to data away from the regulators and ceded agency over it to the private citizen. This equilibrium is today reflected in the EU data protection norms. In India, where norms of social behaviour are evolving concurrently with lawmaking, there is no national consensus on a 'right to privacy', with some constituencies alleging that a 'Western' model may not be fully appropriate, or would need significant redefinition when applied to the Indian context. In India as in other emerging economies, cyberspace regulation has shouldered the additional burden of delineating and guaranteeing rights that are not necessarily available in offline spaces.

The real challenge therefore lies in creating a public sphere and a digital public sphere that attends to the integrity of both conversations.

Ironically, both these conversations are coloured by concerns about security and access. In the developing world, even as countries strive to ensure affordable access, the proliferation of unsecured devices has lowered the overall standard

of digital security. Attempts across the world to enhance cyber security through online intelligence gathering has often had the effect of watering down the right to privacy and stifling free speech, and in some instances even comprising hardware and network integrity. Even though issues around access are largely missing from Atlantic debates, security (motivated by unique and different circumstances) has become an all-encompassing and opaque hindrance in the realisation of the full potential of the internet.

The unique challenge of digital policy is addressing the 'trilemma' of reconciling security, rights and access. When we explore both the sets of conversations as discussed above, it becomes evident that while all three are present in policy formulation on most occasions, one or two are often given more importance. What we must instead strive towards is a re-imagination of these challenges as a equal-sided triangle, where each issue is given the same importance as the other.

Access to the internet is not an end in itself. In India, it is the means for social and financial inclusion. The Indian government has announced plans to slowly transition to a cashless economy while the market remains inundated with cheap and unsecured devices. This, however, is not a central concern to those who remain without access. For instance, individuals in rural India who own smartphones to access government services are often dependent on a family member or another second generation internet user to 'go online'. Often enough their phones serve as communal devices with one source managing many connections and many accounts. Neither privacy nor security is deliberately accounted for in their daily transactions, leaving them entirely to the mercy of technologies available on the device. To the state that is attempting to foster financial inclusion and digital payments, this 'human' component of cyber security is extremely important. How does policy formulation that is still informed by trans-Atlantic notions of privacy contend with these radical realities that defy information or device management?

Of the rights envisaged in the Universal Declaration of Human Rights, many are implicated online. However, the imperative for maintaining the balance between these, sometimes conflicting, rights is more complex online. For instance, the mandate of states to make digital spaces more inclusive and less hostile is often at odds with the overarching imperative to foster freedom of expression. Prominent social media companies like Twitter that were created to allow internet users to voice their opinions online must also constantly attempt to reduce – if not eliminate – online harassment and gender based violence. The translation of offline rights to the digital space is often less than perfect. More often than not it ends up clamping down on one or more rights. For countries that do not have the resources to monitor and tackle online extremism, the restrictions on an open internet are not always imposed by choice but rather by compulsion. How does the objective of maintaining a marketplace of ideas, free of hostility, contend with the universal recognition of free speech?

The threat to an open internet, however, is not only from online radicalisation and hate speech. Opportunities for access – to knowledge, to markets and to people – available online must never cost more than those available offline. Exclusionary mega free trade agreements could potentially render vast swathes of knowledge and data inaccessible to emerging economies. On the one hand, countries and regulators are criticised for heavy-handed censorship or imposing restrictions on an open internet; on the other, restrictive provisions aimed at the

digital economy – which in India is yet to fully bloom – could convert the open internet into a luxury. If draconian laws and oppressive governments cannot be allowed to dismantle the openness of the internet neither should commercial arrangements and mercantilist considerations.

Security presents the greatest challenge of the three vertices of this invisible triangle. Cyber security involves the protection of both infrastructure and information. Difficulties arise when in the name of security, governments start to dictate norms of behaviour in cyberspace. This raises the philosophical question of whether the enhancement of a nation's cyber security automatically means an enhancement of the individual security of every internet user. Or as a corollary, does enhanced individual online security result in higher national security in this sphere? We must also ask: do internal security and cyber security complement each other or will the resolution of one lead to the dilution of the other? This is perhaps best exemplified by the ongoing tussle between the United States government and Silicon Valley. It has been well documented that technological alternatives to bypass government-monitored means of communication are readily available. Keeping this in mind, it seems unlikely that allowing governments access to certain modes of communication will greatly enhance the internal security of a country. The overall security is rather affected by the individual strength of devices and modes of communication available to the citizens.

The common thread that runs through all three issues is data integrity – both national data and individual data. Managing data integrity can serve as the golden median that helps strike a balance between the needs to ensure affordable access, secure cyberspace and enhance rights. Ensuring the integrity of citizens' data can protect them from commercial exploitation by private entities, intrusion into their lives by the state, and from criminal exploitation by hackers. It can strengthen privacy and foster free expression and exchange of ideas over the internet. Maintaining the integrity of data is therefore something that all states must aspire to. This, and digital anonymity are preconditions to ensuring a safe, discursive space online.

As net exporters of data, Asia and Africa are locked in an uneasy relationship with Western companies that provide most services over the internet. The digital trilemma is acute for emerging economies: access is a 'here and now' concern, but is also a factor of the individual security and human rights. A major cyber attack on financial networks could have the consequence of weaning first generation users away from the internet altogether. Regular and unchecked instances of harassment and gender-based violence online could constrain the rights and contribution of women to digital spaces, further skewing inequalities based offline. Platforms purporting to offer affordable internet access should not emerge as walled gardens that restrict the freedoms of speech or expression. Managing the three vertices, therefore, is a delicate process that should eschew dramatic or heavy handed regulation.

The resolution of this invisible triangle, far from being a purely national concern, is central to the stability of digital spaces, which are global commons. Access, rights and security, must be weighed in their own respects and given equal degrees of importance. While responding to the threat of climate change, for instance, all countries recognised that growth, employment and environment were equally important to everyone. A similar realisation must be arrived at in relation to digital policies.

INTERNET AND DIPLOMACY

Jurisdiction on the Internet: How to Move Beyond the Legal Arms Race

Bertrand de La Chapelle and Paul Fehlinger

The transborder nature of the Internet has generated unprecedented social, economic, and political benefits for humankind. At the same time, it creates tensions within an international legal system based on a territorial sovereignty principle rooted in the 17th century Treaty of Westphalia. On the Internet, transnational interactions have become commonplace. Traditional modes of interstate cooperation, therefore, struggle to cope with the digital realities of the 21st century. From cases of objectionable content to cross-border access to user data, online disputes and abuses are an unprecedented challenge to the territorially-bound international legal system.

We are confronted with two major questions: how can the global nature of cyberspace be preserved while respecting national laws? And how can misuse of and abuse on the Internet be addressed while ensuring the continued protection of human rights?

This represents acute concerns for all stakeholders, who are pressured to act yet lack the necessary tools to implement and enforce solutions. As a result, issues of jurisdiction on the Internet have engendered uncoordinated and unrestrained applications of territoriality online. Innovative processes are needed to fill the institutional gap in Internet governance and prevent the present legal arms race from escalating in their absence.

National Jurisdictions and Transborder Cyberspaces

The technical architecture of the Internet was conceived as transborder and non-territorial from the onset, a quality that is generally regarded as advantageous. Yet ubiquity has also fostered tensions, as globally accessible content and services legal in one country may be illegal or even criminal in another. Historically, interactions across borders were rare exceptions. Today, most daily activities on the Internet involve multiple jurisdictions at once, allowing ample possibilities for conflicting laws to come into contact.

Determining applicable laws, allowing for their enforcement, and providing mechanisms for redress in cases of transborder cybercrime or illicit behaviour online becomes increasingly difficult as a result. Such tensions will continue accumulating as Internet penetration approaches four billion users from over

190 countries, each with divergent and potentially conflicting laws, cultures, and social sensitivities. The present situation is a concern for all categories of actors: governments, Internet platforms, technical operators, civil society groups, and international organisations, as well as average users.

In addition to concerning a range of different actors, the jurisdictional challenge of Internet governance directly impacts other policy challenges. These include, among others, developing global digital economies, providing clear and predictable legal environments, protecting the exercise of fundamental human rights, and ensuring cybersecurity and public order. The active involvement of numerous actors and sectors is necessary to resolve jurisdictional tensions online and prevent the fragmentation of the Internet. Recognising the magnitude of this challenge is the first step toward finding a common solution.

Since 2012, the global multistakeholder policy network Internet & Jurisdiction has documented in its Retrospect publication more than 1000 high-level cases illustrating this growing tension, and engaged more than 100 key entities from all stakeholder groups in an ongoing dialogue process to address these issues and catalyse solutions. More than four years of global discussions in over 30 countries have allowed participants to identify three areas that dearly call for multistakeholder cooperation:

Data. Under which conditions can public authorities in one country obtain user information from an operator in another jurisdiction? How can the right to privacy be reconciled with the need for lawful access to user data?

- Content. How can the global availability of content be maintained while handling the diversity of local laws and norms regarding speech? How can proportionality and respect of human rights be ensured in instances of content takedown?
- Domains. How do jurisdictions apply the Domain Name System, and how can the architectural separation between the Internet's application and logical layers be preserved?

In these and other complex issue areas, a lack of coordination between actors can result in unintended consequences and make problems harder - rather than easier - to solve.

A Legal Arms Race in Cyberspace?

Digital sovereignty is becoming the realpolitik of Internet regulation. Examples of extraterritorial extension of national jurisdictions abound: first, governments with Internet platforms or technical operators incorporated on their soil may impose their national laws and regulations on these private actors, with direct transboundary impacts on all foreign users of these services. At the same time, draft legislations increasingly include clauses establishing extraterritorial reach, such as the draft UK Investigatory Powers Bill or the EU General Data Protection Regulation.

Litigation also plays a prominent role in setting new global standards, with de facto impacts far beyond the respective jurisdictions. Although the right to be de-indexed was originally established by Europe for Google, for example, it is

now implemented by other search engines such as Microsoft Bing or Yahoo Search and has produced ripple effects in Asia, Latin America, and Canada. Accordingly, local court decisions can also trigger new international norms for interactions between states and Internet companies.

Re-nationalization is a complementary trend to extraterritorial expansions of sovereignty. Courts and public authorities in countries that do not physically host Internet companies or data experience a sense of powerlessness when trying to levy respect for their national laws on foreign entities. Prompted to nevertheless establish the rule of law and protect citizens online, states are incentivised to erect territorial borders on the Internet. This can manifest itself through "data localisation" laws or the blocking of URLs (uniform resource locators) or IP (Internet protocol) addresses via the national Internet service providers (ISP). Other digital sovereignty measures can range from strong intermediary liability regimes, requirements to open local offices, demanding backdoors to encryption technologies, or the imposition of full-fledged licensing regimes.

The extreme and unrestrained leveraging of territorial criteria introduces two paradoxes. First, as described above, national actions impacting operators with global reach can affect citizens of other jurisdictions. Consequently, such actions appear contrary to the very principle of non-interference - a direct corollary of sovereignty itself. Such interference increases the potential for conflicts between jurisdictions, rewarding the most powerful digital countries and encouraging others to react and adopt measures based on mistrust and the reimposition of national borders.

Second, strong digital sovereignty measures are not scalable globally. Regarding compulsory data localisation laws, for example, it is highly unlikely that the necessary data centers could be established by global companies in every country around the world. Though sovereignty remains definitely relevant in the digital age, measures of extraterritorial expansion or renationalisation put actors in a classic prisoner's dilemma where the sum of actions appearing beneficial in the short-term can have unintended detrimental consequences for the future. In the case of Internet jurisdiction, the outcome of this negative-sum game is unwanted fragmentation and increasing conflicts. Preserving the global nature of the Internet and preventing a legal arms race to establish digital sovereignty call for new mechanisms of transnational cooperation.

Limits to international cooperation

Managing transborder online spaces poses systemic difficulties for the existing international system; existing mechanisms for legal interoperability often fall short in diffusing tension and resolving conflict. Three such tools being employed at present are:

1. Multilateral efforts
2. Bilateral agreements
3. Informal interactions between public and private actors across borders.

Multilateral efforts. Only rare actors advocate the idea of a global, all-encompassing Internet treaty that would harmonise relevant laws and solve the full range of cyber-cooperation issues. Moreover, treaty negotiations are notoriously long. Even the most extensive agreement to date tackling cybercrime, the Budapest Convention, was a lengthy process: if formal negotiations took "only" four

years, more than a decade was required to put the topic on the agenda. In the end, though the Convention was signed by more than 50 states around the world (excluding several large countries such as India and Brazil), some countries use the fact that it was initially elaborated within the Council of Europe as an argument against joining a regime in the drafting of which they had not participated.

In the last few years, many useful declarations have been developed within multilateral organisations at the level of general principles, showing some form of convergence. Still, none of them were able to move towards developing operationally implementable regimes.

MLATs. Historically, the bilateral mutual legal assistance treaties (MLATs) enabling government-to-government legal cooperation were negotiated to handle rare and rather exceptional cross-border criminal cases. However, now that transborder interactions have become commonplace on the Internet and most criminal evidence is digital and hosted by operators in foreign countries, this system is generally described as "broken." MLATs have at least four structural limitations:

- Speed. MLAT processes can take months or even years to be processed, making them ill equipped to handle the instant and viral spread of information on the Internet.
- Scope. MLATs are often limited to "dual incrimination" situations - cases that qualify as a crime in the jurisdictions of both requesting and receiving countries - an obstacle given the disparity of national legislations.
- Asymmetry. Regardless of the physical location of actions or involved parties, the MLAT system de facto imposes the law of the recipient country over the law of the requesting one, even if there is no territorial connection to the latter other than the incorporation of the targeted platform or operator.
- Scalability. Establishing such bilateral relations among more than 190 countries would require more than 15,000 arrangements, an outcome neither feasible nor desirable.

Direct public-private requests. In the absence of timely and appropriate frameworks for international cooperation, public authorities in one country are increasingly sending requests directly to private actors in other jurisdictions, such as Internet platforms, hosting companies, registrars, or registries. This is particularly common in instances of requests for user data, content takedowns, and domain seizures. The internal transparency reports of some major global Internet companies provide a snapshot of the rise of such requests. Though there is a lack of reliable data to show the overall magnitude of this new trend, the increase in the number of requests reflects an attempt to establish modalities of voluntary cooperation.

Direct public-private requests however pose several problems. First, private companies are forced to make determinations on sensitive, high-stakes issues regarding economic conduct, international diplomacy, public safety, freedom of expression, and other human rights issues through procedures and criteria that lack transparency and due process. This can be an especially difficult situation when compliance with a foreign request would contradict the law in the company's country of incorporation. Meanwhile, forgone requests can lead to tensions, or in extreme cases to compulsory data localisation or the blocking of entire

platforms through national ISPs. Finally, while large global platforms can afford to allocate the necessary human and financial resources to managing requests, start-ups and medium-sized companies with globally available content and services struggle more considerably in these circumstances.

A Dangerous Path: Unintended Negative Consequences

The lack of coordination and inability of the international system to provide adequate and scalable cooperation solutions produce a typical "prisoner's dilemma"—actors, employing the only tools available to them, make short-term decisions that appear in their immediate interest, despite such solutions being sub-optimal or even detrimental in the long-term. On a wider scale, the sum of uncoordinated unilateral actions by governments and private actors can have serious unintended consequences.

Economically, a legal arms race would decrease investment in start-ups and medium-sized companies because of legal uncertainty and risks of intermediary liability, thereby stifling innovation, competition, and growth. In terms of freedom of expression and other human rights, increased pressure on Internet companies to accept direct requests could lower due process protections and produce a "race to the bottom", all in the absence of viable mechanisms for transborder appeals and redress for harmed Internet users. Barring other options, actors may be tempted to regulate content by manipulating the technical architecture of the Internet, wielding shutdowns or leveraging the location of registries and registrars to impose national laws. Finally, cooperation across borders is an urgent necessity when tackling cybercrime, terrorism, and other security threats confronting the global community at large.

Filling The Institutional Gap in Internet Governance

Traditional intergovernmental cooperation mechanisms are failing to provide appropriate solutions for the dilemmas of Internet governance, revealing an institutional gap that must be filled to adequately address these new challenges.

An important distinction to be made in this field is the difference between governance "of" the Internet and governance "on" the Internet. While governance "of" the Internet concerns protocols, standards, addresses, and other elements of technical architecture, governance "on" the Internet relates to the use of the Internet, in the applications and services that run on top of the physical and logical layers, as well as in the behavior of Internet users. Though the jurisdictional challenges discussed in this paper are primarily related to governance "on" the Internet, important lessons and possible solutions may be gleaned from the technical management of the Internet.

Over time, an ecosystem has emerged to handle governance "of" the Internet and enable the necessary technical interoperability that the global network requires. Organisations such as the Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C) develop Internet and Web standards, while Regional Internet Registries and the Internet Corporation for Assigned Names

and Numbers (ICANN) respectively organise the allocation of IP addresses and domain names. This ecosystem of transnational institutions is fundamentally distributed - each entity administers a specific issue and has its own internal structure and procedures, with loosely coupled coordination among them.

Despite their differences, each of these institutions covers the five stages necessary for the development and application of governance regimes: issue framing, drafting, validation, implementation, and reviews. Based on the fundamental principle of fostering multistakeholder involvement, governance "of" the Internet has enabled it to expand beyond the ambit of its research background to serve several billion people and permeate almost all human activities.

By contrast, the institutional ecosystem addressing issues related to governance "on" the Internet is embryonic at best. The UN's Internet Governance Forum (IGF) is a touchstone of this nascent field, providing an annual venue for actors to identify challenges, share experiences, and present their work. Yet, despite its essential role and numerous national and regional spin-offs, the IGF still only covers the first stages of the policy-making cycle: agenda setting and issue framing. Beyond some noteworthy efforts to document best practices, no efficient mechanisms exist yet to produce, let alone implement and enforce, the needed transnational arrangements for governance "on" the Internet.

Considering the diversity and distributed nature of technical governance organisations, the solution for governance "on" the Internet is not necessarily the replication of a single model. Indeed, addressing the issue of jurisdiction on the Internet requires neither the creation of a new international organisation nor the attribution of this responsibility to a single existing one, as Internet issues are relevant to the mandates of numerous entities. Filling the institutional gap in Internet governance demands a more innovative approach.

Catalysing Issue-Based Policy Networks

The issues of jurisdiction on the Internet lie at the intersection of four policy areas: legal cooperation, economy, human rights, and cybersecurity. Developing transnational mechanisms for policy coordination in these complex arenas will require ongoing, multistakeholder, and issue-based processes.

Based on the experience of Internet & Jurisdiction in leading a pioneering global dialogue process on these challenges, several key factors for the success of such issue-based policy networks have been identified:

- Framing the problem as an issue of common concern for all actors
- Ensuring the neutrality of the convener and facilitation team/secretariat
- Involving all stakeholder groups: states, Internet platforms, technical operators, academia, civil society, and international organisations
- Engaging a critical mass of actors with sufficient diversity to be representative of the various perspectives and to implement potential solutions
- Constructing and expanding a global network of key actors
- Creating trust among heterogeneous actors and adopting a shared vernacular
- Combining small groups and public reporting on progress to make the process both manageable and broadly transparent
- Informing stakeholders about relevant trends around the world to foster evidence-based policy innovation

- Providing sufficient geographic diversity from the onset to allow scalability in the adoption of any emerging policy solution

Toward Transnational Frameworks

Norms and procedures developed through such multistakeholder processes can be considered as "policy standards." As transnational frameworks for cooperation, they can establish mutual commitments between the different stakeholders, with:

- clear distribution of responsibilities;
- specific norms, procedural mechanisms or guarantees; and
- clear decision-making criteria.

As new forms of transnational soft law, such operational governance frameworks can establish procedural interoperability and due process across borders to handle multiple jurisdictions on the Internet. They can also help reform existing modes of interstate cooperation (for example, the Mutual Legal Assistance system), or fill current governance voids that require the creation of new sets of norms and standards.

Implementation and enforcement of such policy standards can employ a combination of existing tools and cover the range from simple, best practices to strict normative obligations. Public and private actors have different options to operationalise these shared norms. States, for example, can reference policy standards in their administrative procedures, while Internet platforms and technical operators can do so in their terms of service. Multistakeholder policy standards can even be institutionally embedded in national laws, endorsed by international organisations, or enshrined in new international treaties.

Drawing lessons from the governance "of" the Internet, a major advantage of standards is their potential to scale. Multistakeholder policy standards are based on consensus among different stakeholder groups, which augments the likelihood of successful and efficient adoption. They can more easily be implemented across heterogeneous public and private governance systems, which is key to creating interoperability. Moreover, such policy standards can be improved and adapted more quickly than conventional treaties, allowing them to develop further as the Internet ecosystem evolves.

Preserving the global character of the Internet and its social, political, and economic benefits for the next generations to come requires more cooperation among all stakeholders. We need to collectively develop new legal frameworks that are as transnational as the Internet itself in order to ensure legal interoperability and due process across borders.

The US-China Cyber Agreement: New Beginning or Tactical Pause?

Adam Segal

In the weeks before President Xi Jinping's visit to Washington in September 2015, there was little reason to think that the United States and China would be able to narrow the growing gap between the two sides in cyberspace. Washington and Beijing had recently clashed over policies designed to secure supply chains and information and communication technology equipment, the global governance of cyberspace and, most conspicuously, cyber attacks and espionage. In fact, as more details about the theft of data, allegedly by Chinese hackers, from the Office of Personnel Management were revealed, the public demand for some type of reaction against Beijing grew, including calls for cancelling the summit or downgrading it to a working meeting. The White House leaked stories that it was considering sanctioning Chinese individuals or entities that benefit from cyber theft, and President Barack Obama told a meeting of the Business Roundtable eight days before a scheduled dinner with President Xi, "We are preparing a number of measures that will indicate to the Chinese that this [cyber attacks] is not just a matter of us being mildly upset, but is something that will put significant strains on the bilateral relationship if not resolved, and that we are prepared to [do] some countervailing actions in order to get their attention."[1]

Despite all the build up, however, a breakthrough appears to have occurred. Many analysts had argued that China would not accept the US efforts to distinguish between political or military espionage ('good hacking') and theft of intellectual property ('bad hacking'). China saw all hacking as supporting comprehensive national power and—given National Security Agency (NSA) contractor Edward Snowden's revelations of reported NSA attacks on Swiss banks, Chinese telecoms, European trade negotiators and Petrobras, the Brazilian energy company—was unlikely to believe the US did not conduct economic espionage. Yet, at a joint press conference in the White House Rose Garden, President Obama announced that the two sides had agreed that "neither the US or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage."

