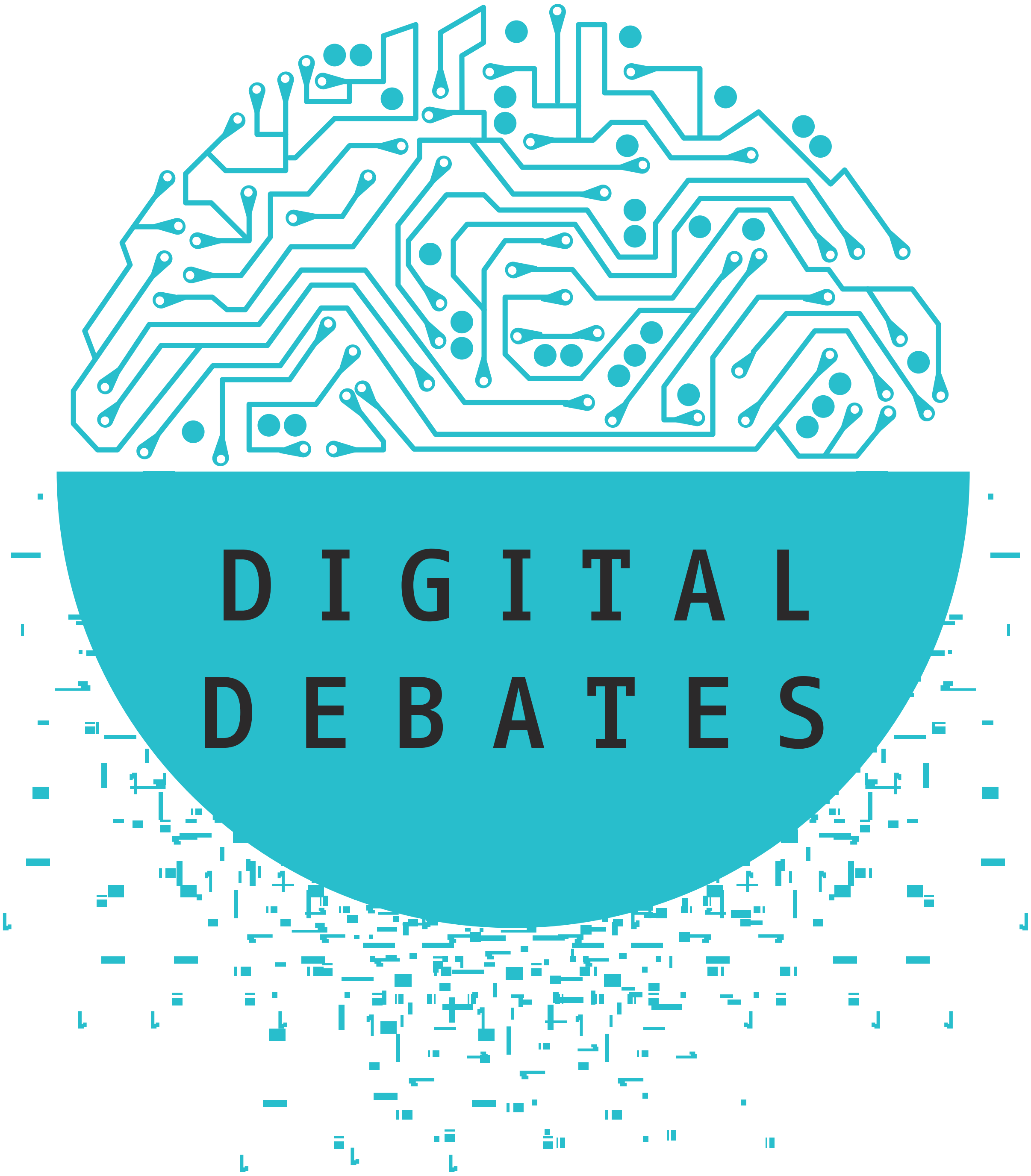
DIGITAL DEBATES



CYFY JOURNAL: VOLUME 1 (2013)
/
OCTOBER 2014

CYFY
THE INDIA CONFERENCE ON CYBER
SECURITY AND CYBER GOVERNANCE

OBSERVER RESEARCH FOUNDATION
25

655 DIGITAL DEBATES

A SYMPOSIUM ON CREATING AN ARCHITECTURE FOR REGULATING CYBERSPACE

SYMPOSIUM PARTICIPANTS

Originally published in Seminar Magazine, Issue 655, 'Digital Debates', published in March 2014

seminar

SAMIR SARAN

THE PROBLEM

THE Snowden affair and the vocal debate on surveillance and cyber espionage have redefined the mostly benign and attractive imagination of the Internet. This medium, which has connected the world like never before, is now witnessing a growing contest among nations. If not addressed and managed, a divisive debate on the control and management of the digital global commons, could not only undermine the huge gains that have accrued from interconnectedness, but might well become a basis for conflict and instability in the real world.

The stakes are high. The idea of the 'global village', the efforts to create a global economy and emerging global digital marketplace, are all likely to be impacted if nations and communities do not find it within themselves to agree to norms and laws that would apply to this realm. The process of discovering the 'rules for the road' is highly contentious. Not only is an 'international digital treaty' unlikely in the near future, the world cannot even agree to who should be negotiating such an arrangement. Yet, this debate must take place with earnestness if common ground is to be discovered at the earliest.

It is crucial to strengthen such a debate, to bring together perspectives from a range of countries and sectors on key facets of the digital discourse – ranging from national priorities and strategies to international treaty frameworks, the role of the private sector to issues such as individual privacy and freedom of expression.

At the outset, we must ponder over some larger issues that are shaping the current global and domestic conversations and inquiries in the digital domain. These can be broadly captured within a few meta-narratives, also key to discerning how a digital India develops, how a vibrant digital society governs itself, and how India must seek to interact with the world in this digital century.

The first narrative is one of development and security. It is a debate on how we create policies and conditions that would allow for the rapid development and spread of cyber infrastructure in the country. On how we could develop tariff and cost regimes that would allow and encourage people to connect to and with it. On the variety of social and economic activities we seek to conduct over the medium and, therefore, the nature and form of regulation and security that must align these networks.

Our decisions on some of these would affect pricing and business models, the rate of penetration and growth of connectivity, our approach to intellectual property rights, and the nature of access available on the Internet to those residing in different economic and social classes. In a number of recent statements and policy pronouncements, the Government of India has indicated its preference to use the digital medium as a means of delivering governance and social services to its citizens. Cash transfers, correspondence and approvals, banking and insurance, health and education services, are all likely to ride on the digital last mile. Therefore, 'digital access to all' must be a national imperative.

India's experience with the telecommunication sector tells us that 'access' closely follows 'price of service' and proliferation of the Internet and IT infrastructure would be dependent on 'price points' that are unprecedented. Connecting 'another billion' citizens to the Internet in the coming decade or two would, therefore, be influenced by business models, tariff regimes, content generation and entrepreneurship at the proverbial 'bottom of the pyramid'.

India's contemporary experience with Internet services also demonstrates that penetration growth is a function of services and content that is offered to the user. It is an open secret that pirated movies, music and entertainment content are significant drivers of Internet penetration. Alongside, applications that assist farmers and SMEs and offer health services and a variety of education and skills also encourage users to connect to the Internet. Content generation, for the potentially huge Indian user base, offers great opportunity with its unique price specificity.

This discussion invariably throws up some interesting posers. While it would be impossible to capture all of them, a few merit attention. The first must be the fundamental tension between the affordability of service and best in class technology and security. We need to achieve both, as business, governance and social security would ride on this medium. The other would be the approach to content generation and intellectual property rights. While India must seek to encourage low cost content creation that caters to its myriad needs, can this be done while it allows (though weak IPR regimes) pirated material that is so essential to rapid proliferation of the Internet? We must ask how much regulation and legislation is ideal before it encroaches on the fluid nature of the Internet, a feature that makes the medium attractive in the first instance. Finally, given the degree of global interconnectedness, would India be able to make these decisions independent of external pressures and global conventions?

This brings us to the second narrative – India's engagement with the world on Internet governance and cyber security. This engagement will have a compelling impact on its domestic socio-economic development and on its ability to secure prosperity for its people from the digital marketplace.

India is one of the biggest beneficiaries of the IT and communications revolution with roughly 25% of India's GDP growth over the past two decades having been created in the IT and ITES sector. There is little doubt that a larger share of India's future growth will originate from or be dependent on this digital medium. Therefore, India must be at the Internet governance high table when agreement is reached on managing this most vital global commons. Would India shed the reticence, characteristic of its 20th century approach to multilateralism and reimagine itself as part of the 'global management' with attendant responsibility and rights? Or will the perceived virtuosity of nonalignment continue to see India lead the global outliers and minority stakeholders in this global governance debate?

How this unfolds will be crucial. Will India be oppositional, critiquing the major powers for their unilateralism and interest based approaches, or will India be propositional and articulate its own interests and negotiate the space and role that it must have, representing as it would (in the days ahead) the largest bloc of Internet users from a largely liberal and vibrantly democratic nation?

It must also be understood that while the world sees a significant role for India at this juncture on Internet governance and security, it will not wait beyond a point. The major powers – US, Russia, China and EU – are all engaging and negotiating the rules for the road with each other and with a larger group of nations. India is a party at some of these conversations and not at others. Trade talks, climate negotiations and other multilateral experiences tell us that 'democracy' within global governance is inefficient and overrated. The relative success of TRIPS and FTAs over a global trading arrangement and the predominance of the arms control architecture of the 20th century, devised between the US and Soviet Union, are all indicative of how a future Internet governance arrangement may emerge. Will it be an arrangement shaped by the conversations among the 'Big 3' (Russia, China and the US), or will it be relatively more inclusive and take into account perspectives from a larger set of countries? Will there be a 'gridlock' or will these countries manage to agree to sets of norms that will allow the Internet to remain a global commons? Any which way India would need to find the means and resources to be an effective contributor to any new arrangement and find its place on the high table.

This discussion on global governance leads us to the third meta-narrative that engages most thinkers and practitioners today – who should engage on the subject and with whom? Unlike arms control treaties such as SALT and the NPT, trade treaties such as GATT and the WTO, or international treaties in force or being negotiated such as the space code and laws of the seas, the Internet involves and affects each one of us individually more than it does states. Each one of us is a contributor and beneficiary, and each one of our actions has the ability to influence the entire cyber sphere.

Therefore, the central question that arises is whether the 'nation state' is the most inclusive and efficient interlocutor on Internet governance and cyber security? This leads to discussions on the tension between multi-stakeholderism (the participation of individuals, academics, citizen groups and non-governmental organizations in the debate) against multilateralism (a largely state to state debate that characterized the architecture of the 20th century). Can they coexist? Can they be aligned constructively? And if so, how?

For instance, should a nation state conduct an internal debate within itself, create a domestic consensus, and (only) then represent this multi-stakeholder proposition at the global forums? Alternatively, should various stakeholders communicate with each other across national boundaries and at international arenas? The former is somewhat more ordered while the latter is far more cumbersome but also more democratic. This issue currently sees different treatment in different countries. More developed democracies see merit in letting their NGOs and corporations into the debate and are in fact clever in using these voices in order to secure national interest. Other countries including India are far more reluctant to include corporations and citizens in governance conversations. While we can debate how best to include views and voices from the private sector and the private citizen, there is no doubt that security and stability of the Internet would be largely dependent on the participation of all stakeholders, particularly the private sector that owns and operates cyber infrastructure.

This brings us to the fourth issue that must be debated in detail – the role of the private sector. On one hand they are the primary service providers and owners of much of the critical infrastructure; on the other they have a sizable vested interest. How may one give the private sector weight in Internet governance decisions without shifting the balance of the narrative away from the users and governments will be a central enquiry of our times.

Banks, for example, want a secure and heavily regulated Internet, which would allow them both reach of this medium and keep transactions safe and secure. Security companies would want to perpetuate a certain appreciation of the Internet architecture that maximizes their ability to leverage the Internet as a business opportunity. On the other hand a plethora of companies, start-ups and SMEs, that see immense opportunity in the fluidity and reach of the Internet, would like to see cyberspace remain loosely regulated, open and free.

What then is the private sector voice to heed? Indeed, should they be on the table or should we be guarded in our approach as we include them in the debate? Balancing private sector participation in governance decisions, while protecting the interests of small companies and individuals, will be a key consideration for most governments.

Engaging with these four 'big issues' is vital. It is even more important for countries like India where the infrastructure and business models are still being developed. There are no clear and globally acceptable positions and propositions that have emerged. And most questions still remain unanswered. Let us look at two sets of questions that would be most critical to any global and domestic policy arrangement.

First, how do we reconcile sovereign constitutional positions on issues such as freedom of expression, free speech, political jurisdiction and state capacity and intervention to arrive at a formulation that works across a medium that is not restricted by territoriality and borders? Is this achievable? And in the absence of such 'universalism', do we face the prospect of the world, as discussed earlier, being railroaded down a path decided by a few?

The second, more fundamental question emanates from the rapid evolution of the digital sphere. This is bringing into question traditional laws, norms, means of communication Andmodesà and modes of trade and commerce. The fundamental assumptions of the previous era are being challenged and changed by the digital (dis)order. Would we now be required to develop legal frameworks sui generis to accommodate new realities? Will nations have to become far more tolerant of expression than their individual constitutions allow? Will notions of extraterritoriality, jurisdiction and sovereignty have to be radically re-imagined? Or will an obstinate defence of the old paradigm lead to a polarization of the web, in effect turning the world wide web into the world divide web, where traditions and ossified power structures lead to a balkanization of the cyber-whole? Then, will the future of the web be one of multiple gateways and access points?

This possibility already looms. The great firewall of China seems more or less effective. Despite some breaches it has succeeded in 'islanding' China and given authorities the ability to clamp down quickly and efficiently. Digital China, therefore, engages with the outside world on a 'need to' and 'convenient to' basis. Is that the future of the Internet then? Or can we recast some of the global assumptions that have defined the realist world of the 20th century to accommodate the digital world of the 21st century? Is a new United Nations of digital media possible? Who would be in its General Assembly and who in its Security Council? Or would the very use of the word 'nation' doom it to be stillborn?

This issue of Seminar does not offer all the answers, but it does raise a series of questions and provides analysis that will allow us all to engage more deeply with this most important element of our contemporary lives.

* Several papers in this issue were presented and discussed at 'CyFy 2013' – The India Conference on Cyber Security and Internet Governance' – hosted by the Observer Research Foundation and Federation of Indian Chambers of Commerce and Industry.

R. SWAMINATHAN

A NEW PARADIGM FOR CYBER SECURITY

THE Internet is more a story of chips and hardware than it is about social media, search engines and algorithms. Fundamental shifts in socio-technical landscapes of the Internet can be traced back to a few technologies that intersect both military and civilian domains, like how specific chips to utilize and amplify the microwave frequencies in 300 MHz-300 GHz band created the converged Internet of today. Arguably the most influential tipping point has been the development and proliferation of the Gallium Arsenide Microwave Monolithic Integrated Circuit (GaAs MMIC).[1] Like most things associated with the foundational architecture of Internet, the history of GaAs MMIC is also rooted in the imperatives of defence doctrines and the Cold War race of countries to achieve mastery over strategic technologies.

The Cold War is filled with fascinating side stories of the constant battle for dominance between western engineers and their Soviet counterparts. One such story involved the tug-of-war to deliver the longest ranging multimode radars for Beyond Visual Range (BVR) aerial combat. The Soviets took an early lead in the 1960s by developing the massive RP-25 Smerch[2] for the interceptor MiG-25 (NATO codename: Foxbat). The radar earned a well deserved reputation for 'burning' through any western electronic counter measures of the day. By early 1970s the American AN/AWG-9 radar, originally developed for the navalized F-111B, and the F-15A's APG-63 radar had neutralized the Soviet advantage. The Russians promptly snatched it back in the early 1980s with the N007 Zaslon developed specifically for the MiG-31 (Nato codename: Foxhound), a fighter-interceptor that has its own fascinating back story of intrigue, secrecy and defection.[3]

It is within this historical context that the development of the GaAs MMIC for the United States Department of Defence (DoD) has to be located. Gallium Arsenide, unlike silicon, is a difficult material to work with for the manufacture of integrated circuits and chips, but the Americans, and subsequently the Europeans, achieved a rare mastery over it. GaAs MMIC are particularly useful at ultra-high radio frequencies, fast electronic switching and weak signal amplification applications. They do all this while generating less noise than most other types of semiconductor components. Militarily, it gave the West a qualitative edge over its competitors by having almost a decade's lead over the technologies, like the Gallium Nitride (GaN) High Electron Mobility Transistor (HEMT) for X-band, associated with Active Electronically Scanned Array (AESA) radar.

But it was the imperatives of the civilian communications market that literally forced open the cloistered club of niche microwave technologies of GaAs MMIC and GaNchips. All modern communication is based on microwave technologies, and the post-1980s generational maturation of cellular phone technologies and the subsequent commonalities between cellular communication, Internet, especially wireless fidelity (Wi-Fi), and digital access devices necessitated the mass production of these chips. Ironically, the availability of Twitter and Facebook on mobile phones can directly be linked to this rivalry between the American and Soviet military establishments. As a side note, the Chinese and Indian scientific community also owe much of their success in developing civilian and defence communication capabilities to the 'democratization' of chips brought about by market forces.

Some of the most critical technical advances in integrated circuits may not have taken place at all had it not been for the Advanced Research Projects Agency Network (ARPANET), the world's first operational packet switching network and the progenitor of what is currently known as the Internet. The network was initially funded by the Advanced Research Projects Agency (ARPA, later DARPA)[4] within the US Department of Defence (DoD) for use by its projects at universities and research laboratories. The packet switching of the ARPANET was based on designs by British scientists Donald Davies and Lawrence Roberts of the Lincoln Laboratory.[5]

Packet switching is the crux of all modern communications, with protocols and security systems having evolved around it. If not for the concept of packet switching, William Crowther, who is best known as the father of gaming and co-creator of the Colossal Cave Adventure, would not have been able to work on implementing a distributed distance vector routing system for ARPANET. Without routing, there would have been no protocols (IPv4 and IPv6) for Internet, no concept of data transmission (bits and bytes), interoperable standards, databases, encryption and security: in short the entire primary and support ecosystems of cyberspace.

The foundations of these ecosystems are literally made up of trillions of chips. It is easy to underestimate the power of a chip, but consider this: a birthday card that plays a tune when opened has a chip that has more computing power than all of the Allied and Axis powers had in 1945.[6] An average smartphone has more computing muscle (a chip) in it than the NASA mission that put men on the moon in 1969; the power (a chip again) inside a Rs 15,000 play station is more than the 10 million dollar American super-computer Cray XMP 24 of the 1990s that was used by the military establishment to design nuclear weapons.

To round off the story of the GaAs MMIC, the Global Positioning System (GPS),[7] or any of its equivalents like the Russian Glosnass or the Chinese BeiDou, and the less-than-one-metre resolution satellite imagery commercially and freely available in Google applications would not have been possible without that particular chip. With chips getting faster, cheaper and smaller all the time, and getting embedded in the unlikeliest of inanimate and animate objects (from plastic cards, furniture, cars to birds, apes and human beings) lies the invisible circularity and interconnectedness of cyberspace. It is this same ecosystem that allows China to develop an open architecture JF-17[8] fighter plane in less than a decade with a million lines of code, transistors and chips freely available in the open market, just as it enables a Micromax to compete with proprietary systems like Apple and Samsung.

Yet the Internet cannot be defined as a singular entity. It is at best an amalgamation of historical and contemporary technological developments and equally, an ever-expanding and mutating landscape of articulations. Conventional frameworks of analyses focus exclusively on the articulatory frameworks, the social media for instance, and visible technological changes such as the convergence of computer and mobile phones.

In maintaining such a focus, the underlying, and by definition invisible, foundational interconnectedness of technologies, hardware and software, like the microwave frequencies, amplification algorithms and GaAs MMIC chips that link each visible technological development and mode of articulation, is either marginalized or completely ignored. Such frameworks create a self-perpetuating and reductive understanding of the Internet as a random and serendipitous territory of mutating articulatory coagulations. The underlying forces of production – real, concrete and physical – which should ideally and exclusively be defined as the cyberspace, a term that has ironically come to mean everything ephemeral, is either marginalized or amalgamated with the multiplicities of articulatory frameworks. The concept and praxis of cyber security is a particular victim of the specific narratives that emerge out of this reductive understanding.

