
global POLICY
GP-ORF Series
DIGITAL DEBATES
CyFy Journal 2015
CYFY
THE INDIA CONFERENCE ON CYBER SECURITY AND INTERNET GOVERNANCE
Durham University
WILEY-BLACKWELL

Digital Debates 2015: CyFy Journal Volume 2

Authors:
Aaron Kleiner, Erin English, Gabi Siboni, Ankur Sarin, Kavitha Ranganathan, Kamlesh Bajaj, Rahul Jain, Fernando Crespo, Renato Flores, Karsten Geier, Jonah Force Hill, Patryk Pawlak, James Lewis, Parminder Jeet Singh, Yu-Chuang Kuek, Siddharth Verma, Sunil Abraham, Elonnai Hickok, Tarun Krishnakumar, Mahima Kaul, Samir Saran

Editorial Team:
Mahima Kaul, Anahita Mathai, Ritika Passi (ORF)

Inside Design:
Simi Jaison Designs

Printed by:
Vinset Advertising, Delhi

MOST OF THE PAPERS IN THIS JOURNAL WERE PRESENTED AT CYFY 2014: THE INDIA CONFERENCE ON CYBER SECURITY AND INTERNET GOVERNANCE, NEW DELHI, INDIA, OCTOBER 14-16, 2014.

Contents

Global Internet Governance

Privacy and Security

Looking Ahead

Notes

Editor's Note

Achieving Digital Proximity and Collective Voice

Samir Saran, Chair, CyFy and Vice President,
Observer Research Foundation, India

The internet is now old enough to be integrated deeply in global life. It is almost impossible to consider subjects as diverse as economics or national security without reserving a place for the internet's role in nearly all global systems. Yet the internet remains young enough to have sharp contradictions and competing visions that our age must attempt to resolve. And it remains deeply local. In his inaugural address at CyFy 2014, India's Minister for Communications and Information Technology Ravi Shankar Prasad said, "Global can never become meaningful unless it is linked to the local. That is how I see it. The internet may have been invented by a particular country, but is today the property of the world. It is the heritage of humanity powered by diverse innovations from every part of the world. All should be welcomed, all should be made a stakeholder. That is the approach of the Government of India as far as the issue of ecosystem is concerned." What the minister alluded to is the inherent structural tension in the management of the internet today. By its very nature, the internet is a revisionist medium, allowing ideas and groups previously disempowered by distance (from each other or from centres of power) to achieve digital proximity and collective voice. Yet Michel Foucault's concern that the narratives of the powerful can become true through their power remains alive in the internet age, as the digital arena remains inequitable and access begets voice. If the internet is democratic, it has a restrictive suffrage.

These restrictions are compounded by the concentration of digital resources in the 'old world' of developed countries; these first-movers are by definition in favour of the status quo that brought them to their current position of pre-eminence. All who can currently

claim to be stakeholders in the internet are in one way or another defending the status quo, not always through the obvious mechanism of naked state control but also through the mainstream media and private companies. The fundamental impulse to protect incumbency is apparent despite many of these actors' declaration that the internet is a disruptive space; such disruption occurs within the limits prescribed by the existing stakeholders. Yet the current governance model being developed strives for the ideal. In his keynote address, British Member of Parliament and Secretary of State for Culture, Media and Sport Sajid Javid said of the decentralised internet governance ecosystem: "The principles agreed upon are as robust as they are simple. Internet governance should be built on a fully inclusive, multistakeholder process, one that ensures the meaningful and accountable participation of everyone involved. Decisions should be made in a bottom-up, open, consensus-driven way. There should be a suitable level of accountability, with mechanisms for checks and balances as well as for review and redress. Anyone affected by an internet governance process should be able to participate in that process."

Clearly, something will have to give if the benefits and reach of the internet as a medium is to empower the 'next billion'—those who are not yet stakeholders but will soon have a screen in their hands. It is at this new frontier that the fundamental questions on internet governance will be played out anew, be they related to legality, society, security, infrastructure, standardisation, economics or development.