Washington and Beijing would also provide timely responses to requests for assistance in cyber crime investigations; cooperate in conducting investigations and collecting evidence; identify and endorse norms of behaviour in cyberspace; and establish two high-level working groups and a hotline between the two sides.[2] After the announcement with the US, China reached a similar agreement

with the United Kingdom, and Germany will sign a deal with China sometime in 2016.[3] In November 2015, China, Brazil, Russia, US and other members of the G20 accepted the norm against conducting or supporting the cyber-enabled theft of intellectual property.[4]

The two sides also "welcomed" the July 2015 report of the UN Group of Governmental Experts [GGE] in the Field of Information and Telecommunications in the Context of International Security, which addresses the norms of behaviour in cyberspace. The 2015 GGE report reaffirmed the findings of a 2013 GGE report that international law, and in particular the Charter of the United Nations, applies to cyberspace. The 2015 report accepted three new peace-time norms proposed by the US: no country should intentionally damage the critical infrastructure of another state; prevent another country's computer security incident response team (CSIRT) from responding to cyber incidents or use CSIRTs for malicious activity; and countries should cooperate with requests from others to investigate cybercrimes and mitigate malicious cyber activity emanating from their territory.[5]

While the cyber espionage announcement attracted most media attention, China and the US also committed to addressing some of the economic issues that have emerged around cybersecurity. Washington, worried about the use of communication technologies by the Islamic State in Iraq and Syria (ISIS) and by so-called 'lone-wolf' attackers – individuals radicalised by extremist content on the web – is considering the insertion of "backdoors" or methods for law or intelligence agencies to bypass encryption or other security measures. Beijing, both in response to Snowden's revelations of US cyber espionage and mass surveillance and a desire to spur indigenous innovation, has said that technologies used in government networks must be "secure and controllable". Beijing has introduced banking provisions, the national security law, and a draft cybersecurity law in pursuit of this objective.[6]

At the summit, China and the US agreed that measures designed to ensure cybersecurity in commercial sectors "should be consistent with WTO agreements, be narrowly tailored, take into account international norms, be nondiscriminatory, and not impose nationality-based conditions or restrictions."[7] In December 2015, China passed a new anti-terrorism law that did not require foreign companies to provide backdoors or store their data locally, but did mandate that they provide "technical interfaces, decryption and other technical support assistance to public security organs and state security organs."[8] The most recent draft of China's proposed cybersecurity law contains similar language.[9]

The question is whether the sum of all these announcements represents a significant narrowing in the US and Chinese positions. Did President Xi's statement signal a change in Chinese behaviour, a tactical manoeuvre to avoid the bite of sanctions, or something else? Not surprisingly, given China has always denied that it conducts any type of cyber operation, the announcement was greeted with scepticism. Only days after President Xi had left Washington, Director of US National Intelligence James Clapper, asked by Senator John McCain whether he was optimistic about the agreement, responded, "I personally am somewhat of a sceptic. It will be our responsibility to look for the presence or absence of their purloining of intellectual property and other information."[10] President Obama himself asserted, "the question now is, are words followed by actions? And we will be watching carefully to make an assessment as to whether progress has been made in this area."[11]

The evaluation of China's intent is difficult at several levels. There was positive follow-up in the first round of cyber talks between the US Department of Homeland Security (DHS) and Chinese Ministry of Public Security (MPS) in December 2015. The two sides agreed on the guidelines for requesting assistance on cyber crime or other malicious cyber activities as well as to conduct "tabletop exercises" in spring 2016 and to define procedures for use of the hotline. Washington said it would consider Beijing's proposal for a seminar on combatting misuse of technology and communications by terrorists; Beijing, meanwhile, said it would study the US' proposal on inviting experts to conduct network protection exchanges.[12]

A subsequent meeting of the DHS-MPS dialogue in June 2016 affirmed that the spring 2016 tabletop exercise had been a success, and that both sides would continue collaborating on network protection, information sharing, and investigating and prosecuting cyber-enabled crime. And in August, the Ministry of Public Security reported that the hotline between DHS and MPS was up and running.[13]

Initial reports about whether Chinese cyber attacks have decreased were mixed. Counterintelligence chief Bill Evanina told reporters in November 2015 there was "no indication" from the US private sector "that anything has changed" in the extent of Chinese espionage.[14] Yet, some cybersecurity firms noted they had seen an overall drop in the level of attacks, or at least a shift in the source of attacks from the People's Liberation Army (PLA) to hackers affiliated with the Ministry of State Security (MSS).[15] In June 2016, US cybersecurity firm FireEye reported a steep decline in Chinese cyber espionage against organizations in the US and 25 other countries. The number of network compromises by 72 suspected China-based groups dropped from 60 in February 2013 to less than 10 by May 2016. US Assistant Attorney General John Carlin subsequently confirmed the company's findings that attacks were less voluminous but more focused and calculated.[16] This shift, if it has indeed occurred, would accord with the recent reforms of the PLA, including reorganisation of the military regions and cuts of 300,000 troops. These and other measures are designed to bolster the PLA's preparedness to fight and win wars, to which economic espionage makes no notable contribution to.[17]

Even if American firms say they are detecting a decline in cyber attacks, it may be because Chinese hackers have become stealthier and not that they have reduced the volume of their activities, which FireEye noted in its June 2016 report. The Washington Post reported in November 2015 that China had arrested hackers responsible for the theft of intellectual property, though the actions have not been confirmed by the US government nor were reported in the Chinese press.[18] This could be a one-time symbolic measure meant to divert US attention and pressure.

Definitional issues could also continue to divide the two sides. Much of the intellectual property that hackers steal is dual-use. It may serve national security interests as well as create commercial advantage to not be covered by the agreement. The phrase "knowingly support" may result in the hacking being shifted to criminal gangs or other proxies rather than be conducted by hackers in the PLA or MSS.

Beijing's embrace of the norm against cyber-enabled theft of intellectual property may also be less than what it first appeared. In December 2015, China hosted

the second annual World Internet Conference. In his opening speech, President Xi mentioned the norm against the cyber-enabled theft of trade secrets but in the context of other cyber crimes, cyber attacks and "cyber surveillance". He also called out double standards and stressed that no one country should define 'acceptable' norms in cyber behaviour. Beijing may intend to use the condemnation of cyber-enabled theft as an opportunity to criticise the US, especially since Beijing has never admitted conducting any type of cyber operations, while Washington has said cyber operations in search of military or political secrets are legitimate.[19]

Also, the apparent consensus reached by Washington and Beijing on cyberspace and international law masks significant differences. The 2013 and 2015 GGE documents refer to sovereign equality, the peaceful settlement of disputes, the prohibition on the use of force, non-intervention and the respect for human rights and fundamental freedoms, but provide no guidance on how they should be implemented. Moreover, while US diplomats are likely to interpret the acceptance of the applicability of the UN Charter to cyberspace to include the right to self-defence, China has been unwilling to embrace the right. Chinese analysts believe the US will use provisions of international law to justify an offensive operation against China.[20]

China and the US remain sharply divided about internet governance, too. At the World Internet Conference in Wuzhen, President Xi robustly defended the principle of cyber sovereignty, the "right of individual countries to independently choose their own path of cyber development, model of cyber regulation and internet public policies, and participate in international cyberspace governance on an equal footing."[21] Xi implicitly criticised the multistakeholder model of governance favoured by the US and its allies, saying governance should not be the purview of a small number of parties. Instead, Xi called for an approach that was multilateral and more state-centric.

Framed against the broad landscape of cyber issues, the agreement on cyber espionage looks less consequential even if it was a significant diplomatic achievement. After years of gaining little traction, the norm against the theft of intellectual property was referenced in quick succession in three agreements — US-China, UK-China and the G20. But the US and China continue to hold fundamentally incompatible conceptions of how cyberspace should be ordered. China will continue to pursue a strategy of exerting sovereignty over cyberspace through economic, technological and diplomatic measures.

The pressing short-term issue in the bilateral relationship will be the scope and scale of cyber espionage. The Obama administration may be happy to run out the clock until 2016 without incident, but if there is new evidence of a major breach, there will be great pressure for the US to sanction China. In April 2015, President Obama issued an executive order that laid the groundwork for more active use of economic sanctions against Chinese, Russian, Iranian and North Korean hackers as well as non-state actors. Declaring "significant malicious cyber-enabled activities" a "national emergency", the order enables the Treasury secretary to sanction individuals and entities with punishments that could include freezing their financial assets and barring commercial transactions with them.[22] If there is no sign that the attacks from China have abated, the US is likely to levy sanctions on high-level officials and state-owned enterprises. Beijing may retaliate with new regulation restricting foreign company access to the domestic market.

In addition to the dialogue between DHS and MPS on cybercrime, the 2015 September bilateral announcement mentions the creation of "a senior experts group for further discussions" on the norms of cyberspace, and the subsequent DHS-MPS meetings have included discussion of the creation of this expert group. Beijing and Washington have a common interest in preventing escalatory cyber operations – attacks that one side sees as legitimate surveillance but the other as prepping the battlefield.[23] The expert group should conduct formal discussions on the acceptable norms of behaviour and possible thresholds for use of force as well as greater transparency on doctrine. These cooperative measures can reduce the chance of misperception and miscalculation and thus diminish the likelihood that a conflict in cyberspace will become kinetic. The membership of the expert group has not yet been publicly announced. It is imperative that it includes members of the PLA.

Beijing and Washington also have a shared interest in preventing extremists and other third parties from attacking critical infrastructure. Terrorist groups have so far shown greater dexterity in the use of the web for recruitment, fundraising and propaganda than in launching destructive attacks but that will change over time. ISIS, for example, has a stated desire to develop cyber weapons and has reportedly recruited hackers from western Europe. To respond to emerging challenges, the US and China should discuss joint measures to prevent the proliferation of cyber attack capabilities, but this is bound to be politically difficult. At the World Internet Conference in 2015, President Xi called for an international convention against terrorism in cyberspace. While Beijing has not offered any details of what the convention will cover, it is likely to touch on removing extremist content from the internet, data storage and retention, and encryption. There are already contentious debates within the US about how best to manage these issues and Washington is unlikely to find common ground on controlling content with Beijing.

While the 2015 agreement on cybersecurity was an important step forward for China and the US, narrowing the gap between the two sides on cyber issues will require multiple dialogues involving a wide range of actors. Given the sharp ideological divisions over the organisation and governance of cyberspace, the best Washington and Beijing may hope for is a greater understanding of each other's redlines so that a conflict in cyberspace does not spill into the real world.

Cyber Capacity-Building in ASEAN: Importance of Confidence-Building Measures

Caitríona Heinl

In August 2016, Singapore and the United States agreed to enhance their strategic partnership and announce a memorandum of understanding on cybersecurity cooperation.[1] Their joint statement reaffirmed that both parties agree to deepen information exchange and sharing, conduct new bilateral initiatives on critical infrastructure cybersecurity and continue to cooperate on cybercrime, cyber defence and regional capacity-building activities, including through joint exercises, regular exchanges and visits, joint research & development and capability development as well as regional cyber capacity-building programmes or initiatives.[2]

Building on the joint statement, the US and Singapore then co-hosted a workshop on cybersecurity for ASEAN member-countries.[3] This regional cyber capacity-building initiative was part of the US-Singapore Third Country Training Program that works with ASEAN on a number of areas, including non-traditional security threats. The workshop focused on several important baseline themes in the cyber field, including:

- The need for multistakeholder cooperation;
- How to expand access and affordability while integrating cybersecurity;
- Elements of an effective national cybersecurity strategy;
- Broad concepts involved in developing and implementing a national cybersecurity strategy;
- National incident management, including the role of a national computer emergency response team (CERT);
- Establishing, managing and maintaining computer security incident response teams (CSIRTs);
- Confidence-building measures (CBMs);
- Promoting a culture of cybersecurity through awareness campaigns;
- How to increase the size and capability of a workforce;
- Supporting an open and secure internet and how this fosters economic growth and social development;
- How industry deals with incident responses to better facilitate public-private collaboration; and
- How government can increase collaboration with private and tech sectors, including for critical infrastructure protection.

This commentary includes some points that were made in the session on CBMs to provide a basic overview for ASEAN countries and to address the session questions.[4] It does so through four short sections that seek to lay the foundation for a case example of a non-ASEAN member-country like Japan. The main questions outlined for the session were: a) a brief overview of CBMs; b) communicating strategic goals and objectives to stakeholders and partners as a CBM; and c) how can policy and diplomacy contribute to cybersecurity.

General Background[5]

CBMs are generally used as tools to improve stability by reducing sources of mistrust, misunderstanding, miscalculation, tension or hostilities and by reinforcing the existing level of confidence. For instance, an overarching goal of military CBMs is to facilitate increased transparency, better information exchanges and restrain military intervention, thus enhancing situational awareness and common understanding. Nevertheless, while CBMs might aim to deescalate an unintended conflict, they may have limited use in cases of intentional conflict. The purpose of non-military CBMs is to build trust between communities like law-enforcement authorities, incident responders and civil society through actions spread across political, economic, environmental, social or cultural fields. Some traditional CBMs can therefore be adapted to the cyber field while taking its more unique characteristics into account.

Why Cyber CBMs should be Important to ASEAN

For many years, several processes have aimed to reduce the risk of conflict in this space by: a) clarifying how international law applies to cyberspace; b) developing norms of responsible state behaviour; and c) developing CBMs.

In early 2016, within what has become known as the Sunnylands Declaration (the Joint Statement of the US–ASEAN Special Leaders' Summit), the heads of state or government of the 10 ASEAN members and the US reaffirmed that there is a "shared commitment to promote security and stability in cyberspace consistent with norms of responsible state behaviour."[6] This is now a central aspect of the US-ASEAN strategic partnership to enable peace, prosperity and security in the Asia-Pacific region.

However, at the bilateral level, the recent US-Singapore joint statement for instance, countries now endorse a common approach to international cyber stability, affirming that international law applies to state conduct in cyberspace and committing themselves to promote voluntary norms of responsible behaviour in cyberspace. They assert that these norms of behaviour include: a) no country should conduct or knowingly support online activity that intentionally damages critical infrastructure or otherwise impairs the use of critical infrastructure to provide services to the public; b) no country should conduct or knowingly support activity intended to prevent national CSIRTs from responding to cyber incidents or use these teams to enable online activity that is intended to cause harm; c) every country should cooperate, consistent with its domestic law and international obligations, with requests for assistance from other states in mitigating malicious cyber activity emanating from its territory; and d) no

country should conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to its companies or commercial sectors.

Cyber CBMs are part of this normative approach to build stability in cyberspace.[7] While they are not norms, cyber CBMs aim to achieve several goals such as:

- Providing practical tools to help manage international expectations in the norms building process.
- Helping ensure that states do in fact have the same understanding of their norm commitments.
- Assisting in achieving such norms of behaviour through the highly interlinked nature of norms and CBMs..
- Improving predictability and mutual understanding where there are concerns over misunderstanding or perhaps false attribution in the use of information and communications technologies.
- Creating an international environment of stability so that economic and social development can flourish.

Several inherent challenges associated with the cyber field validate the need for cyber CBMs. For instance, many of these technologies may be hard to detect or count, rendering state capabilities hard to assess. Many states have either begun to increase their use of these types of capabilities or have at least expressed an interest in doing so, a point reiterated in the workshop. Moreover, the fact that non-state actors may be involved in cybercrimes complicates matters. Thus, for shaping cyber CBMs, political will and commitment to prevent conflict, investment in resilience and skills and strong legal systems of ASEAN countries are needed.[8]

Nature of Cyber CBMs

A simple framework proposal for ASEAN was mooted by the US in the past as a CBM structure in which measures are developed and implemented in sequence.[9] This includes: 1) transparency CBMs; 2) cooperative measures; and 3) stability and restraint measures.

First, transparency measures aim to reduce suspicion as well as to increase confidence and predictability of state behaviour. Some examples include crisis communication mechanisms, information exchanges on national policies and structures, communicating national strategies, and information-sharing on threats. Second, cooperative measures might aim to combine transparency and communication efforts to promote joint procedures. In this case, some examples include assistance in resilience and capacity-building initiatives to strengthen collective capacity, development of national strategies, assisting CERTs and implementing legislation. Third, stability and restraint measures aim to strengthen states' commitment to refrain from certain destabilising activities; in other words, to limit, criminalise or exclude destabilising and offensive activities.

A recent strategic dossier by the International Institute for Strategic Studies explains that these measures must be implemented in line with international law, and practices developed can lead to binding international norms.[10] It outlines that if politically binding CBMs are implemented on a consistent basis over a significant period of time, this may lead to new rules in customary international

law. In addition, given a focus of the workshop on cyber capacity-building, emphasis should be laid on the argument that the implementation of CBMs can be assisted through capacity building.[11] In other words, capacity-building can help if countries want to commit (or have already committed) to certain CBMs and norms but they do not necessarily have the actual capacity to do so. In a region like ASEAN that comprises highly diverse members — including for example, both developing and developed countries — this is an abiding argument. There is now a recognised need for deeper capacity-building to ensure real progress in the implementation of CBMs and norms across the region.

State Efforts

Several cyber CBM efforts have been initiated at global, regional and bilateral levels over the past few years. These include the work of the Organization for Security and Cooperation in Europe (OSCE), UN Group of Governmental Experts (UN GGE), ASEAN Regional Forum (ARF) and the Organization of American States (OAS).

In chronological order, participating states of the OSCE agreed to a set of 11 voluntary measures in 2013, most of which are related to transparency.[12] For example, they agreed to voluntarily share information on measures taken to ensure an open, interoperable, secure and reliable internet. They also agreed to voluntarily share information on national organisations, strategies and policies. Both of these CBMs were subject to analysis at the workshop for ASEAN members. The 2013 UN GGE consensus report then underlined the need for such measures in its recommendations for CBMs (Indonesia was a member of this group).[13] The report asserted that voluntary CBMs can promote trust and assurance, increase predictability and reduce misperception. It recommended that states should consider developing practical CBMs to increase transparency, predictability and cooperation.

The latest UN GGE report of 2015 built on the 2013 CBMs (Malaysia was a member of this group).[14] Analysts expect that this could provide a framework for regional organisations to possibly use or adapt, if necessary, taking regional nuances into account (like those in Southeast Asia and ASEAN). The ARF adopted a work plan in 2015 to focus on practical CBMs to develop trust and confidence in the region; ASEAN members could also consult the OAS work in this area to craft good practices.[15]

In the first half of 2016, OSCE participating states laid out a further set of CBMs.[16] One such measure includes voluntarily sharing national views of categories of critical ICT-enabled infrastructure, another timely topic of discussion for ASEAN at the workshop. Other CBMs may be established bilaterally. It may include extending a traditional hotline to include cybersecurity like US-Russia agreements to do so. Over the near future, however, there are concerns, in academia at least, that measures developed in regional or international forums may evolve differently, perhaps causing further complexity.[17] These are challenges that need to be considered by ASEAN going forward, as it continues work to develop and implement CBMs.

The Public Core of Internet: Towards an International Agenda for Internet Governance[1]

Dennis Broeders

The Internet's core of key protocols and infrastructure can be considered a global public good that provides benefits to everyone. Countering the growing state interference with this public core requires a new international agenda for Internet governance that departs from the notion of a global public good.

Internet Governance: Between Technical and Political

Everyday life without the Internet has become unimaginable. It is inextricably woven with our social lives, purchasing behaviour, work, relationship with the government and, increasingly, with everyday objects, from smart metres to the cars we drive and the moveable bridges we cross en route. For a long time, Internet governance was the exclusive domain of a technical community of cyber experts. This community laid the foundations for the social and economic interconnectedness of our physical and digital lives. Those foundations, with the Internet Protocol Suite (Transmission Control Protocol (TCP) and Internet Protocol (IP)) as their most prominent component, continue to function as the robust substructure of our digital existence. However, the governance of that substructure has become controversial. The many economic and political interests, opportunities and vulnerabilities associated with the Internet have led governments to take a much greater interest in its governance of the Internet. Moreover, in terms of policymaking, the centre of gravity has shifted from what was primarily an economic approach (the Internet economy, telecommunications and networks) to an approach that focuses more on national and other forms of security: the Internet of cybercrime, vulnerable critical infrastructure, digital espionage and cyber attacks. In addition, a growing number of countries are seeking to regulate their citizens' online behaviour, for reasons ranging from copyright protection and fighting cybercrime to censorship, surveillance and control of their own populations on and through the Internet. Attempts by nation-states to 'fence off' their national area of cyberspace and their increased role in its governance may have repercussions for the Internet's core protocols and infrastructure.

The Internet was designed to operate internationally, without regard for the user's status or nationality – an underlying principle that benefits all users. It is mainly the Internet's public core comprising protocols, standards and infrastruc-

ture that routes data so that it reaches all corners of the globe. If these protocols and standards fail or become corrupted, the performance and integrity of the entire Internet will be at risk. The Internet is 'broken' if we can no longer assume that the data we send will arrive unaltered and uncorrupted, we can locate the sites we are searching for and those sites will be accessible. Recently, a growing number of states have tampered with the Internet's core infrastructure to further their national interests.

Internet governance is at a crossroads: the cyberspace has become so important that states are no longer willing or able to regard it with the same 'benign neglect' that long set the tone for most countries. States do have national interests that go beyond governance of the Internet as a global collective infrastructure. It is imperative to determine which part of the Internet should be regarded as a global public good – and thus safeguarded from improper interference – and what should be considered a legitimate part of international politics, where nation-states can stake a claim and take up their role without harming the infrastructure of the Internet itself.

The Internet's Core as a Global Public Good

The public core of the Internet must be regarded as an impure global public good.[2] As such, it should be protected against interventions of states that are acting only in their national interest, thereby damaging that global public good and eroding public confidence in the Internet. Global public goods provide benefits to everyone, benefits that can be gained or preserved only by taking specific action and by cooperating. The means and methods for providing a global public good may differ from one case to another and can be undertaken by private or public parties or combinations of the two. This can be said to apply to the Internet both as a global network and infrastructure.[3]

The Internet as a global public good is not equated with the whole Internet, or with the sociocultural layer of content and communication. It is applied only to a subset of core protocols and infrastructure. Global benefits derive largely from the Internet's core protocols, including the TCP/IP suite, numerous standards, the Domain Name System (DNS) and routing protocols.

As a global public good, the Internet works properly only if its underlying values – universality, interoperability and accessibility[4] – are guaranteed and if it facilitates the main objectives of data security, i.e. confidentiality, integrity and availability.[5] It is vital that end-users can rely on the most fundamental Internet protocols functioning properly: those protocols underpin the digital fabric of our social and economic life and existence. Although states will inevitably want to create an Internet in their own image, especially in the sociocultural layer of content, we must find ways to continue guaranteeing the overall integrity and functionality of the public core.

From Governance of the Internet infrastructure to Governance using it

To highlight the problem, we can use Laura DeNardis' useful distinction between two forms of Internet governance.[6] The first is 'governance of the Internet's infrastructure', i.e., the governance of the core infrastructure and protocols that

drives the Internet's development. The collective infrastructure takes precedence in this form of governance. The second form is the 'governance using the Internet's infrastructure'. In this case, the Internet becomes a tool in the battle to control online content and behaviour – often domestically - as well as a source of threat and a weapon in terms of international security. The issues vary from protecting copyright and intellectual property rights to government censorship, surveillance of citizens, and international intelligence, espionage and military activities online. Increasingly, governments view the infrastructure and main protocols itself as a legitimate means to achieve their policy ends. Whereas Internet governance used to mean governance of the Internet – with the technical management and performance of its infrastructure as the top priority – the trend today is increasingly towards governance using the Internet. Such interventions can undermine the integrity and functionality of the cyberspace and, in turn, undermine the digital lives that we have built on top of it.

Threats to Governance of the Internet Infrastructure

Governance of the Internet's public core – i.e., governance of the Internet infrastructure – is entrusted to a number of organisations that are collectively known as the 'technical community'.[7] Although governance is mostly in good hands, political and economic interests – sometimes combined with new technologies – are challenging the collective character of the community in ways like:[8]

- Economic interests – such as copyright protection and revenue models for data transport – are putting pressure on policymakers to abolish or, conversely, offer legislative protection to net neutrality, which was previously the Internet's default setting.

- The transition of the 'IANA function', which includes the stewardship and maintenance of registries of unique Internet names and numbers. There is currently a transition underway which will remove oversight of IANA from the US sphere of influence mainly for reasons of international political legitimacy.[9] The debate on this transition may result in more politicised management of the DNS, which in turn may have repercussions for the ability to find and locate sites and users. Most countries would benefit from IANA functions that are as 'agnostic' as possible, especially when it comes to the administrative tasks.[10]

- The rise of the national security mindset in cyberspace. The technical approach of the CERTs (with a focus on 'keeping the network healthy') and their international collaboration is at odds with the approach of national security actors such as intelligence agencies and military cyber commands. It is important to prevent these approaches becoming confused and/or mixed because national security conflicts with the collective interest of the network's overall security.

Threats Resulting from Governance Using the Internet Infrastructure

The need for worldwide consensus on the importance of a properly functioning public core of the Internet seems obvious because it is these protocols that guarantee the functionality and integrity of the global Internet. However, recent international trends in policymaking and legislation governing the protection of copyright, defence and national security, intelligence and espionage, and various

forms of censorship show no signs of such a consensus. Some states see DNS, routing protocols, Internet standards, manipulation and building of backdoors into software and hardware and the stockpiling of vulnerabilities in software, hardware and protocols (so called 'zero-day vulnerabilities') as suitable instruments for national policies focused on monitoring, influencing and blocking the conduct of people, groups and companies. Also, 'cyber' is increasingly the part and parcel of international security. Many states have declared cyberspace the fifth domain of warfare and are adding new specialised units to their military and intelligence forces. The negative impact of such interventions is borne by the global collective and impairs the Internet's core values and operation. Illustrations of this trend include:[11]

- Various forms of Internet censorship and surveillance that use key protocols as well as enlisting the 'services' of intermediaries such as Internet Service Providers (ISPs) to block and trace content and users.

- Online activities of military cyber commands, intelligence and security services which undermine the proper functioning of the Internet's public core. By corrupting standards and protocols, by building backdoors into commercial hardware and software and by stockpiling zero-day vulnerabilities, these actors effectively damage the functionality and integrity of the collective Internet infrastructure and make it less secure.

- Legislation to protect copyright and intellectual property that permits the use of vital Internet protocols to regulate and block content. 'Side-effects' of such legislation include the collateral blocking of content and users (overblocking), damage to the DNS and intermediary censorship through ISPs.