There are three quixotic paradigms of cyber security. The first looks at cyber security as simply an issue of protection of specific digital devices against a malware or a virus. The second, which has two sides to it, either sees in cyber security a conspiratorial state-corporate elite meta-strategy, a sort of a hegemonic imperative of global market forces, to take control of society and polity, or conceives it as a necessary prerequisite of national security of an emerging technoglobal order. The third, of social construction of digital technology, while rightly identifying the human foundations of technology and focusing on the socio-technical relational dynamics of daily life, ends up conceptualizing cyber security as an institutional domain/concern better addressed by the state and market. These paradigms are derived from a larger body of academic and non-academic writing on technology.

In writings dealing with the socio-technical landscapes of daily life, the relational dynamics between digital technology and its multitude of spaces are conceptualized within frameworks architected by three dominant perspectives. None of these perspectives deal with the concept and praxis of cyber security as an integral component of daily life. The first perspective of substitution of human territoriality and place-based dynamics of life by digital technologies is derived from the spatial and territorial metaphors[9] used to visualize the abstract flow of electronic signals that are coded as information, representation and exchange.

The inherent technological determinism in the frameworks anchored to this perspective leads to narratives and discourses about the *apparent inevitability*[10] of technology and progress. Conceptually, technology is seen to acquire an agency of its own that is independent of the social relationships of power of daily life.[11] In such frameworks, digital technology is conceived and measured as a value neutral additive that has an impact where ‘time becomes instantaneous and space becomes unnecessary’.[12] Derived from these logical constructs of timespace compression is the narrative of transmission and transference of space where values, cultures, economies and entire human societies are seen to migrate into electronic spaces and seep into other lived spaces. As a corollary, security of the cyberspace is seen in personal territorial terms of ‘hacking, computer protection, antivirus software, bugs, fixes and patches.’

Nicholas Negroponte, Chairman Emeritus of the Massachusetts Institute of Technology (MIT) Media Lab, sums up the substitution and transference perspective best: ‘Digital living will include less and less dependence upon being in a specific place at a specific time, and the transmission of place itself will start to become possible. If I could really look out the electronic window of my living room in Boston and see the Alps, hear the cowbells, and smell the (digital) manure in summer, in a way I am very much in Switzerland.’[13]

The second perspective of simultaneous processes of evolution informing the relational dynamics of digital technology, human territoriality and space recognizes that the social production of material and digital spaces are inextricably linked.[14] The frameworks derived from this perspective suggest that these linked interactions are creating a complex set of articulation, engagement, contestation and negotiation that are constructing hybridized cultural representations which are co-located in material and digital spaces. The co-location enables the experiences of ‘de-realization and de-localization’ while allowing users to continue having ‘physical and localized existences’.[15]

This perspective by questioning the universalizing logic of virtual reality extends its reach to create a framework for the conceptualization of real virtuality where processes of the material productions of space ‘tap into digitally available resources of the world to enrich reality in real places’.[16] This ‘culture of real virtuality’[17] is experienced through new and integrated digital systems that capture lived reality, virtualize them by embedding an ordered logic and communicate them, creating an experience that is simultaneously real and digital.

Such co-located processes embody ‘complex global-local articulations between space of places and space of flows’ and digital ‘ordering of the urban’.[18] At a fundamental level, then, global circulation of money, information, capital and services is seen to require relatively ‘fixed’ telecommunication infrastructure (e.g., undersea fibre optic cables) and movement of labour and commodities requires relatively ‘fixed’ transportation infrastructure (e.g., railroads, container services) to link dispersed areas of production, consumption and exchange. Space therefore becomes an entity that needs to be scripted in order to be commanded and controlled in an international scale. Such a perspective constructs the concerns of cyber security in terms of maintaining the ‘continuity of information patterns’, protection of ‘economic systems of globalization’ and the creation of an ‘emergent scripted daily reality’.

One can actually trace the roots of this perspective to the cultural foundations of modernity that define modern capitalism. The inevitability of development is seen to be executed through the totalizing shifts of a secular technological utopia. Any social or environmental crisis of development, as a corollary of this discourse, is expected to be resolved by the application of technology. Explaining the self-perpetuating nature of the discourse of technologicaldeterminism, Hayles writes: ‘In a world bespoiled by overdevelopment, overpopulation and time-release environmental poisons, it's comforting to think that physical forms can recover their pristine purity by being reconstituted as informational patterns in a multidimensional computer space.’[19]

The third perspective takes the concept of co-evolution and co-articulation further to conceive digital technologies and their intermingling with spaces as a relational social construction. Such relational perspectives are broadly located within the actor-network theories[20] that emphasize how ‘bits and pieces; bodies and machines, and buildings, as well as texts, are associated together in attempts to build order.’[21] In this perspective, space, time and agency are never absolute. They are constantly defined and redefined through their relational dynamics. As a consequence, the frameworks that emerge from this perspective consider the virtual and lived space and spatiality created due to the intersecting mediation of digital technologies as ‘fragmented, divided and contested’.

Such socio-technical relationships of power link ‘local and nonlocal in intimate relational, reciprocal connections’.[22] The relational conceptualization of space and time has, in the last decade and half or so, influenced critical thinking on the intermeshing of technology in social geography, urban studies and social anthropology. Such relational frameworks allow for the construction of ‘multiple realities’[23] and experiential diversity that can be simultaneously anchored to fixed material means and modes of spatial production and mobile nodes of narratives and discourses.

Such a perspective of ‘multiple, fragmented and contested’ socio digital realities inadvertently marginalizes or ignores the concept of cyber security by co-locating it within the spaces of contestation. Cyber security, by extension, then becomes one more node of contestation. But cyber security by its very nature requires an integrated meta-narrative of *commonality.*

There is also another unintended, and arguably larger, reason for the marginalization of cyber security as a valid field of inquiry of social sciences. Theorizations of digital technology predominantly conceptualize it as a flat evolutionary landscape with a quantifiable and chartable linearity. Such unintended structuralism leads to a reductionist understanding of the unique trajectories of specific digital technologies. This results in digitalization inadvertently being configured as an overarching methodological and paradigmatic framework. In such frameworks the marginalized and simplified analytical focus on socio-technical discontinuities and departures within the landscape of digital technologies leads to an a priori epistemological architecting of digital technology as a monolithic entity.

The landscape of technology is as much a site of articulation, engagement, contestation and negotiation as its social counterpart. When the intersectional relational dynamics between digital technologies and physical and imagined spaces is traced using the methodological framework of a *flat* pervasive digitalization, only the hybridized representations of the articulations emerging from experiential diversity of multiple realities are prominently captured. But the technological specificities of the construction of particular nodes of intersection and its resultant socio-technical engagement with space and territoriality are marginalized or ignored. Without understanding the unique techno-structural architecture of specific nodes of intersections, the *spaces of flows* would always get configured with inherent relational asymmetries. As a result, digital technology is often reductively imagined as the worldwide web and its access devices.

The narratives and discourses emanating from such an imagination position themselves within the framework of sense and meaning created by the hybridized representations of technologically mediated cultural practices. Such a strictly manicured understanding is based on an earlier generation of constructed electronic spaces that were anchored in a relationship of coded dependency on the *fixed* telecommunications infrastructure for their means and modes of articulation, engagement and negotiation.

The mobility of such electronic spaces was measured through the transference of values, systems, and sometimes even the space itself, to another similarly constructed electronic realm. The mobility was ephemeral in nature, ceasing to exist once the coded structural logic of the dependency was changed. The relational dynamics between these electronic, physical and imagined spaces were configured in terms of virtualization of identities and communities, hybridization of representations derived from it and the *impact* of such cultural forms on the social landscape.

The relative fixity of a self-perpetuating and dependent set of physical interconnections between code and infrastructure and the limited technical capabilities of access devices architected a framework of constraints that modulated the intensity and power of the digitally mediated perceptual lenses. It was done through a system of exchange and transaction that was essentially based on verbal, written and audiovisual communication. Consequently, for instance, a Usenet evolved into a Facebook, but the essential communicative structure remained the same. A new generation of digital technologies – a suite – has emerged in the last decade that have nuanced and customized degrees of autonomy with the *fixed* telecommunications infrastructure.

This staggered autonomy, sometimes bordering on independence, has been configured by five intersecting technologies: infrastructure agnostic coding, rich pixilation display systems, storage, satellite geo-positioning and information and autonomous networked portability. The new suite, while spatially locating itself above the worldwide web, integrates itself selectively with the Internet for transmission, storage and replication. Each specific digital technology of this suite, like the CAD-CAM software, is an independent node by itself, always connected to the larger ecosystem of cyberspace, but not necessarily to the Internet. It also interacts, intersects and integrates with other digital technologies creating relational dynamics that construct an emergent *scripted* logic that define a perceptual reality of the social landscape.

Architected through continuous, simultaneous and seemingly autonomous processes of visual distance and visual granularity, it captures specific aspects of a multivocal social reality, segregates them into discrete units and stores and strings them together in an emergent asocial configuration that redefines notions of space, spatiality and territoriality in singular terms.

Consequently, for instance, a physical land use map of a city mediated through *scripted* layers of satellite images, street views and earth cams integrates a simultaneous distant, granular and segregated view. This reconstitutes the relational dynamics between physical and imagined spatiality and territoriality, creating an imaginary of an urbanity that is seen to be constituted by interchangeable and transformable Lego-like urban parts, an emergent artificial-asocial intelligence similar to the ones constructed by the electronic brains of networked military unmanned combat vehicles.

This *scripted* perceptual framework, over a period of time, informs the narratives, discourses and imaginaries of the institutions of state, market and civil society into one of configurable spaces. This leads to a set of articulations that augments processes of asocial spatiality, while creating new modes of social inclusion and exclusion. Existing asymmetries are also reconfigured, amplified and accentuated.

This emergent digitalization is fundamentally different from the earlier forms of digitalization in the manner in which it intersects and integrates with existing social relationships of power, shaping discourses that transcend institutional and non-institutional underpinnings. Such self-perpetuating autonomous discourses come together in a seemingly serendipitous manner creating an emergent intelligence[24] that is as ephemeral as it is lasting, as also acutely highlighting a need to paradigmatically mainstream cyber security as a subject of social enquiry.

Several conspiracy theorists believe that the US and Israel formally attacked Iran in June 2010 through the Stuxnet computer worm. There might be some heft to their belief, but it is still circumstantial at best. But if anyone needs a specific marker to advocate a new paradigm for understanding ubiquitous digitalization and the emergent cyber security thereof, the discovery of Stuxnet can be red flagged as the critical moment. When experts dug deeper to understand it, they found that the worm had a programmable logic controller (PLC) hidden in its root kit. It was a first in any virus or a worm.

A PLC changes the logical and sequencing structure of an infected programme or a machine. As they tumbled further into the hole, as Alice once did in a storybook, they discovered that the worm had a special fondness for the Supervisory Control and Data Acquisition (SCADA) systems of Siemens. These systems control and monitor specific industrial processes. This is where it becomes circumstantial with a number of ifs and buts.

In Iran, these proprietary systems do not run any ordinary industrial processes. They are at the heart of the uranium enrichment infrastructure across six locations in the country. By August, when the hole had been dug deep enough, Symantec found that 60 per cent of the infected computers across the world were in Iran. Kaspersky Lab came to the conclusion that such a sophisticated attack could have been conducted only with a 'nation-state's support'. American and Israeli officials were privately delighted at the disruption of the Iranian nuclear programme.

In the shadowy world of cyber attacks, a buzz did the rounds that Stuxnet was a joint US-Israeli attack called Operation Olympic Games started by former US President George W. Bush and expanded by the current incumbent Barack Obama. The retaliation – whispers claim it is from Iran – was from a virus called Shamoon that took out the administrative operations of the world's largest oil company Aramco. The Saudi-owned oil company is America's largest supplier. This is a warless war, and it can be speculated that it has not seen its end yet.[25]

The heart of any Siemens system, from uranium enrichment plants to smart automatic washing machines, is a PLC, as it is for any networked or non-networked system or a gadget that has an embedded artificial intelligence powered by a chip. A Stuxnet, then, can as easily infiltrate any individual's home. By extension, and looking into the future, it can also equally enter a pacemaker and any human embedded enhancement application (read wearable applications) that may emerge. In short, cyber security has to be conceptualized, in the first instance itself, as security of the personal self and bodily space. If cyber security is to be seen as part of the realm of a digitally mediated personal and public space, then there are four major conceptual and practical shifts that need to be negotiated and managed.

First, national security has to be equated with cyber security and then eventually be subsumed within the larger landscape of cyber security. Cyber attacks and cyber warfare are no longer esoteric in nature, confined to digital assets that do not have any direct implications of the socio-economic and cultural foundations of daily life. In fact, the very definition of security has to undergo a change and include the security of digital assets, networks, smart systems and any digitally mediated personal and public space.

Any unauthorized attempt to undermine or compromise a system, device or a daily lived experience based on a digital logic (chip), leading to a denial of service, access to resources or disruption of existential patterns must be defined as a cyber attack. It has to cover a broad range of activities, from a virus or a worm stalling to taking over a single individual's digitally mediated lived/virtual experience to bringing down an entire network, like a power grid or the process infrastructure of an industry.

Any unauthorized attempt to undermine or compromise a system, device or a daily lived experience based on a digital logic (chip), leading to a denial of service, access to resources or disruption of existential patterns must be defined as a cyber attack. It has to cover a broad range of activities, from a virus or a worm stalling to taking over a single individual's digitally mediated lived/virtual experience to bringing down an entire network, like a power grid or the process infrastructure of an industry.

The concept and practice of cyber security has to take into account the transformation of an analogue society into a digital one. Everything from money, utilities, civic services, financial and social transactions to governance, home security, transportation, entertainment and even one's own identity is now becoming digital. With each step towards digitization, a previously analogue and physical asset turns into a digital one, redefining the concept of security. A digital asset is both physical and amorphous, requiring an integrated system of proactive and reactive systems that is both anticipatory and defensive.

Second, the global governance architecture of cyber security has to take into account that security is as much a part of the larger lived digital experience of daily life as it is about protecting the institutional digital foundations of state, market and civil society. A 2012 report on Windows and Mobile Malware released by the antivirus firm Quick Heal found social media platforms are the favourite haunts of cyber criminals to plant malware. The report found an increase of over 90 per cent in Windows malware and a massive 170 per cent in its modifications. Interestingly, the report also found that the virus attacks on mobile digital devices increased by 30 per cent, with a concomitant 80 per cent increase in its modifications.

The cyber security challenges are not only granular, statal and global, but are also multidimensionally intermeshed. For instance, security firm McAfee in December 2012 released a report that a gang of cyber criminals had developed a sophisticated Trojan capable of siphoning off billions of dollars from banks. Thirty banks in the US were high on the target list. McAfee says the cyber criminals are so organized that they are recruiting other criminals to ensure that the amounts siphoned off from each bank is limited in order not to rouse suspicion. All banks in the US were put on high alert and the US government organized a special team of cybercops to track this case, which continues as of date.

Such simultaneously granular and inter-regional threats not only target individuals, but also systems of global economy and polity. The new and emerging paradigm of cyber security has to understand that such threats to, and within, cyberspace cannot be seen in singular and confining terms of sanitizing specific digital access points. The concept of cyber security has to move beyond specific digital boundaries and engage with larger technologically mediated spaces. In short, cyber security has to necessarily embrace an approach of internationalism, global cooperation, open standards, protocol based systems and of digitally mediated ecosystems, rather than one of digital devices and nodes.

Third, cyber security has to involve ordinary people as stakeholders. It has to move beyond the current confined landscape of experts, technocrats and digital industry professionals. There has to be a conscious effort to engage with people to understand their mediated digital experiences as part of their daily life. Apart from standard operating procedures for protection of personal and sensitive information, the changing nature of digital transactions and the consequent changing relational social dynamics have to be understood in all their nuances and complexities. For instance, the levels of digital engagement of an average Indian with the ecosystem of a banking correspondent, Aadhaar-linked bank account and direct benefits transfer (DBT) not only reorients the basic character of democracy-state-citizen relationship, but also throws up cyber security challenges that are quite different from the conventional cyber security concerns of malware, viruses and firewall breaches.

The cyber security concerns range from identity theft forms and modes of partnership with private players and institutions and civil society organizations to fundamental questions of a state's responsibility towards it citizens. In involving people as stakeholders in digitally mediated experiences, the emergent concerns of cyber security will require a reorientation of the legal and institutional structures of digital governance at global, regional, national, local and hyper-local levels. Such a reorientation will create the foundation for a new paradigm of cyber security.

Fourth, and finally, cyber security has to be located within a larger global policy push for 'digital by default' approach towards citizen services, governance structure, business of government, commerce, banking systems (including financial inclusion practices) and entertainment. Cyber security is not only national, but is also uniquely global. It requires an international consensus on identifying the foundations of cyberspace and creating a set of protocols for accessing it transparently and securely. The logic of digital is becoming embedded from mobile phones to human beings. The approach to cyber security must look at the future of digitally scripted spaces, where digital information increasingly becomes part of the contemporary built environment.

As expressed by Nigel Thrift, the digital logic is 'extending its fugitive presence through object frames as diverse as cables, formulae, wireless signals, screens, software, artificial fibres and so on.'[26] Policy makers have to quickly realize that cyber security is basic and fundamental security.

In this emergent Internet of Things, cyber security faces its greatest challenges and its greatest opportunities. They are both not in the realm of technology or technical possibilities, but more in the area of human imagination and our own ability to foresee the trajectory and scope of ubiquitous digitalization, a task mined with humble pies in the best of circumstances. The future and emergent digitally scripted spaces are going to be at once political, social, cultural, economic, functional, transactional and aesthetic. It will not only intersect with physically lived-in spaces, but in many cases will mutate them by constant interaction, engagement and contestation. Such digital spaces will create their own set of exclusions and inclusions, where one can be logged in or logged out (left out), depending on access/accessibility to digital resources.

The starting point for the new and emergent paradigm of cyber security has to be ubiquitous digitalization. In conceptualizing society as sets of intersected and intermeshed spaces that are digitally mediated, even as they are transformed and mutated, cyber security will find a way to decouple its current tight relationship with the Internet. It is only by renegotiating its almost obsessive focus on the world wide web and Internet that the structure and architecture of cyber security will reorient itself to understand, analyze and accommodate the paradigmatic changes being brought about by ubiquitous digitalization.

Footnotes:

[1] Monolithic microwave integrated circuit devices typically perform functions such as microwave mixing, power amplification, low noise amplification, and high frequency switching. MMICs are dimensionally small (from around 1 mm^2 to 10 mm^2) and can be mass produced.

[2] It was rumoured at the time that the radar was so powerful that it would kill rabbits near the runway as the plane took off. The radar used vacuum tubes, which was ridiculed in the West. The Soviet choice, however, was intentional as it made the radar immune to EMP (electromagnetic pulse) from nuclear blasts and it was cheaper.

[3] Soviet pilot Viktor Belenko defected with his MiG-25 to Hakodate in Japan on 6 September 1976. This prompted the Soviet Union to develop the MiG-31.

[4] The Defence Advanced Research Projects Agency (DARPA) is an agency of the United States Department of Defence responsible for the development of new technologies for use by the military. DARPA has been responsible for funding the development of many technologies which have had a major effect on the world, including computer networking, as well as NLS, which was both the first hypertext system, and an important precursor to the contemporary ubiquitous graphical user interface.

[5] The first published description of packet switching was an 11-volume analysis, On Distributed Communications, prepared by Paul Baran of the Rand Corporation in August 1964. This study was conducted for the United States Air Force (USAF), and it proposed a fully distributed packet switching system to provide for all military communications, data, and voice. The study also included a totally digital microwave system and integrated encryption capability. The air force's primary goal was to produce a completely survivable system that contained no critical central components.

.

[6] Theoretical physicist and a strong advocate of the string theory, Michio Kaku, in his book Physics of the Future: How Science Will Shape Human Destiny and Our Daily Lives by the Year 2100 (Anchor, New York, 2012), says Adolf Hitler, Theodore Roosevelt and Joseph Stalin would have killed for that chip.

[7] As with most things associated with cyberspace, GPS was mainly developed for the US fleet of nuclear submarines and sea-based nuclear missiles as part of a viable second strike deterrent. After Korean Airlines Flight 007 carrying 269 people was shot down in 1983 after straying into the USSR's prohibited airspace, the then US President Ronald Reagan issued a directive making GPS freely available for civilian use. The first civilian GPS satellite was launched in 1989, and the 24th satellite was launched in 1994.

[8] The JF-17 Thunder is how Pakistan, which helped co-develop it, refers to the aircraft. The Chinese refer to it as FC-1 Xiaolong. The programme is written in C++ rather than the Ada programming language, which is optimized for military applications. This has allowed the aircraft designers to integrate a number of commonly available civilian software programmes as well as developers.

[9] M. Stefik (ed.), From Internet Dreams: Archetypes, Myths and Metaphors. MIT Press, 1996; H. Sawhney, 'Information Superhighway: Metaphors as Midwives', Media, Culture and Society 18, 1996, pp. 291-314, p. 293.