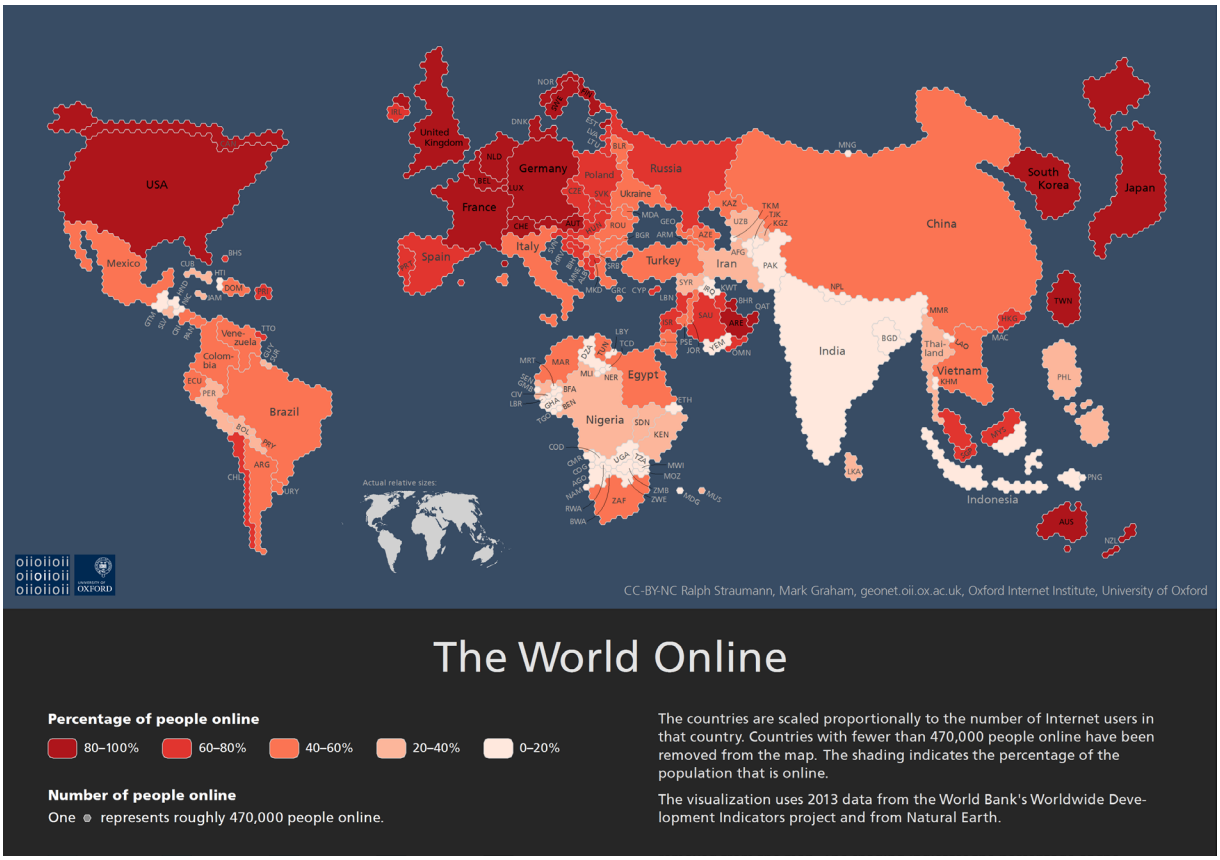
- Some forms of Internet nationalism and data nationalism – in which states seek to fence off a national or regional part of the Internet – which require interventions in routing protocols. In extreme forms, this could lead to a splintering of the Internet.

Challenges for Internet Governance

The international political landscape of Internet governance is changing rapidly. The next billion(s) of users will mainly go online in emerging economies that may have a different cultural and political outlook on cyberspace from a still dominant western view. Figure 1 shows the absolute numbers of Internet users globally and highlights the potential for future growth which is especially vast in Asian countries such as India, China, Indonesia and many African and South American nations. In contrast, the West is nearing the saturation point and growth is now more about the number of devices than the number of users.

With its growing importance for the economy and high dependence of national (critical) infrastructures on it, more countries will become increasingly active and vocal in debates on Internet governance and cyber security. The global political rift that emerged in the vote on the new ITRs during the 2012 World Conference on International Telecommunications in Dubai indicates that more political contention is likely to emerge in the coming years on both fronts.

Moreover, many countries will have upgraded their technical cyber capacity considerably within a few years, giving a much larger group of states capacities that



Source: Graham, De Sabatta and Zook (2015)[12]

are currently reserved for only a few superpowers. What is cutting edge today will be much more commonplace in five years' time. If in that same timeframe – and against this background of international demographic and geopolitical shifts - the idea takes hold that states are at liberty to decide whether or not to intervene in the Internet's main protocols to secure their own national interests, it is likely to damage the Internet as a global public good. For these reasons, there is no time to lose in securing the public core of the Internet.

Internet's public core should be International Neutral Zone

Given these developments, it should be a multilateral priority to work towards establishing a global norm that identifies the main protocols of the Internet as a neutral zone in which governments are prohibited from taking action that damages the public core for the sake of their national interests. This should be considered an extended national interest[13] , i.e. a specific area where national interests and global issues coincide for all states that have a vital interest in keeping the Internet infrastructure operational and trustworthy. With the continuing spread of the Internet and ongoing digitisation, that is increasingly a universal concern.

To protect it as a global public good, there is a need to establish and disseminate an international norm stipulating that the Internet's public core must be safeguarded against unwarranted intervention by governments.

The starting point should be to place the drafting of such a norm on the international political agenda, something that will entail making governments worldwide aware of the collective and national importance of public core of the Internet. Given the enormous differences between countries in terms of Internet access, overall digitisation and technological capacity, this will require a serious diplomatic and political effort. This norm could be disseminated through relevant UN forums as well as through regional organisations such as the Council of Europe, Organisation for Economic Cooperation and Development, Organization for Security and Cooperation in Europe, Association of Southeast Asian Nations and the African Union. This strategy could lay the foundations for what could eventually expand into a broader regime.

Need to Disentangle Internet Security and National Security

The emphasis on national security comes at the expense of a broader range of views on security and the Internet. Defining and disentangling different views on security may in fact improve the security of the Internet as an infrastructure.

It is therefore vital to advocate at the international level that a clear differentiation be made between Internet security (security of the Internet infrastructure) and national security (security through the Internet) and to disentangle the parties responsible for each.

It is of paramount importance to delineate the various forms of security in relation to the Internet. The technical community and the diplomatic/international security community mean different things when they talk about security. The first refer to the security of the Internet as a global infrastructure, or more specifically the notion Internet security, i.e., ensuring that the network itself is secure and operational. The latter usually refer to national and international security, which is mostly defined in geopolitical and military terms. In this vision, the Internet is regarded simultaneously as a source of threat and as a potential policy instrument. For example, it is important to separate the technology-driven strategy of the CERTs, which involves a public health-type approach to the overall network security, from the logic of national security, which places national interests above those of the network. Indications of movement on this issue can be found in the latest report of the UN Group of Governmental Experts (GGE), for example in its argument that states are urged to 'neither harm the systems and activities of other (national) CERTs, nor to use their own to engage in malicious international activity'.[14] More generally speaking, a more precise demarcation of national security issues from other forms of cyber insecurity would allow more room for the logic of residual risk in matters of cyber security and would apply the logic of national security more selectively to avoid or mitigate escalation.[15] More precise terminology and a clear division of labour between various agencies can in itself function as a confidence-building measure in the international cyber domain.

Need to Build New Coalitions

Given the international demographic and political shifts in cyberspace, it is time to open, broaden and expand the arena for cyber diplomacy. There is a need to involve states that are still building their technical and political cyber capacities – and occupy a certain middle ground between the multistakeholder camp and the national Internet camp - fully in the debates about Internet governance and international cyber security issues.[16] Secondly, there is a strong case to be made for targeting the large, Internet-based companies as explicit subjects of cyber diplomacy, as well as a need to think through and regulate what the role and position of intermediary organisations on the Internet – such as ISPs and Internet exchanges – is and should be.[17] Finally, states need to make more productive use of the expertise of the technical community, NGOs and other private stakeholders, especially in thinking through the effects of national and foreign policies on the technical operation of the Internet as a whole.

The Way Forward

Ideas similar or related to the idea of protecting the public core of the Internet have been emerging recently. In January 2016, William Drake, Vint Cerf and Wolfgang Kleinwächter published an excellent paper on the issue of Internet fragmentation for the World Economic Forum.[18] Some forms of Internet fragmentation – those that may have severe, long-term consequences for the functioning of the Internet as a global infrastructure – are akin to the notion of the public core of the Internet. In June 2016 the Internet Society (ISOC) published a beta version of its Policy Framework for an open and trusted Internet in which it states that the technical community shares "a sense of collective stewardship towards the public core of the Internet and the open standards on which its technologies and networks are based".[19] Also in June 2016, the Global Commission on Internet Governance (the Bildt Commission) published its final report called One Internet, which included a policy recommendation on the protection of the public core that read: "Consistent with the recognition that parts of the Internet constitute a global public good, the commission urges member states of the United Nations to agree not to use cyber weapons against core infrastructure of the Internet".[20] The Netherlands government issued its formal response to the report on the public core of the Internet in May 2016 and made the protection thereof a long-term priority for its foreign policy on cyber issues.[21] The first port of call to establish a norm protecting the public core will be the 2016-2017 round of the UN GGE of which the Netherlands is one of 25 members. One way forward is to use various diplomatic channels and to create strategic alliances around the idea of protecting the core of the Internet as a global infrastructure to the benefit of all nations and users.

SECURITY AND PRIVACY

The Missing Option: India, Pakistan and Armed Conflict in Cyberspace

Arun Mohan Sukumar

Likely to be among the options weighed by India's National Security Advisor (NSA) in response to Pakistan's alleged complicity in the Uri terrorist attack of September 18, 2016 is coercive cyber action. In theory, a cyber attack could be swift, minimise the risks of causalities, offer plausible deniability and could likely inflict serious damage on Pakistan's economic infrastructure. In reality, however, the picture is more complicated. Any assessment by New Delhi of this option should account for the following:

1. India's offensive cyber capabilities
2. The defensibility of such action under international law
3. The desirability of coercive cyber measures against Pakistan's networks

Capacity

Coercive cyber measures, like any military option, should be the culmination of extensive assessments by India of its intelligence and technical capabilities. Take as two possible targets, the Hub Power Station in Karachi and the Karachi (now Pakistan) Stock Exchange. The Hubco plant is among the largest thermal power-generating projects in Pakistan, capable of "provid[ing] 10+% of [the] country's electricity demand".[1] The KSE (now Pakistan Stock Exchange) is its premium financial trading platform. To mount a cyber attack against either installation, military planners should be supported by intelligence inputs from the ground, providing valuable information about:

i) personnel who may (wittingly or otherwise) introduce a vulnerability into the facilities, and;
ii) the physical location of computers/servers which form part of the network to be infected

Both require an assessment of the installation that goes well beyond aerial or satellite reconnaissance. Without strengthening India's intelligence networks in Pakistan, therefore, a serious attack on its digital networks will be difficult to conceive or execute.

Then there is the matter of the 'cyber weapon' itself. Not many government agencies in India, including the National Technical Research Organisation, have the in-house expertise required to build and exploit vulnerabilities that can manipulate or destroy the integrity of electronic data. India's armed forces fare

marginally better, having deployed 'red teams' that do penetration testing to protect their own networks. But the military too may not be in a position to create a sophisticated cyber-weapon designed for the specific purpose of bringing down, say, Pakistan's electricity grid.

It is worth remembering that Stuxnet was the product of an inter-agency effort involving the United States and Israel. Stuxnet owes its origins in no small part to the United States' well-developed bug bounty programme, which invites hackers to identify vulnerabilities in operating systems and communications platforms. Having a bug bounty programme (which in the US is tightly regulated by the White House) contributes to a strategic culture that can co-opt technical expertise in India into the national security narrative. There is no reason why New Delhi should shy away from a programme for its defence and intelligence agencies, given the talented pool of computer scientists in the country. In fact, internet giants like Facebook and Google routinely rely on Indian citizens to identify fixes and flaws in their products through their own bug bounty schemes. Today, Indian agencies rely on private expertise on an ad hoc basis, or buy zero-day vulnerabilities from the 'dark net'.[2]

An evaluation of coercive cyber measures against Pakistan by the NSA – the last step in the chain of decision-making before it is presented as a credible option before the Prime Minister – can be done only if he is able to lean on multi-agency coordination that will supply both human intelligence and technical expertise.

The tail, however, should not wag the dog. Conceiving and creating a cyber weapon will likely involve months, but this process should be guided by a political strategy as to its specific objective, likely impact, and potential fallout. Unlike conventional weapons or weapons of mass destruction, it is impossible to create an 'arsenal' of cyber weapons that can be deployed at will.

The first step for India's defence planners, then, would be to absorb coercive cyber measures as a central pillar of its Pakistan policy. This would involve:

1. An identification of targets, and their potential vulnerabilities
2. Assessing the deterrence value of a declared 'cyber doctrine'
3. Enhancing capabilities, in ways referred to above

Defensibility

Cyber attacks are difficult to attribute to governments, as they often originate from non-state actors and sometimes, through servers based in a third country. Links between non-state actors and the governments of the territory in which they are based can at best be established using circumstantial evidence. In India's case, military planners need to walk a fine line between denying any involvement in a cyber attack, and signalling to Islamabad that its so-called 'asymmetric' actions will be met by similar responses. Were New Delhi to be implicated in a coercive cyber manoeuvre against Pakistan, Indian diplomats should be prepared to defend the legality of its conduct in multilateral venues like the United Nations.

In essence, India's legal defence against a cyber attack on Pakistan would be to claim an act of reprisal. Given the UN's visible lack of enthusiasm in enacting a Comprehensive Convention on International Terrorism, India will have to rely on

traditional principles of state responsibility to hold Pakistan responsible for the actions of groups like the Jaish-e-Mohammed and Lashkar-e-Taiba. Without wading into the vast and rich jurisprudence on the subject, it is sufficient to say that even if India should produce evidence linking terrorist groups to the Pakistani government, it may be difficult to satisfy purely legal requirements.

Article 8 of the draft articles on Responsibility of States for Intentionally Wrongful Acts[3] states:

"The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct." (emphasis added)

The 'direction/control' test is a high standard to which India or the international community may never hold Pakistan. The first hurdle for India is to meet this threshold, absent a 'smoking gun'.

The second (and related) difficulty is to establish that attacks by terrorists are not only attributable to Pakistan but that they also violate a prohibition on the "use of force" enshrined in Article 2(4) of the UN Charter. If that seems incredulous, there's more. For India to claim "self-defence" in international law under Article 51 of the Charter, attacks such as the one in Uri should constitute an "armed attack" by the Pakistani state, a legal threshold that is generally accepted to be higher than the plain "use of force".[4]

In the aftermath of the 9/11 attacks, the United States invoked its "clear right of self defence"[5] under Article 51 to bomb Afghanistan -- a decision that polarised international opinion on the legality of its claim. In that instance, however, the US had the overwhelming support of the UN Security Council, which subsequently legitimised the intervention through the establishment of the International Security Assistance Force in 2001. In India's case, no such support from UNSC members will be forthcoming. In any case, New Delhi has no appetite for an armed intervention of the scale seen in Afghanistan.

Simply put, it is improbable that India can convincingly make the case for "self-defence" through a cyber attack against Pakistan. Reprisals on the other hand involve the use of force, but need not be reported[6] to the UN Security Council, and constitute an act akin to self-defence for attacks of a lesser degree.

Amidst this legalese, it is important not to miss the larger, political picture. For India to offer a convincing defence of retaliatory cyber measures against Pakistan requires coordinated planning between the Ministry of External Affairs (MEA) and the National Security Council Secretariat. Irrespective of what New Delhi may term its actions, the cyber attack should be a proportionate response to Pakistan's transgressions. The MEA and its lawyers should advise the NSA on this count and thoroughly review the cyber weapon's impact on civilian populations. To help mould the evolving body of international law in its favour, India must also step up engagement with international platforms such as the UN Group of Governmental Experts on ICT security and the Tallinn Manual consultations on the law of armed conflict in cyberspace.

Desirability

Coercive cyber measures offer some advantages to a policy planner where conventional military options appear limited, as in India's case against Pakistan. Nevertheless, several concerns persist, which should prompt New Delhi to examine the desirability of this option.

1. Such measures will have the same impact as the use of conventional weapons in turning the world's attention to the Kashmir conflict. Were India to target critical infrastructure in Pakistan, New Delhi can be certain the rhetoric across the border would escalate. In its aftermath, India may find it difficult to manage heightened international concerns, especially as the risks of cyber warfare are relatively unknown.

2. Coercive measures against Pakistan may give away India's presence in digital networks that have been penetrated for the primary purpose of espionage and surveillance. For instance, were New Delhi to target Pakistan's telecommunications infrastructure, it will reveal vulnerabilities in such networks that enabled the attack, prompting Pakistan to fix them. In the short and medium term, India may lose some valuable channels of intelligence gathering which must be weighed against the impact of the cyber weapon.

3. It would be reasonable to expect an escalation of low-intensity cyber attacks from China immediately following the incident. The creation of a cyber-weapon, or malicious tools to damage the integrity of Pakistan's digital networks, needs extensive planning but it is a project that involves a select group of parties. India's preparedness to defend its own networks, on the other hand, is a national conversation that needs to be continually had with organisations from the public and private sectors. As things stand, India has not fully assessed the resilience of its critical sectors and may not be able to limit the damage from a retaliatory attack. Deepening of the China-Pakistan strategic relationship, leading to eventualities like the co-development of cyber weapons, can further limit the political and military options available to India in the event of conflict.

4. The United States is unlikely to offer India material support in planning or executing the attack, or shield New Delhi from political criticism in its aftermath. At the UN Security Council, however, both Russia and the US can be expected – for reasons purely driven by self-interest – to veto any proposal from China condemning the use of cyber weapons. India has not reached out to possible interlocutors like Israel to begin collaboration on the creation of sophisticated cyber instruments.

5. Whether or not the attack on Pakistan's digital networks forces its military to revisit the country's sponsorship of terrorist groups, the overall stability of cyberspace in South Asia will be seriously called into question. Denial of service attacks, large-scale hacks, and disruption of internet services could become the norm, if the Pakistani state pursues a strategy of continuous, low-intensity engagement against New Delhi. A cyber attack is only as effective as the lure of the digital economy, and India stands to lose big in this game of chicken.

The lesson here, perhaps, is that a declared doctrine on the use of cyber weapons, pursuant to the building of capacities, can signal deterrence to Pakistan more effectively than the use of such instruments in isolation by India. It will

likely take years to bring such a strategy to fruition: after the May 1998 tests, it took India nearly 5 years to articulate a nuclear weapons doctrine. The rapid advancement of digital technologies suggests that a cyber doctrine, if articulated, should be flexible, and open to review and possible restatements. Pakistan's nuclear weapons capability is often cited as a dead-end for India's conventional superiority, but cyberspace opens a new theatre of conflict. But it is critical this process begins now, failing which India could be drawn towards an inevitable confrontation in digital spaces with Pakistan without a clear assessment of its goals or outcomes.

Bundeswehr: Cyber Security, the German Way

Isabel Skierka

In late April 2016, German Defense Minister Ursula von der Leyen unveiled a plan to establish a dedicated "cyber and information command" in the German military, the Bundeswehr. A reorganisation of the armed forces to bolster its computer systems and network defence capabilities had long been overdue and was discussed in the German Federal Ministry of Defence for more than a decade.[1]

But when the Defense Minister announced the cyber security plans for the armed forces, she faced significant scepticism from parts of the German public. Several media outlets and politicians warned of the dangers that Germany could gear up toward 'cyber war' and engage in an uncontrollable digital arms race.[2] This view was aptly expressed at a parliamentary hearing by a German security policy expert who argued that the development of "preparatory measures for placing malware in opponents' computer systems" amounted to a "colonisation of the web [which] contradicts the German culture of military restraint".[3] Many argued that the Bundeswehr should adopt purely defensive measures to protect its own networks and not conduct any operations in foreign networks.[4] The Ministry of Defence itself responded that the Bundeswehr would act only within the provisions of its constitutional mandate and would not engage in any offensive computer network operations, unless it was mandated to do so by the Parliament.

This year's debate over the Bundeswehr's relatively modest new cyber plans shows how the German public's long-fraught relationship with its military and intelligence agencies now encompasses the digital arena. The Edward Snowden revelations in 2013 brought the field of cyber security out of its niche existence in Germany, sparking a debate and anti-surveillance backlash that was more intense in the country than just about anywhere else. The Snowden revelations also shone a spotlight on how far behind the curve the German government was in the realm of cyber security. In the three years since, Germany has struggled to shape a new digital agenda to improve both its IT security efforts and its cyber intelligence capabilities. It has been hampered both by limitations in resources and personnel, as well as the German public's unease with surveillance and the use of force.

The German government has in recent years launched a range of digital security initiatives, including a law regulating the protection of critical infrastructure. This article focuses on one of the latest and most controversial initiative: plans to form a new cyber command in the German military. The debate around the plans and the nascent efforts to implement are emblematic of the broader political and institutional tensions in Germany at the intersection of information security and national security.

The Reorganisation of the Bundeswehr's Cyber Capabilities

Until recently, the German armed forces played a minor role in cyber security compared with militaries in North Atlantic Treaty Organization allied countries such as the United States, France or the United Kingdom. This year's adoption of a military strategic guideline for cyber defence and reorganisation of the armed forces for this purpose thus set a milestone in German defence policy. From the military's new White Paper published shortly after, it becomes clear that cyber security has become an integral part of national defence strategy in the context of hybrid and conventional warfare threats. The word 'cyber' alone appears 74 times in the 125-page White Paper.[5]

The strategy has been hyped both by proponents and critics, either as a major step forward towards being able to finally defend the nation in the digital realm, or as a dangerous move toward Germany's participation in a possible cyber war.

Looking at the reorganisation more closely, it is firstly a task that any large organisation or company faces on the path of digitalisation: the Bundeswehr has to maintain a reliable and secure IT architecture for its 280,000 users. Beyond that, it has to recruit highly qualified personnel, keep pace with technological innovation, and reflect often conflicting political interests.

To date, the Bundeswehr's cyber defence capabilities consist of three components: a Computer Emergency Response Team (CERT), a secretive 'computer network operations' (CNO) unit, and participation in an inter-agency centre for information sharing. The CERT is responsible for incident response of the Bundeswehr's networks and systems. On the offensive side, the CNO unit is part of the 'strategic reconnaissance and intelligence' command, and is able to intrude into and disrupt foreign networks and systems. It employs around 80 IT security experts. In addition, the Bundeswehr contributes to the information sharing in the 'National Cyber Defense Center', which is led by the Federal Office for Information Security (BSI).[6] However, the center consists of only around ten members in total and its existence has been declared unjustified by the German Federal Court of Audit on grounds of a lack of effectiveness.[7] It will likely be strengthened by an updated national cyber security strategy.

With its new cyber security plan, the Ministry of Defence established two new organisational structures: a cyber and information domain (CIR) command in the military and a cyber/IT department in the Ministry of Defence.[8] "We have a great deal of expertise in the Bundeswehr, but we must bundle it more sensibly, make it more visible, and set it up to be more powerful," Defence Minister von der Leyen said when she announced the plan in April.[9]

The CIR command will combine existing IT capabilities of the Bundeswehr and become operational in April 2017. An inspector with the rank of a lieutenant general will lead the CIR, in which 300 officers will command around 13,700 soldiers. These soldiers will be assigned to CIR from other branches of the military, the criterion being that they have been dealing with IT in one way or the other in their previous jobs. The command's responsibilities include IT security, military intelligence, geo-information, and operative communications. The cyber/IT department in the Ministry will be responsible for the IT architecture and infor-

mation security of the Bundeswehr. It will become operational by October 2016 and be headed by a chief information officer (CIO). The new CIO has already been found and comes from one of the biggest German industrial firms: Klaus-Hardy Mühleck from ThyssenKrupp.[10]

Human Resources

One of the major challenges for the military will be to recruit, educate, and train the personnel necessary to fulfil the task. While the 13,500 soldiers that are supposed to staff the cyber command represent existing personnel to be assigned from other branches of the military, many of the other positions that compose the 'top layer' of the cyber command and the cyber/IT department will need to be more highly qualified.