[10] S. Hill, The Tragedy of Technology. Pluto, London, 1998. p. 23.

[11] A. M. Townsend, Smart Cities: Big Data, Civic Hackers and the Quest for a New Utopia. W. W. Norton & Company, New York, 2013.

[12] M. Pawley, Architecture, Urbanism and New Media, (mimeo), 1995.

[13] Nicholas Negroponte, Being Digital. Hodder and Stoughton, London, 1995. p. 165

[14] V. Mosco, The Political Economy of Communication. Sage, London, 1996; E. Soja, Postmodern Geographies: The Reassertion of Space in Critical Social Theory. Verso Press, London, 1989; M. Castells, The Rise of the Network Society, The Information Age: Economy, Society and Culture (Vol. I). Blackwell, Oxford, 1996.

[15] K. Robbins, 'Cyberspace and the World we Live in', in M. Featherstone and R. Burrows (eds.), Cyberpunk/Cyberspace/Cyberbodies. Sage, London, 1995, p. 153.

[16] R. Abler, Everywhere or Nowhere? The Place of Place in Cyberspace, (mimeo), 1995, p. 3.

[17] M. Castells, The Informational City: Information Technology, Economic Restructuring and the Urban Regional Process. Blackwell, Oxford, 1989 p. 373.

[18] Ibid., pp. 423-28.

[19] K. Hayles, 'Virtual Bodies and Flickering Signifiers', October 66, 1993, pp. 69-91.

[20] M. Callon, 'Technoeconomic Networks And Irreversibility', in J. Law (ed.), A Sociology of Monsters: Essays on Power, Technology and Domination. Routledge, London, 1991; D. Haraway, 'A Manifesto for Cyborgs: Science, Technology, and Socialist-feminism in the Late Twentieth Century', in D. Haraway (ed.), Simians, Cyborgs and Women: The Reinvention of Nature. Routledge, New York, 1991, pp.149-81; B. Latour, Science in Action: How to Follow Scientists and Engineers Through Society. Oxford University Press, Oxford,1993.

[21] N. Bingham, 'Objections: From Technological Determinism Towards Geographies of Relations', Environment and Planning D: Society and Space 14, 1996, pp. 635-57.

[22] S. Graham, 'Imagining the Realtime City: Telecommunications, Urban Paradigms and the Future of Cities', in S. Westwood and J. William (eds.), Imagining Cities: Scripts, Signs and Memories. Routledge, London, 1998, pp. 31-49.

[23] D. Harvey, The Urbanization of Capital. Blackwell, Oxford,1996.

[24] Futurologist Raymond Kurzweil says that by 2025, human beings would have integrated themselves with smart chips creating a cyborgian singularity.

[25] Contrast this with what occurred about 30 years ago. Iraq was constructing a nuclear reactor just outside Baghdad. As usual, Israel's security hackles were raised, and a fleet of F-16As escorted by F-15s took a risky manoeuvre violating Jordanian and Saudi Arabian airspace and bombed the reactor.

[26] N. Thrift, 'Movement-Space: The Changing Domain of Thinking Resulting From the Development of New Kinds of Spatial Awareness', Economy and Society 33(4), November 2004, pp. 582-604.

References:
A. Amin, and N. Thrift, Cities: Reimagining the Urban. Polity Press, Cambridge, 2002.

A. Appadurai, Fear of Small Numbers. Duke University Press, Durham N.C., 2006.

A. Appadurai, (ed.), Globalization. Duke University Press, Durham N.C., 2001.

A. Appadurai, The Social Life of Things: Commodities in Cultural Perspective. Cambridge University Press, Cambridge, 1986.

M. Foucault, The Order of Things: An Archaeology of Human Sciences. Routledge, London, 1989.

S. Graham, 'The End of Geography or the Explosion of Place? Conceptualizing Space, Place and Information Technology', Progress in Human Geography 22, Sage, London, 1998, pp. 165-185.

J. Holston and A. Appadurai, 'Introduction: Cities and Citizenship', in James Holston (ed.), Cities and Citizenship. Duke University Press, Durham NC, 1999, pp. 1-20.

K. Jenkins, At the Limits of History: Essays on Theory and Practice. Routledge, Abingdon, 2009.

H. Lefebvre, The Production of Space. Blackwell, Oxford, 1984.

A. Marc, Non-places: Introduction to an Anthropology of Supermodernity. Translated by John Howe. Verso, London, 1995.

A. Ong, Flexible Citizenship: The Cultural Logic of Transnationality. Duke University Press, Durham NC, 1999.

E. Swyngedouw, 'Communication, Mobility and Struggle for Power over Space', in G. Giannopoulos and A. Gillespie (eds.), Transport and Communications in New Europe. Belhaven, London, 1993, pp. 305-25.

PETER GRABOSKY

SECRECY, TRANSPARENCY AND LEGITIMACY

AS a starting point, a key principle in a democratic state is that the public should participate in the determination of public policy, and be kept informed of how that policy is being implemented. In other words, taxpayers are entitled to know what their taxes are buying,and to have some say in how their taxes are being spent. They should also be able to know how well their taxes are being spent, and to know if and how their taxes have been wasted. After all, in a democracy, the state exists to serve the people. Of course, in populous democracies such as India and the United States, pure democracy is logistically unfeasible. Democratic institutions such as legislatures and courts exist to overcome these logistical impediments. In addition to these institutions of the state, a free and robust press can play an important role in ensuring that governments are accountable for their actions.

But even a democracy requires a degree of secrecy. The secret ballot is, after all, the bedrock of democratic elections. Many governmental processes, and details of public policy, are best shielded from public view. In the Westminster system, cabinet deliberations are arguably best undertaken in confidence, in order to encourage open and robust discussion. This essay discusses the place of transparency in the development and implementation of national cyber security policy in democratic states. Examples are mostly drawn from recent US history, largely because of recent events that have shed considerable light on cyber security issues in that country.

Most if not all organizations, whether public or private, have three basic goals. One is to increase their resources, the other is to maximize their power, and the third, somewhat related, is to be shielded from external scrutiny of their internal dynamics. It should come as no surprise that some of the most powerful organizations of the 21st century are those dealing with national defence and intelligence. In many countries their aversion to transparency and accountability is evident on a daily basis.

Clearly, not all of the public's defence and intelligence business can be placed on full display. Complete transparency would be self-defeating. There are, quite simply, some things that must be concealed from one's adversary. For example, it would be unwise to publicize one's own vulnerabilities. Nor would it be appropriate to divulge the location and timing of a planned attack, or to reveal the true identity of an undercover agent. Conversely, total opacity may also be counter-productive. When one's capabilities are completely invisible to an adversary, that adversary may be tempted to try its luck; when one's capabilities are hidden from one's own citizens, opacity may induce either unwarranted anxiety or a false sense of security, depending upon the individual's mindset. Either way, opacity, by definition, limits the information available to the citizens of a democracy to make informed decisions.

The decision to go to war in the absence of an actual or imminent attack by an adversary is arguably a violation of international law and is, therefore, one that requires significant public consultation. Paradoxically, this cannot be based on complete information, as details of war plans, targets, specifics of one's own military capabilities, and one's knowledge of the adversary's capacities are often appropriately concealed. Cyber espionage and cyber war depend even more on stealth (not to mention deception), and are areas of activity that have revived the discussion of just how much a citizen should know.

The term legitimacy refers to public acceptance – the extent to which the citizenry regards an institution, a law, or a policy as rightful and appropriate. The tension between legitimacy and opacity is immediately apparent; the public cannot regard as appropriate something of which it is unaware. There are nevertheless circumstances in which opacity does not negate legitimacy. Trust in an institution or a policy may be so great that one may not wish to question it. There are those citizens who trust their government to do the right thing and would prefer not to know the details of how policies are implemented. So it is that many matters of national security are placed in the hands of defence and intelligence agencies with 'no questions asked'. This involves what might be called a willing suspension of inquisitiveness, where citizens place themselves as beneficiaries of a national security 'blind trust'.

Unfortunately, fiduciaries in matters of security, no less than of finance, may abuse the trust bestowed upon them. The eventual exposure of their abuses may lead to an erosion, if not a crisis, of legitimacy.

This cautionary note must not be interpreted as a mandate for cover-up. All citizens, concerned or not, have a right to know about the harm committed by their government on their behalf. And prospectively, it is important for citizens to be informed about whether a policy is misguided or not.

Turning a blind eye to the less pleasant aspects of security and intelligence may be a source of comfort in the short-term, but it can lead to future headaches.

Depending upon the extent to which surveillance impacts the rights and liberties of one's citizens, or those of foreign states, some form of formal authorization and oversight may be appropriate. In many common law countries, for example, the interception of one's telecommunications requires prior judicial authorization.

When the state exercises its power, four questions arise: (i) Whether the state should have the power in the first place; (ii) Whether there is oversight and supervision over how that power is exercised; (iii) What response is appropriate when this power is abused; and (iv) Whether and if so, how much the citizenry should be made aware of the above.

Democratic states that intercept telecommunications for purposes of law enforcement or national security are usually bound by strict legislative and procedural requirements often requiring judicial oversight. The same should apply when Internet Service Providers are compelled to disclose telecommunications content or meta-data. The fact that there is a legislative basis for such activity makes it public knowledge. Any abuses of these practices should be dealt with in open court.

Unilateral surveillance of telecommunications content, such as that reportedly practised by the US National Security Agency, tends to occur outside of the public gaze. Although there may be a basis in law for such activity, the circumstances of its implementation are often invisible, as are responses to the abuse of such power. Countries such as the United States distinguish between their own citizens, and those of other countries. The latter are accorded less protection.

The interception of communications of friendly governments and their leaders as well as those of one's adversaries, tends to be concealed from public view because of the very great potential for embarrassment and loss of legitimacy of the eavesdropping nation. The loci of decision making and supervision/authorization tend to be cloaked in secrecy. Whilst an outright renunciation of such power may be desirable, one can imagine exigent circumstances when such practices may be necessary to prevent widespread loss of life and/or property damage. There may be merit in disclosing the general outlines of such a policy without identifying target individuals or jurisdictions.

While governments are disinclined to publicize such activities, if they are to be undertaken at all, they should be governed by strict guidelines, with accountability residing at the highest level of government. The decision to engage in spying on one's friends should not be taken lightly, and should weigh the potential knowledge gain and its strategic value against the obvious risks that would arise from its disclosure.[1]

It has been reported that over a hundred states around the world have, or are developing, offensive cyber capabilities. Presumably, a comparable number have also invested in cyber defence. By what principles have these capabilities been developed? What degree of public consultation or legislative deliberation has been undertaken as a basis for these practices? To what kind of oversight (if any) are they subject? One suspects that most governments would be unwilling to reply to these questions, simply stating that they, as a matter of policy, do not comment on matters of intelligence. The tension with democracy is self-evident.

There are established principles in international law regarding when and how a state may resort to the use of force.[2] Their direct application to cyber warfare does not make for a perfect fit; for example, the appropriate response to an electronic levée en masse, or popular uprising in response to a cyber attack may differ from that occurring in physical space.[3]

But the principles of necessity and proportionality are more robust. One should not use force unless it is essential to achieve an objective. If less intrusive means of attaining the objective are available, they should be used. If force must be employed, one should not use more than is required. And steps should be taken to avoid collateral damage.

Determining necessity and proportionality often requires judgment calls. Circumstances that underlie a conflict are not always crystal clear, and perceptions and interpretations of reality may be flawed. One may recall the weapons of mass destruction said to have been at the disposal of Saddam Hussein. Actions undertaken in pre-emptive self-defence may be based on hasty judgment; the line between a potential threat and an imminent threat may be obscure. Dealing with these difficulties in physical space is hard enough. In the cyber domain, they are hardly conducive to public deliberation.

If momentous decisions are delegated to officials to deal with, beyond the public gaze, one would hope that certain mechanisms of accountability might be available to ensure the public's business is conducted with integrity.[4] An agency established for the purpose of offensive or defensive cyber operations, including surveillance, should operate under the rule of law. Ideally, there would be a legislative basis for the agency's activity. This should clearly prescribe the agency's roles, and should specify the limitations on its powers.[5]

Moving from the realm of abstraction and generalization to the real world, here is a case of offensive cyber operations which resulted in the infliction of actual physical damage, Operation Olympic Games.

The tension between secrecy and transparency in the domains of offensive and defensive cyber operations is boldly apparent. Consider the example of recent attempts to disrupt the enrichment of uranium by the Iranian state. Assuming the description of The New York Times correspondent David Sanger regarding a joint US-Israeli cyber attack on Iran's Natanz nuclear enrichment facility is correct and sufficiently comprehensive, how much of this might have been appropriately disclosed to the public?[6]

Here is a reconstruction of the background to the activity that Sanger has described; the code name for the operation was Olympic Games. The Government of Iran had publicly and repeatedly called for the annihilation of the state of Israel. Meanwhile, Iran began enriching uranium, ostensibly for the purpose of peaceful use in electric power generation. Concerns on the part of Israel that Iran had the ulterior motive of developing nuclear weapons led it to threaten pre-emptive action – preferably in partnership with the United States, though if not, then unilaterally.

The possibility of a unilateral attack was real, given Israel's 2007 attack on a nuclear facility in Syria. The G.W. Bush administration, preferring alternatives to the overt use of force, undertook a top secret cyber operation based on the insertion of complex malicious software in the Natanz facility's systems. This operation, reportedly undertaken in collaboration with Israel, was continued by the Obama Administration after the 2008 US presidential election and substantially slowed Iranian enrichment processes. Only the subsequent escape of the so-called Stuxnet virus, central to this operation, revealed that someone had been interfering with Iranian nuclear enrichment activities. Sanger's disclosures in June 2012 transformed what had been a top secret into public knowledge.

Despite its untimely disclosure, the operation not only served to delay the Iranian enrichment process, it may have prevented or postponed an Israeli attack and allowed the political processes in both Iran and Israel to cool off somewhat. The recent leadership change in Iran appears to have been accompanied by a relaxation of tensions.

The full consequences of Operation Olympic Games are uncertain, as neither the victims nor the perpetrators are inclined to discuss it. The apparent success of the operation came at the cost of the escape of a very sophisticated piece of malware into the public domain. With knowledge of the operation now widespread, there are individuals and states who may follow the example of perpetrators and engage in cyber attacks for their own purposes. The ultimate consequences of this potential turn of events are unpredictable. One has seen apparent Iranian retaliation in the form of cyber attacks against US financial institutions and Saudi oil facilities.[7] The violation of Iran's sovereignty was also regarded by some as wrong (the operation, after all, entailed criminal activity), despite the higher purpose of the undertaking of trying to prevent even greater harm.

Was the decision by President Bush to launch Olympic Games (and its continuation by President Obama) an appropriate one? Based on the words and deeds of the Iranian government, it would seem so. To do nothing would have allowed the enrichment process to proceed, and Iran had done little to dispel suspicions that their activities were aimed at weapons development. Israel seemed intent on stopping the Iranian programme, with or without US assistance. Armed intervention, whether unilateral or as part of a joint US-Israeli attack, would risk collateral damage to innocent Iranian civilians, and the real possibility of an escalation of conflict. However, the threat of attack by Iran was not imminent, although, ironically, the threat of attack by Israel may have been.

Was the secrecy surrounding the operation justified? Probably so. Such an operation could never have been the subject of widespread public debate. Simply stating that 'all options were on the table' to discourage Iran's uranium enrichment was sufficient; specifying that a cyber attack was imminent or indeed, in progress, would have enabled Iran to enhance its cyber defences and possibly thwart the operation.

Was the eventual disclosure of the operation (apparently by a knowledgeable insider) also appropriate? The United States Government apparently thinks not; the matter remains the subject of a criminal investigation. The revelation of US capacity for offensive cyber operations may encourage potential adversaries to redouble their efforts at cyber security. It does not appear that Operation Olympic Games resulted in any significant damage to the legitimacy of the United States and its agencies, except perhaps in Iran.

One should be cautious about uncritically accepting government pronouncements relating to security. Historically, many governments, democratic and otherwise, have invoked national security as a justification for domestic surveillance and political repression, to freeze democratic political debate, to shield shortcomings in governance from public and media attention, and for the inappropriate use of armed force. History is riddled with examples where national security justifications have been fabricated outright, or where underlying circumstances have been grossly exaggerated in order to meet the requirements of an extraordinary response.[8] More recently, national security concerns in the United States have served to obscure the contours of (and thereby inhibit debate on) the massive electronic surveillance programme undertaken by the National Security Agency.[9] The publication of a recent report by a Presidential Review Group,[10] instigated by the Snowden disclosures,[11] may herald a refreshing departure from previous patterns, at least in the United States.

Some of the more significant cyber threats to national security are self-inflicted. States that commit cyber crime may themselves be weakened as a result, especially when their activities come to public attention. States that present themselves as paragons of virtue, only to be found to have been engaged in criminal activities, may see their moral authority eroded. Hypocrisy tends to be inconsistent with leadership. The state that does not practice what it preaches may lose legitimacy, both domestically and internationally. When hypocrisy is masked by secrecy, ultimate disclosure can be painful. One could perhaps suggest that the state which reveals its own transgressions is better off than the state whose transgressions are revealed by an independent team of cyber forensics investigators, or by a whistle-blower. It would appear that more public discussion of cyber security issues would be beneficial.

Footnotes:

[1] United States, President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World. The White House, Washington, 2013. http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (accessed 8 January 2014).

[2] Dorothy Denning, 'The Ethics of Cyber Conflict', in Himma and Tivani (eds.), *The Handbook of Information and Computer Ethics*. John Wiley and Sons, New York, 2008, pp. 407-428.

[3] David Wallace and Shane Reeves, The Law of Armed Conflict's "Wicked" Problem: *Levée en Masse* in Cyber Warfare', International Law Studies 89, 2013, pp. 646-668; Michael Schmitt (ed.), Tallinn Manual on the *International Law Applicable to Cyber Warfare*. Cambridge University Press, Cambridge, 2013.

[4] Institute for Defence Studies and Analyses, *India's Cyber Security Challenges*. Institute for Defence Studies and Analyses, New Delhi, 2012.

[5] Pranesh Prakash, 'How Surveillance Works in India', *The New York Times*, 10 July 2013. http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/ (accessed 8 January 2014).

[6] David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. Crown Publishers, New York, 2012.

[7] N. Perlroth, 'In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back', *The New York Times*, 23 October 2012. http://www.nytimes. com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?page wanted=all (accessed 8 January 2014); N. Perlroth and Q. Hardy, 'Bank Hacking was the Work of Iranians, Officials Say', *The New York Times*, 8 January 2013. http://www. nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html (accessed 8 January 2014); Tom Groenfelt, 'Did U.S. Cyberattacks on Iran Backfire on American Banks?' Forbes, 6 August 2013. http://www.forbes.com sites/tomgroenfeldt/2013/06/08/did-u-s-cyberattacks-on-iran-backfire-on-american-banks/(accessed 8 January 2014)

[8] Robert J. Hanyok, 'Skunks, Bogies, Silent Hounds, and the Flying Fish: The Gulf of Tonkin Mystery, 2-4 August 1964', *Cryptologic Quarterly* 19(4)/20(1), 2001, pp. 1-55. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB132/relea00012.pdf (accessed 8 January 2014); James Bamford, *The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America*. Random House, New York, 2008.

[9] *The New York Times*, 'More Fog from the Spy Agencies' NYT, 31 July 2013. http://www.nytimes.com/2013/08/01/opinion/more-fog-from-the-spy-agencies.html?emc = edit_tnt_20130731&tntemail0=y (accessed 8 January 2014).

[10] United States, 2013, op cit.

[11] Miren Gidda, 'Edward Snowden and the NSA Files – Timeline', *The Guardian*, 26 July 2013. http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline?INTCMP=SRCH (accessed 8 January 2014).

Refernces:

Glenn Greenwald, 'XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet"', theguardian.com, 31 July 2013. http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data (accessed 8 January 2014).

Glenn Greenwald and Ewen MacAskill, 'Obama Orders US to Draw Up Overseas Target List for Cyber-attacks', *The Guardian*, 8 June 2013. http://www.theguardian. com/world/2013/jun/07/obama-china-targets-cyber-overseas (accessed 8 January 2014).

Glenn Greenwald and Ewen MacAskill, 'NSA Prism Program Taps in to User Data of Apple, Google and Others', *The Guardian*, 7 June 2013. http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data (accessed 8 January 2014).

Tim Weiner, *Enemies: A History of the FBI*. Random House, New York, 2012.

MAHIMA KAUL

ENSURING PRIVACY IN A REGIME OF SURVEILLANCE

ACCORDING to India's Telecom Regulatory Authority, at the end of 2013 India had over 904 million telecom subscribers. This includes both wireless and wireline subscribers – a significant number of India's population that with modern communication technologies can help improve the quality of their lives. These modern technologies have another benefit – user data can be collected, users themselves can be tracked, monitored, intercepted and traced by the long arm of the Indian government. The competing need for privacy, data collection and surveillance, in part, lays out the landscape of a technology-led society we are building today.