There are a number of measures the Bundeswehr needs to take to fill the ranks of its planned cyber command: it needs to offer more flexibility in the armed forces' institutionalised career tracks, pay higher salaries for experts, and offer education for new recruits and advanced training possibilities.

According to the Bundeswehr's report on expanding its cyber security capabilities, it is planning steps to improve career opportunities and salary levels for IT security experts.[11] The report does not further specify these measures and it remains to be seen how the Defence Ministry is going to implement them. In the fields of education and training, the Ministry has already taken more concrete action. It has launched a new cyber security studies Masters programme at the Bundeswehr University from which around 70 students will graduate every year.[12] While it will take years until a sufficiently large number of graduates will be able to work in the Bundeswehr, this is an important first step. Moreover, the military has launched a large scale advertising campaign and promised to accept some applicants without formal educational qualification, recognising that it is already having trouble recruiting sufficient personnel for the military as a whole.

All of these measures will help, but won't succeed in fully staffing the necessary workforce in the coming years. Therefore, the armed forces will need to consider hiring private contractors for some tasks—potentially raising some of the same legal and security issues that have emerged related to the National Security Agency contractors in the US.[13] So far, the Bundeswehr has only suggested it will cooperate with reservists who are now working in IT security.

Innovation

A major challenge for the government will be how to ensure it has access to the technologies it needs in order to stay on the leading edge of technological innovation of electronic and cyber defence. This is an issue that governments struggle with around the world. The Bundeswehr will need to cooperate more closely with research institutions and private sector firms. The ministry wants to make this issue a priority by establishing a separate sub-department on cyber innovation and wants to expand cooperation with private companies and start-ups. In the mid-to long-term the military should probably think about establishing a supporting technological innovation agency modelled after the US Defence Advanced Research Projects Agency.

Use of Force in the Digital Domain

Perhaps the most difficult issue, however, is how the military's new cyber capabilities will fit with Germany's culture of military restraint. As mentioned earlier, Germany's postwar constitution requires any use of force by Bundeswehr troops abroad to be mandated by the Parliament—an expression of Germany's postwar suspicion of an overly powerful security apparatus.[14]

The Defence Ministry said this year that the requirement for a parliamentary mandate also holds true for cyber operations.[15] In the context of the current threat landscape of hybrid warfare and conventional warfare, a realistic scenario is that the offensive use of cyber capabilities is one of several means that Parliament allows the Bundeswehr to use as part of a broader mission mandate. In fact, a report from September 2016 publicized the Bundeswehr's only publicly known offensive cyber operation to date was part of Gemrany's mission in Afghanistan, mandated by parliament.[16]

The requirement for a parliamentary mandate presents several challenges. While in theory, it seems simple to distinguish between offensive and defensive measures in the digital domain – anything that happens in the Bundeswehr's own networks is defensive and anything that involves action in foreign networks crosses the threshold to offensive action—this distinction is not easily upheld in practice. Since the threshold for when a computer network operation is equivalent to an armed attack is not clearly defined in international law, it also remains unclear when the Bundeswehr would require the involvement of the Parliament. Moreover, in practice, operations which have been deemed to require secrecy for their success, have been subject only to limited parliamentary control.[17] This might be the case for operations in the digital sphere, which rely on secrecy even more than conventional attacks.[18] Hence, the executive and legislative need to consider a range of different scenarios when examining this question.

In addition, it is not clear whether the Bundeswehr itself is capable of conducting its own sophisticated cyberattacks—raising legal questions about cooperation with intelligence services, which are also viewed with caution by much of the German public. With its current operational capabilities, it is unlikely, that the Bundeswehr would be capable of launching a major computer network attack, for example, as a retaliatory measure. Depending on the target, attackers would need intelligence about the characteristics of the network and systems they want to breach and the vulnerabilities that can be used. This kind of work is the task of intelligence agencies in most cases and indeed all publicly known large-scale cyber espionage or sabotage attacks – for example, Stuxnet, the Saudi Aramco hack, the German Bundestag hack, the US Office of Personnel Management hack – seem to have mostly been projects of intelligence agencies.[19]

The military's new cyber command will likely need to cooperate with German intelligence agencies, but the legal and political modalities of this cooperation are far from clear. While in the US, intelligence and military cyber operations operate under common leadership—as of this writing, General Michael Rogers, Commander of the US Cyber Command and Director of the National Security Agency—in Germany, such overlap would be unthinkable. The German Chancellery oversees the foreign intelligence agency Bundesnachrichtendiesnt (BND), the Interior Ministry oversees the domestic intelligence agency Bundesamt für Verfassungsschutz (BfV), while the Defence Ministry oversees the Bundeswehr. Even infor-

mation sharing between the military and the Germany's BND foreign intelligence agency is politically sensitive and on complex legal ground.[20] Two leading lawmakers on digital and security issues have said that due to the unavoidable cooperation between intelligence agencies and the Bundeswehr on cyber issues, "the classical separation of responsibilities is blurred," requiring parliamentary oversight of military and intelligence cooperation in cyberspace "to be urgently established."[21] The military's efforts to strengthen its digital firepower will thus be met with constitutional and parliamentary roadblocks and public scrutiny that, in this combination, are unfamiliar in many other countries.[22]

Conclusion

The defence of national networks and systems in the digital realm blurs the boundaries between domestic and external security, and therefore also the responsibilities of civilian and military branches of government. "Ensuring cyber security and defen[s]e is … a whole-of-government task that must be performed collectively" by the Defence, Interior and Foreign Ministries, including the "joint protection of critical infrastructure", the Defence Ministry's White Paper states. The Bundeswehr must therefore "make an increasingly important contribution to general government preventive security."[23]

How this whole-of-government approach will look and who in the government will be leading it eventually is yet to be seen. Resolving these issues will be a major challenge, given both the political sensitivities described above and that cyber security measures are currently scattered across government ministries and departments. The German government's digital policy efforts have so far been fragmented and led to incoherence among different government departments' approaches. While Germany's "Digital Agenda 2014 to 2017" lays out a number of priorities for the German government to take, including for cyber security, responsibilities are assigned to a range of different ministries with often conflicting views. Fragmentation is a common problem many countries face in a number of policy areas, especially 'novel' ones like digital policy. But the German government lacks a coordinating element for digital policy, which could take the form of an own ministry, a coordinating subdivision in the Chancellery or an inter-ministerial department. The government will need to coordinate its digital policy, and cyber security policy in particular, to gain more trust from the public for its endeavors. Its updated cyber security strategy to be published in November 2016 should shine more light on the way ahead. The road map laid out will likely be the result of a political struggle for responsibilities and resources between different government departments and the Ministries of Interior and Defence, in particular.

Beyond this political struggle, the public debate surrounding the government's cybersecurity strategy illustrates broader tensions around the militarisation of German digital policy. This public scrutiny risks stymieing progress in cybersecurity policy making. However, the discussion is necessary to safeguard the balance between national security, network and information security and the protection of fundamental rights in the digital age.

India and the Budapest Convention: Why Not?

Alexander Seger

Worldwide, governments are struggling not only with the increasing levels of cybercrime but also with the complexities of securing electronic evidence (e-evidence) of any type of crime or economic offence.

If only a minuscule portion of cybercrimes and other offences entailing e-evidence is brought to justice, it risks failure of governments in their obligation to protect the rights of individuals and society against crimes and loss of faith in the rule of law.

Securing e-evidence for criminal justice purposes is particularly challenging in the context of cloud computing where data is distributed over different services, providers, locations and often jurisdictions, and where mutual legal assistance is often not feasible.

These challenges are currently being addressed by the Council of Europe's Cybercrime Convention Committee, which represent the parties to the Budapest Convention on Cybercrime. Solutions to enable criminal justice access to evidence in the cloud are a priority of the committee.

While India is confronted with the same challenges, it is not participating in this work, nor sharing its experience and shaping future international solutions as it has not yet decided to join this treaty.

International agreements form an important node in a web of solutions needed to address security and the rule of law in cyberspace. The more cyber issues affect core national interests, the more difficult it becomes to reach international consensus. However, all-inclusive solutions covering cyber warfare, terrorism and crime does not seem feasible.

With regard to "cyber" as a matter of state-to-state relations and international security, the work of the UN Group of Governmental Experts seems to be the most promising avenue at present. On cybercrime and electronic evidence as a matter of criminal justice, the Budapest Convention on Cybercrime is functioning.

So far, foreign policy considerations may have prevented India's accession to the Budapest Convention. Given the surge in cybercrime and the vision of a Digital India, it may be time for the government of India to reconsider its position.

Challenges

Cybercrime – that is, offences against and by means of computer systems – has been around for some 45 years and can hardly be called a new phenomenon. However, with the evolution of the information society and its dependence on information and communications technologies (ICT), the vulnerability of societies worldwide to cybercrime has increased considerably.

The current scale, nature and impact of cybercrime are such that it not only undermines confidence and trust in ICT but also represents a serious threat to the fundamental rights of individuals, rule of law in cyberspace and democratic societies.

This is reflected, for example, in the large-scale theft of personal data that affects the right to privacy; attacks against the dignity and integrity of individuals, in particular children; denial of service and other attacks against media or civil society organisations affecting the freedom of expression; attacks against governments, parliaments and other democratic institutions as well as public infrastructure; or the misuse of ICT for xenophobia and racism or radicalisation and terrorist purposes. Cybercrime causes economic cost and risks to societies and undermines human development opportunities and threatens international peace and stability.

Trillions of security incidents are reported each year and millions of attacks against computer systems and data are recorded every day. However, a tiny portion of such attacks is actually reported to criminal justice authorities.

India is no exception. According to the National Crime Records Bureau, 9,622 incidents of cybercrime were recorded in 2014 under the IT Act, Indian Penal Code and state and local laws. Even if this represents an increase of 69 percent from 2013, cybercrime accounted for only 0.13 percent of all crimes recorded in 2014.

There is, however, another dimension often neglected in discussions on cyber security and in policies and strategies on cyberspace: electronic evidence. Again, India is no exception. The National Cyber Security Policy of 2013 refers to effective law-enforcement capabilities for investigation and prosecution of cybercrime, but not to the broader issue of electronic evidence.

Criminal justice authorities need access to data for use as evidence in criminal proceedings; without data, there will be no evidence, no justice and no rule of law. Increasingly, evidence in relation to any crime is stored in the electronic form on computer systems. This includes serious and violent crime, such as location data in cases of murder or rape, subscriber information related to ransom e-mails sent during kidnappings, data to identify and locate victims of child abuse or data on communications between terrorists.

It can be assumed that this is increasingly a reality in India and that a growing proportion of the more than seven million crimes recorded entails e-evidence.

The more real-world crime involves e-evidence, the greater the need for law-enforcement officers, prosecutors or judges to have the skills to deal with e-evidence. Major capacity-building within the criminal justice system is required and clear rules for access to e-evidence and its admissibility in court need to be established.

Securing e-evidence is an increasingly complex undertaking. The sheer volume of cases involving e-evidence, the number of devices, users and victims involved, and technical complications such as encryption or anonymisers present major challenges.

The transnational nature of e-evidence – it may be stored in foreign jurisdictions even in cases that are otherwise fully domestic – combined with the transversal scope of e-evidence – in that any crime may entail such evidence – has implications on international cooperation in criminal matters. Most mutual legal assistance (MLA) requests for e-evidence are not related to cybercrime but to fraud and financial crimes followed by violent and serious crimes.

Given the volatility of e-evidence, the mutual legal assistance process is rather inefficient. Response times of six to 24 months to MLA requests appear to be the norm. Many requests and thus investigations are abandoned. This adversely affects the obligation of governments to protect society and individuals against cybercrime and other crime.

Cloud computing further complicates the matter. MLA requests are about cooperation between competent authorities. But if evidence is less held on a specific device or in closed networks but is distributed over different services, providers, locations and often jurisdictions, it is difficult to identify to which authorities to send a request.

Furthermore, law-enforcement powers are tied to the principle of territoriality, meaning that a criminal justice authority can only enforce its laws – such as ordering a service provider to produce data, or searching and seizing a computer system – on its own territory. But what principles govern the jurisdiction to enforce in a cloud context: the location of data, nationality or location of the data owner, location of the data controller, headquarters of a cloud provider, location of a subsidiary of a cloud provider or the territory where a service is offered?

The Cybercrime Convention Committee has been analysing these challenges for some time. In 2014, it adopted a set of recommendations to render MLA requests more efficient. However, it also recognised that the feasibility of MLA may be limited, given cloud computing. In 2015, therefore, it established a Cloud Evidence Working Group to identify additional solutions by the end of 2016.

These questions and solutions to them are not only relevant to the parties to the Budapest Convention but also to India. Other parties would also benefit from the experience of India.

International Agreements

Security challenges in cyberspace require a web of responses by public and private sector stakeholders at all levels down to the individual. International agreements are an important part of the response but – with exceptions – they have been difficult to reach.

Quest for International Treaties

International efforts to address cybercrime and e-evidence as a matter of criminal justice have been pursued since the 1980s, initially by the Council of Europe and the Organisation for Economic Cooperation Development (OECD), and from the mid-1990s also by G8. At the Council of Europe, this led to the adoption of soft-law Recommendations providing guidance on the criminalisation of computer-related offences (1989) and on law enforcement powers regarding cybercrime and electronic evidence six years later (1995). These were precursors to the Budapest Convention which was opened for signature in 2001.

By 2001 the problems of cybercrime and e-evidence were sufficiently important to warrant an international treaty but cybercrime and information technologies were not yet considered too relevant on national interests and security of states to prevent consensus. Therefore, the Budapest Convention was forged by the member-states of the Council of Europe as well as Canada, Japan, South Africa and the US. By August 2016, all of these countries, with the exception of two members of the Council of Europe, (the Russian Federation and San Marino) had signed the treaty.

At the United Nations, it has not been possible to reach a consensus so far as to whether an international treaty on cybercrime was necessary and feasible and what it would possibly comprise. The matter of "combating the criminal misuse of information technologies" was the subject of a resolution at the UN Congress on Crime Prevention and Criminal Justice in Havana in 1990. It referred to the work of the OECD and the Council of Europe, but no follow-up was given by the UN. In 2001 and 2002, it was taken up again in UN General Assembly Resolutions but at that point, the Budapest Convention had been opened for signature.

Subsequently, the question was on the agendas of UN Crime Congresses (in 2005, 2010 and 2015) and annual UN Crime Commissions but not much progress had been made. The Intergovernmental Group of Experts on Cybercrime, established at the Salvador Crime Congress in 2010, "in view of examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime", noted in its most recent meeting in 2013 "broad support for capacity-building and technical assistance" and "diverse views" on options of new international instruments.

It would seem that from around 2001, the focus within the UN had shifted from cybercrime as a matter of criminal justice to the protection of critical information infrastructure and cyber or information security as a matter of international security. From 2004, Groups of Governmental Experts (GGEs) have been meeting to examine "existing and potential threats from the cyber-sphere and possible cooperative measures to address them". Though progress is slow at the UN towards norms, rules or principles of "responsible state behaviour" in cyberspace, it is considered the most relevant forum on state-to-state relations concerning cybersecurity.

These observations are meant to illustrate the following:

- International consensus on rules for cyberspace will remain difficult to achieve given strong and often diverging (national) interests.

- An all-inclusive international agreement encompassing cyber (or information) warfare, terrorism and crime as proposed by some states would hardly be feasible.

- Separating the issues into more manageable portions would seem a wiser approach. Concerning "cyber" as a matter of state-to-state relations and international security, the work of the UN GGE seems to be the most promising avenue at present, complemented, for example, by confidence-building measures agreed on by the Organisation for Security and Cooperation in Europe, bilateral "cyber diplomacy" or initiatives such as the London process.

- On cybercrime as a matter of criminal justice, not much progress has been achieved by the UN since 1990, while the Budapest Convention is in place and functioning.

Budapest Convention on Cybercrime

The Budapest Convention provides for (i) the criminalisation of conduct, ranging from illegal access, data and systems interference to computer-related fraud and child pornography; (ii) procedural law tools to make the investigation of cybercrime and the securing of e-evidence in relation to any crime more effective and (iii) international police and judicial cooperation on cybercrime and e-evidence.

States which participated in the negotiation of the Convention (members of the Council of Europe, Canada, Japan, South Africa and the US) can sign and ratify the treaty. Under Article 37, any other state can become a party by ratification or accession if it is prepared to implement the convention.

By August 2016, 49 States were parties (those already mentioned as well as Australia, Dominican Republic, Israel, Mauritius, Panama and Sri Lanka). Another six had signed it (including South Africa) and 12 had been invited to accede (most recently Ghana; from the Asia/Pacific region these include the Philippines and Tonga).

These 67 states – together with 10 international organisations (such as the Commonwealth Secretariat, INTERPOL, International Telecommunication Union and the UN Office on Drugs and Crime) participate as members or observers in the Cybercrime Convention Committee. The Committee, among other things, assesses implementation of the Convention by the parties, adopts guidance notes or prepares additional legal instruments such as draft protocols to the Convention.

The Budapest Convention is backed up by capacity-building programmes. In 2014, the Council of Europe established a dedicated Programme Office on Cybercrime (C-PROC) in Bucharest, Romania. In the Asia/Pacific region, the Philippines, Sri Lanka and Tonga are priority countries for technical assistance given their commitment to implement the Convention. They benefit from law-enforcement and judicial training and strengthening of legislation, including rule of law and human rights safeguards, of specialised institutions, public-private partnerships and international cooperation. By August 2016, C-PROC managed a portfolio of projects worth some €23 million, many being joint projects with the European Union.

This triangle of common standards (Budapest Convention), follow-up and assessments (Cybercrime Convention Committee) and capacity building (C-PROC) represents a dynamic framework. It helps ensure that states joining the Convention are actually able to keep improving the quality of implementation of its provisions and cooperation with other parties.. And it allows parties to keep the Budapest Convention up-to-date and negotiate additional solutions if necessary.

Access to Evidence in Cloud

Obviously, defining the conduct that constitutes cybercrime in criminal law is essential. In the Budapest Convention, this is reflected in Articles 2 (illegal access to a computer system) to 12 (corporate liability). In recent years, the Cybercrime Convention Committee has adopted a series of guidance notes to show how these provisions cover the phenomena such as botnets, distributed denial of service attacks and identity theft that did not exist when the Convention was adopted. The Committee is currently assessing to what extent parties have adopted sanctions and other measures that are effective, proportionate and dissuasive as foreseen in Article 13. On substantive criminal law, the Convention remains up-to-date.

The question of procedural law powers to secure e-evidence and, by extension, efficient access to evidence in a transnational and cloud context is a complicated challenge, given the limitations of the MLA process which is normally designed to protect the rights of individuals as well as the interests of states in which evidence is located.

The Cybercrime Convention Committee has, therefore, been focusing on the following questions:

- how to ensure effective access to evidence on servers stored on, or distributed or moving between servers in foreign, multiple or unknown jurisdictions; and

- how to reconcile the need for efficient law-enforcement access to data with the need to respect rule of law and human-rights requirements, and thus how to avoid the trap of undermining the rule of law through actions meant to protect it.

A number of options have been proposed by the Cloud Evidence Group of the Cybercrime Convention Committee and are currently under discussion:

- Rendering the MLA process more efficient. Specific recommendations to this effect have already been adopted by the committee and relate, for example, to resource allocation in parties, the role of 24/7 points of contact for urgent cooperation and streamlining of MLA procedures.

- Specific and lighter domestic rules and procedures for production orders for subscriber information in line with the Article 18 of the Convention given that subscriber information is the most sought information in domestic and international criminal investigations. Subscriber information is less privacy sensitive than traffic or content data and production orders are less intrusive than search, seizure or interception powers. A lower threshold for the disclosure of such information would thus be justified.

- A Guidance Note on the Article 18 on production orders for subscriber information to clarify the scope of this provision. It would require service providers located in or "offering a service in the territory" of a party – under certain conditions – to disclose subscriber information irrespective of the actual location of such data.

- A clearer (legal) and more predictable basis for the current practice of voluntary disclosure of subscriber information by service providers directly to foreign criminal justice authorities. For example, in 2015, parties to the Budapest Convention other than the US sent about 140,000 requests to six major American providers and received data in 60 percent of the cases on average. (Incidentally, India sent about 20,000 to the same providers – of which more than half to Facebook – with a response rate of 48 percent in 2015.) It is yet to be confirmed whether the Article 18 can serve as the legal basis for such direct cooperation or whether a protocol to the Convention would be needed.

- An additional protocol to the Budapest to cover, for example, a simplified regime for MLA requests for subscriber information and/or international production orders; direct cooperation between judicial authorities; joint investigations; emergency procedures; direct cooperation with providers in foreign jurisdictions; a clearer framework and safeguards for transborder access to data; and data protection rules and other safeguards.

The Cybercrime Convention Committee – with its 67 parties and observer states – will consider these proposals in November 2016 and decide a further course of action.

These issues are of relevance to India as reflected, for example, in questions 15 and 17 of the Consultation Paper on Cloud Computing circulated by the Telecommunication Regulatory Authority of India in June 2016.

So far, however, India has not taken part in Cybercrime Convention Committee deliberations.

India and the Budapest Convention: Why not?

In 2007 and 2008, India and the Council of Europe cooperated in the reform of India's Information Technology Act. These reforms brought the legislation of India broadly in line with the Budapest Convention.

While membership in the Budapest Convention more than doubled since then, India is yet to join this treaty. The reasons are not entirely clear. Concerns voiced by different stakeholders include:

- That India did not participate in the negotiation of the Convention and thus should not sign it. Obviously, participation by India in the negotiation of the original treaty would have been preferable. This concern is not unique to India. Yet, other states recognised that the benefits of joining it outweigh this concern. They can now fully participate in the further evolution of the treaty, including the possible negotiation of additional protocols. India has come to a similar conclu-

sion on two other Council of Europe treaties which it did not negotiate, namely on international cooperation in tax matters (to which it became a party in 2012) and on the transfer of sentenced persons (it requested accession and was invited to accede in 2016).

- That the Budapest Convention – through its Article 32b – allows for trans-border access to data and thus infringes on national sovereignty. After thorough scrutiny, the Cybercrime Convention Committee confirmed the limited scope of Article 32b in a Guidance Note in 2014. This then led some quarters in the government of India to criticise that Article 32 was too limited and that additional options would be needed.

- That the MLA regime of the Convention is not effective, "the promise of cooperation not firm enough", or that there are grounds for refusal to cooperate. It is true that the Cybercrime Convention Committee has come to the conclusion that while the level of MLA keeps increasing among parties, the process needs to be made more efficient overall. This matter is being addressed through follow-up to a set of recommendations adopted in 2014 and the proposals made by the Cloud Evidence Group. The 'algorithm' of the Convention – the triangle of standards, follow-up and capacity-building – allows it to address possible shortcomings. Nevertheless, one should remain realistic and not expect one treaty to resolve all possible problems. India would certainly not expect this from other international treaties to which it is a party.

- That it is a criminal justice treaty and thus does not cover state actors or that some of the states from which most attacks affecting India emanate have not signed the Convention. Indeed, it is a criminal justice treaty and the question of state-to-state relations need to be addressed in other fora such as the UN GGE.

- That India should promote a treaty at the UN level. This proposal seems to be favoured in the context of BRICS but the intended scope remains unclear – is it meant to be a criminal justice treaty, to focus on terrorism, or to address state-to-state relations and matters of international security or all of these? Taking into account the experience since 1990, it is unlikely that a binding UN treaty will be available any time soon. Meanwhile, cybercrime keeps growing day by day.

Overall, it would seem that India joining the Budapest Convention has so far been primarily hostage to diplomatic and foreign policy considerations and less to concerns of actual criminal justice cooperation on cybercrime and e-evidence. From the latter perspective,

- the challenges currently being addressed by the parties to the Convention through the Cybercrime Convention Committee are highly relevant also for India;

- the Convention offers a legal basis and practical framework for police-to-police and judicial cooperation on cybercrime and e-evidence with an increasing number of other parties. This framework is constantly under review to make it more effective;

- as the Convention evolves, India would be able to contribute to shaping future solutions if it were a party;

- India would become a priority country for capacity-building.

Given Prime Minister Narendra Modi's vision of a Digital India and considering the surge in cybercrime, it would be beneficial for India to join this treaty.

Keep the Doors Locked and Turn On the Light: Why Less Security Online Does Not Make Us More Secure Offline

Paula H. Kift

Introduction

In the aftermath of the San Bernardino shootings in December 2015, the battle over encryption came back to the fore. Two cases stood out prominently in this regard: the first concerned the question of whether the Federal Bureau of Investigation (FBI) could oblige the American technology company, Apple, to bypass the passcode security of an iPhone 5s pertaining to a New York resident suspected of drug trafficking;[1] the second, which received widespread media attention, was whether the FBI could force Apple to create and electronically sign new software to unlock the work related iPhone 5c of Syed Farook[2] who, together with his wife Tafsheen Malik, killed 14 people and injured 22 others in a shooting spree in San Bernardino, California.[3] The government argues that current industry encryption standards seriously undermine its ability to engage in legitimate law enforcement and national security investigations. For its part, Apple argues that it cannot undermine the security of one iPhone without undermining the security of all iPhones. Meanwhile, the found echoes in Europe after rumours spread that the terrorists behind the Brussels[4] and Paris[5] attacks exploited secure communication channels to achieve their nefarious ends.[6] This raises the question: What is the relationship between offline and online security? Can less security online make us more secure offline? In order to explore these questions, this paper distinguishes between three types of security: technological security, national security, and personal security. Technological security protects infrastructures, networks and devices; national security protects territorially bounded populations; and personal security protects individuals. The contribution not only argues that personal security in the digital age depends on both technological and national security, but also that technological and national security depend on each other. Undermining technological security thus not only weakens personal security but also national security – a conclusion that was already reached over 20 years ago in the context of the so-called Crypto Wars.[7] Most importantly, the recurrent national security obsession with criminals and terrorists "going dark" is misguided. First, if criminals want to "go dark," they will "go dark," regardless of whether the government has backdoor access to encrypted communications. Weakening industry encryption standards will merely compromise personal and technological security for the rest of us. Second, even if criminals want to "go dark," this does not imply that law enforcement cannot continue doing their

work as there is a host of data trails that criminals cannot avoid leaving behind if they continue to rely on digital communications. Indeed, the vast amount of information that intelligence services can access regardless of whether or not the content of communications is encrypted suggests that we are far from "going dark" but rather are living in a "golden age of surveillance."[8] Finally, repeated calls for weakening industry encryption standards raise the question of whether the means employed by governments to protect national and personal security are well suited towards achieving their end. More specifically, recent events in Orlando,[9] Nice[10] and Munich[11] call into question whether the ability to monitor the online communications of all is the most effective way of preventing crimes and terrorist attacks perpetrated by a few. This article argues against technological solutionism:[12] perhaps the best way to protect national, personal and ultimately also technological security is to renew our focus on investigative powers offline.

Background

Over the course of 2015, Apple received nearly 2,000 requests from the US government to make the personal data of its customers available to law enforcement.[13] While Apple generally complies with government requests that it deems lawful, it has also occasionally challenged others, most notably in the case of the personal data stored on the handheld devices pertaining to Jun Feng, a New York resident suspected of drug trafficking,[14] and Syed Farook, one of the suspects in the San Bernardino shootings.[15] In both cases, Apple received court orders seeking to compel the company to make personal data from its handheld devices accessible to law enforcement agencies under the All Writs Act (AWA).[16] While the relevant order in the former case, which "only" required Apple to bypass the passcode security of Feng's iPhone 5s, was significantly less burdensome than that of the latter case—which would have required Apple to create and electronically sign new software to unlock Farook's work-related iPhone 5c—Apple challenged both, on the grounds that the government could not force companies to undermine their own encryption standards. Setting aside the question of whether the government's requests were good law – that is, "necessary or appropriate" and "agreeable to the usages and principles of the law" in the sense of the AWA – this piece will focus on the question of whether they are good policy – that is, whether less security online can make us more secure offline.

"A Rose By Any Other Name…"

Might not smell as sweet in the field of security (with apologies to William Shakespeare). Classifications matter. And distinguishing between different types of security is important, not least because one type of security might conflict with another. The following section will first distinguish between three types of security that are relevant to this conversation – technological, national, and personal security[17] – before making an assessment of the question of whether undermining one can ultimately reinforce another.

1. Technological security

In this case, 'technological security' refers to the security of information technology (IT) infrastructure, networks and devices. According to this definition, the Internet as a whole constitutes the infrastructure, which is composed of a variety

of networks—such as internet service providers (ISPs), operating systems, platforms, and intrawebs—which in turn depend on the accessibility and functionality of devices. This contribution follows the traditional information technology (IT) security triad, according to which IT security is protected when the confidentiality, integrity and availability (CIA) of the system are preserved.[18]

2. National security

The term 'national security', by contrast, refers to the protection of territorially bounded populations. The definition of what constitutes a threat to national security inevitably differs from one country to another and changes over time. But in the aftermath of the terrorist attacks of September 11, 2001, the focus of national security in the United States and in most of Western Europe has primarily been on the prevention of such attacks on domestic soil. At the same time, concerns about cyberattacks are growing,[19] demonstrating that protecting technological security is in fact a part of the responsibilities of national security.

3. Personal security

Finally, the concept of 'personal security' is concerned with the wellbeing of individuals. This includes not only the protection of physical but also psychological integrity, as well as the ability of individuals to enjoy their basic rights, offline and online, such as privacy, freedom of expression and participation in a social and political community.

The Paradox of Security

It seems odd that these security goals could be at odds with each other. After all, as mentioned earlier, technological security is also an explicit goal of national security, and the meaningful protection of personal security in the digital age includes not only the protection of the physical person offline but also that of their communications and exchanges of personal data online. Similarly, national security depends on technological security, e.g., to protect critical infrastructure of both the public and private sector.[20] But the relationship can just as well be negative: in the name of national security, governments can be tempted to ask businesses to weaken technological security (e.g., by introducing backdoors into encrypted communications) which in turn threatens personal security (by making the personal data and communications of individuals more accessible to governments and criminals alike). After all, as soon as a security loophole is created, public and private actors (both good and bad) will rush to exploit it. At the same time, governments claim that they cannot guarantee personal and national security when they are among the actors that technological security protects against. In the words of FBI Director James Comey, "We all care about safety and security on the Internet – and I'm a big fan of strong encryption – we all care about public safety, and the problem we have here is those are in tension in a whole lot of our work."[21] This raises the question: Would less security online make us more secure offline?

Crypto Wars: Back to the Future

This conflict is far from new. As several commentators have pointed out,[22] the debates we are witnessing today eerily resemble those surrounding the Clinton administration's attempts to introduce a state-of-the-art encryption system with a built-in tamper resistant backdoor for law enforcement access in the early 1990s. The Internet was not yet commercially viable back then and encryption was limited to a few government and private sector providers, but US and UK government and intelligence representatives already warned that, if encryption were to become more widespread, then the capability of law enforcement to prevent and solve crimes would be severely restricted. Accordingly, the US government suggested that technology companies should provide law enforcement access by design, e.g., by building a government backdoor into the security systems of their products. Specifically, the government advocated for the adoption of the so-called Clipper Chip, which, by means of key escrow, would send law enforcement a string of data that would allow it to decrypt encrypted communications, akin to providing the key to a lock.[23] The proposal was faced with strong resistance by technology companies and IT specialists who criticised the substantial social, economic, political and, inevitably, security risks and costs that would be entailed by the implementation of such proposals.[24] Now that government and law enforcement officials are singing a familiar tune, the opposition of technologists has only increased.[25] The types of risks that unilaterally inserting vulnerabilities into the digital ecosystem would introduce have not changed. What has changed, however, is the magnitude of the havoc that such proposals could wreak. If the American government demands that multinational technology companies such as Apple provide backdoor access to secure communication channels, what is to keep other governments around the world, with varying commitments to human rights and the rule of law, from following suit? What if companies and nonprofit organisations abroad start offering alternative encryption and data storage solutions, which not only undermines the business interests of domestic companies but also risks contributing to a splintering of the infrastructure of the web into separate jurisdictions?[26] How can we protect particularly vulnerable communication channels, e.g., those of journalists,[27] activists,[28] whistleblowers,[29] refugees,[30] courts[31] and even the government[32] —when the government itself is chipping away at those protections? And yet, despite the obvious tradeoffs, government and law enforcement officials cannot rid themselves of the gnawing feeling that we cannot protect national and personal security if we enable criminals and terrorists to "go dark." The final part of this contribution will therefore attempt to shed some light on the contentious debates surrounding "darkness."

Keep The Doors Locked...

First, if criminals want to "go dark," they will "go dark," regardless of whether the government has backdoor access to encrypted communications. The kinds of criminals we should be concerned about are not that unintelligent. Further, in the unlikely case that they do not manage to circumvent government surveillance of their communications online, nothing prevents them from continuing to plan and execute their criminal wrongdoing offline. As an incredulous Anthony Soprano pointed out to one of his associates in the popular 2000's American television series, The Sopranos: "We're supposed to leave phone calls about

interstate hijacking now? How about faxes, e-mails, make it even easier for the cops? This is a face-to-face business, Christopher."[33] Weakening industry encryption standards will thus merely compromise personal and technological security for the rest of us.

Second, even if criminals want to "go dark," this does not imply that law enforcement officials cannot continue doing their work as there is a host of data trails that criminals cannot avoid leaving behind if they continue to rely on digital communications. Indeed, the vast amounts of information that intelligence services can access regardless of whether or not the content of communications is encrypted suggests that we are far from "going dark" but rather living in a "golden age of surveillance."[34] For instance, data about communication transactions – or in common parlance: metadata – cannot easily be encrypted, if at all, and yet provides a rich and reliable source of information about a person's private interests, habits and concerns.[35] Furthermore, as long as many businesses themselves depend on the unencrypted access to their customers' data, they have no incentive to engage in full-scale encryption[36] – unless, of course, the government antagonises them to the extent that they feel pressured into assuming the privacy-protective position.[37] Finally, the fact that the FBI ultimately dropped the case against Apple because it was able to break into the iPhone itself[38] undermines its own argument that law enforcement is lagging behind technological advancements.

...And Turn On The Light.

Finally, repeated calls for weakening industry encryption standards raise the question of whether the means employed by governments to protect national and personal security are well suited towards achieving their end. After all, encryption can only be a problem when the large-scale monitoring of communications is the solution to national security's many woes. However, the inability of law enforcement and intelligence officials to predict and prevent the concerted terrorist attacks in Brussels[39] and Paris[40] calls into question whether monitoring the online communications of all is the most effective way of preventing crimes and terrorist attacks perpetrated by a few. The case of France, in particular, seems to suggest otherwise, considering that the country currently has some of the most intrusive government surveillance laws in Western Europe.[41] This article thus ultimately argues against technological solutionism:[42] Perhaps the best way to enhance national, personal and technological security is to renew our focus on investigative powers offline. As one commentator suggested in the aftermath of the Brussels attack, "the answer to the scourge of homegrown terrorism in Europe is [...] found in the basic tools of routine police work: learning the ins and outs of a tightly knit neighbourhood where dozens of people could lend support to a plot, and only a few of whom would know, or care, that it was terrorism."[43] This primarily requires boots on the ground, not analysts in a room full of cables. That is not to say that signals intelligence (SIGINT) does not contribute to the prevention of crimes. Of course it does. But at the same time, we should not lose focus of the importance of human intelligence (HUMINT) to explore and develop relationships with communities online and off. Most importantly, the lone-wolf attacks in Orlando,[44] Nice[45] and Munich[46] suggest that the concerns of national security may increasingly have to include the phenomenon of contagion;[47] that is, that people participate in senseless mass killings not because of any particular ideological conviction but because the threshold for doing so has become

dangerously low.[48] This problem will not be solved by introducing backdoors into secure communication channels online, but through a painful and potentially protracted offline conversation between policymakers, police officers, educators and community representatives. Preventing criminals and terrorists from "going dark" does not amount to much more than treating a symptom. But what we need to be doing is to shine light on the cause.[49]

The NCIIPC & Its Evolving Framework

Saikat Datta

Only eight years after India passed the Information Technology Act, did the term cybersecurity appear in a statute through a series of amendments to the Act approved by the Indian Parliament. In 2008, the amendments recognised the need for a focussed approach to cybersecurity and divided it into two segments: Critical and Non Critical.

The amendment defined '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."[1] The law also added two sections - 70 (A) for all 'Critical' systems and section 70 (B) for all non-critical sections and assigning the responsibility to two separate agencies - one new and one old.

The National Critical Information Infrastructure Protection Centre (NCIIPC) was deemed to be created by a gazette notification with specific responsibilities for protecting all CII. The Computer Emergency Response Team - India (CERT-IN) would be responsible for all non-critical systems, but would continue to be responsible for collecting reports on all cyber attacks / incidents. While the law was amended in 2008, it would take six years before NCIIPC was formally created through a Government of India gazette notification in January 2014.[2]

The NCIIPC started off with several sectors, but has now truncated them into five broad areas[3] that cover the 'critical sectors'. These are:

- Power & Energy
- Banking, Financial Institutions & Insurance
- Information and Communication Technology
- Transportation
- E-governance and Strategic Public Enterprises

While defence and intelligence agencies have also been included under the CII framework, these have been kept out of the purview of the NCIIPC's charter. Instead, the Defence Research and Development Organisation (DRDO) has been tasked with protecting these bodies.

A key point that has been factored in while identifying CII is the inter-dependencies that they have, to determine which are the 'most critical'. Therefore, using this matrix, NCIIPC settled on the Power Sector as the most critical followed by the Energy Sector. However, these inter-dependencies are likely to change and could evolve into a more complex model at a later stage to decide the criticality of systems.

However, NCIIPC has also been mindful of the fact that even though some systems are isolated, the accelerated developments of the IT sector and the advent of Internet of Things (IOT) will increase the complexity of protecting CII. NCIIPC's guidelines states "Presently many of these critical systems may relatively be isolated or the complementarities may be progressing at a snail's pace and thus considered relatively secure from intrusion. However, with the accelerated pace of development within the IT sector it will be difficult for these critical systems to isolate themselves from the outside world, and to maintain the boundaries between "inside" and "outside"[4].

Over time, NCIIPC has been able to sharpen its charter to ensure better "coherence"[5] across the government to respond to cyber threats against CII. This also means that it will provide the strategic leadership to the government's efforts to "reduce vulnerabilities…against cyber terrorism, cyber warfare and other threats".[6] This also includes identification of all CII systems for "approval by the appropriate government for notifying them" as "protected systems". This is a critical element in NCIIPC's charter and helps it embrace the private sector and work with them.

The Benefits of Identifying CII

Under its charter, NCIIPC has been working towards recognizing many of the Government of India's systems as 'protected systems', which has several positive consequences. Under the current laws, any IT (Information Technology) or Supervisory Control and Data Acquisition (SCADA) systems that lie at the heart of the CII can only seek three years imprisonment for any cyber attack. However, after the NCIIPC has undertaken an elaborate Vulnerability, Threat and Risk (VTR) assessment, the system is forwarded for notification by the "appropriate government authority."[7]

Once notified as a "protected system" the CII is immediately placed under the ambit of section 66 (F) of the IT Act (Amended) 2008, which defines any cyber attack as an act of Cyber terrorism. This increases the quantum of punishment from three years imprisonment to life imprisonment, increasing the deterrence levels of attacking CII. Furthermore, it also ensures that NCIIPC is able to offer its services to a post-incident risk mitigation as well as investigation process. As per the existing protocol, the Chief Information Security Officer (CISO) of the designated CII entity is also given access to the intelligence on cyber threats and vulnerabilities gathered by NCIIPC.

The agency has also started approaching various sectors to create guidelines that can set standards for private and public sector entities across the board. To achieve this, NCIIIPC began a process of interfacing with various stakeholders in several sectors to understand their IT and SCADA systems, along with normative practices such as vendor selection, patch management, legal contracts, etc that are particular to a given sector. Working with these stakeholders, NCIIPC managed to create the first sector-specific draft guidelines of the Power sector, which was submitted to the Ministry of Power in May 2016. If accepted, this will be the first set of national sector-specific guidelines to be promulgated by the Government of India.

NCIIPC has also been instrumental in declaring two major entities as protected - systems of the Aadhar unique identification project and the Long Range Identification and Tracking (LRIT) system of the Ministry of Shipping.[8]

Addressing The Trust Deficit

It has been frequently noticed that any possible interface between the private sector and the government is usually fraught with risk. The government is essentially a regulator while the private sector seeks freedom to conduct business. Any interference by the government not only threatens its profitability, but can also prove to be an existential threat. This is a framework that NCIIPC has consciously chosen to not follow.

Its approach is based on the principle that cyber security is a shared responsibility. NCIIPC's charter includes its role to "...coordinate, share, monitor, collect, analyse and forecast, national level threat to CII for policy guidance, expertise sharing and situational awareness for early warning or alerts". However, it also maintains that "the basic responsibility for protecting CII system shall lie with the agency running that CII."[9]

The role of the entity holding the CII is clear and NCIIPC aims to strengthen the agency that runs the CII systems. To achieve this, it has embarked on a formal private sector interface that will establish joint partnerships to increase awareness on the kinds of threats that the CII owners are likely to face in the coming years. As a case in point, its close cooperation with a private power sector company was used as a base for drafting the national guidelines for the sector. This has also sensitised NCIIPC to the challenges that the private sector faces, in terms of alignment with the management as well as budgetary support for acquiring the latest counter-measures against future cyber threats / attacks.

The Road Ahead

The Snowden revelations has revealed that as long as propriety software created by developed economies dominate the cyber landscape, systems will remain extremely vulnerable. This has prompted an initiative to ensure that India develops an eco-system that can support the development of indigenous software and hardware.

However, that eco-system is incomplete unless there are adequate cybersecurity professionals available to partner with NCIIPC to cover the whole sector. This calls for forging partnerships between public and the private entities, leveraging each other's strengths by avoiding the traditional regulatory approach. While section 70 (A) and its sub clauses empower NCIIPC to take the regulatory route, it has drawn more on the US Critical Infrastructure Information Act 2002, that emphasises 'voluntary' cooperation rather than enforcement and compliance-driven. This has created a cooperative framework that has served the US well and continues to strengthen its CII's cyber security. This ensures the merging of the strengths of the private and public to not only create standardised operating procedures, but also build a eco-system that is sensitive to each other's lacunae and strengths.

ACCESS AND INCLUSION

Digital Is Not Just Narrowing the Gender Gap, It Is Empowering Women to Shatter the Glass Ceiling

Shaili Chopra

For women, the internet hasn't been a feature, a convenience or a tool; it's been an agent of change. The global digital story cannot be complete without mentioning the impact it has had on reducing the gender gap and opening access and opportunity for women. Digital fluency has helped in closing the gender gap at the new age workplace. Nothing empowers as fiercely as equal access to information.

Digital has had a positive impact on women's education, skills and therefore, employment openings. In countries where digital access and abilities are more widespread, there is a stronger sense of gender equity. Women who are familiar with the internet also display a strong sense of leadership because they are self-confident and skill-confident. Women want to return to the workforce and are finding new tracks to economic achievement; entrepreneurship is a big part of this.

Companies and governments face a disparity between the skills they need to stay aggressive and the pool of talent available to them. Because women are underrepresented in the workplace in most countries, they are a significant source of untapped talent. The future looks promising as the youth mature and move into the workplace and grow through ranks of leadership at work, using their skills to turn agents of change for their gender.

According to a report by Accenture, "If governments and businesses can double the pace at which women become digitally fluent, we could reach gender equality in the workplace by 2040 in developed nations and by 2060 in developing nations."[1]

India adds five million connected users every month. These statistics are testimony to the opportunity in India's internet story. In 2016, the number of mobile internet users in India is above 400 million as per internetlivestats.com.[2] That's second only to China and ahead of the United States. However, despite these powerful figures, there is gender gap when it comes to access to internet. The internet and Mobile Association of India (IAMAI) report shows that men account for 71 percent of internet users, while women account for just 29 percent. The gap is

slightly lower in urban India, with men accounting for 62 percent and women 38 percent. These are the major findings of a report titled "Mobile Internet in India 2015," released by the IAMAI and the Indian Market Research Bureau International.

Rural India has this ratio completely skewed in favour of men, where they constitute 88 percent of the total internet users. However, these disappointing figures present an opportunity and spell out the possibilities of providing women with new life skills.

Women Make in India

While the Make in India initiative has a lion for a mascot, the campaign offers scope to create lionesses out of women. A focus on entrepreneurship over job seeking can make change-makers of Indian women. These entrepreneurial industries can be big and small—operated from home or an office, virtual or on the shop floor.

Ananya Birla runs India's third largest microfinance outfit called Svatantra. Every other week she is in a village, understanding how her clients—small, unorganised, often self-help groups and women—are utilising their funds. "We call it microfinance 2.0, lending small loans to many people and integrate that with technology," she explains, on the heels of her return from Amravati in Maharashtra. "When I go down and talk to our clients, they are very happy with these, which is inspiring and refreshing." Svatantra provides loans to tailors, farmers, housewives etc., depending on their businesses. "Women in these places are very enterprising," notes Ananya, referring to the female populations in rural India.

There's Devita Saraf, whose VU Technologies is turning 10 even before she is 35. She sells high-end televisions in India, from Maharashtra to Manipur. "Never underestimate your customer," she says, citing how India's appetite for luxury is growing. Saraf's business has spread to interior India after she took VU online. First, she started selling in big metros but now, her products reach areas such as Sohlapur and Salem. Another female founder, Uma Reddy of Hitech Magnetics in Bangalore, is an electrical engineer running a company that manufactures transformers, feeding India's heavy industry and defence needs. These are just some examples of women in businesses. In addition to them, there are champions of digital, branding and ideas. There's Siddhi Karnani of Parvata Foods—primarily responsible for farming and organic produce in Sikkim—producing home-grown spices such as ginger and packaging them for the markets across India. It is evident that the breadth of businesses women are involved in is wide-ranging and impactful.

"Women entrepreneurs have an edge over male entrepreneurs," says Amitabh Kant, CEO of National Institution for Transforming India (NITI Aayog). He insists that this fact is going to radically change the story of the country's future and its approach to creating economic value. "They will outperform for several valid reasons. Women leaders in India have a better feel of the household spending patterns. They understand consumer perspective better. They have a way of building trust with customers, shareholders, etc. Also, there is a great level of diversity when women occupy top positions."[3]

Tech has fundamentally given many the flexibility to work when they want, according to Shikha Sharma, CEO of Axis Bank. It allows people to work from home, without taking away from the productivity, as it saves on costs for some companies and the time and stress involved in travel for employees. "From a workplace perspective, it's giving women the opportunity to continue to participate in their careers without giving up the other roles as mothers or a daughter or daughter-in-law or whatever."[4]

The new workplace is far more flexible. Attitudes have changed in the new entrepreneur-led organisation and the rise of digital business that have a start-up-like culture, allowing freedom of ideas, flexibility in terms of place of work and more. "When we started, there were few role models as women who were able to balance work and home," says Sharma. "For all of us as women, you don't want to be a loser in your family role. And therefore, it's a constant question in your mind by becoming a career woman—are you going to compromise on your family?" So having a mentor to go to, whose able to balance that well is very important in your ability to stay down that path. The following question arises: what is the role of peers and do they accept women as equals in the workplace? According to Sharma, "Now we have got to the point that people are recognising having balance in your workforce, having men and women you get different perspectives and you could actually have a richer decision coming through."

Power of Language

India's diverse cultures manifest themselves in its 22 languages and thousands of dialects. A new wave of interest in the internet is seen in those who have discovered that the internet should not be limited to English. Rajan Anandan, Google's Asia Head, mentions the surge of local Indian languages as part of his larger emphasis on rise of content in India. "Hindi internet in India has grown at eight times more than English internet," he said at the Digital Women Awards in November 2015.

Going forward, there will be more vernacular content will be more vernacular as the user base diversifies and grows to include larger numbers of rural consumers. The use of vernacular content online is estimated to increase from 45 percent in 2013 to more than 60 percent in 2018, according to a report by Boston Consulting Group, mirroring broadening consumption patterns in off-line media, such as print and television. English language still accounts for 56 percent of the content on the worldwide web while Indian languages account for less than 0.1 percent. However, although internet in India is predominantly English, there is high potential for regional language content. According to the report, in the last year alone, Hindi content on the web has grown by about 94 percent, whereas English content has grown only at 19 percent. This is a relevant scenario in promoting the inclusiveness of women across the country.