This paper examines the legality of surveillance structures in India today (including mass surveillance programmes), and an expanding e-government project, and juxtaposes them against the missing privacy legal framework that is needed in a liberal democracy such as India. It concludes that accountability mechanisms and laws are needed to safeguard a society that is increasingly adapting to mass surveillance and the lack of privacy.

In India, as is the case globally, there is no doubt that a necessary argument must and will be made for being able to use the same technologies for policing and security as are used to perpetrate crimes and acts of terror. With increasing Internet penetration in the country, India released its first Cyber Security Policy in 2013, flagging the biggest areas of concerns for the country, including protecting critical information infrastructure and training more cyber security personnel. There is also growing concern in the country about the security of mobile networks given the increasing number of cheap and unverified products entering the market. With the increasing frequency of terror attacks on Indian soil there is a necessity for law enforcement officials to be able to investigate suspects with speed. At the same time, there is also a need and desire to use digital technologies to make governance more effective and efficient for the citizenry.

Therefore, there are two broad aspects that need to be examined. The first relates to the surveillance mechanisms that exist via previous legislation, and new mass surveillance schemes that are being built by leveraging current technology. The second concerns the mass (and secure) collection of citizen data to build governance tools for smoother delivery of public services.

A recent NATO publication flagged the problems with the first issue well: 'State-sponsored surveillance tends to be discounted as a "passive" or invisible intrusion, but when conducted on a pervasive scale, it is an activity that can severely harm rights in several dimensions. First, the invasion of privacy occurs at the point of intrusion and capture of material, not only at the point of access or use of information. The inability to direct one's communications to only those who are intended recipients is a serious loss of control over one's identity and autonomy; everyone has experienced the sensation of literally "being a different person"when in public, as opposed to among intimates. The uncertainty over which communications will be accessed when, and by whom, can also chill the exercise of many rights: freedom of expression, access to information, association with others, religious belief and practice, and assembly, for example.'[1]

India has a number of laws that offer a basis for the kinds of surveillance that exists in the country. Some of these are listed below:

- The Indian Telegraph Act of 1885 was drafted to cover the use of telegraphy, phones, communication, radio, telex and fax in India. Section 5 of the act allows for legal wiretapping, and the guidelines state that only the home secretary, either of the Government of India or of a state government, can give an order for lawful interception. The order for the wiretapping is valid for a period of two months and should not exceed six.

- The Indian Wireless Telegraphy Act of 1993 does not permit anyone to own wireless transmission apparatus without a license, and in Section 7 gives power to any officer specially empowered by the central government to search any building, vessel or place if there is reason to believe that there is any wireless telegraphy apparatus which has been used to commit an offence.

- The Indian Post Office Act of 1898, Section 26, confers powers of interception of postal articles for the 'public good'.

* Section 91 of the Code of Criminal Procedure, 1973, grants other powers to the police; it states that:
‘Whenever any court or any officer in charge of a police station considers that the production of any document or other thing is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under this code by or before such court or officer, such court may issue a summons, or such officer a written order, to the person in whose possession or power such document or thing is believed to be, requiring him to attend and produce it, or to produce it, at the time and place stated in the summons or order.’

The most recent and currently controversial legislation is the Information Technology Act of 2000, amended in 2008 after the horrific Mumbai terror attack. Currently, the act contains some sections that require persons to reveal personal information without much room for recourse. Section 44 lays out punishment and fines in case of failure to furnish any document, return or report to the controller or the certifying authority. Article 66 A lists out punishment upto three years with a fine for sending any communication through electronic means which could be considered grossly offensive, menacing, false information for annoyance, inconvenience, hatred, ill-will and so on. Section 80 gives police and senior government officials the power to enter any public place and search and arrest without warrant any person found therein who is reasonably suspected or having committed or of committing or about to commit an offence under this act.

However, in 2013, information about a mass surveillance scheme being rolled out by the Government of India came to light. The Central Monitoring System (CMS) was launched in 2009, but became public knowledge four years later. According to reports and interviews, the CMS will automate already existing data from other interception and monitoring programmes, and will have a non-erasable command log of all provisioning activities. Simply put, ‘CMS targets private information of individuals since it will enable real-time tracking of online activities, phone calls, text messages and even social media conversations.’[2]

Further, CMS will not need permission from nodal officers of the Telecommunication Service Providers (TSPs), and will provision requests from all law and enforcement agencies. It isn’t quite clear what the legal basis of CMS is, but it has been suggested that it will operate under Section 52 (2) of the Indian Telegraph Act, which as we know allows for interception of (telegraphic) messages for various reasons including ‘public emergency’ and ‘public safety’. It has not been created by, or answers to, Parliament.

According to available information, the CMS can tap information from various other monitoring and interception schemes across India. These include the Crime and Criminal Tracking Networks and Systems (CCTNS), Lawful Intercept and Monitoring Program (LIM), Telephone Call Interception System (TCIS) and the Internet Monitoring System (IMS). The various department/agencies that will have access to all this gathered data, through CMS, include the Central Bureau of Investigation (CBI), Defence Intelligence Agency (DIA), Department of Revenue Intelligence (DRI), Enforcement Directorate, Intelligence Bureau, Narcotics Control Bureau, National Intelligence Agency, Central Board of Direct Taxes, Ministry of Home Affairs, the Military Agencies of Assam and Jammu & Kashmir, and the Research and Analysis Wing (RAW).

As reported in The Hindu, ‘The CMS will have unfettered access to the existing Lawful Interception Systems (LIS) currently installed in the network of every fixed and mobile operator, ISP, and International Long Distance service provider. Mobile and long distance operators, who were required to ensure interception only after they were in receipt of the “authorization”, will no longer be in the picture. With CMS, all authorizations remain secret within government departments. This means that government agencies can access in real time any mobile and fixed line phone conversation, SMS, fax, website visit, social media usage, Internet search and email, including partially written emails in draft folders, of “targeted numbers”. This is because, contrary to the impression that the CMS was replacing the existing surveillance equipment deployed by mobile operators and ISPs, it would actually combine the strength of two, expanding the CMS’s forensic capabilities multiple times.’[3]

At the same time, limited resources to store citizen data are becoming a thing of the past. New technologies like cloud computing have allowed space for storage to increase exponentially. Therefore, as the capacity of the state to accumulate data increases, for example with MeghRaj, a National Cloud launched by the Government of India in February 2014, it will be able to expand its e-government services. Therefore, the common refrain among privacy experts and other stakeholders is that the crux of the matter lies in India passing an all-inclusive privacy law. This, they believe, would take into account not just protection for the individual viz-a-viz civil and criminal laws in India, but ensure there are privacy safeguards in the ambitious projects that the government of India is undertaking with regards to citizens private data.

These would include the massive rollout of e-governance projects under the National e-Government Programme, which includes 31 mission mode projects that seek to, in the first phase, digitize all available citizen data (such as land records and health records) for respective ministries, and then, in the second phase, build responsive and efficient government service delivery platforms. In some states this means accessing healthcare through smartcards, while in others citizens can access and pay their electricity bills online.

For example, Bhoomi, an e-government project in Karnataka under the revenue department has already computerized over 20 million land records of over 6.7 million farmers. These digitized ministries will soon not function as islands. The NATGRID – the National Intelligence Grid – is a system that will connect several government departments and data-bases to collect ‘comprehensive patterns of intelligence that can be readily accessed by intelligence agencies.’ While this means a single point to access citizen data from a variety of sources, it also allows a single window to steal this personal information.

Then there is the controversial UID – Universal ID card – that the Government of India plans on issuing to every resident of India, after collecting his or her biometric data. Simply put, the UID will become a citizen identifier. This means that the government will now be able to confirm that it is indeed citizen ‘x’ who is making phone calls or sending emails of some interest to the authorities, by immediately identifying the person through biometric data available with the state. Conversely, this also means that the state now has not just biometric data on its people, but it will be linked to all their communication data in an easy-to-find manner.

All this is happening without a comprehensive privacy law passed by the Indian Parliament. Article 21 of the Indian Constitution declares that no citizen can be denied his life and liberty except by law, and the right to privacy has been interpreted to be part of that. Further, Article 43A of the IT Act directs corporate bodies who ‘possess, deal or handle’ any ‘sensitive personal data’ to implement and maintain ‘reasonable’ security practices, failing which they would be liable to compensate those affected by any negligence attributable to this failure. This must necessarily extend to the government as well.

It is instructive to refer to the Report of the Group of Experts on Privacy, chaired by Justice A.P. Shah, former Chief Justice of the Delhi High Court.[4] The report suggested a conceptual framework for privacy regulation in India, touching upon five salient points.

1. Technological neutrality and interoperability with international standards: the privacy act should not refer to any specific technologies and should be generic enough to adapt to changes in society, helping build trust of global clients and users.

2. Multi-dimensional privacy: the privacy act must include concerns related to a number of platforms including audio, video, personal identifiers, DNA, physical privacy and so on.

3. Horizontal applicability: any legislation must extend to the government and private sector.

4. Conformity with privacy principles: this means that the data controller should be accountable for the collection, processing and use of the data, therefore, guaranteeing privacy.

5. Co-regulatory enforcement regime: establishing the office of a privacy officer is also recommended as the primary authority for the enforcement of provisions in the act. However, it is also suggested that industry specific self-regulation organizations also be established.

The document also refers to court judgments from Indian courts that have helped shape some form of privacy safeguards into the system. For example, in the 1997 case, PUCL vs Union of India, the court observed: ‘Telephone-tapping is a serious invasion of an individual’s privacy. It is no doubt correct that every government, howsoever democratic, exercises some degree of sub rosa operation as a part of its intelligence outfit, but at the same time citizen’s right to privacy has to be protected from being abused by the authorities of the day.’ The court then placed restrictions on the class of bureaucrats who could authorize such surveillance and also ordered the creation of a review committee, which would look at all surveillance measures authorized under the act.

The Shah Report lays out a road map of acts passed by the Indian Parliament that would need to be reviewed for balance between individual privacy and national security. For example, when reviewing the UID scheme, the report points out that citizens should be informed if their data is breached. They should also be informed about where and how their data will be used, and notified of any changes in UID’s privacy policy. These and other suggestions are then placed in a broader regulatory framework that imagines a privacy commissioner for India.

At the same time it is pertinent to remember that while there is no privacy law to safeguard citizens, the government itself does not have a legal framework for the kind of mass surveillance India is moving towards. As pointed out by privacy experts: ‘The two laws covering interception are the Indian Telegraph Act of 1885 and the Information Technology Act of 2000, as amended in 2008, and they restrict lawful interception to time-limited and targeted interception. The targeted interception both these laws allow ordinarily requires case-by-case authorization by either the home secretary or the secretary of the department of information technology.’[5]

Where do these competing interests end up? There is no privacy law to shield citizens from upgraded mass surveillance technology and systems, which themselves constantly need updated legal grounding. Ironically, just before the Snowden revelations, in his April 2013 report to the Human Rights Council of the United Nations, Special Rapporteur Frank La Rue noted that he was 'deeply concerned by actions taken by states against individuals communicating via the Internet, frequently justified broadly as being necessary to protect national security or to combat terrorism. While such ends can be legitimate under international human rights law, surveillance often takes place for political, rather than security reasons in an arbitrary and covert manner.'[6] The report also highlights the fact that national legal standards that impose little or no judicial oversight, or allow warrantless surveillance powers in the name of national security without any particular demonstration of a genuine need or threat and that 'every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files.'

Today, the concept of privacy is also undergoing a sea change due to the increasing ease with which citizens and customers are handing over data to governments and businesses. This has been seen with information shared on social media – 93 million Indians are on Facebook – and was seen in the almost unquestioned way in which e-governance projects were welcomed in the early days without any flags being raised about any data security or privacy safeguards in the design.

In his essay, 'The Real Privacy Problem',[7] writer Evgeny Morozov wrestles with the evolving concept of 'privacy'. He writes of a privacy scholar named Spiros Simitis who grappled with data protection in the 1980s, and the three ideas he grappled with. The first was that with virtually every employee, taxpayer, patient, bank customer, welfare recipient, or car driver handing over their personal data to private companies (and of course, government) privacy was now everyone's problem. The second was that CCTV and other recording technologies like smart cards were normalizing surveillance, weaving it into our everyday life. The third was that by allowing everyday activities to be recorded, citizens were actually allowing 'long-term strategies of manipulation intended to mould and adjust individual conduct.'

Ultimately, while technology itself is always faulted for being the cause of privacy failures, the truth is that these gaps enter the system through poor legislation. As discussed, when projects are created without thinking of who could have unwarranted access to information, or how the information could be used and abused outside the scope of what it is collected for, is when the problems truly begin. Privacy safeguards, transparency about the intent and extent of a project (even when it was intended for surveillance) injects accountability into a system that remains static, despite the dynamic leaps in technology. This is the best way forward should India want to retain its spirit and label of being a liberal democracy.

Footnotes:

[1] Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*. International Law, International Relations and Diplomacy. NATO CCD COE Publication, Tallinn, 2013.

[2] Kalyan Parbat, 'India's Rs 40 Crore Automated Surveillance System Faces Delay', *The Economic Times*, 1 February 2014. Accessed at: http://articles.economictimes.indiatimes. com/2014-02-01/news/46897898_ 1_cms-project-surveillance-system-cdot

[3] Shalini Singh, 'India's Surveillance Project May be as Lethal as PRISM', *The Hindu*, 21 June 2013. Accessed at: http://www.thehindu. com/news/national/indias-surveillance-project-may-be-as-lethal-as-prism/article 4834619.ece

[4] Report of the Group of Experts on Privacy, chaired by Justice A.P. Shah, Planning Commission, October 2012. Available at: http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

[5] Pranesh Prakash, 'How Surveillance Works in India', *India Ink, The New York Times*, 10 July 2013. Accssed at: http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_r=0

[6] Frank La Rue, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (UN GA Doc. A/66/290, 10 August 2011). Accessed at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

[7] Evgeny Morozov, 'The Real Privacy Problem', *Technology Review*, 22 October 2013. Accessed at: http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem/?src=longreads

SANDRO GAYCKEN

A SUPERPOWER FOR AN INFORMATION SOCIETY?

THE revelations of Edward Snowden might bring unforeseen responsibilities in its wake for Germany. The country might have to become a superpower for a global information society.

This new responsibility emerges from the loss of moral leadership of the US in global IT matters. That American leadership developed historically, and it was only contested by Russia and China. Russia has been a direct and outspoken ideological rival, while China has been vocal, but less so, working rather in the background with pragmatic, non-ideological reasons. The main difference of this moral, West-East divide was the role of surveillance and censorship and the amount of control realized through information technology. The West seemed to be the herald of freedom, of a civil and uncontrolled Internet, driven only by innovation, while the East seemed the agent of government-led monitoring and paternal supervision.

This difference has been levelled by the PRISM incident. Granted, there is still a significant difference in the sense that China and Russia primarily aim at internal stability and monitoring their own people while the US collects foreign intelligence. But it is no longer a clear-cut distinction between freedom and control. This strong polarity has been lost. Now, the divergence seems to be between one kind of control and another.

Being concerned about the loss of such a distinction might seem academic, but this particular loss bears a potential to evoke a disaster of historical proportions. Distinctions are a part of our perceptions. Our perceptions form our visions of the future. And while the industrial countries and superpowers might already live in an information society, with an established vision and a technologically and regulatory solidified ideology on what the Internet is all about, many other countries – in fact, the majority of the world – still struggle with their views on this new tool. What should it be? How should it be used? What is accepted? What is acceptable?[1]

Many of the above questions will and should demand strictly national, culturally sensitive and specific decisions, and they will become part of their own discourses once the technology is commonplace enough. However, contrary to the established information societies, this process does not start from zero for these countries. They are already confronted with a reality of views, of regulations and of technical terms and conditions emanating from the more advanced countries. While these frameworks can always be rejected, any immediate rejection usually comes at a high cost; therefore, many framing elements will have to be accepted for a few innovation cycles before they can be altered. And some will probably not even be noticeable as disputable conditions – since apart from the more explicit contracts and machines, an implicit notion of normality and acceptability is transported as well.

At this point, the PRISM incident and the ensuing loss of the clear-cut argument of 'freedom versus control' bares its fangs. The incident is influencing the creation of a particular kind of 'normality': for political decision-makers, it renders the control paradigm more common and acceptable than its counterpart. Control no longer seems a mark of fear and instability, but a reasonable and responsible step on the way to becoming an information society.

This 'new normal' could have a tremendous impact on humankind at large. The famous techno-anthropologist André Leroi-Gourhan explained why in his masterpiece 'Le gesteet la parole': humans are evolutionarily altered by how they get used to technology. This is a very plausible hypothesis, which can be observed over and over in history. For information technology, this translates into a simple projection: once IT-based surveillance and censorship – the online control of knowledge, of opinion, of perception – are perceived as acceptable, surveillance and censorship at large will be accepted as normal, as a new kind of technological fait accompli. Logically, this is a *non sequitur*. But techno-evolutionarily, a step-wise mutual adaption of perception and technical realities has been a rule.

There might even be an infectious impulse from these multiple ontogeneses – the many nationally, culturally specific versions of an information society – on the phylogenesis of 'the' information society at large. Mass is important in the evolution of a particular species of technology. The mass of its users and their most dominant interests will ultimately provide a mass of the resources for its development. The larger mass of Internet users is yet to come. It resides in all those countries which are still 'developing' information societies. These latecomers are frequently sceptical about the present US-dominated multistake holder, industry-heavy approach, and they may quite well dictate and design their own decisions and governance issues. This will not happen in the very next innovation cycles, but it could happen in the coming decades. If their acceptance of surveillance and censorship transports an acceptability of such measures in general, these techniques could become part and parcel of the technological and regulatory framework of our IT future around the world. The Internet will become an ultimate tool of control.

This process could very well be a quiet and creeping one. It will be difficult to observe and interfere with because the decision between freedom and control will rarely be made in such a categorical way. It will be splintered into many smaller technological, economical and political decisions, mostly settled in seemingly harmless frameworks such as trade agreements, copyright laws, software plug-ins, or entirely legal and uncontroversial techniques of law enforcement. In most of these cases, the question of freedom versus control will not be visible, especially if the discourse is not as established and emotional as it is in the industrial countries. These countries still place a lot of emphasis on the trade-off between freedom and control, and any IT development is still under close scrutiny of a sufficiently large and tech-savvy part of civil society. If this independent vector of control is not in place, upper-level rational microprocesses will decide the path, and the path will only become visible ex post-facto.

Given this potential evolutionary impact of a strong, yet in its details barely visible global shift towards control, the material implementation of a 'new normal' cannot be accepted. Freedom has to be an option. It has to come back on the agenda. But it needs a strong and outspoken apologist. The US will no longer be able to fill this role. It should even refrain from trying to do so. Any such attempts will only reinforce the impression that freedom has just been the sugar coating of an entirely different kind of cake. So who should replace the US? Europe could step in. It has sufficient experience with technology and IT governance and clear-cut and outspoken ideologies, trying to strike a balance in favour of freedom. But the European Union will not be a good representative. It is far too bureaucratic, too static and inflexible.

Turning towards specific European nations, which could take the lead? Britain is too close to the US. The club of the five-eyes is not suitable for this task. France is too focused on itself, and would be expected to try to turn this into some kind of self- promoting industrial policy. Spain, Italy and Greece are struggling with financial crises and do not yet have any determined positions on the future of an information society.

As for smaller countries, some of them have established strong and knowledgeable positions, such as the Netherlands with its Internet Freedom Agenda, Sweden with the Pirate Party and an associated societal debate, and Estonia with its very own thoughtful design of an information society, thanks to its IT-savvy president Toomas Ilves. But these countries are too small to pick up the role of a global leader. Other countries will doubt whether they understand the concerns and the determinants of different regions and larger societies.

That leaves one option: Germany. Germany is a big country, able to understand many different concerns. It knows how to design and how to regulate technology. It is secure and economically stable. It has a large and established societal debate about the future of an information society. It is a western democracy, but in its own way, and by far not as intrusive as the US. Furthermore, it has good relations with the West and the East and is unlikely to attract strong opposition from either. Germany would therefore be a good choice. If it would develop an outspoken position on digital freedom, the world would listen. An alternative path would be back on the table, in a solid and credible fashion.

But first, a conundrum has to be solved. Germany is trustworthy and influential because it is rational and not ideological, because it is moderate and cautious in its foreign policy, and because it tends to think things through before it acts. These three elements should be taken as a basis and a background for becoming a new apologist of a free version of an information society. But they cannot determine the emergence of an apologist as such.

Germany would need to have a declared and – to some extent – confrontational ideology. The clear-cut distinction must be formulated again, based on a set of values, which must be loudly and explicitly formulated. The message must be heard, or it will not be listened to. Moreover, Germany will have to be quick about adopting this new role. Much will be decided in the coming months and years, and many political decisions should be broached as issues of freedom versus control, if they bear this potential, or the process might not recognize its own political character.

And this is a problem. Assuming ideological leadership in a loud, explicit and quick fashion would be extremely un-German – all of it, and especially in foreign policy. It is entirely against any German instinct regarding its role in the world after its troubled past. It doesn't want to be 'superpowerish' in any respect. But those historical concerns might as well be interpreted in a different way. Hannah Arendt should be revisited. The lesson of the two world wars was not that all Germans are evil. It was that evil lurks in the small steps we take towards totalitarianism and away from freedom and civil empowerment. And if, this time, it takes Germany to be an explicit advocate of freedom, the historical responsibility must be to accept this role, not to reject it.

In conclusion, Germany will have to seriously consider if it should be the new superpower in global IT matters. German foreign policy makers will have to decide whether they want to continue to be cautious as quiet bureaucrats in the background, or whether they want to try something else: to stand up in bright daylight as the representatives of something they believe in, of something humankind might direly need to continue to make the right choices for the imminent next steps in its technological evolution.

A change of mentality for the better might be in place. And Germany will not be the only one to change its mentality. If it should accept this role, the US must refrain from trying to influence and dominate its course. Such an absence would be un-American in cyber matters, but it will be in its own interest. If freedom and democracy shall structure our digital futures, an independent and believable representative is what is needed now. Any attempt to influence this new representative will only weaken its posture and a truly important cause.

* Sandro Gaycken is a strategic advisor to the German DAX companies, the Bundestag, the German ministries and other institutions on IT matters, a director of NATO's SPS programme on national cyberstrategies, and has been a lead author of Germany's foreign and security policy on cybersecurity and Internet freedom.

Footnotes:

[1] Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*. International Law, International Relations and Diplomacy. NATO CCD COE Publication, Tallinn, 2013.

[2] Ethics of technology hold that there is a big difference between acceptance and acceptability. The first is what is accepted empirically by people who are usually not competent or interested enough to foresee side effects and long-term developments for them and for others. The second is what should be accepted if an informed and responsible decision were to be made.

JENNIFER MCARDLE AND MICHAEL CHEETHAM

INDO-US CYBER SECURITY COOPERATION

> Science knows no country, because knowledge belongs to humanity, and is the torch which illuminates the world. Science is the highest personification of the nation because that nation will remain the first, which carries the furthest the works of thought and intelligence.
> – Louis Pasteur

THE Internet has experienced an astonishing expansion over the past two decades, starting as a small network limited primarily to the scientific community before growing into a global network serving over 2.5 billion users. The expansion of the Internet has facilitated the creation of the cyber economy, widespread automated regulation of key control systems, financial transactions, the sharing and storing of information (including highly sensitive data) [JLM1] and the emergence of new forms of communication such as email and social media.[1] The evolution of digital communications has allowed for their integration into all facets of daily existence, causing people to rely upon them in much the same way that we rely on traditional infrastructure. However, despite the ubiquitous benefits of the cyber domain, it is also vulnerable to crime and conflict.

The computer security company McAfee, a wholly-owned subsidiary of Intel Corporation, notes that every year there is an increase of over a million new viruses and logic bombs, and that this figure is increasing.[2] Cyber security threats come from a multitude of sources: criminal networks and syndicates, states actors, and politically motivated 'hacktivists' and terrorists. These threats can manifest in many different forms: 'phishing' scams that entice people into revealing sensitive data; denial of service attacks; espionage; terrorist recruitment; and cyber warfare or cyber terrorist attacks that could degrade widespread systems, incapacitating critical infrastructure like power and water and destabilizing economic and national security.

In India, the Minister of State for Telecommunications Milind Deora noted in the Lok Sabha that cyber attacks rose to 22,060 in 2012 from 23 in 2004, with malware infections and targeted denial service increasingly reported by private users and the government.[3] In the United States, outgoing Homeland Security Secretary, Janet Napolitano, warned her successor in late August to strengthen US cyber defences, noting, 'Our country will, at some point, face a major cyber event that will have a serious effect on our lives, our economy and the everyday functioning of our society.'[4] Reports of cyber attacks and potential cyber threats have become widespread in India and the United States, and in both cases this can partly be attributed to the intrinsic vulnerability of the underlying technologies in digital communications.

To better understand the cyber challenges that lie ahead for India and the United States, both nations must develop a common scientific language and a stronger scientific basis for computer security. As the US National Science Foundation (NSF), Intelligence Advanced Research Projects Activity (IARPA), and the National Security Agency (NSA) noted in 2011, while some scientific work in computer security has been conducted, the field could benefit from a stronger scientific foundation: universal laws, fundamental principles, the scientific method, and the systemization and generalization of knowledge.[5] Developing a science of cyber security could help fill this conceptual void.

This paper will proceed in three parts: first, it will clarify what the science of cyber security is by examining the history and current research presently underway in the field. Second, it will show how science can be used as a mechanism to deepen collaboration between India and the United States in cyber security. While both states are strategic partners with cooperative cyber security consultations and dialogues, substantive cyber security cooperation between the two has been sluggish. Science, which provides opportunities for trust and capacity building, can be used as a diplomatic tool to enhance that cooperation.

Finally, this paper will present a current initiative that seeks to bring Indian and American scientists and social scientists together to explore and make recommendations to jointly develop a foundational science to cyber security. While the science of cyber security cannot guarantee complete protection against cyber security threats, it will provide both India and the United States greater certainty about the capabilities and limitations of each state's security mechanisms, allowing both New Delhi and Washington to make well-informed risk decisions.

In 2008, the Information Security Panel of the NSA initiated a conversation on the scientific underpinnings of computer security. 'Their concern stemmed from the growing use of commercial off the shelf technology in critical government systems, and they questioned whether the frequency of high profile security failures could be attributed to a lack of scientific rigour in security engineering. In contrast, they noted that the science and engineering associated with cryptographic systems, while still imperfect, seemed to result in far fewer catastrophic failures.'[6]

To address these concerns, in November 2008, the NSA in cooperation with IARPA and the NSF convened a Workshop on the Science of Security (i.e., science of cyber security) in Berkeley, California. The dialogue focused on the complexity of creating a foundational science to cyber security and the ability to produce systems that are secure in real world settings. The global Science of Security Virtual Organization (SoS VO) notes that a science of cyber security would encompass 'a body of knowledge containing laws, axioms and provable theories relating to some aspect of system security. Security science should provide an understanding of the limits of what is possible in some security domain, by providing objective and qualitative or quantifiable descriptions of security properties and behaviours.'[7]

Articulating a concise definition for the science of cyber security is problematic due to the abstract and artificially constructed nature of the cyber environment. For the purposes of this paper, Dusko Pavlovic's parallel with the challenges of fortress defence is a particularly insightful example.[8]

Fortresses have throughout history been used as a mechanism to protect a populace from external adversaries. A fortress consisting of walls and gates can be paralleled to cyber space's access controls and authentication protocols. These are static architectural views of security. However, as the Greeks' use of the Trojan horse in the Greco-Trojan wars demonstrates, there is a need to protect a city once adversaries penetrate, infiltrate, or subvert static defences. This requires a more dynamic form of flexible defence. The science of cyber security would provide those dynamic defences. It would rely on 'predictive analytics, based on mining the data gathered by active or passive observations, network probes, honeypots, or direct interactions' to identify and respond to those adversaries.[9] Similar to an immune response in the body, a science of cyber security would identify threats, adapt to those threats, and seek to eliminate them.

Complicating the security picture is the difficulty in establishing the difference between systems and the external environment in the cyber domain. 'In large networks, with immense numbers of processes, the distinction between the system and the environment becomes meaningless.'[10] The task of science is to delineate the distinction between the system and the environment, dynamically responding to changes and adapting to them. To meet these challenges cyber security specialists are drawing on diverse disciplines for inspiration: physics, mathematics, cryptology, the social sciences, and even fields as diverse as astronomy, meteorology, agriculture, and medicine.

The Berkeley workshop gave birth to new research programmes such as the Team for Research in Ubiquitous Secure Technology (TRUST),[11] research 'lablets' at select research institutions throughout the United States,[12] and cooperative initiatives with foreign partners in the United Kingdom and Canada. Recent scientific initiatives have included Geometric Logic for Analyzing Security with Strands, Quantifiable/Refinement of Hyper Properties, and Integrity of Untrusted Computations.[13] Despite these commendable efforts, there is a need to expand cooperative programmes to study the science of cyber security beyond historically close US allies to areas of future geostrategic importance. As Robert Meushaw, the former technical director of the NSA's Information Assurance (IA) Research laboratory has noted, developing a robust science of cyber security will be a long-term process that will require broad-based collaboration. Indian and US common threat perceptions emanating from the cyber environment, when coupled with both states' strong science and technology research and education, make them natural partners to pursue the study of the science of cyber security in an unclassified manner.

At first glance it may seem as if India and the United States have the beginnings of a robust cyber engagement – India and the United States conducted a second round of cyber consultations in June 2012 as part of the overall US-India Strategic Dialogue; through a Cyber Security Forum, India and the United States have agreed to a Computer Emergency Response Team (CERT) cooperation; India has participated in a cyber war game hosted by the Department of Homeland Security; there is ongoing dialogue through a Joint Working Group on Information and Communications Technology; and India and the United States have cooperated in attempting to develop some norms and confidence building measures in cyber space for the United Nations Group of Government Experts on Information Security.

In reality, however, Indian and US cyber engagement lacks substantive progress and continues at a slow pace. This can largely be attributed to a lack of trust and larger diplomatic discrepancies in cyber security between the two governments.[14] There is a need to build trust, develop capacity and better align interests in the field of cyber security in New Delhi and Washington. Science could provide the diplomatic mechanism to achieve that goal.

The great American philosopher Henry David Thoreau once quipped, 'The language of friendship is not words but meaning.' What is science if not the quest for greater meaning? Science diplomacy seeks to go beyond mere words and to bridge differences through meaningful cooperation. The soft power of science allows it to be an effective foreign policy instrument. The fundamental principles of science – rationality, transparency and universality – are the same the world over, allowing people to communicate in a common language. Science provides a non-ideological environment in which to share ideas, build capacity, and solve common problems.

Using science to establish deeper diplomatic relations in overall state-to-state relations or simply in a given area of tension is not without historical precedent. Indeed, science played an integral role in the Sino-US rapprochement of 1972, the easing of US-Soviet tensions during the Cold War, and even more recently in building trust networks between American and Iranian scientists.[15] Discussing the scientific implications of international or diplomatic issues provides an alternative means of communication. 'Scientific discussions have the advantage of being fact based, potentially more objective than typical diplomatic discussions, and in many cases less susceptible to the vicissitudes of standard diplomatic relations.'[16]

Jointly discussing and developing a science of cyber security may provide India and the United States the ability to surpass the diplomatic inertia that has plagued current cyber security negotiations and move towards a more substantive dialogue that targets the root of security problems. By first addressing the science of cyber security, India and the United States can develop trust that can later be used as the basis for broader diplomatic policy discussions.

Recognizing the need for a more robust cyber security engagement between the United States and India, the American Association for the Advancement of Science (AAAS), Centre for Science, Technology, and Security Policy (CSTSP)[17] and the International Science and Technology Partnership (INSTP)[18] programme have partnered to sponsor an Indo-US Science of Cyber security Initiative.

With support from both government and industry, AAAS will convene a three-day workshop in Bangalore in 2014 to bring together key scientific stakeholders in India and the United States to discuss the scientific underpinnings of cyber security. An inter-disciplinary group of thought leaders from both India and the United States will be selected to participate in the workshop in order to explore, study, and make recommendations to jointly develop a more reliant cyber security environment.

The workshop will provide key inputs to both the US-India Strategic Dialogue and the Joint Commission on S&T Cooperation. Outcomes from the workshop will be published in workshop reports for participants as summary reports and in peer reviewed journals and op-eds as science policy articles. Potential topics for the three-day workshop are: human perception, psychology, physiology, economics, data analytics, model checking, cryptography, type theory, and new technologies to combat phishing, spyware, botnets, and other relevant threats.

As a follow-up to the workshop, AAAS will support early stage interactions between Indian and US scientists on issues identified at the workshop. The sub-awards for these interactions will be selected through a competitive process coordinated by CSTSP and INSTP. Grants will be judged on scientific merit, scientific and technical feasibility, and demonstration of Indo-US cooperative possibilities. A variety of grants could be supported under this aspect of the programme, ranging from student and faculty fellowships, to more substantial awards for technical workshops or virtual joint research.

In 2015, AAAS will hold a symposium at AAAS headquarters in Washington, D.C. to bring together the grantees to present their results and share lessons learned with scientific and policy stakeholders. The proceedings will be published in a final report and disseminated. Key policy makers – particularly those involved in the Joint Commission on S&T Cooperation with India and the US-India Strategic Dialogue – will receive individual briefings by staff and key stakeholders engaged throughout the process.

The [JLM2] present state of Indo-US cyber security cooperation is falling far short of its full potential. Relations between the two countries in cyber security have been characterized by mistrust, misread expectations, and different diplomatic obligations. Cyber attacks and potential cyber threats in both India and the United States are pervasive; this can be partially attributed to the vulnerable nature of the technologies underlying digital communications. These threats in India and the United States will continue to grow as both states more readily rely on digital communications to support key infrastructure, economic, and security activities. There is a need for India and the United States to more deeply cooperate to jointly address these threats.

The science of cyber security provides a mechanism for Indian and American scientists to build trust and address core cyber security challenges, which can later be translated into larger cyber security policy initiatives. Utilizing science diplomacy offers an alternative channel for deeper Indo-US cyber security engagement.

Footnotes:

[1] Andrew Krepinevich, 'Cyber Warfare: A "Nuclear Option"?' Center for Strategic and Budgetary Assessments, 2012.

[2] Brigid Grauman, 'Cybersecurity: The Vexed Question of Global Rules', *Security and Defence Agenda*, 2012, p. 8.

[3] 'Govt. to Chart Road Map to Safeguard India's Cyber Security Architecture', *Business Standard*, 24 August 2013. Retrievable at: http://www.business-standard.com/article/news-ani/govt-to-chart-road-map-to-safeguard-india-s-cyber-security-architecture-113082400153_1.html

[4] Jordy Yager, 'Napolitano Warns Large-Scale Cyberattack on US is Inevitable', *The Hill*, 27 August 2013. Retrievable at: http://thehill.com /blogs/hillicon-valley/technology/318937-napolitano-warns-large-scale-cyber-attack-on-us-is-inevitable

[5] David Evans, 'NSF/IARPA/NSA Workshop on the Science of Security: Workshop Report', NSF/IARPA/NSA Workshop on the Science of Security, 17-18 November 2008.

[6] Robert Meushaw, 'NSA Initiatives in Cybersecurity Science', *The Next Wave* 19(4), 2012, p. 9.

[7] Science of Security Virtual Organization, retrievable at: http://cps-vo.org/group/SoS/about

[8] Dusko Pavlovic, 'On Bugs and Elephants: Mining for Science of Security', *The Next Wave* 19(2), 2012, p. 23.

[9] Ibid.

[10] Ibid., p. 27.

[11] 'The Team for Research in Ubiquitous Secure Technology (TRUST) is focused on the development of cyber security science and technology that will radically transform the ability of organizations to design, build, and operate trustworthy information systems for the nation's critical infrastructure.' For more information: http://www.truststc.org/index.html

[12] A small number of academic research groups, or 'lablets' were funded to conduct specific work in science. The original 'lablets' included Carnegie Mellon University, University of Illinois, and North Carolina State University. The number of 'lablets' conducting science of cyber security has expanded with time due to outreach requirements stipulated to the original three 'lablets'.

[13] See the Science of Security Virtual organization for more information: http://cps-vo.org/node/5991

[14] See, Franz-Stefan Gady, 'US-India Cyber Diplomacy: A Waiting Game', *The National Interest*, 24 October 2012, and Cherian Samuel, 'Prospects for India-US Cyber Security Cooperation', *Strategic Analysis* 35(5), September 2011, pp. 770-780.

[15] For more on historic and current examples of science diplomacy see The Royal Society, 'New Frontiers in Science Diplomacy: Navigating the Changing Balance of Power', *The Royal Society*, January 2010; Micah Lowenthal, 'Science Diplomacy for Nuclear Security', USIP *Special Report*, 2011, and the AAAS Quarterly publication, *Science Diplomacy*.

[16] Micah Lowenthal, 'Science Diplomacy for Nuclear Security', USIP Special Report, 2011, and the AAAS Quarterly publication, *Science Diplomacy.*

[17] CSTSP, established in 2004, has a robust international security portfolio. Ongoing initiatives include scientific engagement in the Middle East and North Africa, Central Asia, and selective engagement through non-sensitive scientific cooperation with Iran and North Korea. These latter activities are done together with the AAAS Centre for Science Diplomacy for such initiatives are indeed trust-building, diplomatic exercises. The goal of CSTSP is to bring high quality analysis and greater transparency to uses at the intersection of science and security while also remaining culturally sensitive to the social needs of multiple international communities. http://www.aaas.org/cstsp/

[18] Based at AAAS, INSTP hosts the US office of the Indo-US Science and Technology Forum (IUSSTF). IUSSTF was created in 2000 to promote mutually beneficial cooperation in science, technology, and health between individuals and institutions in the two countries. IUSSTF has supported the interaction of over 12,000 scientists, 300 bilateral workshops, 40 advanced schools or training programmes, 45 virtual centres, and hundreds of faculty and student fellowships each year. INSTP and IUSSTF have developed a detailed understanding of India's science and technology landscape and built an extensive network of the leading scientists, engineers, health professionals, and research institutions in India. http://www.aaas.org/instp

GABI SIBONI

THE CIVILIAN SECTOR

MOST systems in developed societies rely on computer communication and information infrastructure. This growing dependence on information and communication technologies is a blow to computers and information flow processes, which are liable to disrupt, paralyze, and sometimes cause substantive physical damage to essential systems. Computer based capabilities and their near global ubiquity exposes states to harm in cyberspace through various elements, including hostile countries,[1] terrorist organizations, criminal elements, and even individuals driven by personal challenges or anarchist motives.

Even though states in the past decades have progressed and profited in their production and provision of national services, they have been exposed to new threats. Yet, insufficient attention has been paid to appropriate means of confronting such threats. In the recent past, industry (private and public) was protected by the state. For example, excluding workplace accidents, power stations producing electricity (whether private or publicly owned) were exposed to physical damage only if the state encountered a physical war, and it was the state's job to protect such infrastructure along with economic institutions, industrial facilities and so on.

Public and civilian institutions were protected by virtue of their existence in the territorial space under the state's authority and control. That has changed. In addition, the trend in recent decades to privatize government services has placed a large portion of infrastructure plants traditionally in the hands of the government in private hands, including those relating to communications, transportation, electricity, energy and heavy industry. Moreover, traditional industries in recent decades have been joined with new industries in the hi-tech realm that constitute a significant component of the state's GDP.

In order to create a common language, one may distinguish the cyber-space into three groups. The first group comprises of government security and intelligence organizations. These are the nation's security organizations that are typically investing some effort in their cyber defence. The intensity of this effort is usually subject to the extent of threats and overall awareness levels of the organization's management. In some countries, this is also the case found in government ministries and services. The second group is commonly considered to be the nation's critical national infrastructure. These are civilian services such as communications, transportation, electricity, energy and heavy industry. Advanced countries will have a special authority dealing with or special regulations for cyber defence of these critical infrastructures.

The last group is the rest of the cyberspace users and includes civilian sector industries and private sector businesses. This group is left with no guidance for cyber defence, though a coordinated cyber attack on entities in this group may result in heavy damage. One can only imagine a successful attack occurring on a food or pharmaceutical manufacturer or the effect of IP cyber theft.[2] At the same time, changes in the structure of the nation's economy and the emergence of elements, processes, assets and projects – which, if damaged, could potentially cause significant harm on a national level – have exposed and increased the range of weak points and the targets for cyber attacks.

Moreover, potential damage is not restricted to what can be quantified in financial terms or what impacts the GDP: significant damage can also be caused to assets and values that have cytological effect. Thus, for example, in the United States, defensive plans also apply to heritage and memorial sites.[3]

The aim of this article is to propose a concept and methodology to categorize private sector cyber risks and ways to enhance cyber defence of the civilian and private sector by means of regulations and mandatory minimal security measures. The process proposes to categorize civilian and private sector cyber risks for the effect they may pose to the public.[4]

Who will be subject to regulation? It is commonly understood that a company or organization from the private sector will invest resources for cyber defence only if this is in line with its business needs. Thus, it is unlikely for a company to voluntarily invest resources for cyber security measures that would reduce the impact and consequences on the public from a cyber attack on the company. This is why governments would need to step in with regulations, thus creating one of the main tools of enforcing cyber security standards in the private sector.