Social Fabric

A little known important fact is that most of the unconnected population are women. Not enough of them own mobile phones. In low- and middle-income countries alone, 1.7 billion females do not own a mobile phone today, says a McKinsey Report.[5] For those who do own phones, the internet usage is prohibitively low, and consumption of data and content is less intense. An opportunity is spelt

by this gap, which reflects the fact that phone penetration is less ubiquitous in rural regions. Successfully targeting women not only unlocks significant growth potential for the mobile industry but also advances women's digital and financial inclusion. In fact, closing the gender gap in mobile phone ownership and usage could unlock an estimated $170 billion market opportunity for the mobile industry in the period from 2015 to 2020. Women in South Asia are 38 percent less likely to own a mobile phone. Social media statistics also reflect this disproportion. Less than 30 percent women use social media, purportedly because it's an unsafe place. Ankhi Das, Policy Head of Facebook, brings an important and real perspective to these figures. "It has a lot to do with access to resources. The deeper normative values we need to look at as a society before saying that it's only because of safety concerns that people aren't online. If I as a family have a data plan, and I come from a middle income status, which is subject to certain kind of normative values, and if I have both a son and a daughter, I will give the data plan to the son and not the daughter. I think this is a false binary that safety issues are keeping women from coming online." According to a United Nations (UN) Women Survey, "Gender barriers are real. One in five women in India and Egypt believes the internet is not 'appropriate' for them."

Inside India

The most powerful outcome of internet use is the fact that it decentralises work centres and therefore, makes empowerment widespread. India's growing cities are the hotbed of talent, especially among women. SheThePeople.TV does a monthly workshop with women entrepreneurs who use the internet for their brand or business outreach. In Lucknow, Indore, Jaipur, Pune and many other cities, there is a growing network of women entering the start-up space. Many are turning homes into home-offices, some are catering food for orders made via the internet, several women are selling fashion garments on WhatsAPP and artists and musicians are building pages to extend their reach from Gachibawli to global audiences.

The trends are fascinating. Despite challenging and evolving business cycles, entrepreneurs are reinventing ideas to gratify the needs of the current market. The young generation is open to change—to diversify and go with ideas that will work in the new, demanding environment. There are various factors at play in these mini metros—one of them is the surge of the smartphone usage. There is increasing penetration and enhanced reach as feature phones are populating the cities allowing for higher reach of e-commerce. People want more choice and are hungry for access, fuelling demand that is more pointed. Little wonder then that in Jaipur and Lucknow, SheThePeople documented many entrepreneurs setting up e-commerce centric businesses and internet services. Going online is the first threshold of moving business out of just their hometowns. Women owners are running unique business models—one set up a local food aggregator's forum, another one a platform that buys failed start-ups and re-pitches to investors after a revamp. In both Jaipur and Lucknow, a large number of entrepreneurs have put together local chains, bakeries and more, with an equally adept online arm. Women entrepreneurs shared insights that tear a new thought away from the stated objectives of scaling up, raising funds, growing big businesses and leveraging significantly. First, entrepreneurs needn't always think large scale. If they meet the demand and are able to grow their business a few times per that market environment, they are good stead. Not every business needs to be

national. Not all entrepreneurs need to multiply before they make money. Many have profits to show and can expand basis internal accruals. Second, most entrepreneurs—some large and established and others who were still ideating—have said that they were not in a rush for funding from investors. There is a thinking that's emerged that start-up owners can grow ideas faster if it's cash positive and allows for the same to churn the next cycle. Are women taking this approach because it's practical and keeps risks at bay? Many women asserted that they were reluctant to leverage someone else's money, leading them to opt for commerce businesses that have high margin products that allowed them to make money on every sale.

The Bad and the Ugly

The proliferation of misogyny via trolls on the internet speaks volumes about the ways in which the wider, global online environment may in itself be hostile towards women. In India, too, the internet has brought about a great degree of vulnerability, despite being a tool that is designed to empower. The threats come in the form of cyber-crime, trolling, harassment and sometimes physical abuse.

Women receive far more social media abuse than their male counterparts and the intensity of the abuse is higher. Nitin Pai of Takshashila Institute in Bangalore says, "There is a contest between narratives of prejudice and tradition. Whichever way you cut it—political or ideological—women are at the receiving end. If any of these narratives—conservatism, prejudice, tradition—win, women are at the losing end. It's important for women to stand up and take this stance much more than men." He notes how trolling attracts audience as the drama plays out for all the entire spectators.

For an action to qualify as violence—as illustrated through the UN Declaration's emphasis on 'psychological harm or suffering'—physical proximity and contact is not a necessary condition. While forms of violence change with the medium through which it is carried out, it continues in its new and multiple digitised avatars.[6]

We can put a phone in a woman's hand, but how does that empowerment play out into her real life? A male dominated society continues to ostracise efforts by women to stand on their feet and take charge.

Policy and Government

A government survey shows that almost 79 percent of the women establishments are self-financed. Women entrepreneurs find it easier to turn to family to start a business with money that already belongs to them.[7]

We need policies that are holistic for women. On the economic front, many states and the centre have talked about funds to support female founders. However, most of the procedures to access those funds are complex and tedious. The government on its part is trying to simplify the process, but the fact remains that for the administration, start-ups are a new story and they too face a steep learning curve. There are women centric funds that have come up but these are not sufficient to cover the entire canvas of new ideas that are emerging. Traditional investors, on the other hand, are mostly chasing valuation driven stories.

A few years ago, the government had mooted the idea of the Bharatiya Mahila Bank. Now, it is being merged with State Bank of India. Why has it not been grown as an independent bank? How does a merger help women for whom this was to be a go-to place for funding? This is the big question: how do we set up a framework? We don't need just one, but many policy moves to create sufficient outlets of funding and loans for women.

Policy challenges also remain, with respect to getting more women online or preventing those already in the internet universe from retreating. Social media trolling and sexual abuse are making the internet a tough place for women. Recently, the Women and Child Development Minister Maneka Gandhi said that the government would take action again trolls. However, there remains ambiguity as to how this would be implemented and whether this is a policy decision or a knee-jerk reaction.

Could the condition of women's economy be an answer to India's growth-stickiness? Could this be the one factor that goes beyond public spending in infrastructure? Is it time to go beyond a gender-neutral approach to recognising and rewarding efforts by women towards building the new economy?

The Industrial Revolution was one of the big turning points in economic history because it brought economic identity, empowerment and wealth to people. However, the beneficiaries were mostly men. Women only received by-product benefits from those economic returns. The revolution cut down distances, created shop floors, but it didn't collapse any societal gender gaps.

However, with this digital revolution, women can lead the way. Not only can they contribute by being a force of growth and wealth, they can use it to shatter the glass ceiling of archaic workspaces and build their own success stories. This new context and construct of the new age and internet-dependent India we live in, there is a massive shift towards self-start companies and risk-hungry "digital and dot" projects. There is a shift from being employed to being the employer. Women are at the centre of this. One merely has to browse through Twitter or Facebook to find stories of successful women leading businesses from e-commerce to content companies. In India, there are two million SMEs registered on Facebook, and a big chunk of those are women-led businesses.

Harnessing the power of women could change the growth matrix, says a KPMG report. "Given the current economic scenario, some of the key national imperatives to propel India into the next wave of growth include creating employment opportunities for special segments such as women workforce."

Women are at the heart of the country's manufacturing, digital and service boom. "Making in India" is, simply, putting an idea to work.

Debunking Lynch Mobs: An Ethical Approach to Online Harassment and Free Speech

Catalina Ruiz-Navarro

In 2013, Justine Sacco ended up sabotaging her own career with a tweet just before boarding a plane to South Africa: "Going to Africa, I hope I don't catch AIDS. It's a joke. I'm white." Sacco was then the global head of communications for the digital media conglomerate, InterActiveCorp (IAC). She had some 200 followers on Twitter. That tweet, intended to be sarcastic, sparked what would be called, "an ideological crusade." Twitter users contacted Sacco's boss, who in turn tweeted: "This is an intolerable and offensive comment. The employee is under question, we cannot contact her until she gets off the plane." This, for many, was a sign that their complaints and criticisms "paid off." The anger quickly turned into euphoria: "I'm dying to see Justine Sacco get down that plane"; "Dumb bitch, we'll see how you get fired live."

Since Sacco worked for a private company and in the area of communications, her boss had every right to fire her. Perhaps Sacco's tweet was a mistake but she should have known about the scope of these blunders within the competence of her work. Justine Sacco was not fired just because a "lynch mob" on the Internet asked for her head. Rather, she was fired because a mistake she made at work – while her job was managing communications – triggered a virtual version of a "lynch mob".

In social media, language co-exists in the paradox of having an oral intent but a written format. What we say online is thought with immediacy and somehow, we still expect our words to be forgotten in the same way any reckless joke we say to our friends would be. But our words on social media are of a written nature and a message can be on the internet for eternity; since dissemination over the internet has a global reach, our words are very susceptible to being taken out of context. This has ethical and moral implications and requires changes in our behaviour. It is not the same for Justine Sacco to say her tweet as a joke to a friend (who perhaps will quickly forget it), than to say it in writing, in a social network, where it can be read by people who do not know her enough to understand her sense of humour and intentions. The same tweet would have different weight if it were written in a book or in an official statement letter; in these cases it would be much more serious than something said casually on social media. Not everyone is obliged to such high degrees of political correctness, but everyone with a public persona – journalists, communicators, politicians, public figures – should have, if not considerable care, at least awareness of how technology amplifies the impact of their words (and even more so of their mistakes).

This awareness of speech is not the same as self-censorship. A lynch mob on social media is undoubtedly better than one in the real world, and definitely preferable to silence because, at the end, censorship is even more violent than verbal violence. The effect of words on the Internet is different from the effects of a fist fight, or pitchforks and torches. After all, civilisation began when humans went from shooting each other stones to shooting insults. But insults on the Internet can be amplified, and there is no denying the hurt that can be caused by words. So what happens when the cyberbullying has effects beyond smear or dismissal? Can you blame online bullying for generating irreparable damage? If so, how can we regulate it?

For "angry mobs" on social media there is often no plan, no conspiracy and no leader. They are not necessarily right or fair, and we cannot be sure that they are as big as they feel. A lot of noise can be made on the internet by just few influencers. The vast majority of online lynch mobs are spontaneous and emotional, governed by the same rules Gustave Le Bon (1895) explored in the psychology of the masses.[1] However, no matter how uncontrollable the "lynch mob" turns out, its effects are directly related to the vulnerability of its "victims." As in three-dimensional life, mass demonstrations are highly powerful and meaningful, especially when they occur peacefully and collectively for a cause that is considered "fair." But all crowds are susceptible to irrational and violent behaviour. The control of these situations often depends on individuals developing the sensitivity to resist their own cruelty.

In April 2014, the programmer Rachel Bryk, 23 years old and famous for her contributions to the development of the emulator Dolphin, killed herself. Bryk was also a prominent figure within the transgender community and amongst applications developers. She had been the subject of repeated and constant attacks of transphobia and online bullying which triggered a bout of depression that eventually led her to suicide.

There are radical differences between bullying someone because of their sexual orientation, and bullying a professional in communications for not foreseeing the effect of a clearly discriminatory comment on the Internet. For Bryk, Internet was a place where she could elaborate her own identity but also a channel through which she could be attacked. A situation of vulnerability, coupled with attacks on the Internet, encouraged her suicide. It is not exactly a hate crime, although the similarities are enormous.

In Bryk's case, harassment (whether the aggressor knows it or not) goes far beyond a "death threat on Twitter." The insults may have the same intention as an obscene scribble in the bathroom door, but their impact is much stronger. In circumstances like Bryk's, discourse takes a performative role. According to John L. Austin (1962), the concept of performative language is when words, rather than describing an action, perform it.[2] For example, verbs like 'swear', 'promise', 'declare', 'gamble', 'baptise' and 'marry', actually have an effect on reality when they are enunciated.

Words are powerful; they build a symbolic field that affects the way we understand the world and our emotions. In cases of online harassment, ceaseless messages come through smartphones and personal computers, two of the most intimate devices a person can have in modern times; there are many who literally take them to bed every night. Imagine having the violence of bullying so

close. However, a hurtful word, persistent as it may be, does not oblige Sacco's dismissal nor drives a person to suicide. A person without a history of discrimination and living in a stable environment with a strong support system may not be as vulnerable to bullying as another one in more vulnerable conditions. The effects of online lynch mobs are psychological and should not be underestimated; it means reactions are as complex as human emotions and they too depend on context and environment. To withstand online bullying, all of these social vulnerabilities must be attended to and support systems must be strengthened. To counter the emotional effects of online harassment, people need plenty of support. A policy of social inclusion of minority groups (both online and offline) will be more effective in reducing the harmful effects of online bullying than the "preventive" self-censorship.

In 2014, the scientist Matt Taylor managed to land a spacecraft on a comet. When he spoke to the media about his achievement, he wore a shirt illustrated with a blonde woman wearing a corset and holding a gun. Some feminists said Taylor's shirt design was 'sexist'; opinion pieces came out, analysing what his shirt meant. Taylor himself then came on TV to apologise while crying, which led people to talk about the "evil horde of feminists" who had "lynched" and "censored" Taylor. However, online bullying against Taylor had in no way the effects (or intentions) that online harassment had in the cases of Sacco and Bryk. Several people criticised Taylor's shirt on social networks, a few opinion journalists joined the criticism, the man apologised on television and spoke again of his scientific achievements. No one complained nor censored or fired him. Criticism, in its most flamboyant form, cannot be equated with bullying, online harassment or censorship. Being embarrassed on the Internet, like Taylor, is far from being a victim of lynching. Feelings of shame, according to David Hume (1739), are appropriate and useful to regulate our ethical behaviour and moral emotions.[3] In Taylor's case, there was no job loss or permanent psychological damage. It is not that people have different sensitivities, rather, there are clear lines that distinguish criticism from online harassment. However, often on the Internet, legitimate, good, bad or exaggerated criticisms are indistinctly called lynching.

Interactions on social networks show that, in fact, the distinction between good and evil is not based solely on rational deliberation, and that moral judgments are not absolute or universal. People are not motivated solely by reason and logic; moral feelings are an important drive for our actions. The Internet is a privileged space to observe social regulation. If only David Hume had been alive to see it.

Hume said that morality is essentially based on feelings called "moral sentiments", positive feelings associated with happiness of mankind and resentment of its misery. They motivate what we call "virtuous actions" that awaken "moral sentiments" and this leads to social regulation. For Hume, sympathy represents the tendency to get involved with other people's emotions; this allows subjects to relate with each other. In many cases in social media, a Like, Fav, or Retweet has to do with a simple, perishable feeling of immediate sympathy.

This sympathy is one of the things that motivate people to act collectively as a group or even a mob on the Internet. In fact, some say that the mobs that "lynched" Sacco were well-intentioned at first, aiming to "defend rights." But whose rights? Maybe that was exaggerated and people simply defend political correctness because it easily provokes feelings of virtue and belonging. With

each “Like” or “Fav” on social media, we build shared values, a symbolic field of what is considered “good” and what is regarded as “bad.” To wear a shirt with a so-called sexist illustration and to make a racist tweet did not always awaken collective indignation. We have spent years building a symbolic field of language where these actions are rejected. In the exercise of public debate, we construct symbols that change how we perceive actions and the moral emotions that these actions stir.

Undoubtedly, the Internet is a great tool for participation in the global public debate. Social rejection is needed to regulate our behaviour, especially because legal punishment or criminal law may lead to censorship or other restrictions of the right to freedom of expression. When someone makes a racist or homophobic comment, or when he or she attacks or discriminates against any group, censorship is the least desirable solution; even the most absurd or prejudiced arguments should be said out loud in order to be debated.

“Lynch mobs” on the Internet exist and have real effects. But the only way to effectively regulate them is social regulation. Criminal or legal punishment has dire consequences; it would be crazy to send all internet trolls to jail, or to prosecute online harassment groups, especially since the term “lynch mob” is usually inaccurate, and it is also often used to stigmatise minority groups. Emotions cannot be dimmed or penalised. Censoring offensive speeches goes against the right to freedom of expression; we must remember that sometimes insults are legitimate social complaints. Social media is a space for scrutiny of public figures and this is unlikely to change. It is also a natural area for debating public opinion, and it should be assumed that everything said in social networks is some sort of opinion unless explicitly stated otherwise. The right to freedom of expression implies that each person must be held responsible for what he or she says on and off the Internet. In addition, in most countries there are extensive laws against harassment, threats, extortion, slander and libel, which can be used to handle cases of “cyberbullying” without inventing “new laws” for the digital realm.

In the end, each person has to go through an inner ethical negotiation between being respectful and empathetic, or aggressive and confrontational. Both positions may be valid depending on the circumstances, and both are protected by the right to freedom of speech. Sometimes, one speech strategy is more effective than the other. Of course, nothing exempts us of being aware of context in which we say things, of the privileges that we have and the potential impact of our amplified words. The verbal violence users experience online does not emanate from networks or computers; hatred and brutality are human emotions that can only be regulated with other human emotions like empathy and compassion. Maybe it is as simple as being mindful of the specific circumstances of the person we are engaging online and being aware of our desires to exert control over others. Communication should not be a violent act of conquest.

THE FUTURE OF ENTERTAIN-MENT

Netflix – Is the Film Censorship Law There Yet?

Japreet Grewal

Online subscription-based platforms like Netflix that provide video on demand services are becoming increasingly popular among internet users in India who want to watch films sitting at home. The troublesome question is whether these platforms have a legal obligation to show only those films that are certified by the Central Board for Film Certification (CBFC) in India. This requirement for certification has been laid down in the Cinematograph Act, 1952 (hereafter 'the Act'). In this article, I examine this question by analysing how this requirement under the Act applies when films are exhibited across different media of delivery.

The Problem of 'Exhibition'

Under Section 4 of the Act, one requires an approval (in the form of certification) from the CBFC in order to exhibit a film.[1] The CBFC undertakes the process of examining the film and: sanctions it for unrestricted public exhibition (U); sanctions it for public exhibition restricted to adults (A); directs cuts or modification in the film; or refuses to certify the film. The CBFC can refuse to certify the film only if it is against the "interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or involves defamation or contempt of court or is likely to incite the commission of any offence".[2] This requirement for approval applies to the exhibition of films produced in India as well as films imported into the country.

Section 3 of the Act, which provides for the establishment of the CBFC, states that the CBFC is set up for the purpose of certifying films which are intended for "public exhibition". The term "public exhibition" has also been used in Rule 2 (iii) of the Cinematograph Rules, 1983 which defines an applicant under Section 4 of the Act.[4] This means that the Act applies to all films that are intended for public exhibition. However, "public exhibition" is not defined under the Act. Does the term refer to making a film available for watching only in public places such as cinema halls, or making a film available to the public whether for watching in public or in private?

Of Public and Private Exhibitions

The Delhi High Court, when dealing with this question in the case of Super Cassettes Industries v. Central Board for Film Certification, held:

"Even if there is no audience gathered to watch a film in a cinema hall but there are individuals or families watching a film in the confines of their homes, such viewers would still do it as members of the public and at the point at which they view the film that would be an "exhibition" of such film."[4]

In this case, the court held that exhibition of films by sale and distribution of DVDs or VCDs would be subject to the Act. Thus, exhibition of films under the Act means exhibition to the public whether for public or private viewing.

Netflix is an online, subscription-based platform which allows us to watch films privately and on demand. Would Netflix therefore be subject to the Act based on this understanding of 'exhibition'? In order to answer this question we need to find out if the Act applies to public exhibition of films through any medium including cable television networks, DVDs and the internet? I have addressed this question later in the article.

The draft Cinematograph Bill, 2013 defines "exhibition" as "audio or visual dissemination of a film or part thereof or making available a film or part thereto through use of a public medium".[5] The Bill also defines "public medium" as a "medium, forum or place to which members of the general public have access to with or without the payment of a fee or charge". Thus, platforms like Netflix – which the public can access to watch films with payment of a subscription amount – would be understood as exhibiting films under the draft Bill. The draft Bill was listed for introduction in the Monsoon Session of the Parliament in 2010. To our knowledge, there has not been any progress on the status of the draft Bill. It is interesting to note that an Expert Committee (chaired by Shyam Benegal) was constituted to formulate recommendations for certification of films by the Central Board of Film Certification (CBFC), and submitted its report on the issue in April 2016. However, the report does not make any reference to the draft Bill and unlike the draft Bill, it has not provided any clarity on the interpretation of the term 'exhibition'.

Netflix as On-Demand Private Exhibition of Films

It is noteworthy that under the Cable Television Network (Regulation) Act, 1995 (hereafter the 'Cable TV Act'), cable network operators are required to ensure that the films that can be accessed by their users at home must be certified by the CBFC. Rule 6 (n) of the Cable Television Network (Regulation) Rules, 1994 provides that the content provided by cable network operators to their users must comply with the Act. This suggests that the term 'exhibition' of films under the Act has been understood under the Cable TV Act to include exhibition of films for private viewing by the public. As mentioned earlier, with this understanding of 'exhibition', films exhibited on Netflix would have to undergo the certification process under the Act.

It would not be right to draw this conclusion without comparing Netflix with different media of exhibiting films – such as VCDs and DVDs, movies on demand provided by cable network operators, internet protocol television channels, and online content-sharing platforms such as YouTube – and examine which medium Netflix closely resembles. It is necessary to do this because different media are regulated by different legislative frameworks.

One can compare Netflix to a cable television network provider (hereafter 'cable network operator') as both services allow multiple users to watch films privately at home by payment of a subscription. Cable network operators are regulated under the Cable TV Act and related rules and guidelines. The Cable Network Rules and the Downlinking Guidelines, 2005 formulated under the Cable TV Act, require cable network operators to ensure compliance with the certification requirement under the Act while determining their programme content. Therefore the films that are made available by cable network operators must be only those films that have been certified by the CBFC. Cable television networks are however different from Netflix in the way they operate. This is critical because cable television networks are defined[6] under the Cable TV Act in terms of their operation. They use satellite signals to distribute content to multiple subscribers while Netflix rides on the networks of telecom service providers and internet service providers to provide content to its users. Therefore, the cable television regulation cannot be applied to Netflix.

What Happens When Internet becomes the Medium of Delivery?

Now, let us compare Netflix with internet protocol television (IPTV). IPTV is a service which uses the internet for delivery of multimedia content to a customer and makes it available on television, cellular, and mobile TV terminals with STB modules or similar devices. Both Netflix and IPTV use the internet to provide services to their users (which is also referred as streaming) and both are paid services. However, in India, IPTV services can only be provided by registered cable television network operators (because IPTV is treated like cable television service) and telecom service providers and internet service providers who operate under a license given by the Department of Telecommunications[7] (because IPTV is a television service that runs on the internet). As a condition under these licenses, it has been made clear that the content restrictions applicable to cable network operators, as discussed in the earlier section (which includes compliance with the certification requirement under the Act) would apply to IPTV as well.[8]
Although Netflix also provides content over the internet (like IPTV) it is treated as an over the top (OTT) service and does not need a license to provide services in India. Since Netflix does not operate under a license, it does not need to comply with the Act unlike IPTV.

Netflix and VCDs/DVDs are similar in that both can be accessed at home to watch films privately on a certain payment of money. The difference between the two is that VCDs/DVDs are sold through a physical medium whereas Netflix uses internet to provide access to films online. Also, the buyer owns a copy of the VCD/DVD containing the film while a user of Netflix does not own the copy of the film that he/she watches on Netflix. The Act does not clearly provide that it regulates the exhibition of films through VCDs/DVDs. The Delhi High Court has however held in the case of Super Cassettes Industries v. Central Board for Film Certification that DVDs come within the purview of the Act. The Court held that under Section 52A (2) (a) of the Copyright Act, one could not make a film which is a cinematograph film available to the public (here by sale/distribution of VCDs/DVDs) that requires certification under the Act unless it was accompanied with a copy of the certificate from CBFC. We know that Netflix makes cinematograph films available to the public using internet. We also understand that the under the Copyright

Act, cinematograph film could be film that is available on any medium including internet. Therefore the requirement to display particulars about certification of a cinematograph film as provided under Section 52A(2)(a) of the Copyright Act would also apply to films available on Netflix.

Netflix and YouTube – Same Difference?

It is also useful to make a comparison between Netflix and paid movies provided by YouTube, an online content (video) sharing platform which allows users to watch films privately using internet by payment of money. Both Netflix and YouTube are OTT services. They do not need prior approval or a license to operate in India and are based outside India. We know that the Act does not clearly provide that it applies to exhibition of films irrespective of any medium. It is however clear that under Section 52A (2)(a) of the Copyright Act, films available to public, in this case on YouTube, must have received certification from CBFC under the Act. In my conversation with the YouTube customer support team for paid content, it was not clear whether, in practice, they only exhibited films which were certified by the CBFC. This then raises several questions about the difficulty in applying the Act to platforms like YouTube and Netflix.