Of course, not all private companies will be subject to the same regulations. For example, cyber security requirements for a large food manufacturer would differ from those for a small restaurant. Methodologies and tools need to be therefore developed in order to identify and categorize the private sector: it is proposed to divide the private sector according to risk levels based on the impact of a cyber attack on the public and on national security.

The methodology is based on a two step process. The first step is a screening phase. Private sector companies and organizations will be screened based on a few basic criteria such as activity sector and business volume. In the second phase, each company that has passed the screening round will be graded on the basis of a set of criteria aimed at defining the severity of a cyber attack on national security or the public. At the end, each analyzed company will be given a risk grade between 1 (lowest) to 5 (highest). A set of minimal cyber security standards would be defined for each group. These standards can then be adapted to the type of business or sector the graded company is active in. For example, companies from the energy sector will probably need different cyber security measures than companies in the health sector.

Implementation of statutory regulations of any kind requires a legal framework. It is always preferable to use existing laws rather than trying to initiate new legal frameworks. The aim is to make cyber protection a built-in component of the existing statutory process, both during the establishment stages (i.e., the permits required for new projects) and the operational process (i.e., during the business licensing permit). It is proposed that the legal framework process be also used to ensure compliance with minimum cyber security standards.

This is similar to other regulations. Those businesses that are screened and scored for their cyber risks shall be required to submit a Cyber Resiliency Assessment. This assessment will constitute the main statutory tool for examining the project's and business's exposure to the possibility of cyber attacks. Protective measures against these risks/vulnerability would be based on the minimal defence standard for each particular risk group. At the same time, within the framework of business licenses (licenses requiring periodic renewal), the relevant authority can check for ongoing compliance with cyber protection instructions of the organization under review.

The establishment of every project requires compliance with the processes of statutory planning. Thus, projects need to build facilities and structures that must be approved by various planning commissions in accordance with relevant regulations at local, regional, and national levels. A review of the planning documents submitted for approval is the planning authorities' central tool of control over these projects. Currently in most states, among the documents submitted for review by the planning commissions, one may find reports concerning firefighting, public health issues, environmental aspects, handling of hazardous materials, home front defence requirements, etc. The documents define the steps the project initiator is required to take in order to comply with the necessary requirements in each of these areas. These steps are then to be relayed to the authorized regulatory authorities, who would employ experts to ensure that the project is being implemented with public interest in mind and public security is maintained throughout the various spheres.

In Israel, dozens of projects that could potentially damage or might harm national security are discussed every year, including infrastructure facilities, water and sewage treatment facilities, delivery systems, transportation projects, energy facilities and communications. Expansion and establishment of industrial factories and a wide range of other projects are discussed as well. Cyber damage to some of the projects and ventures is liable to harm the country's economy not only directly, such as through the inability to supply an essential service, but also in the form of commercial damage where targeted Israeli companies would be unable to supply their products for a given period.

An example clarifying the above process of documentation is the requirement to submit an Environmental Impact Assessment. The goal of the assessment is to identify the environmental hazards likely to be caused by the project, along with ways to minimize the damage to a tolerable level. Submission of the review is anchored in the planning and building regulations (of 1982, and in its final version of 2003). The idea for this review originated as a response to the magnified public awareness in the United States on environmental issues, and in 1970, legislation was passed requiring the Environmental Impact Assessment to be a part of the preparation for the planning process.

Together with the planning component of new projects, it is also possible to make use of the business licensing process. This requires periodic renewal to ensure the project meets the necessary criteria in various spheres over the years, including protection from cyber attacks.

When a decision is made, the organization must submit a Cyber Resiliency Assessment. This process will adhere to a defined procedure, as follows:

a) Assessment guidelines. It is the responsibility of the regulator to provide guidelines for carrying out the assessment. These guidelines must be suited to the sector of the specific body and cover a number of components, including: mapping potential damage to national or to public security from a cyber attack; mapping vulnerability of the business; and issuing instructions making it possible to minimize exposure and damage.

b) Assessment preparation. The assessment will be prepared under the auspices and from funding of the project initiator or the business seeking the permit. This is best done with the help of designated consultants trained and authorized by the regulator.

c) Checking the assessment. This lies under the responsibility of the regulator and may also involve use of external advisors trained and authorized to check the reviews, with the cost charged to the project initiator of the business.

d) Approval of the assessment. This would include examination and a review by regulator officials and a decision on guidelines in this context for the business. This approval can also address aspects of the stipulations for the business license.

Who will be the regulator? There are three options in regard to the identity of the government's regulator: the sectorial approach, the centralized approach and the hybrid approach. All have their advantages and disadvantages.

1. The sectorial approach entails each ministry being responsible for the business and projects within its sector. This enables the cyber security regulation process to be more professional and sector oriented. For example, the ministry for communication shall be in charge of the regulation of Internet service providers, telecom companies, web hosting services, etc. On the other hand, utility providers (energy, water, petrol, etc.) shall be regulated by the relevant sectorial bureau/ministry.

2. In the centralized approach, all cyber security related regulation will be handled by a single regulator, either from a dedicated cyber defence ministry or from the government's appointed authority designated in charge of cyber security regulation. A single authority shall develop knowhow on cyber security regulation and advocate necessary adaptations for each sector.

3. The hybrid approach is a mixture of the above two. Some of the string sectors regulators (i.e., ministries) will be given cyber security regulation authorities and the rest shall be put under a centralized authority. This approach takes into account the existing linkages within the government to provide an optimal level/ strategy of cyber security defence for the private sector.

Threats to civilian companies and the private sector have grown not only because of increased competition in the marketplace, but also because of their exposure to attacks by hostile elements. Hostile parties identify the potential damage to the country's economic infrastructure inherent in striking these companies. States tend to mainly protect bodies that have a direct connection to national security. This traditionally and primarily includes government offices, intelligence and security bodies, organizations engaged in sensitive/classified security manufacturing, and classical critical infrastructure such as electricity, water and transportation.

The logic defined within the criterion of this privileged class was derived from the classic strategic concept: a list of national infrastructures susceptible to disaster in the event of war, and which, if damaged, could cause direct harm to the country's fighting ability and resilience. However, this raises questions regarding the fate of civilian and private sector companies such as the pharmaceutical industry and food manufacturing companies. Additionally, what of cable and insurance companies, not to mention memorial and heritage sites? A quick examination shows damage to these organizations is liable to cause significant damage to the country and harm the fabric of civilian life.

Now, with increasing realization that cyberspace is becoming a combat zone before our very eyes, the ability of the states and their economies to weather cyber attacks must be enhanced. Introducing cyber defence regulation in the statutory processes can allow continuous, systematic monitoring of the immunity of a nation's cyber security system.

* This article is partially based on research published by the author in *Military and Strategic Affairs* 3(1), May 2011.

Footnotes:

1. Mandiant, 'APT1: Exposing One of China's Cyber Espionage Units', February 2013. http://intelreport.mandiant.com/Mandiant_ APT1_ Report.pdf

2. Office of the Counter-intelligence Executive, 'Foreign Spies Stealing US Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011', Annex B – West and East Accuse China and Russia of Economic Espionage, October 2011. http://www.ncix. gov/publications/reports/fecie_all/ Foreign_ Economic_Collection_2011.pdf

3. Patrick Beggs, 'Securing the Nation's Critical Cyber Infrastructure', US Department of Homeland Security, 25 February 2010.

4. The idea is to identify how severe a successful cyber attack on a certain civilian or private sector company is to the public. The proposed method does not deal with the consequences of a cyber attack on the internal organization's business and operations.

OLEG DEMIDOV

LESSONS FROM RUSSIA

BEFORE making any analysis of Russia's or India's national cyber security policies, it is necessary to stress the fact that cyber security itself is a complex concept bringing together efforts and policies on a large number of different but interconnected issues (including countering cyber crime and cyber terrorism, privacy protection, global identification of users, resilience of networks, dealing with cyber espionage and cyber sabotage). Prevention of cyber wars and politically motivated malicious activities in cyberspace is a different set of issues.

Even the understanding of cyber security can be drastically different. Russian official documents and international agreements to which Russia is party (like the Shanghai Cooperation Organization Agreement on cooperation in the field of IIS from 16 June 2009) refer to the information space as a 'sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information'; Indian National Cyber Security Policy, based on the ISO standard, refers to cyberspace as 'an environment consisting of interactions between people, software and services supported by worldwide distribution of ICT, devices and software.' Germany understands cyberspace as 'the sum of all IT systems linked at data level on a global scale' – however, no air-gapped Supervisory Control And Data Acquisition (SCADA), are part of cyberspace, if a literal understanding is taken.

Diverging conceptual paradigms of cyberspace give birth to differing cyber security strategies, and this is a major reason behind ongoing global debates on cyber security treaties and international legal mechanisms for making cyberspace more secure.

The official Russian approach towards information security is focused on four major threats to the system of international information security. Those include the strategic triad of threats (the use of ICTs in (i) criminal, (ii) terrorist and (iii) military-political purposes) and also the threat of using ICTs for undermining the nation's political sovereignty and spreading extremism. The fourth element was introduced to Russian documents and proposals after the events of the Arab Spring of 2011.

These four priorities are perceived in a set of documents and initiatives which are developed and promoted by Russia on several levels: global (through the UN mechanism), regional (Collective Security Treaty Organization, CSTO), Commonwealth of Independent States (CIS), Shanghai Cooperation Organization (SCO), BRICS and with a less priority–G8, G20, Asia-Pacific Economic Cooperation forum (APEC) and Organization for Security and Cooperation in Europe (OSCE) and bilateral.

At the global level, a major Russian initiative is the concept of Convention on International Information Security, presented to the world in November 2011 at the first International Conference on Cyberspace in London. The document is designed as a UN Convention – a first ever legally binding global instrument for cyberspace. Though the convention was not adopted at the UN level and provoked severe criticism from a number of Russia's partners, including the USA and most western European states, it remains a top priority on the Russian agenda in the field of international information security.

At the bilateral level, some important developments have taken place in recent years. For example, in 2010, a bilateral intergovernmental agreement on cooperation in the field of international information and communication security was signed by Russia and Brazil. However, it has not yet been ratified, although recent events related to the disclosures by Edward Snowden increase the probability that work on ratification will continue. Another important bilateral achievement took place on 17 June 2013, when the Russian president and his US counterpart signed a joint statement and three agreements on CBMs in cyberspace, which imply the establishment of a 24x7 US-Russian hotline on cyber incidents, strengthened cooperation of national Computer Emergency Readiness Teams (CERTs) and information sharing on cyber incidents. Implementation of these three agreements, however, could be adversely affected by the Snowden disclosures, as the information on massive electronic surveillance programmes conducted by NSA threatens to seriously undermine mutual trust between Moscow and Washington.

Nationally, Russia has a number of bodies dealing with cyber security. Federal Security Service (FSB), Federal Protective Service (FSO), special units of the Ministry of Interior/Home Affairs and Ministry of Defence, Federal Service on Technical and Export Control (FSTEK) are some of the major ones. On 15 January 2013, President Putin signed the Order 15N, which delegated the responsibility of building a nationwide system protecting governmental networks to FSB – which shows that Russia and India are following a similar path in setting up national institutional frameworks for a cyber security agenda. In the area of cyber defence, the situation has developed dynamically as well. Starting from the winter of 2012, work is ongoing to establish a Russian analogue of a Cyber Command within the structure of the General Staff of Russian Armed Forces.

Going back to the hierarchy of Russia's approach, all of its international priorities are parts of an integrated vision that was recently summarized in a national level document, signed by President Putin in August 2013. It is called the National Policy Guidelines of the Russian Federation in the Field of International Information Security to 2020. The fact that the document was signed just a month after the Indian National Cyber Security Policy (NCSP) makes for an interesting comparative analysis of these two strategic documents and approaches embedded in them.

At first glance, the two documents seem to be almost completely different – the Russian policy guidelines are totally dedicated to the international dimension of cyber security policies, whereas the Indian NCSP is focused on interaction among national stakeholders and strongly emphasize the vital role and contribution of the private sector to Indian cyber security system and policy.

In general, the NCSP is a timely strategic document, which provides a strong incentive for further elaboration of a cyber security agenda and strategy for India Its advantages are quite clear: correct and clear understanding of the role of the private sector, accent on coordinating role of the government instead of direct and rigid regulation, priority of critical information infrastructure (CII) protection.

Still, there are certain aspects of the NCSP which might benefit from further efforts and improvement. First, that the NCSP is not a cyber strategy in itself should be clearly understood. A cyber security strategy implies an action plan, probably a concrete time frame with a set of measurable objectives to reach, as well as integrated vision of the institutional framework for its implementation, the range of stakeholders and partners to counteract with and, finally, some resource parameters.

What is it that seems to be missing from the NSCP in particular?

1. An international cooperation component. India needs to know with whom to develop international PPPs in the field of cyber security. Another part of the issue is how to cooperate with transnational IT corporations on the issues of identification, privacy and personal data protection. Given that Facebook and Google are transborder actors, what should be the strategy of their engagement in the process of implementation of the NCSP goals? The question then veers towards who could possibly partners India for developing confidence – and trust – building measures (CTBMs) in cyberspace, including information sharing, incident reporting, joint monitoring, etc.

   Another aspect is the international framework for fighting cyber crime. While significant attention is now paid by Indian experts to the Council of Europe's Convention on Cyber Crime, there is no mention in the NCSP on India's place in the international system of coordinates in countering cyber crime. This agenda should not be approached in an isolated framework of a separate document, as it is an inherent part of a national cyber security strategy.

2. An integrated institutional framework of a nation level cyber security system. Several important steps are mentioned in the NCSP, including establishment of a 24x7 National Critical Information Infrastructure Protection System, as well as the setting up of a nodal agency responsible for coordination of all national cyber security matters and strengthening the national system of CERTs. Still, there is no holistic institutional framework visible in the document. Which cyber issues remain in the domain of the Defence Ministry, how are they handled and how are the responsibilities divided between military and civil agencies and units? Who is in charge of conducting a response against a massive cyber attack against government and private assets in cyberspace? What should be the hierarchy and division of responsibilities between the newly established nodal agency and previously established units like monitoring centres and IT security task forces?

There is much work to be done in order to make the next important step – i.e., elaboration of an Indian national cyber security strategy, a currently ongoing process. Among many other vital issues that the authors of Indian strategy will certainly face is international cooperation in the field of CII protection. This is particularly important because recent practice shows that most sophisticated attacks target CII, including nuclear, oil and gas facilities and power grids, and in many cases they are too complicated to be effectively investigated only by national security services or private experts of a state which is facing the attack. A case in point is Stuxnet: the first known precedent of cyber sabotage implemented through the use of a very advanced malware to covertly control the work of SCADA. It was first discovered and investigated by a Belorussian IT-security company, then the Russian Kaspersky lab. Kaspersky lab was invited through the ITU-IMPACT mechanism to investigate the case of sophisticated attacks on SCADA of an oil plant in one of the Gulf states as local experts were not even able to identify the malware properly.

The conclusion here is quite clear – the best talent must be recruited not only nationally, but the world over, in order for the best world practices, skills and experience to counter sophisticated attacks against critical information infrastructure. And therefore, a mechanism to share best practices globally is needed. One promising option for that is the mechanism of international public-private partnerships (PPPs), which is also the legal format of the IMPACT-ITU alliance bringing together many private enterprises from the IT security sector (Russian Kaspersky lab and Group IB among them) and 146 nation states including India. The role of ITU-IMPACT in the context of Indian cyber security strategy must be identified. Whether India should use this experience in order to develop similar mechanisms on a regional level where states will be engaged also needs deliberation.

Another topical agenda for India that might require some push on the international front concerns cyber security of nuclear infrastructure. In July 2013, PIR Centre conducted a situation analysis dedicated to cyber attacks against nuclear infrastructure by unknown politically motivated proxy actors. According to the situation analysis, two Indian Nuclear Power Plants (NPPs) Tarapur-1 and Tarapur-2 located 130 kilometres from Mumbai, with their old single circuit reactors were attacked when their SCADA systems of external power grid and condensate-feed water systems were hit by a sophisticated worm. Many issues related to international law emerged, but most of them remain unanswered. One of them was surprisingly related to the India-Pakistan Non-Attack Agreement of 1988 and its provisions concerning a ban on attacks on NPPs. Would a cyber attack similar to Stuxnet fall under the agreement if presumably conducted by Pakistan or Pakistani-led proxy actors? The answer is not clear, and thus the question demands clarification. There are plenty of similar conceptually challenging issues related to critical infrastructure protection, cyber defence and adaptation of international law to cyber conflicts that need hammering out.

To conclude, it seems that some homework remains to be done by the Indian government and all major stakeholders to reach a consensus on an integrated national vision of cyber security agenda in its international aspects and implications. The time to do so is now. The NCSP is a timely step, which should be followed by a document focusing on an international agenda. Here, Russia with its rich experience and well developed vision could be an important partner for India; a strategic Russian-Indian dialogue on international cyber security ecosystem might be a fruitful and mutually beneficial initiative, given that Russia also has much to learn from India's cyber security background, particularly the experience of engaging the private sector to play a leading role in achieving national cyber security goals.

RAJESWARI PILLAI RAJAGOPALAN

GLOBAL AND NATIONAL SECURITY IMPERATIVES

CYBERSPACE security challenges are generally considered the 'emerging frontiers' in the security discourse although the reality is that they already represent a clear and contemporary danger to India and the rest of the world. While states are aware of and have acknowledged the challenges, it has been difficult to agree upon a common approach to addressing these challenges. Therefore, unlike in the nuclear arena and to a more limited extent the outer space domain (another emerging security frontier), cyberspace continues to be driven by broad acceptance on basic principles rather than specific agreements, institutions or norms. The imperative today is to move from the former to the latter. Given the global nature of the issue, this is an effort that has to be inclusive rather than one limited to just the major powers.

I argue here that there are both global and domestic imperatives that push for clear articulation of policies and strategies that could contribute to ensuring safe, secured and uninterrupted use of the cyber domain. In this essay, I first outline the current global architecture governing cyberspace and its weaknesses and then at the challenges faced by India in this domain from a national perspective. This is followed by a discussion on India's approach thus far to meet these challenges, which has essentially been more ad hoc in nature. The paper concludes with some suggestions about how we might move forward at both the national and the global level.

A major problem with cyber security is defining it. The International Telecommunication Union (ITU) uses a fairly broad explanation, describing it as 'systems and services connected either directly to or indirectly to the Internet, telecommunications and computer networks.'[1] But we also need to make a distinction between information security and cyber security. States have an obvious interest in securing information for national security purposes. But cyber security should ideally be looking at integrity and availability of computer networks. A serious concern here is the difficulty of identifying sources of attacks, as well as the fact that cyber attacks could prevent authorized and legitimate users access to systems and technologies when these are most required.[2] However, measures to secure this domain should not replicate the more traditional ones related to arms control.[3]

This is particularly so for two key reasons: one, the technology is widespread and given the centrality of individuals in the larger consumer base, efforts to effectuate control through arms control-like measures is unlikely to work. Put simply, controlling state behaviour alone is insufficient. Two, non-traditional aspects of the cyber domain also need to be emphasized as terrorists or criminals intending to create large-scale chaos and interruption can deploy dangerous programmes such as 'cyber-worms' to attack and disrupt a country's critical assets. Traditional arms control measures cannot control these actors.

As noted earlier, tackling cyber security at the global level has had far less success as compared to some of the other security domains. There are no overarching laws and regulations as yet in place for the cyber sector. With no treaty and such like arrangements, cyber security is ensured through a few broad guidelines underlined in ITU's key principles for 'cyberpeace' and the Group of Governmental Experts (GGE) reports.[4] These loose set of norms are also non-binding in nature, depending upon the goodness of states for their enforcement.

Being the principal UN body on information and communication technologies (ICT), the key function of the ITU is to act as the coordinating point for governments and private sector. In addition, the ITU is also central to creating and sustaining security and confidence in the domain by developing appropriate networks and services.[5]

According to the ITU Secretary General, there are five key principles that should govern cyber peace: (i) every government should commit itself to giving its people access to communications; (ii) every government should commit itself to protecting its people in cyberspace; (iii) every country should commit itself to not harbour terrorists/criminals in its own territories; (iv) every country should commit itself to not be the first to launch a cyber attack on other countries; and (v) every country must commit itself to collaborate with each other within an international framework of cooperation to ensure that there is peace in cyberspace.[6]

Three GGEs has so far been convened under the aegis of the UN and their reports have addressed many of these issues. The first GGE was established on the basis of a Russian proposal in 2003 and the group came into existence in 2004 to look at the entire gamut of issues involved in cyber security. However, disagreements within the group meant that it did not arrive at any consensus about how to proceed further. These disagreements centred around implications of ICTs on national security and military affairs.[7] The second GGE that was convened in November 2009 managed reasonable consensus and recommended development of norms in order to reduce risks while protecting vital infrastructure such as information exchange regarding national legislation. However, the divide regarding the protection of information content versus information infrastructure continued.[8]

As compared to the two previous GGEs, the third one has achieved far more success. Established in August 2012, it submitted its report in June 2013 and acknowledged the applicability of international law to cyber-space. It stated that, 'International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.'[9] The report also recommended that 'state sovereignty and international norms and principles that flow from sovereignty apply to state conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.'[10] However, 'respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments' are to be given equal emphasis and recognition. The report also suggests that states must 'meet their international obligations regarding internationally wrongful acts attributable to them.' The report details a series of suggestions in the area of confidence building measures (CBMs) and exchange of information. While these are ideal steps that states must adopt and promote, the weakness of the entire exercise is that these are merely recommendations and not binding on states.

Furthermore, the report asserts that 'there is a need to enhance common understanding' without making an effort on actual definition or clarification of, for instance, what constitutes responsible behaviour in the cyber domain. The report nevertheless reflects progress over the previous initiatives, the major addition being a reference to international law.

The key problem in cyber security is that there exist two broad sets of concerns – one articulated by the West and the US in particular, and the other by China and Russia and some of the developing countries. The West's concerns are with regard to potential attacks on their cyber networks: essentially, how others could break into their networks, jam them, change the communication channels, send wrong and misleading information, and so on. The West has particularly emphasized protection of networks and critical infrastructure while being generally supportive of the free flow of information. The West's approach is far more comprehensive and includes information and communication technologies as well as cyber networks, whereas the Chinese and Russian focus is only on the former.[11]

Concerns from China and Russia have centred around a fear of use of social media and other information sharing platforms to incite social tensions and threaten regime security, particularly with external help. The Chinese concerns are specifically related to their need to control restive populations in the Uighur and Tibet regions and anti-regime groups such as the Falun Gong. Russia is concerned about the so-called 'colour revolutions' and how external players may use social media and other means of communication to spark domestic uprisings. However, protection of vital infrastructure is an equally important priority for Russia, even if not so articulated in their larger discourse.[12]

Russia and China, along with Uzbekistan and Tajikistan, have proposed an international code of conduct for information security. Their proposal talks about instituting rights and responsibilities of states in safeguarding information and cyber networks while calling on states to respect domestic laws and sovereignty. The Chinese emphasis has been on the technologies, including social media platforms such as Twitter and Facebook, which Beijing sees as 'weapons if their use violate[s] individual state laws.'[13]

The proposed code says that states should not 'use information and communication technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies.'[14] It goes on to say that states should not engage in 'the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment.' While these clauses sound innocuous as general principles, they could impinge upon freedom of speech, among other basic freedoms and human rights. Though some aspects of the Russian-Chinese proposals are important, some of these negative elements need to be removed.

Despite the differences between these two camps, the proposed international code still provides an opportunity for 'continued discussion about mutual restraint, cooperation, and on what should be the rules of cyberspace.'[15] In fact, it did provide for a broader debate at the global level on measures to govern outer space, such as norms, transparency and CBMs or more binding mechanisms such a treaty. The code specifically, however, does not delve into such measures, which is a key limitation.

In the broader global context, cyber concerns and challenges include cyber fraud, defamation, privacy intrusion, cyber attacks through proxy actors, attacks on critical infrastructure, cyber espionage, sabotage and disturbance of social harmony. Finding the right balance between internet freedom and cyber warfare is going to be a major challenge but is nevertheless essential to making cyberspace safe, secure and predictable.

Google Transparency Report
India: 'In response to a court order, we removed 360 search results. The search results linked to 360 web pages that contained adult videos that allegedly violated an individual's personal privacy.'

What has India's approach been to these disputes and the challenge of cyber security? India's approach towards cyber security is unclear when compared to traditional security issues. Its broad policy approach is guided by two drivers: national security and social harmony, something of an amalgamation of the western and the Russian-Chinese approach. Earlier, India's approach used to be driven primarily by the former concern, given the large number of hacking and jamming related incidents in the country and on Indian missions abroad. Lately, the debate has shifted to one with a greater emphasis on social cohesion, which has resulted in stricter monitoring and surveillance of internet and social media activities.

In April 2011, India brought out new Information Technologies (IT) rules under the IT Act 2000 that mandate websites and service providers to act on requests to remove content that is considered 'blasphemous', 'hateful' or 'disparaging' within thirty-six hours of notification. Later in the year, the government lodged formal complaints against major IT firms like Microsoft, Facebook, Yahoo and Google, asking for the removal of objectionable and inflammatory content as well as 'pre-screening' of content.

The statistics from the Transparency Report of Google is evidence of the tighter control that New Delhi is seeking.[16] While requests from governments across the world on user information have been on the rise, India has made the second largest number of such requests – 2,691 during January-June 2013.[17] The numbers have gone up since the previous year. The report for 2012 said that in the six-month period between January and June 2012, the Indian government had asked for web user details of as many as 2,319 cases and got 596 items removed (doubled over the previous six months) from Google's associated pages such as YouTube videos, Orkut, certain search results and images.[18] The government's rationale for such intrusive measures included privacy and security, defamation issues, pornography, anti-government criticism, impersonation, national security and copyright issues.

New Delhi points to serious social stability issues in defence of such activism. In August 2012, miscreants used social media to spark rumours of attacks on citizens from Northeastern India living in South Indian cities leading to one of the largest internal exodus in the country. Up to 30,000 people fled the IT capital of Bangalore that August. Following the incident, the Indian government decided to block over 250 websites that it accused of carrying 'inflammatory' pictures and videos that triggered this mass exodus.

Meanwhile, to deal with the challenge of critical infrastructure protection, the government amended the IT Act 2000 with IT (Amendment) Act in 2008 (ITAA 2008), instituting more stringent measures for data protection. With the passage of ITAA 2008, IT organizations were asked to consider stricter audit practices, including ISO 27001, as a means to strengthen IT security practices in India. However, there are vague terms and concepts such as 'reasonable security practices' and 'sensitive personal information' in the act that need to be defined with greater clarity. Further amendment of the IT act and the IT Rules are required although the government appears to be putting off tougher issues from the agenda for the time being. Instead, it has plans to erect a cyber security architecture with 24/7 monitoring equipped with adequate manpower so that the system remains foolproof.

New Delhi's other efforts, such as the 2011 IT rules, have generated sharp criticism with critics pointing out that these infringe on individual freedom of speech and expression enshrined in Article 19 of the Constitution. The government's blanket ban approach is unlikely to curb this problem because the penetration of cyber technology is taking place in a manner that makes these measures ineffective. For example, since cell phones (particularly the new generation smartphones) have now penetrated India's remotest areas, even those without computers or internet are active in the social media. The reach of social media through such technologies is far greater than computer ownership or even literacy, and thus no government measure can be fully effective. A country with 900 million mobile subscriptions, of which around 70 million use 3G/ 4G connections, indicates the challenges. The 70 million 3G/4G users are forecast to grow at a rapid pace, and government measures to restrict web users through intermediaries (one of the measures suggested in the 2011 IT Rules) will be difficult.

Therefore, India's concern regarding the protection of its cyber networks is going to be far more challenging. A report card on the government approach in handling such threats does not inspire confidence. India's justification has been that it is not well networked and, therefore, the vulnerability to attacks is remote. However, the reality is different: India is prone to data theft, hacking and cyber terrorism, and has been regularly attacked by cyber 'warriors' from outside the country for the last few years. The Computer Emergency Response Team-India (CERT-IN) data depicts this story in numbers: hacking incidents on government websites went up to 303 in 2010, 308 in 2011 and 294 in 2012 (till October).[19] CERT-IN says that the total number of 'security incidents' have tripled since 2007, having handled more than 22,000 cases in 2012. Both hacking and defacement have direct economic costs as well as demonstrate India's vulnerability. Some hacking (many originating from China), such as that of Indian think tank websites, may not have resulted in the loss of any confidential information nor have had much economic impact but they prove India's continuing vulnerability. In addition, of the 7,000-odd government websites, half remain outside the ambit of security audit, which is mandatory. Lack of adequate manpower is the usual explanation for not carrying out the mandatory security audits.

While there is no universally adopted definition of cyber security, in simple terms, it means the ability to guarantee safe, secure, uninterrupted and sustained access to for the use of cyber-space. But India needs to move from a purely defensive approach to a deterrence based approach. Even as achieving deterrence in cyberspace is going to be extremely challenging, deterrence will be the key driver in India's approach to cyberspace security.

As India formulates its cyberspace policy, a few issues have to be highlighted and addressed. First, India needs to clearly mark the boundaries that cannot be crossed when it comes to cyber security. It is important to draw these boundaries in terms of activities from a national security as well as an international rule making perspective. Codification of activities and marking clear red lines is the first step in ensuring deterrence in cyberspace. A code or a mechanism that identifies certain activities as irresponsible and unacceptable would help in deterring such actions. Identifying boundaries and codifying activities will go a long way in determining, at the national level, when an activity can be termed as an act of war, and when defensive responses can be activated and justified. Lack of clarity or ambiguity about red lines not only undermines deterrence but increases the potential for miscalculation: states would benchmark red lines for others based on their own internal calculations which others might not be aware of, thus leading others to cross such red lines inadvertently.

However, drawing red lines and boundaries in the cyber domain will prove to be very challenging. Will a state's deliberate attack on another's critical infrastructure be categorized as an 'armed' attack and, if so, how should states respond? Under what circumstances should states invoke their right to self or collective defence under the UN Charter? Clearly, states have an inherent right to respond if their vital infrastructure and installations come under attack, but this becomes complicated if it is a cyber attack rather than a traditional military attack. In addition, states need to be able to correctly assess who the attacker is. Identification and attribution are critical in determining any counter-attack measures.

Second, while there are difficulties in identification and attribution of prohibited activities, the bigger challenge is to design punitive steps once prohibited activities are verified. Means to effectively deter those actions in the future will also prove to be difficult. States have to agree upon a set of temporary and reversible measures to make deterrence effective in the cyber domain. Identification and attribution are much harder in the case of cyber threats. Indeed, with a growing number of players in the cyber arena, including private sector actors, attribution and verification are likely to become even harder in the future. Moreover, attributing the role of states or state support to a particular cyber crime is going to be a major challenge.

Meanwhile, India's institutional mechanism and structures to deal with cyber security are at an early phase and there is far less clarity as compared to the more traditional security domains. The cyber domain is relatively new and the structural mechanisms are slowly taking shape in the face of multiple incidents in the last few years. The government has begun to appreciate the criticality of issues involved and is thus taking a few baby steps. The Minister for Telecom and Information Technology, Kapil Sibal stated that India is investing about US$ 200 million over the next four years to create the necessary infrastructure.[20]

In 2013, the government took the next step in formulating a cyber policy.[21] Releasing its National Cyber Security Policy, it appointed CERT-IN as the nodal agency for cyber security issues in India.[22] The government is also in the final stages of approving the establishment of a Joint Cyber Space Command that would synergize the efforts of the armed forces as well as the civil agencies involved.[23] The policy also announced the establishment of a 24/7 National Critical Information Infrastructure Protection Centre (NCIIPC) under the National Technical Research Organization (NTRO), meant to protect and enhance resilience of national critical information infrastructure. The policy also envisages appointment of a Chief Information Security Officer (CISO) who will oversee the government efforts in enhancing cyber security. Furthermore, India aims at creating a workforce of 500,000 cyber professionals within the next five years. The policy also encourages involvement of private sector to strengthen its preparedness by conducting security audits. The role of private sector is also significant with respect to developing indigenous security products to meet domestic demand as well as developing 'standard security practices and processes.'

In June 2013, the National Technical Research Organization (NTRO) released the Guidelines for Protection of National Critical Information Infrastructure that outlines key principles for critical sectors so as to develop a road map for protection of their information infrastructure.[24] In a move that will strengthen India's indigenous capacity to provide certification for electronics and IT products, India was acknowledged as an 'Authorizing Nation' under the international Common Criteria Recognition Arrangement (CCRA) in September 2013. India is the 17th nation to be so recognized. This recognition allows India to test and certify electronics and IT products related to cyber security. This new status means India is no longer only a 'consuming nation' and opens up the opportunity to invest in and develop laboratories and technologies. It also makes a strong case for public-private partnership in the cyber domain.

Given the increasing number of challenges in the cyber domain, there is a need to draw clear lines that will bring about certain restraints in terms of national capabilities and behaviour. Currently, there is no globally agreed upon approach to addressing these challenges. In the interest of prudence, it may be worthwhile to start with the least common denominator: one possibility is establishing broad norms regarding acceptable behaviour and strengthening Transparency and Confidence Building Measures (TCBMs), which could gradually move towards more legally binding and verifiable agreements and institutions.

At the domestic level, India's policy initiatives represent a good start, although the policy requires more clarity. While some of these measures are deemed necessary from a security perspective, issues of privacy, intrusion and infringement on individual freedoms are equally important to consider in mind. As a democracy, it is particularly important for India to find a balanced and nuanced approach as it streamlines its policy.

Finally, India should play an active role in the global dialogue on cyber security. Such a dialogue can lead to a cyber security regime, which initially could be in the form of broad norms and TCBMs. Taking an active role will enable India to shape the regime in accordance with its security concerns. More importantly, it will ensure that a regime is not imposed on New Delhi at a later stage but rather will be one which India has actively helped shape, thereby giving it a sense of ownership and legitimacy.

Footnotes:

[1] Frederick Wamala, The ITU National Cybersecurity Strategy Guide, September 2011, http://www.itu.int/ITU-D/cyb/cyber-security/docs/ITUNationalCybersecurity StrategyGuide.pdf.

[2] Ibid.

[3] Russia, for instance, has suggested 'measures limiting the spread of information weapons; regime prohibiting the development, proliferation and use of information weapons', among others. However, approaching the cyber domain in the traditional arms control sense is not feasible given the permeating nature of ICT. See, Statement by the Russian Participant at the UNIDIR Cyber Security Conference, What Does A Stable Cyber Environment Look Like? Geneva, 8-9 November 2012, http://www.unidir.ch/files/conferences/pdfs/looking-towards-the-future-of-cyber-security-what-does-a-stable-cyber-environment-look-like-russian-federation-en-1-794.pdf

[4] For an excellent overview of instruments on cyber security, see Ben Baseley-Walker, 'Transparency and Confidence-Building Measures in Cyber Space: Towards Norms of Behaviour', UNIDIR, http://www.unidir. org/pdf/articles/pdf-art3166.pdf

[5] Hamadoun I. Toure, Secretary-General of the International Telecommunication Union and the Permanent Monitoring Panel on Information Security, World Federation of Scientists, The Quest for Cyber Peace, January 2011, http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf

[6] Ibid.

[7] United Nations Office for Disarmament Affairs, 'Developments in the Field of Information and Telecommunications in the Context of International Security', *Fact Sheet*, June 2013, http://unoda-web.s3.amazonaws.com/wp-content/uploads/2013/06/Information_Security_Fact_Sheet.pdf

[8] United Nations, Report of the First Committee, 'Developments in the Field of Information and Telecommunications in the Context of International Security', 9 November 2010, available at http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/544/25/PDF/N1054425.pdf?OpenElement.

[9] Report of the Group of Governmental Experts on Development in the Field of Information and Telecommunication in the Context of International Security. Submitted to the UN General Assembly 68th Session, 24 June 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98

[10] Ibid.

[11] India, too, has articulated a broad approach incorporating both information and communication technologies. See Amandeep Gill, 'What Does a Stable Cyber Environment Look Like?' UNIDIR Cyber Security Conference, 8-9 November 2012, Geneva, http://www.unidir.ch/files/conferences/pdfs/looking-towards-the-future-of-cyber-security-what-does-a-stable-cyber-environment-look-like-india-en-1-793.pdf

[12] For instance, a Russian statement emphasized this aspect, saying, 'the danger of use of information weapons against critical structures is comparable to the danger of use of weapons of mass destruction.' See, statement by the Russian participant at the UNIDIR Cyber Security Conference, op cit., fn. 3.

[13] Timothy Farnsworth, 'China and Russia Submit Cyber Proposal', *Arms Control Today,* November 2011, http://www.arms control.org/act/2011_11/China_and_Russia_ Submit_Cyber_Proposal

[14] Ministry of Foreign Affairs of the Republic of China, 'China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations', 13 September 2011, http://www.fmprc.gov.cn/eng/wjdt/wshd/t858978.html

[15] Robert Deibert, 'Tracking the Emerging Arms Race in Cyberspace', *Bulletin of the Atomic Scientists*, January/February 2011, http://thebulletin.org/2011/januaryfebruary/ronald-deibert-tracking-emerging-arms-race-cyberspace.

[16] For a more detailed and updated coverage, see, Google Transparency Report: India, https://www.google.com/transparencyreport/removals/government/IN/?p=2013-06

[17] Shruti Dhapola, 'Google Transparency Report: India Second in Seeking User Data', *First Post*, http://www.firstpost.com/tech/google-transparency-report-india-second- in-seeking-user-data-1235285.html?utm_ source=ref_article

[18] PTI, 'India's Requests for Web Content Removal, User Details Rise: Google', 15 November 2012, available at http://articles. economic times.indiatimes.com/2012-11-15/news/35111753_1_data-from-government-entities-transparency-report-orkut

[19] PTI, 'Over 270 Government Websites Hacked During Till July This Year', *The Economic Times*, 4 September 2012, http://articles.economictimes.indiatimes.com/ 2012-09-04/news/33581976_1_government-websites-cyber-attacks-cert; Indian Computer Emergency Response Team (CERT-In), Department of Information Technology, Ministry of Communications and Information Technology, Government of India, *Annual Report* 2012, pp. 4-7.

[20] PTI, 'Government to Invest $200 mn in Four Years on Cyber Security Infrastructure', *The Economic Times*, 30 October 2012, http://articles.economictimes.indiatimes.com/2012-10-30/news/34817067_1_cyber-security- cyber-crime-fight-cybercrime.

[21] Ministry of Communication and Information Technology, Department of Electronics and Information Technology, National Cyber Security Policy-2013 (NCSP-2013), 2 July 2013, http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security %20Policy%20(1).pdf

[22] CERT-IN has established counterparts within various departments such as CERT-Army, CERT-Navy and CERT-Air Force. The National Technical Research Organization (NTRO) and Intelligence Bureau are also among those also involved. However, the role and functions are still scattered.

[23] Rajat Pandit, 'Tri-service Commands for Space, Cyber Warfare, '*Times of India*, 18 May 2013, http://articles.timesofindia. india-times.com/2013-05-18/india/39353403_1_ aerospace-command-cyber-command-new-commands

[24] National Technical Research Organization, Guidelines for Protection of Critical Information Infrastructure, June 2013, http://www.ficciweb.info/conf-cell/Guidelines.pdf

C. RAJA MOHAN

NEGOTIATING CYBER RULES

AFTER man learnt to split the atom and put it to military use nearly seven decades ago, the relations among major powers have changed irrevocably. When coupled with missile technology, it became possible to deliver enormous explosive power within minutes at any other point on the earth. This compelled fundamental changes in the logic of military strategy thanks to the deterrent effect – on one's adversaries as well as the possessor of nuclear weapons and missiles. Although nuclear weapons were used only once, the prospect for such development and the perceived need for deterrence saw an expansive race to build nuclear weapons and deploy them in different domains – land, air, on and under water.

Even as the great powers sought a delicate balance of nuclear terror between themselves, they joined hands to prevent the spread of nuclear and missile technologies to other states. Regulating the nuclear arms race among the great powers and building a firewall between civilian and military uses of atomic energy became one of the most intense political, diplomatic and strategic activities in the second half of the twentieth century. Even after the Cold War ended and the prospect of a nuclear conflict among the major powers diminished, the spread of nuclear weapons and associated weapons of mass destruction has remained at the top of the global security agenda and a source of continuing conflict.

For the first time since the Second World War came to a close, a new kind of warfare has begun to eclipse the international concerns about nuclear weapons and the proliferation of weapons of mass destruction. Cyber security has begun to overtake the traditional concerns about weapons of mass destruction and their proliferation. Unlike nuclear weapons, whose ownership is limited to a few, many countries have cyber warfare capabilities and have not been shy about using them. Unlike nuclear energy, whose military applications came before civilian uses, cyber warfare is emerging out of an expansive civilian industry that has become integral to the lives of most people in the world.