What kind of films can Indian users watch on Netflix? Are these films that are produced and certified in India and made available on Netflix, films that are produced in India but are exclusively available on Netflix, uncertified versions available on Netflix of films that are produced outside India which have been censored by CBFC and released through traditional channels in India, films that are produced outside India that have not been certified or released in India but are available to Indian users on Netflix?

We know that where an applicant is informed that certification of a film by CBFC is contingent upon removal of certain portions of the film, the applicant is required to "remove such portions from the negative of the film and all copies of the film in the possession of the applicant or the laboratory where the film was processed, the distributor, the exhibitor or any other person is required to be surrendered".[9] Therefore, after a film (whether produced in India or outside India) has been reviewed by CBFC, only the version of the film that has been approved by CBFC would be made available to the public. All other versions in possession of "any other person" must be surrendered under the Act. Releasing versions to the public which are other than the censored and certified versions of such films would be considered illegal under the Act. Recently, in a public interest litigation filed before the Punjab & Haryana High Court against the release of the films Mastizaade and Kya Kool Hain Hum 3, the court directed the producers/directors to submit an undertaking that they would not release the excised portion of the feature/film to anyone in any medium including the internet.[10] It may however prove difficult to regulate exhibition of films on Netflix that are produced and released outside India and films only released on Netflix.

Conclusion

Technology always precedes regulation. This is why for regulation to be effective, it must be technology-agnostic. What we see in this microscopic analysis is an example of a law that is not technology agnostic and thus fails to keep up with new technologies of exhibition of films. The applicability of the Act certainly depends on how we understand the term 'exhibition' of a film. Neither the Act nor the

relevant case law provides a clear and effective interpretation of this term. There is no legal provision in the Act that states or implies that it is applicable to exhibition of films through the internet. It is however clear that there are separate regulatory frameworks in India for different media of exhibition of films. These frameworks require these media owners or service providers to ensure that they only exhibit CBFC certified films to the public. There is no distinct regulatory framework that ensures that the Act applies to platforms like Netflix.

It is beyond doubt that with the advent of the 'Netflix era', the interplay between media content and ownership, service provision and regulatory choices will undergo significant disruption. In the Indian context, the state has unfortunately chosen to deal with this paradigm shift by creating separate regulatory frameworks in an ad hoc manner instead of trying to realise some sort of convergence. This multiplicity of regulatory frameworks comes at a time when the boundaries between these regimes are increasingly difficult to define. Thus, the need to adopt a technology agnostic approach is one of the most central issues that must be addressed in any new reform.

On a separate note, the regulatory uncertainty that the Act has created allows the use of other tools for content regulation online. For instance, the Information Technology Act, 2000 allows the government and the courts to direct ISPs, on whose networks users access Netflix, to either block or take-down films available on Netflix that they consider objectionable. While we know that one could bypass censorship filters and access content that is not available in the country by using free/paid proxy services, this type of content regulation could force players like Netflix to give in to the state's paternalism and inspire self-censorship to carry out their operations smoothly within the country. That is a dangerous precedent to set in the industry as far as freedom on the internet is concerned.

There is an urgent need to initiate discussions about reform in the present framework(s) for film regulation that addresses technology neutrality and does not stifle the freedom of expression of the film industry and the viewers.

REFERENCES

02

1 White House, Remarks by the President to the Business Roundtable, September 16, 2015, https://www.whitehouse.gov/the-press-office/2015/09/16/remarks-president-business-roundtable

2 Office of the Press Secretary, FACT SHEET: President Xi Jinping's State Visit to the United States, White House, September 25, 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

3 Wendy Wu, "Handshake to end the hacking: China and Germany pledge for peace in cyberspace by 2016,"South China Morning Post, November 9, 2015, http://www.scmp.com/news/china/diplomacy-defence/article/1877288/china-and-germany-aim-reach-commercial-cyberspying-deal.; Chen Qin, "China, Germany Working on Cybersecurity Deal, Envoy Says," Caixin, March 17, 2016, http://english.caixin.com/2016-03-17/100921423.html.

4 Robert Abel, "G-20 nations agree: No cyber-theft of intellectual property," SCMagazine, November 19. 2015, http://www.scmagazineuk.com/g-20-nations-agree-no-cyber-theft-of-intellectual-property/article/454845/

5 Joseph Marks, "U.N. body agrees to U.S. norms in cyberspace," Politico, July 9, 2015, http://www.politico.com/story/2015/07/un-body-agrees-to-us-norms-in-cyberspace-119900#ixzz3veYOOKwf

6 Paul Mozur, "China Tries to Extract Pledge of Compliance From U.S. Tech Firms," The New York Times, September 16, 2015, http://www.nytimes.com/2015/09/17/technology/china-tries-to-extract-pledge-of-compliance-from-us-tech-firms.html?ref=technology

7 Office of the Press Secretary, FACT SHEET: U.S.-China Economic Relations, White House, September 25, 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-us-china-economic-relations

8 Counter-Terrorism Law of the People's Republic of China, China Law Translate, http://chinalawtranslate.com/%E5%8F%8D%E6%81%90%E6%80%96%E4%B8%BB%E4%B9%89%E6%B3%95-%EF%BC%882015%EF%BC%89/?lang=en

9 "People's Republic of China Cybersecurity Law (Second Reading Draft)," China Copyright and Media, July 6, 2016, https://chinacopyrightandmedia.wordpress.com/2016/07/06/peoples-republic-of-china-cybersecurity-law-second-reading-draft/.

[10] Aaron Mehta, "Clapper Skeptical of US-China Cyber Deal," DefenseNews, September 29, 2015, http://www.defensenews.com/story/defense/policy-budget/cyber/2015/09/29/clapper-skeptical-us-china-cyber-deal/73027008/

[11] White House, Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference, https://www.whitehouse.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint

[12] First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes, December 2, 2015, http://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary-outcomes-0

[13] DHS Press Office, "Second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue," Department of Homeland Security, June 15, 2016, https://www.dhs.gov/news/2016/06/15/second-us-china-cybercrime-and-related-issues-high-level-joint-dialogue.; Ministry of Public Security, "China-U.S. high-level dialogue on striking cybercrime and related issues formally establishes hotline mechanism," August 28, 2016, http://www.cac.gov.cn/2016-08/28/c_1119466923.htm.

[14] Mark Hosenball, "U.S. counterintelligence chief skeptical China has curbed spying on U.S.," Reuters, November 18, 2015, http://www.reuters.com/article/us-usa-cybersecurity-idUSKCN0T72XG20151119

[15] Ellen Nakashima, "Following U.S. indictments, Chinese military scaled back hacks on American industry," The Washington Post, November 30, 2015, https://www.washingtonpost.com/world/national-security/following-us-indictments-chinese-military-scaled-back-hacks-on-american-industry/2015/11/30/fcdb097a-9450-11e5-b5e4-279b4501e8a6_story.html

[16] FireEye, "Red Line Drawn: China Recalculates its Use of Cyber Espionage," June 2016, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.; Dexter Roberts, "Chinese Hackers Like a 'Drunk Burglar,' 'Kicking Down the Door,' Says FBI Director," Bloomberg, October 6, 2014, http://www.bloomberg.com/news/articles/2014-10-06/fbi-chief-james-comey-lambasts-chinese-hackers.; Joe Uchill, "Obama administration confirms drop in Chinese cyber attacks," The Hill, June 28, 2016, http://thehill.com/policy/cybersecurity/285153-obama-administration-confirms-drop-in-chinese-cyber-attacks.

[17] Peter Mattis, "Three Scenarios for Understanding Changing PLA Activity in Cyberspace ,"China Brief, December 7, 2015, http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=44865&tx_ttnews%5BbackPid%5D=789&no_cache=1#.VoKkKPkrK70

[18] Ellen Nakashima and Adam Goldman, "In a first, Chinese hackers are arrested at the behest of the U.S. government," The Washington Post, October 9, 2015, https://www.washingtonpost.com/world/national-security/in-a-first-chinese-hackers-are-arrested-at-the-behest-of-the-us-government/2015/10/09/0a7b0e46-6778-11e5-8325-a42b5a459b1e_story.html

[19] Adam Segal, "China's Internet Conference: Xi Jinping's Message to Washington," Net Politics, December 16, 2015, http://blogs.cfr.org/cyber/2015/12/16/chinas-internet-conference-xi-jinpings-message-to-washington/

[20] Elaine Korzak, International Law and the UN GGE Report on Information Security, Just Security, December 2, 2105, https://www.justsecurity.org/28062/international-law-gge-report-information-security/

[21] Ministry of Foreign Affairs of the People's Republic of China, Remarks by H.E. Xi Jinping, President of the People's Republic of China, at the Opening Ceremony of the Second World Internet Conference, December 16, 2015, http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml

[22] Office of the Press Secretary, "Executive Order—'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,'" White House, April 1, 2015, https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

[23] Adam Segal, "Stabilizing Cybersecurity in the U.S.-China Relationship," National Bureau of Asian Research, September 16, 2015, http://xivisit.nbr.org/2015/09/16/stabilizing-cybersecurity-in-the-u-s-china-relationship-2/

03

[1] Channel News Asia, "Singapore, US enhance strategic partnership", http://www.channelnewsasia.com/news/singapore/singapore-us-enhance/3007834.html, 3 August 2016.

[2] Ibid.

[3] United States-Singapore Workshop on Cybersecurity for ASEAN countries, Singapore, 16-18 August 2016.

[4] As one of the trainers within the group on CBMs, this material presents the bulk of the author's commentary for the United States-Singapore Workshop on Cybersecurity for ASEAN countries, Singapore, 16-18 August 2016.

[5] For a fuller analysis of these issues, see Patryk Pawlak's recent article, "Confidence Building Measures in Cyberspace: Current Debates and Trends." https://ccdcoe.org/multimedia/international-cyber-norms-legal-policy-industry-perspectives.html, 2016.

[6] Sunnylands Declaration, "Joint Statement of the U.S.-ASEAN Special Leaders' Summit: Sunnylands Declaration", Principle no.12, https://www.whitehouse.gov/the-press-office/2016/02/16/joint-statement-us-asean-special-leaders-summit-sunnylands-declaration, 15-16 February 2016.

[7] For the full overview of normative approaches to international cybersecurity, see the IISS Strategic Dossier, "Evolution of the Cyber Domain: The Implications for National and Global Security", http://www.iiss.org/en/publications/strategic%20dossiers/issues/evolution-of-the-cyber-domain-fb56, December 2015.

8 Ibid.

9 Ibid. For full analysis, see Pawlak2016.

10 IISS Strategic Dossier, Evolution of the Cyber Domain.

11 See arguments within Pawlak 2016.

12 Organization for Security and Co-operation in Europe. 2013. “INITIAL SET OF OSCE CONFIDENCE-BUILDING MEASURES TOREDUCE THE RISKS OF CONFLICT STEMMING FROM THE USEOF INFORMATION AND COMMUNICATION TECHNOLOGIES.” Decision No. 1106, Permanent Council, 3 December.

13 UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013.

14 UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,A/70/174, 22 July 2015.

15 ASEAN REGIONAL FORUM WORK PLAN ON SECURITY OF AND IN THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES (ICTs), http://aseanregionalforum.asean.org/files/library/Plan%20of%20Action%20and%20Work%20Plans/ARF%20Work%20Plan%20on%20Security%20of%20and%20in%20the%20Use%20of%20Information%20and%20Communications%20Technologies.pdf, 7 May 2015.

16 Organization for Security and Co-operation in Europe. 2016 . “OSCE CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES.” DECISION No. 1202, Permanent Council, 10 March.

17 Pawlak, Patryk. 2016. “Confidence Building Measures in Cyberspace: Current Debates and Trends.” In International Cyber Norms: Legal, Policy and Industry Perspectives, edited by Anna-Maria Osula and Henry Rıigas, 129-153. Tallinn: NATO CCDCOE Publications.

04

1 This contribution is based on the report The Public Core of the Internet. An international Agenda for Internet Governance presented by the Netherlands Scientific Council for Government Policy to the Dutch Minister of Foreign Affairs, Mr. Bert Koenders, on the 31st of March 2015. The full report can be downloaded here: http://www.wrr.nl/fileadmin/en/publicaties/PDF-Rapporten/The_public_core_of_the_Internet_Web.pdf

2 For early thinking on global public goods, see: I. Kaul, I. Grunberg, and M. Stern (1999, eds.) Global Public Goods. International Cooperation in the 21st Century. Book published for the United Nations Development Programme Oxford: Oxford University Press.

[3] As it is technically possible to exclude people from the Internet, economists refer to it as a 'club good', i.e. a good whose benefits accrue only to members. Our reference to the Internet's core as an impure global public good is based on the technical and protocol-related set-up of the Internet with universality, interoperability and accessibility as its core values, which underscore the values of non-rivalry and non-excludability.

[4] See for example L. DeNardis (2013) Internet Points of Control as Global Governance, CIGI Internet Governance Papers no. 2 (August 2013), p.4: 'With the exception of repressive political contexts of censorship, the Internet's core values are universality, interoperability and accessibility'.

[5] These are the key aims of data security, also known as the CIA triad; see for example P. Singer and A. Friedman (2014) Cyber Security and Cyberwar. What Everyone Needs to Know, Oxford: Oxford University Press, p. 35.

[6] See L. DeNardis (2012) 'Hidden Levers of Internet Control. An Infrastructure-based Theory of Internet Governance', Information, Communication and Society, 15 (5): 726.

[7] This community includes – but is not limited to - organisations such as the Internet Architecture Board, the Internet Engineering Taskforce and the World Wide Web Consortium that develop protocols and standards and organisations such as the Internet Corporation for Assigned Names and Numbers and Regional Internet Registries that deal with the distribution of Internet resources such as IP numbers and domain names. Also the global informal community of CERTs or CSIRTs can be considered part of the technical community.

[8] See for a more elaborate analysis of these matters: D. Broeders (2015) The Public Core of the Internet. An International Agenda for Internet Governance. Amsterdam: Amsterdam University Press, chapter 3.

[9] See for example E. Taylor (2015) ICANN: Bridging the Trust Gap. OurInternet.org. Paper series, nr. 9. Waterloo: CIGI

[10] See M. Mueller and B. Kuerbis (2014) 'Towards Global Internet Governance: How To End U.S. Control of ICANN Without Sacrificing Stability, Freedom or Accountability', TCPR Conference Paper, available at SSRN: http://ssrn.com/abstract=2408226.

[11] See for a more elaborate analysis of these matters: D. Broeders (2015) The Public Core of the Internet. An International Agenda for Internet Governance. Amsterdam: Amsterdam University Press, chapter 4.

[12] M. Graham, De Sabbata, S., Zook, M. (2015) Towards a study of information geographies: (im)mutable augmentations and a mapping of the geographies of information, Geo: Geography and Environment. Vol. 2(1) 88-105. doi:10.1002/geo2.8

[13] See for a definition of an extended national interest B. Knapen, G. Arts, Y. Kleistra, M. Klem and M. Rem (2011) Attached to the World on the Anchoring and Strategy of Dutch Foreign Policy. Amsterdam: Amsterdam University Press, p. 47.

[14] See paragraph 13(k) of the Report of the Group of Governmental Experts On Developments in the Field of Information and Telecommunications In the Context of International Security, Report as adopted, Friday 26 June.

[15] For this line of reasoning see: M. Van Eeten and J. Bauer (2009) 'Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications, Journal of Contingencies and Crisis Management, 17 (4): 221-232.

[16] These countries are sometimes referred to as 'swing states', see: T. Maurer and R. Morgus (2014) Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate, CIGI Internet Governance Papers no. 7 (May 2014).

[17] Broeders, D. & L. Taylor (2016) 'Does great power come with great responsibility? The need to talk about Corporate Political Responsibility', in: L. Floridi and M. Taddeo (eds.) Understanding the responsibilities of Online Service Providers in information societies. New York: Springer

[18] W. Drake, V. Cerf and W. Kleinwächter (2016) Internet Fragmentation: an overview. Future of the Internet Initiative White Paper, January 2016. World Economic Forum. http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

[19] Internet Society (2016) A policy framework for an open and trusted Internet An approach for reinforcing trust in an open environment, p. 7. http://www.Internetsociety.org/sites/default/files/bp-Trust-20160621-en.pdf

[20] Global Commission on Internet Governance (2016) One Internet. Waterloo/ London: Centre for International Governance Innovation and Chatham House ,p. 75. https://www.ourInternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf

[21] https://www.rijksoverheid.nl/documenten/kamerstukken/2016/05/19/kabinetsreactie-op-aiv-advies-het-Internet-een-wereldwijde-vrije-ruimte-met-begrensde-staatsmacht-enwrr-advies-de-publieke-kern-van-het-Internet-naar-een-buitenlands-Internetbeleid

05

[1] "Our Business", Hub Power Station, accessed September 1, 2016, http://www.hubpower.com/our-business/hub-power-station/#CC

[2] N. Perlroth and D.E. Sanger, "Nations Buying as Hackers Sell Flaws in Computer Code", The New York Times, July 13, 2016, accessed August 30, 2016, http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html

[3] "Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries", United Nations, accessed September 5, 2016, http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

[4] See D. Bowett, Reprisals Involving Recourse to Armed Force, The American Journal of International Law. Vol 66(1), pp. 1-36, http://heinonline.org/HOL/LandingPage?handle=hein.journals/ajil66&div=5&id=&page=

[5] "Bush announces opening of attacks", CNN.com, October 7, 2001, accessed August 29, 2016, http://edition.cnn.com/2001/US/10/07/ret.attack.bush/

[6] J.A. Green, The Article 51 Reporting Requirement for Self-Defense Actions (2015), Virginia Journal of International Law. Vol 55(3) http://www.vjil.org/assets/pdfs/vol55/VJIL_55.3_Green_FINAL.pdf

06

[1] Thomas Wiegold, "Ein Update ist verfügbar," ZEIT Online. April 27, 2016, accessed on August 28, 2016 http://www.zeit.de/digital/internet/2016-04/bundeswehr-cyberkrieg-it-aufruestung-nachwuchs

[2] For example see: Anna Biselli, "Es cybert bei der Bundeswehr: Digitales Aufrüsten um jeden Preis mit Gamern und Nerds," Netzpolitik.org, April 27, 2016, accessed on August 28, 2016 https://netzpolitik.org/2016/es-cybert-bei-der-bundeswehr-digitales-aufruesten-um-jeden-preis-mit-gamern-und-nerds/; "13 500 Soldaten im Cyberkrieg,". taz.de, April 26, 2016, accessed on August 24, 2016 http://www.taz.de/!5299284/; Konstantin von Notz, "Engagement für IT-Sicherheit statt Bundeswehr im Cyber-Krieg,". GrünDigital, April 26, 2016, accessed on August 24, 2016 https://gruen-digital.de/2016/04/engagement-fuer-it-sicherheit-statt-bundeswehr-im-cyber-krieg/; Andre Meister, "Geheime Cyber-Leitline: Verteidigungsministerium erlaubt Bundeswehr "Cyberwar" und offensive digitale Angriffe," Netzpolitik.org, July 30, 2015, accessed on August 24, 2016 https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/;

[3] Marcel Dickow, "Stellungnahme zur Öffentlichen Anhörung des Verteidigungsausschusses des Deutschen Bundestages am 22. Februar 2016," Deutscher Bundestag, February 22, 2016 accessed on August 24, 2016 https://www.bundestag.de/blob/409382/b9419561ac01bebea40956c403b8391d/stellungnahme-dickow-data.pdf

[4] See supra note ii and iii as well as Deutscher Bundestag. "Die Rolle der Bundeswehr im Cyberraum," (Protocol of parliamentary hearing, February 22, 2016)

[5] "White Paper On German Security Policy and the Bundeswehr," The German Federal Government, 2016

[6] For more information, see: "Dossier: Cyber Verteidigung," German Federal Ministry of Defence, accessed on August 24, 2016 https://www.bmvg.de/portal/a/bmvg/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9pNyydL2s_NIioKheSn5xcWZqUbFecmVSapF-QbajIgD93eVB/

[7] John Goetz und Hans Leyendecker, 7.06.2014. "Rechnungsprüfer halten Cyber-Abwehrzentrum für "nicht gerechtfertigt"," Sueddeutsche Zeitung, June 7, 2014, accessed on August 22, 2016 http://www.sueddeutsche.de/digital/behoerde-in-bonn-rechnungspruefer-halten-cyber-abwehrzentrum-fuer-nicht-gerechtfertigt-1.1989433

[8] "Abschlussbericht Aufbaustab Cyber- und Informationsraum," The German Federal Ministry of Defence, April 2016

[9] "Von der Leyen: Die Bundeswehr im Cyber- und Informationsraum 'besser und professioneller aufstellen'," Press Release of the German Federal Ministry of Defence, April 26, 2016, accessed on August 24, 2016 https://www.bmvg.de/portal/a/bmvg/!ut/p/c4/NYvBCsIwEET_aDcBQeqtJSAe9aL1lrYhrHSTsm7qxY83OTgD7zCPwSfWJr9T9Eo5-RUfOM5Omj4w8R7hlYvUFZgSvTUIFcZ7-ywB5pyCNmpISpVRvGaBLYuuzRSRaoAWHI11g7HmH_vtO3e-HjtzcJfhhhtz_wMlMw79/

[10] "Von der Leyen umwirbt Thyssen-Manager für digitale Kriegsführung," Frankfurter Allgemeine Zeitung, April 23, 2016, accessed on August 24, 2016 http://www.faz.net/aktuell/politik/inland/bundeswehr-von-der-leyen-umwirbt-thyssen-manager-fuer-digitale-kriegsfuehrung-14195057.html

[11] "Abschlussbericht Aufbaustab Cyber- und Informationsraum," The German Federal Ministry of Defence, April 2016, p.34

[12] "Abschlussbericht Aufbaustab Cyber- und Informationsraum," The German Federal Ministry of Defence, April 2016

[13] Shane Harris, @ War: The Rise of the Military-Internet Complex (Ashgate: Blackstone Audio, Inc, 2015)

[14] Julian Junk and Christopher Daase, "Germany," in Strategic Cultures in Europe: Security and Defense Policies Across the Continent, eds Heiko Biehl, Bastian Giegerich, and Alexandra Jonas (Wiesbaden: Springer, 2013)

[15] "Abschlussbericht Aufbaustab Cyber- und Informationsraum," The German Federal Ministry of Defence, April 2016, p5

[16] Matthias Gebauer, „Bundeswehr-Hacker knackten afghanisches Mobilfunknetz", Spiegel Online, September 23, 2016, accessed on September 23, 2016 http://www.spiegel.de/politik/ausland/cyber-einheit-bundeswehr-hackte-afghanisches-mobilfunknetz-a-1113560.html

[17] For operations which require secrecy, the government only informs specific parliamentary party leaders and parliamentarians. This is practice, but not in the law to date. A report on the reform of the parliamentary mandate requirements suggests to establish this practice in the law. See: Michael Bothe,"Stellungnahme zu Rechtsfragen des Cyberwar für den Verteidigungsausschuss des Deutschen Bundestages," Deutscher Bundestag, 2016, Pp. 9-11.

[18] Michael Bothe, Ibid.

[19] "Die Rolle der Bundeswehr im Cyberraum," (Protocol of parliamentary hearing, February 22, 2016), accessed on August 24, 2016 https://www.bundestag.de/blob/405090/f97d7ece26be2a34d19762c99b4b1511/61--sitzung_-22-02-2016-data.pdf

[20] Kai Strittmacher,"Warum schickt der BND der Bundeswehr abgehörte Daten?," Zeit Online, March 18, 2015, accessed on August 24, 2016 http://www.zeit.de/politik/deutschland/2015-03/bnd-bundeswehr-daten-ueberwachung/komplettansicht

[21] Rainer Arnold and Lars Klingbeil, "Ein digitales Update für das Völkerrecht," Frankfurter Allgemeine Zeitung, May 10, 2016

[22] For context, see Heiko Biehl, Bastian Giegerich, Alexandra Jonas (eds.),Strategic Cultures in Europe: Security and Defense Policies Across the Continent (Springer, 2013)

[23] "White Paper On German Security Policy and the Bundeswehr,"see n. V, p38

08

[1] In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, Case No. 1:15-mc-01902-JO, Memorandum and Order (E.D.N.Y. February 29, 2016), available at https://epic.org/amicus/crypto/apple/Orenstein-Order-Apple-iPhone-02292016.pdf.

[2] In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS1300, California License Plate 35KGD203, Case No. 15-0451M (C.D. Cal. February 16, 2016), available at http://www.wired.com/wp-content/uploads/2016/02/SB-shooter-MOTION-seeking-asst-iPhone.pdf.