Regulating the military uses of this technology and preventing states using cyber weapons to destabilize each other will be far more demanding than efforts that went into the management of the atom over the last decades, and the need for it has become increasingly self-evident as more countries develop cyber warfare capabilities. According to a recent report by the United Nations Institute for Disarmament Research, at least 40 nations have developed cyber warfare capabilities. Although a late entrant to the cyber warfare domain, India is set to press ahead and announced a national cyber security strategy in 2013. India is also reportedly considering the establishment of a 'cyber command' as a joint enterprise among the navy, air force, and the army to coordinate India's cyber defence and offence capabilities.

This essay is divided into three parts that follow this introduction. The first reviews the current efforts at generating international cooperation in regulating security competition in cyberspace. The second deals with the relevance of past negotiations on arms control for the management of international security in cyberspace. Whether we want it or not, the language of nuclear arms control as we know has already begun to suffuse the international debates on cyber security. The third and concluding part attempts to draw a set of lessons for India as it seeks to influence the global negotiations on cyber arms control and governance.

The increasing frequency and intensity of cyber attacks and a growing recognition of the vulnerability of corporations and states have generated a growing demand for some form of negotiated international control over cyberspace. It is also widely understood that the solutions to cyber security cannot be found within the national framework alone. Much in the manner that states negotiated norms for newly emerging domains – like oceans and outer space – they have begun to cope with the challenges of devising some rules of the road for cyberspace.

The recognition of these trends have generated considerable support for the idea of a cyber treaty or a cyber convention. The only international agreement so far in the cyber domain has been the Budapest Convention on Cybercrime which came into effect in 2004. Developed by the Council of Europe, the convention is yet to garner widespread ratification. Meanwhile discussions have begun at the United Nations and other international forums to assess the impact of information and communication technologies on international security and explore the prospects for drafting a convention for cyber security that will have a much broader ambit than the Budapest Convention. Such an instrument could be similar to the Land Mines Convention that came into force in 1998, the Chemical Weapons Convention (1997), the Nuclear Non-Proliferation Treaty (1970), or the Outer Space Treaty (1967).

There is much skepticism in some quarters on the possibility of negotiating such a comprehensive cyberspace treaty or convention. Others, however, argue that such a convention is becoming a vital necessity. What in theory could such a convention among states achieve? For one it could simply come up with acceptable definitions of the terms in the emerging discourse on cyber security. As a new but consequential domain, there is need for clarity on how the discourse is intelligible to each other and accessible to the wider public. The convention could articulate a broad set of norms that states must comply with in cyberspace. It could also outline a set of confidence building measures to improve trust among state parties and reduce tensions in the management of cyberspace.

More ambitiously, the cyber treaty could agree on a set of restrictions or limitations on what nations could do and not do in cyberspace during war and peace. The treaty could also impose certain forms of state responsibility in the arena of cyber security. Finally, the treaty could promote regional and international mechanisms for interstate cooperation on cyber security and the enforcement of a new set of agreed cyber norms.

The good news is that a broad consensus appears to be emerging among major nations on some important issues relating to cyber security. A discussion initiated among governmental experts appointed by the UN Secretary General since 2010 has made considerable progress in generating some shared understanding on cyber security issues. A report issued by a governmental group of experts in August 2013 put out a set of recommendations that the UNSG said 'point the way forward for anchoring ICT security in the existing framework of international law and understandings that govern state relations and provide the foundation for international peace and security.' One of the central recommendations of the report was an assertion that the traditional principles of international law are applicable to the cyber domain, thereby clinching an important debate. Given the virtual nature of the cyber domain and the difficulties of delimiting state boundaries and affixing state responsibilities, many had argued that traditional international law is not of much use in regulating cyberspace.

The explicit affirmation that international law, particularly the principles of the UN Charter, is applicable to state activities in cyberspace, including to activities of non-state actors attributable to states, will allow the international community and affected states to react to violations more effectively. In cyberspace, states have to comply with the prohibition on use of force, the requirement to respect territorial sovereignty and independence, and the principle of settling disputes by peaceful means in much the same way as in the physical world. The right, specified in Article 51 of the UN Charter, to self-defence including the use of force would apply if a cyber attack reached the level of an 'armed attack'. The report, however, refrained from spelling out when this could be the case as the legal debate on this issue has only just begun.

The report offered a set of recommendations on the principles of responsible behaviour in cyber space, proposed a slew of confidence building measures such as exchange of information on national cyber policies, sharing knowledge on best practices, promotion of regional consultations, and expansion of cooperation in law enforcement and international assistance for capacity building. While the recommendations of the report are a step forward, translating them into treaty language will not be easy. The devil as they say is always in the detail, and there is continuing resistance in many influential quarters against a formal treaty to regulate cyberspace.

As the world prepares to negotiate norms and restrictions on state behaviour in cyberspace, it might be relevant to recall the experience of arms control. At least four tensions that dominated the negotiation of past arms control treaties are likely to have some bearing on the prospective negotiations on cyber security. First is the enduring tension between lawmaking, technological change and national strategies. Unlike the earlier technologies – chemical, nuclear and space – changes in the communication and computing technologies has been much faster. Laws defined at a point in time might look impractical soon after. There is also a deeper problem of understanding the nature of international law.

Much of the discussion on cyber governance is centred on the challenges of extending international law to the cyber domain. In concentrating the international efforts on developing legal principles for the cyber domain, it is easy to forget that great power interests have long shaped the evolution of international law. Any serious framework for regulating cyberspace must therefore consider the dynamic interaction between law and strategy, for strategy compels a reconsideration of laws, while the law itself shapes strategy. Meanwhile technological changes and their application for warfare compels great powers to redefine their security strategies.

The second is the tension between multilateralism and great power relations. Multilateral negotiations tend to focus on general principles and norms, but past experience suggests they can't always prevail over the interests of the dominant powers. The 1967 Outer Space Treaty, for example, emphasized space as the common heritage of mankind and its peaceful uses. Yet, within the first decade after the treaty came into force, there was a dramatic expansion of using space for military purposes by the great powers.

Another limitation of most multilateral treaties is that they do not have enforcement mechanisms; any legitimate use of enforcement measures requires consensus among the five permanent members of the United Nations Security Council. The NPT, CTBT and many other treaties emerged out of a formal multilateral process, but understanding and compromises among major powers was critical for many of the major outcomes in the treaties. And when treaties tend to limit the options of the major powers down the road, they have not hesitated to reinterpret the meanings or ignore the original text wherever convenient or necessary.

The negotiations on cyber security are likely to be complicated by the notion of 'multi-stakeholderism' that brings in the private sector and civil society groups into the global negotiations on cyber security. Many functional nuclear arms control agreements have come from bilateral talks among the major powers, especially America and Soviet Union, reflecting the distribution of power in the international system during the Cold War. The current discourse on cyber security is taking place amidst a historic power shift among the major powers. The rise of China is the most notable new factor, as is the growing capabilities of other powers in what was once considered the South. It is interesting to note that while America and the Soviet Union dominated the nuclear arms control process, the talks between the US and China are today seen as critical for any cyber security arrangements in the world.

That in turn brings us to the third set of tensions between great power relations and arms control treaties. If, as we noted, great power agreement is critical for the creation and enforcement of norms, the rivalry between them makes it difficult to develop cyber norms. Today, the divisions between the West on the one hand and China and Russia on the other are profound when it comes to understanding the nature of the cyber domain and how the world should approach its regulation. The US, for example, focuses on the protection of computer networks from theft and attack. Russia and China, in contrast, emphasize information security and right to control cyber-space within their territories. America, for example, is interested in prohibiting attacks against civilian targets. The Chinese and Russians believe this protects the American reliance on private networks while leveraging its strengths in the military sector. They would like to focus, then, on American vulnerabilities.

Often times, the great powers could agree on prohibitions that have no real operational meaning, for example the ban on deployment of nuclear weapons on the moon. More broadly, each great power wants to protect its strengths from treaty limits while its adversary focuses on constraining these very specific advantages. There is also the possibility that major powers will try and enforce a common understanding between themselves on other countries in the international system.

The enduring asymmetry of interests and structures forms the fourth set of tensions in the negotiation of a cyber treaty. A set of norms derived logically from first principles will be unacceptable to one or another great powers because of the asymmetric impact on the adversaries. Given the variation in the strategic geographies of great powers, the differences between their domestic political orientation and the competing objectives, negotiating a mutually acceptable set of norms will remain a big problem. Even within alliances that share a common set of political objectives, the impact of norms can be different given the asymmetry in the distribution of power.

Unlike nuclear and missile technology, cyber capabilities are already widely dispersed and are not the monopoly of a few countries. That makes controlling the spread of these technologies difficult, although efforts to do so have begun within the Wassenaar Arrangement – a group of advanced countries that regulates the sale of conventional arms and associated technologies. The arms control agreements arrived through mutual understanding among the great powers might not be acceptable to many nations. More importantly, it does not require massive capabilities for a weak state or a non-state actor to target the cyber vulnerabilities of a major power.

The attractiveness of the asymmetric warfare, then, complicates the traditional power calculus among states and reinforces all the difficulties that the major powers had to deal with in facing terrorism from non-state actors. Consider, for example, the idea of fixing state responsibility for cyber crimes originating from the territory of a particular state, one of the central themes of the current debate on cyber security. We have seen how hard it is to compel regimes to take responsibility in the case of controlling international terrorism. In some cases, it could be a genuine lack of capacity to control cyber events on one's soil; some states could deliberately build ambiguity. Pakistan, for example, maintains plausible deniability in supporting terror groups operating in Afghanistan and India, and the international system has been unable to compel Pakistan to change its behaviour.

The reference to all these challenges does not mean there is no value in the development of cyber security norms for the international community. In all likelihood some kind of a cyber treaty or at least a code of conduct might well be within grasp in the coming years. What kind of a role and strategy should India adopt in the current international discourse on regulating cyberspace? India has an active and unique record of participation in global negotiations on arms control. Three D's can be used to sum up this record. One is the emphasis on disarmament rather than arms control that underlines India's extraordinary idealism in international affairs. The former focuses on comprehensive abolition of weapons of mass destruction, while the latter seeks to regulate interstate competition rather than eliminating it. The second is a focus on what we might call 'developmentalism' that prioritizes the application of strategic technologies for peaceful uses, demands liberal international transfer of technologies, and claims to represent the interests of the developing countries as a whole. The third is a determined defiance of what it consider as unequal or discriminatory arms control arrangements.

Although these features gave a special cache for India in the early years of arms control negotiations, this idealist baggage tended to become a millstone around India's neck and prevented it from effectively pursuing its national interest. India refused to declare itself a nuclear weapon power in 1974 when it conducted a 'peaceful nuclear explosion'. This mix of developmentalism and idealism placed the country in the worst of all worlds. It provoked the world into imposing sanctions against India, while Delhi refused to announce itself as a nuclear weapon power for another quarter of a century. India's emphasis on equity and fairness had little resonance with the constituency that Delhi thought it was representing – the developing world. Most countries of the South signed onto the NPT to make it near universal, fully accepting its inequities.

After it declared itself a nuclear weapon power in 1998, India has adopted a different, pragmatic approach to bring its national interests and international negotiating positions in line with each other. India has begun to project itself as a responsible major power that is willing to support the objective of nonproliferation and make some concessions to become a part of the global nuclear order. Instead of rejecting all forms of arms control, India has begun to initiate arms control and confidence building measures with its two nuclear neighbours – China and Pakistan.

The transition towards pragmatism, however, is not complete. In the domain of outer space India continues to emphasize that its primary focus is on peaceful uses, even as pressures mount to develop a coherent military space programme. Its scientific, military and diplomatic establishments speak with different voices when it comes to India's outer space policy. India, however, does not have the luxury of taking a long detour to get its approach to international negotiations on cyber security right. For unlike the nuclear and space domains, cyber technologies are evolving at a rapid pace and envelop a much larger segment of the domestic economy. Its security implications cover the full spectrum from crime to protection of industrial infrastructure, intellectual property and securing the international balance of power. India's own ICT sector, which has contributed significantly to its recent economic growth, has become a major target of cyber attacks and a source of attack on others. In a belated response to these imperatives, Delhi announced its national cyber security policy in July 2013 that has put in place a broad architecture for the management of cyber challenges.

India's policy, however, does not dwell very much on the international dimension of cyber security. At the practical level, of course, cyber cooperation with other countries has emerged as a major component of India's diplomacy in recent years. At the public level, at least, little attention has been devoted to the impact of cyber technologies on the global balance of power between Washington, Moscow and Beijing and its consequences for India's interests. Nor has there been much clarity on how India should position itself in the current discourse on regulating cyber security at the international level. That India will be compelled to join the debate and respond effectively is not in doubt. A number of lessons from India's past experience with arms control present themselves.

For one, India must strive to find an appropriate balance between the articulation of universalist principles and national security interests. Far too much focus on the former has tended to load the dice against India in the real world. A temptation to present itself as a champion of the South must be resisted for there is always the danger that India will find many weak states with very different stakes from those of India as an emerging major power in the international system. The emphasis must be on building functional coalitions that will serve India's best interests.

India must also resist being trapped into all-or-nothing arguments. Delhi must retain sufficient flexibility and be ready to find compromises on issues of secondary interest while protecting the core concerns. India must also recognize that successful cyber diplomacy will have to be rooted in building strong domestic capabilities. Failure to build domestic competence could put India at the mercy of possible nonproliferation arrangements agreed upon by the United States, Europe, Russia and China. Given the speed at which international cyber dynamic is evolving, there is not much time to lose.

FURTHER READING

BOOK

Anderson, Ross J. Security engineering: a guide to building
dependable distributed systems. John Wiley & Sons, November 2010.

Assange, Julian, Jacob Applebaum and Andy Muller Maguhn.
Cypherpunks: freedom and future of the internet. OR Books, November 2012.

Betz, J. David. Cyberspace and the state: toward a strategy for cyber-power.
London: Routledge, 2011.

Choucri, Nazli. Cyberpolitics in International Relations.
Cambridge, Mass: MIT Press, 2012.

Clarke, Richard A. Cyberwar: the next threat to national security and what to do about it.
Ecco, April 2010.

Deibert, Ronald and Rafal Rohozinski. Good for liberty, bad for security?
Global civil society and securitization of the internet. Cambridge, Mass: MIT Press, 2008.

Howard, Rick. Cyber security essentials. Auerbach Publications, 2010.

IDSA. Task force report: India's cyber security challenges.
New Delhi: Institute for Defence Studies and Analyses, March 2012.

Kirkpatrick, David. The Facebook effect: the inside story of the company
that is connecting the world. Simon and Schuster, 2011.

MacKinnon, Rebecca. Consent of the networked: the worldwide struggle
for internet freedom. Basic Books, 2012.

Mitnick, Kevin D. and William L. Simon. The art of intrusion: the real stories
behind the exploits of hackers, intruders and deceivers. John Wiley & Sons, 2005.

Mitnick, Kevin D. Ghost in the wires: my adventures as the world's most wanted hacker.
Back Bay Books, April 2012.

Mitnick, Kevin D. The art of deception: controlling the human element of security.
John Wiley & Sons, October 2002.

Nye Jr., Joseph S. The future of power. New York: PublicAffairs, 2011.

Reveron, Derek (ed.). Cyberspace and national security: threats, opportunities,
and power in a virtual world. Washington D.C.: Georgetown University Press, 2012.

Rid, Thomas. Cyber war will not take place. London, UK: Hurst & Company, 2012.

Schmitt, M.N. Tallinn manual on the international law applicable to cyber warfare.
Cambridge: Cambridge University Press, 2013.

Singer, P.W. and Allan Friedman. Cyber security and cyber war: what everyone needs to know.
USA: Oxford University Press, 2014.

ARTICLES

Bronk, Christopher and Eneken Tikk-Ringas. The cyber attack on Saudi Aramco.
'Survival: Global Politics and Strategy' 55(2): 2013: 81-96.

Burton, Joe. Cyber security: the strategic challenge and New Zealand's response.
'New Zealand International Review' 38(3): 2013: 5-8.

Burton, Joe. Small states and cyber security: the case of New Zealand.
'Political Science' 65: December 2013: 216-238.

Canann, Taylor J. Software vulnerability analysis in cyber security: a network structure approach.
BYU Macroeconomics and Computational Laboratory Working Paper, 2013-05: December 2013.

Choucri, Nazli et al. Institutions for cybersecurity: international responses and global imperatives.
'Information Technology for Development': Taylor and Francis Online: October 2013.

Dale Peterson. Offensive cyber weapons: constructive, development, and employment.
'Journal of Strategic Studies' 36(1): 2013: 120-124.

Edwards, Charlie and Luke Gribbon. Pathways to violent extremism in the digital era.
'RUSI Journal' 158(5): October 2013.

Farwell, James P. and Rafal Rohozinski. Stuxnet and the future of cyber war. '
Survival' 53(1): 2011: 23-40.

Fidler, David P.. Internet governance and international law: the controversy concerning revision
of the international telecommunication. 'Journal of American Society of International Law' 17(6): [Insights]: 2013.

Fleck, Dieter. Searching for international rules applicable to cyber warfare?
a critical first assessment of the new Tallinn manual. 'Journal of Conflict and Security Law' 18(2): 2013: 331-351.

Friedman, Allan A. Cybersecurity and trade: national policies, global and local consequences.
Centre for Technology Innovation, The Brookings Institution, September 2013.

Gartzke, Erik. The myth of cyberwar: bringing war in cyberspace back down to Earth. 'International Security' 38(2): 2013: 41-73.

Grabosky, Peter. Organised crime and the internet: implications for national security. 'RUSI Journal' 158(5): October 2013.

Guitton, Clement and Elaine Korzak. The sophistication criterion for attribution-identifying the perpetrators of cyber-attacks. 'The RUSI Journal' 158(4): 2013: 62-68.

Guitton, Clement. Cyber insecurity as a national threat: overreaction from Germany, France and the UK? 'European Security' 22(1): 2013: 21-35.

Hansen, Lene and Helen Nissenbaum. Digital disaster, cyber security, and the Copenhagen school. 'International Studies Quarterly' 53: 2009: 1155-1175.

Heinl, Caitríona H. Regional cyber security: moving towards a resilient ASEAN cyber security regime. RSIS Working Paper 263, 9 September 2013.

Inkster, Nigel. 'Chinese intelligence in the cyber age. 'Survival: Global Politics and Strategy' 55(1): 2013: 45-66.

Inkster, Nigel. Chinese intelligence in the cyber age. 'Survival: Global Politics and Strategy' 55(1): 2013: 45-66.

Julisch, Klaus. Understanding and overcoming cyber security anti-patterns. 'Computer Networks' 57(10): 2013: 2206-2211.

Kello, Lucas. The meaning of the cyber revolution: perils to theory and statecraft. 'International Security' 38(2): 2013: 7-40.

Koblentz, Gregory D. and Brian M. Mazanec. Viral warfare: the security implications of cyber and biological weapons. 'Comparative Strategy' 32(5): November 2013: 418-435.

Lindsay, Jon R. Stuxnet and the limits of cyber warfare. 'Security Studies' 22(3): 2013: 365-404.

McGraw, Gary. 'Cyber war is inevitable (unless we build security in). 'Journal of Security Studies' 36(1): 2013: 109-119.

McGraw, Gary. Cyber war is inevitable (unless we build security in). 'Journal of Strategic Studies' 36(1): 2013: 109-119.

Mueller, Milton, et al. Internet security and networked governance in international relations. 'Journal of International Studies Review' 15(1): 2013: 86-104.

Pedersen, Christian. 'The rising digital missile gap: the security threat of the United States ' cyber inactivity. 'Pepperdine Policy Review' 6(11): 2013.

Rid, Thomas and Peter McBurney. Cyber weapons. 'RUSI Journal' 157(1): 2012: 6-13.

Rid, Thomas. Cyber sabotage is easy. 'Foreign Policy': 2013.

Rid, Thomas. Cyberwar will not take place. 'Journal of Strategic Studies' 35(1): 5-311-28.

Rid, Thomas. More attacks, less violence. 'Journal of Strategic Studies' 36(1): 2013: 139-142.

Rothkopf, David. The cool war. 'Foreign Policy': February 2013.

Rudner, Martin. Cyber-threats to critical national infrastructure: an intelligence challenge. 'International Journal of Intelligence and Counter Intelligence' 26(3): 2013: 453-481.

Stone, John. Cyber war will take place! 'Journal of Strategic Studies' 36(1): 2013: 101-108.

Stone, Richard. A call to cyber arms. 'Science' 339(6123): 2013: 1026-1027.

Van der Meulen, Nicole S.. Following in the footsteps of terrorism? as a crowded policy implementation space. 'Canadian Foreign Policy Journal' 19(2): August 2013: 123-126.