[3] Christine Hauser, San Bernardino Shooting: The Investigation So Far, NEW YORK TIMES (December 4, 2015), http://www.nytimes.com/2015/12/05/us/san-bernardino-shooting-the-investigation-so-far.html.

[4] BBC, Brussels Explosions: What We Know About [sic] Airport and Metro Attacks, BBC (April 9, 2016), http://www.bbc.com/news/world-europe-35869985.

[5] BBC, What Happened at the Bataclan? BBC (December 9, 2015), http://www.bbc.com/news/world-europe-34827497.

[6] This was soon disputed, however. See Dan Froomkin, Signs Point to Unencrypted Communications Between Terror Suspects, THE INTERCEPT (November 18, 2015), https://theintercept.com/2015/11/18/signs-point-to-unencrypted-communications-between-terror-suspects/. See also Thorsten Benner and Mirko Hohmann, How Europe Can Get Encryption Right, POLITICO (April 13, 2016), http://www.politico.eu/article/how-europe-can-get-encryption-right-data-protection-privacy-counter-terrorism-technology/ (pointing out that "[i]n the investigations following the Brussels and Paris attacks, the problem was not encrypted data, but data that was unavailable to the appropriate agencies").

[7] Sean Gallagher, What the Government Should Have Learned About the Clipper Chip, ARS TECHNICA (December 14, 2015), http://arstechnica.com/information-technology/2015/12/what-the-government-shouldve-learned-about-backdoors-from-the-clipper-chip/.

[8] Peter Swire, 'Going Dark' Versus a 'Golden Age for Surveillance', CENTER FOR DEMOCRACY AND TECHNOLOGY (November 28, 2011), https://cdt.org/blog/%E2%80%98going-dark%E2%80%99-versus-a-%E2%80%98golden-age-for-surveillance%E2%80%99/.

[9] Ralph Ellis et al., Orlando Shooting: 49 Killed, Shooter Pledged ISIS Allegiance, CNN (June 13, 2016), http://www.cnn.com/2016/06/12/us/orlando-nightclub-shooting/.

[10] Alissa J. Rubin et al., Scores Die in Nice, France, as Truck Plows into Bastille Day Crowd, NEW YORK TIMES (July 14, 2016), http://www.nytimes.com/2016/07/15/world/europe/nice-france-truck-bastille-day.html.

[11] Emma Graham-Harrison et al., Munich Attack: Teenage Gunman Kills Nine People at Shopping Centre, GUARDIAN (July 23, 2016), https://www.theguardian.com/world/2016/jul/22/munich-shopping-centre-evacuated-after-reported-shooting-germany.

[12] For an extensive critique of technological solutionism, see EVGENY MOROZOV, TO SAVE EVERYTHING, CLICK HERE: THE FOLLY OF TECHNOLOGICAL SOLUTIONISM (2014).

[13] Apple, Government Information Requests, APPLE (last accessed August 13, 2016), http://www.apple.com/privacy/government-information-requests/.

[14] See In re Order Requiring Apple supra note 1.

[15] See In the Matter of the Search of an Apple iPhone supra note 2.

[16] 28 U.S.C. §1651(a) ("The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of the law").

[17] See also Helen Nissenbaum, Where Computer Security Meets National Security, 7 ETHICS AND INFORMATION TECHNOLOGY 61 (2005) (distinguishing between computer and national security).

[18] See Chad Perrin, The CIA Triad, TECH REPUBLIC (June 30, 2008), http://www.techrepublic.com/blog/it-security/the-cia-triad/.

[19] See James R. Clapper, Statement for the Record Worldwide Threat Assessment of the US Intelligence Community, SENATE ARMED SERVICES COMMITTEE (February 9, 2016), https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf (where "Cyber and Technology" and "Terrorism" feature as the first and second top priorities, respectively).

[20] See also Susan Landau, The National-Security Needs for Ubiquitous Encryption, in Matt Olsen et al., Don't Panic: Making Process on the "Going Dark"

Debate, Appendix A: Individual Statements from Signatories 1-3 BERKMAN CENTER FOR INTERNET AND SOCIETY AT HARVARD UNIVERSITY (February 1, 2016), https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

[21] Giuseppe Macri, Comey on Encryption and Criminals 'Going Dark': 'We're Not Making it Up,' INSIDE SOURCES (September 10, 2015), http://www.insidesources.com/nsa-cia-fbi-and-dia-heads-warn-congress-about-encryption-future-cyberattacks/.

[22] See Gallagher supra note 7; Harold Abelson et al., Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications, MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY TECHNICAL REPORT (July 6, 2015), https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf; Eric Geller, A Complete Guide to the New 'Crypto Wars, DAILY DOT (last updated May 5, 2016), http://www.dailydot.com/layer8/encryption-crypto-wars-backdoors-timeline-security-privacy/.

[23] See Gallagher supra note 7.

[24] See Harold Abelson et al., The Risks of Key Recovery, Key Escrow and Trusted Third-Party Encryption: A Report by an Ad Hoc Group of Cryptographers and Computer Scientists, 3 DIGITAL ISSUES 1 (June 1998).

[25] See Abelson et al. supra note 22.

[26] For criticism of various European proposals promoting technological sovereignty, see Mirko Hohmann et al., Technological Sovereignty: Missing the Point? An Analysis of European Proposals after June 5, 2013, GLOBAL PUBLIC POLICY INSTITUTE (November 24, 2014), http://www.gppi.net/publications/global-internet-politics/article/technological-sovereignty-missing-the-point/.

[27] See Freedom of the Press Foundation, Donate to Support Encryption Tools for Journalists (last accessed August 15, 2016), https://freedom.press/bundle/encryption-tools-journalists (describing the protection of secure communication channels as "one of the biggest press freedom challenges in the 21st Century").

[28] See Beats, Rhymes & Relief et al., Letter Re Apple v. FBI (March 3, 2016), available at https://www.apple.com/pr/pdf/Beats_Rhymes_Relief_Center_for_Media_Justice_The_Gathering_for_Justice_Justice_League_NYC_Opal_Tometi_and_Shaun_King.pdf (urging the judge presiding over the Apple v. FBI case "to consider the dire implications for free speech and civil liberties if the FBI is permitted to force Apple to create technology to serve its investigatory purposes. The FBI's historically questionable surveillance procedures do not bode well for a precedent that allows the agency universal access to private smartphone data"). See also Jenna McLaughlin, The FBI Vs. Apple Debate Just Got Less White, THE INTERCEPT (March 8, 2016), https://theintercept.com/2016/03/08/the-fbi-vs-apple-debate-just-got-less-white/ (describing the opposition of racial justice activists against weakening encryption standards).

[29] Micah Lee, Ed Snowden Taught Me to Smuggle Secrets Past Incredible Danger. Now I Teach You, THE INTERCEPT (October 28, 2014), https://theintercept.com/2014/10/28/smuggling-snowden-secrets/ (demonstrating that encrypted communications played an integral role in Edward Snowden's whistleblowing efforts).

[30] See Mark Latonero, Refugees' New Infrastructure for Movement: A Digital Passage, DATA & SOCIETY (February 1, 2016), https://points.datasociety.net/refugees-new-infrastructure-for-movement-d31c3ab53b20#.3t3pctf9k (arguing that "[p]hones, social media, mobile apps, online maps, instant messaging, translation websites, wire money transfers, cell phone charging stations, and Wi-Fi hotspots have created a new infrastructure for movement as critical as roads or railways"). See also Paula Kift and Mark Latonero, On Digital Passageways and Borders: Refugees and the New Infrastructure for Movement and Control, talk at DATA & SOCIETY (May 12, 2016), http://datasociety.net/events/databite-no-80-mark-latonero-paula-kift/ (arguing that the same digital technologies refugees have come to depend upon could just as easily be exploited, by public and private actors alike, for surveillance and control).

[31] See In re Order Requiring Apple supra note 1 at 33, FN 28 (pointing out that, "[j]ust as the criminal Feng has done, the United States government has chosen to entrust extremely sensitive communications and secret documents – including those of many of the prosecutors and judges who work in this court – to the passcode protections and other robust data security measures available on a variety of Apple devices. That observation does not mean Apple should have any greater or lesser obligation, as a matter of law or morality, to accede to the demands of law enforcement agencies. But it does highlight the proposition that forcing Apple to compromise the data security measures it offers its customers may adversely affect many who rely on such technology for purposes the government would endorse").

[32] Id.

[33] THE SOPRANOS, "Walk Like a Man," Season 6, Episode 17.

[34] See Swire supra note 8.

[35] See Olsen et al. supra note 20 at 3 (arguing that "[m]etadata is not encrypted, and the vast majority is likely to remain so"); see also ACLU v. Clapper, Case No. 13-cv-03994, Declaration of Edward Felten 11 (S.D.N.Y. 2013) (arguing that "it is practically impossible for individuals to avoid leaving a metadata trail when engaging in real-time communications, such as telephone calls or Internet voice chats"); see also Paula Kift and Helen Nissenbaum, Metadata in Context: An Ontological and Normative Analysis of the NSA's Bulk Telephony Metadata Collection Program, 13 I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY (forthcoming) (arguing that changes in the social and technological environment have vastly increased the revelatory power of metadata).

[36] See Olsen et al. supra note 20 at 10 (pointing out that "[c]urrent company business models discourage implementation of end-to-end encryption and other technological impediments to company, and therefore government, access").

[37] See Apple supra note 13 (explicitly responding to the Crypto Wars by claiming that "Apple has never worked with any government agency from any country to create a 'backdoor' in any of our products or services. We have also never allowed any government access to our servers. And we never will").

[38] See Kim Zetter, The FBI Drops its Case Against Apple After Finding a Way into that iPhone, WIRED (March 28, 2016).

[39] See BBC supra note 4.

[40] See BBC supra note 5.

[41] See Alyssa J. Rubin, Lawmakers in France Move to Vastly Expand Surveillance, NEW YORK TIMES (May 5, 2016), http://www.nytimes.com/2015/05/06/world/europe/french-legislators-approve-sweeping-intelligence-bill.html.

[42] See MOROZOV supra note 12.

[43] Joshua Hersh, What to Do About Brussels, NEW REPUBLIC (March 23, 2016), https://newrepublic.com/article/131918/brussels.

[44] See Ellis et al. supra note 9.

[45] See Rubin et al. supra note 10.

[46] See Graham-Harrison et al. supra note 11.

[47] See Benedict Carey, Mass Killings May Have Created Contagion, Feeding on Itself, NEW YORK TIMES (July 26, 2016), http://www.nytimes.com/2016/07/27/science/mass-killings-contagion-copycat.html?rref=collection%2Fnewseventcollection%2Fattacks-in-paris (arguing that "public, widely covered rampage killings [may] have led to a kind of contagion, prompting a small number of people with strong personal grievances and scant political ideology to mine previous attacks for both methods and potential targets to express their legal anger and despair").

[48] See Malcolm Gladwell, Thresholds of Violence, NEW YORKER (October 29, 2015), http://www.newyorker.com/magazine/2015/10/19/thresholds-of-violence (citing Stanford sociologist Mark Granovetter's theory of thresholds in the context of mass shootings in the United States).

[49] See also Ramzi Kassem, France's Real State of Emergency, NEW YORK TIMES (August 4, 2016), http://www.nytimes.com/2016/08/05/opinion/frances-real-state-of-emergency.html?smid=pl-share&_r=0 (arguing that, "[r]ather than extending a state of emergency that serves only to further marginalize them, the French government should address the root causes of alienation among its minority communities").

09

[1] Section 70, information technology Act, 2000

[2] Department of Electronics and Information Technology, Notification No. 9(16)/2004-EC http://meity.gov.in/sites/upload_files/dit/files/S_O_18(E).pdf

[3] National Critical Information Infrastructure Protection Centre, Sectors in NCIIPC, https://nciipc.gov.in/?p=sector (Accessed September 1, 2016)

[4] Guidelines for protection of CII Version 1.0, June 2013

[5] National Critical Information Infrastructure Protection Centre, Functions and Duties, https://nciipc.gov.in/?p=function (Accessed September 1, 2016)

[6] Ibid

[7] The appropriate government authority can be the federal or the state government, depending on the location of the CII. So far the only two systems identified by NCIIPC as CII has been notified by the federal government. NCIIPC is examining the efficacy of notifying CII through state governments, where appropriate.

[8] The notification for both these systems were notified by the Government of India earlier this year

[9] As articulated in the Functions and Duties of NCIIPC, Supra Note 5

[10] Title II—Information Analysis And Infrastructure Protection https://www.dhs.gov/sites/default/files/publications/CII-Act_508.pdf (Accessed September 1, 2016)

10

[1] Accenture, "Narrowing the Gap," https://www.accenture.com/in-en/gender-equality-research-2016

[2] Internet Live Stats, "India Internet User," http://www.internetlivestats.com/internet-users/india/ (Accessed on August 8, 2016)

[3] Shaili Chopra, With gender parity India's economic growth can get a boost by 27%, DNA (August 15, 2016) http://www.dnaindia.com/money/report-celebrating-india-s-independence-with-women-taking-the-lead-2245164.

[4] Sadaf Vasgare, From heading PepsiCo to the State Bank of India, these women don't only rule their homes but the boardrooms of some leading companies, DNA (May 8, 2016) http://www.dnaindia.com/money/report-five-powerful-indian-mothers-in-business-2209997.

[5] Indo-Asian News Service, Over 1.7 Billion Women in Emerging Economies Do Not Own Mobiles Phones: GSMA, NDTV GADGETS (March 4, 2015) http://gadgets.ndtv.com/mobiles/news/over-17-billion-women-in-emerging-economies-do-not-own-mobiles-phones-gsma-667123

[6] Anja Kovacs, Richa Kaul Padte and Shobha SV, 'Don't Let it Stand!' An Exploratory Study of Women and Verbal Online Abuse in India, Internet Democracy Project , April 2013, https://internetdemocracy.in/wp-content/uploads/2013/12/Internet-Democracy-Project-Women-and-Online-Abuse.pdf

7 All India Report of Sixth Economic Census, Government of India, 2012, http://mospi.nic.in/Mospi_New/upload/census_2012/AIR6EC_main.html

11

1 Le Bon, Gustave. [1895] 2002. The Crowd: A Study of the Popular Mind. Mineola, New York: Dover Publications.

2 Austin, John L. 1962. How to Do Things with Words. Oxford; Clarendon Press.

3 Hume, David. [1739] 2003. A Treatise of Human Nature. Mineola, New York: Dover Publications.

12

1 Section 4(1), The Cinematograph Act, 1952 states that "Any person desiring to exhibit any film shall in the prescribed manner make an application to the Board for a certificate in respect thereof."

2 See Section 5B, The Cinematograph Act, 1952. This language has been borrowed from Article 19 (2) of the Constitution of India which imposes reasonable restrictions on freedom of expression.

3 Rule 2 (iii), the Cinematograph (Certification) Rules, 1983: "applicant" means a person applying for certification of a film for public exhibition under section 4.

4 Super Cassettes Industries v. Central Board for Film Certification, W.P.(C) No. 2543 of 2007

5 [Draft] Cinematograph Bill, 2013, available at http://www.prsindia.org/uploads/media/draft/Draft%20Cinematograph%20Bill,%202013-.pdf

6 Section 2(c), the Cable Television Network (Regulation) Act, 1995 states that "Cable television network is a system of closed transmission paths and associated signal generation, control and distribution equipment, designed to provide cable service for reception by multiple subscribers."

7 Guidelines For Provisioning of Internet Protocol Television (IPTV) Services, 2006 issued by Ministry of Information and Broadcasting

8 Unified License Agreement, Chapter VIII, Provision of IPTV Service, Clause 5.1(d) - The provisions of Programme code and Advertisement code as provided in Cable Television Network (Regulation) Act 1995 and Rules there under shall be applicable.... Since the Licensee will be providing this content, the Licensee shall be responsible for ensuring compliance to the codes with respect to such content. In addition to this, such LICENSEEs will also be bound by various Acts, instructions, directions, guidelines issued by the Central Government from time to time to regulate the contents. 5.1(e) If the contents are being sourced from

content providers other than Licensee, then it will be the responsibility of Licensee to ensure that their agreements with such content providers contain appropriate clauses to ensure prior compliance with the Programme and Advertisement Codes and other relevant Indian laws, civil and criminal, regarding content.

[9] Rule 26, Cinematograph (Certification) Rules, 1983

[10] Raghav Ohri, Bad news for movie buffs! Censored parts of films to stay out of internet, ET TECH (MARCH 03, 2016) http://tech.economictimes.indiatimes.com/news/internet/bad-news-for-movie-buffs-censored-parts-of-films-to-stay-out-of-internet/51233972

AUTHORS

Adam Segal

Adam Segal is the Maurice R. Greenberg senior fellow for China studies and director of the Program on Digital and Cyberspace Policy at the Council on Foreign Relations (CFR). An expert on security issues, technology development, and Chinese domestic and foreign policy, Dr. Segal was the project director for the CFR-sponsored Independent Task Force report Defending an Open, Global, Secure, and Resilient Internet.

Alexander Seger

Alexander Seger has been with the Council of Europe (Strasbourg, France) since 1999. He is Executive Secretary of the Committee of the Parties to the Budapest Convention on Cybercrime and heading the Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest, Romania, which is responsible for global capacity building on cybercrime.Before 1999, he was with what now is the United Nations Office on Drugs and Crime in Vienna/Austria, Laos and Pakistan. Alexander Seger is from Germany and holds a PhD in political science, law and social anthropology after studies in Heidelberg, Bordeaux and Bonn.

Arun Mohan Sukumar

Arun heads ORF's Cyber Initiative and is Co-chair, CyFy. He is a lawyer by training, educated at NALSAR and the Fletcher School of Law and Diplomacy, Tufts University. He has served on the editorial board of The Hindu, as a writer on law and foreign policy. Arun also serves as the Vice Chair of the Asia Pacific Regional Internet Governance Forum.

Bertrand de la Chapelle

Bertrand de la Chapelle is the co-founder and Director of the Internet & Jurisdiction Project, a global multi-stakeholder dialogue process launched in 2012 to address the tension between the cross-border nature of the Internet and the diversity of national jurisdictions. Bertrand was previously a Director on the ICANN Board (2010-2013), France's Thematic Ambassador and Special Envoy for the Information Society (2006-2010) and an active participant in the WSIS process (2002-2005).

Caitriona Heinl

Caitríona Heinl joined the Centre of Excellence for National Security at RSIS as Research Fellow responsible for cyber-related matters in October 2012. She

previously led the Justice and Home Affairs policy group and Justice Steering Committee at the Institute of International and European Affairs (IIEA), Ireland. Caitríona was a legal researcher on a European Commission study for the then Directorate- General Justice, Liberty and Security on non- legislative measures to prevent the distribution of online violent radical content. Caitríona qualified as a U.K. trained Solicitor (non- practising) and she is admitted as an Attorney- at-Law in New York.

Catalina Ruiz Navarro

Catalina is a Weekly op-ed columnist at El Espectador and El Heraldo in Colombia, and Sin Embargo in MØxico. She is the Executive Director and Founder of Hoja Blanca magazine-NGO (HojaBlanca.net). She specialises in journalism with perspectives on gender, human rights and culture. She is a professor of Opinion Journalism at the School of Communications at the Pontificia Universidad Javeriana and of Digital Journalism at Jorge Tadeo Lozano University, both in BogotÆ until 2013.

Dennis Broeders

Prof. Dr. Dennis Broeders is a senior research fellow at the Dutch Scientific Council for Government Policy (WRR) and professor of Technology and Society at the Erasmus University Rotterdam. He recently published The public core of the internet: towards a new international agenda for internet governance advising on foreign policy and internet governance.

Isabel Skierka

Isabel Skierka is a researcher on industrial cybersecurity and digital policy at the Digital Society Institute (DSI) at the European School for Management and Technology in Berlin. She is also a non-resident fellow with the Global Public Policy Institute (GPPi) in Berlin and serves as a co-chair of the Internet Governance Forum Germany's steering committee. Prior to joining the DSI, Isabel worked with GPPi, NATO, and the European Commission. She holds a master's degree from King's College London's War Studies Department and a bachelor's degree from Maastricht University.

Japreet Grewal

Japreet is a Programme Officer at the Centre for Internet and Society, Bangalore. She works on issues surrounding technology and regulation with emphasis on issues affecting freedom of expression and intermediary liability at the domestic and international levels under the Internet Governance and Freedom of Expression Project at CIS. She has previously worked at Amarchand Mangaldas & Suresh A Shroff, New Delhi and graduated in 2013 from Gujarat National Law University with a degree in law.

Paul Fehlinger

Paul Fehlinger is the co-founder and Manager of the Internet & Jurisdiction Project. He is actively engaged in global Internet fora, including as a speaker at the

UN Internet Governance Forum, OECD, Council of Europe or EuroDIG. Paul was appointed to the Advisory Network of the Global Commission on Internet Governance, to the Working Group on Rule of Law of the Freedom Online Coalition and as a participant in the Council of Europe Committee of Experts on Cross-border Flow of Internet Traffic and Internet Freedom. He holds a Master in International Relations from Sciences Po Paris, where he specialized in Internet politics and new modes of global governance.

Paula Kift

Paula Kift is a doctoral student in the Department of Media, Culture, and Communication at NYU. She is interested in privacy, migration, transborder data flows, and current and emerging technologies of border control. Paula earned a BA summa cum laude from Princeton University in 2012, where she studied French Literature and Political Science as a major, and Near Eastern Studies and European Cultural Studies as minors. During her undergraduate studies, she completed exchange semesters at the universities of Barcelona and Paris. In 2014 Paula received a master's degree in public policy from the Hertie School of Governance in Berlin. Previously she worked as a research assistant at the Alexander von Humboldt Institute for Internet and Society (HIIG) and at the Global Public Policy Institute (GPPi) in Berlin. She is a member of the GPPi Circle of Friends and an Associate Member of the American Council on Germany (ACG).

Shaili Chopra

Shaili Chopra is an award winning business news Presenter and Editor with prime time stints in India's largest television networks NDTV and ETNow. She just finished writing her third book - When I Was 25 where she captures the essence of leaders in their 20s. She also writes for DNA and Mint. She was recently awarded the Ramnath Goenka Award for Excellence in Journalism. She is considered among the 30 witty and intelligent women to follow on Twitter by CNN IBN and in 2010, FICCI awarded her the Young Women's Achiever Award for contribution to media.

Saikat Datta

Saikat Datta is the former Editor (National Security) with the Hindustan Times, Delhi. He has been a journalist for over 19 years, writing on the intersection between government, policy, security, intelligence and defence. His work has been awarded the International Press Institute award, the National RTI award for journalism and the Jagan Phadnis Memorial award for investigative journalism. He has also authored a book on the history and the future of India's Special Forces. He is currently working on several cyber security and risk assessment and mitigation projects for Global Corporate Security (GCS).

Global Policy is an innovative and interdisciplinary journal and an online hub bringing together world class academics and leading practitioners to analyse both public and private solutions to global problems and issues. It focuses on understanding globally relevant risks and collective action problems; policy challenges that have global impact; and competing and converging discourses about global risks and policy responses. It also includes case studies of policy with clear lessons for other countries and regions; how policy responses, politics and institutions interrelate at the global level; and the conceptual, theoretical and methodological innovations needed to explain and develop policy in these areas.
www.globalpolicyjournal.com

Observer Research Foundation (ORF) is a not-for-profit public policy think tank that aims to influence policy formulation for building a strong and prosperous India in a globalised world. It pursues these goals by providing informed and productive inputs, in-depth research and stimulating discussions on a wide range of issues of national and international significance. Some key areas of research include international relations, security affairs, politics and governance, resource management, and economy and development. ORF is supported in its mission by a cross-section of India's leading public figures, academics and business leaders. Headquartered in New Delhi, it has chapters in Chennai, Mumbai and Kolkata.
www.orfonline.org

Last year saw an unprecedented debate on the role of cyber norms, and how non-binding, "soft" guidelines and statements of intent by governments, business and civil society can shape the conduct of state and non-state actors on the internet. This year, Digital Debates dives deep into the conception, articulation and content of these norms in an attempt to crystal gaze the future of cyberspace. This 10th volume in the GP-ORF series, the third edition of Digital Debates, brings to the fore some of the most important policy considerations affecting cyberspace. Cyber policy practitioners from around the world discuss issues including online gender disparity; transnational jurisdiction; the conundrum of privacy and security; and cyber diplomacy. Digital Debates is an integral part of CyFy: The India Conference on Cyber Security and Internet Governance,the annual internet policy conference organised by the Observer Research Foundation. CyFy 2015 was held from October 14-16 in New Delhi, India.