Engaging in this new frontier of the next billion will create new opportunities to rethink the status quo and shrug off the tyranny of incumbency. The next billion also possess the next priorities that will matter, entailing emerging players taking greater responsibility and domestic regimes aligning better with an emerging international order. Even as this greater role develops for new players, they can shape the existing order through bilateral and regional cooperation. For example, we can expect to see India's 'Act East' policy in the conventional diplomatic realm take on a digital aspect through collaboration with partners, such as Japan, in developing economic and trade elements in the digital domain.

Though mutually-beneficial development dominates in the economics of connecting the next billion, security poses the biggest fundamental challenge and could upset the applecart of progressively closer global digital ties. After decades of expanding internet presence, the world has still not answered—or rather, has many different answers—to the question of where the agency of the state should begin and end on internet issues. The question of jurisdiction also lies open for debate. Dr. Uri Rosenthal, Special Envoy, Cyberspace Conference 2015, and Former Foreign Minister, Kingdom of the Netherlands, in his keynote address at CyFy offered a view from his country: "Cyberspace presents challenges to the national security of societies and states. Citizens expect their governments to take responsibility for their security in cyberspace as long as they do so to protect privacy. It is logical, therefore, that state sovereignty also play its part in cyberspace… The existing

It is at the new frontier of the 'next billion' that fundamental questions of internet governance will be played out anew.

system for regulating international relations between sovereign states is applicable in cyberspace. The system I am talking about is international law, and it offers far more opportunities than it is sometimes assumed."

Yet the truth is that flatter, less hierarchical forms of communication like the ubiquity of Twitter among everyone from technorati to terrorists makes governments nervous even as it enables their peoples—to both positive and negative ends. Actors in any security framework risk co-option by forces far from home as the line between state and non-state blurs. Thus far, efforts to solve these problems, like mutual legal assistance treaties, run the risks of failing to both serve mutual interests and effectively curtail stateless entities. This concern was echoed by Ravi Shankar Prasad: "Do we have the technical and legal architecture available to identify the perpetrators and the sources of attack? Do we have any international mechanism for sharing information and [taking] determined action against perpetrators? This unhindered growth of networks of infected computers across the world—how do we propose to address this problem in the absence of global cyberspace norms to regulate and guide responsible behaviour in cyberspace?"

Achieving Digital Proximity and Collective Voice

For countries like India that are stepping into a leadership role on the global internet stage, the national decisions of today will shape the global environment of tomorrow. The line between incumbents and newcomers is ambiguous, but it is clear that small actions by anyone anywhere will together contribute to the new normal on the internet. For a country like India, with hundreds of millions of internet users and soon hundreds of millions more, that is a huge responsibility. India first has to answer for itself whether it wants to be a status quo or a revisionist power. Are its interests aligned with the big digital economies? Or are those interests instead different from the established players? In either case, India will be brought to a different and nearly mutually exclusive set of answers.

The time for this decision is now, as the tide of users' aggregate actions shape the debate on its own terms. Capacity and capability, rather than residing with institutions or nations as they do in many traditional realms of policy, are instead radically disaggregated. On the internet, the currency of ideas has the potential to outstrip conventional tools of government policy like laws and ordinances; one need look no further than widespread piracy and the patchiness of censorship regimes to see that individuals rather than institutions constitute

cyber culture. Societies should search for new tools to confront this emerging reality, even as they are in the process of choosing to prioritise global connections or local security for their internet networks. Irrespective of the direction of this or other choices, what is inescapable for modern states is the building of a cyber force that can contend with the implications of these new realities for cyber security. India's Deputy National Security Advisor Arvind Gupta addressed the challenges of capacity building in his valedictory address: "Early implementation of the cyber security policy and architecture, finding the necessary resources—human resources and financial resources—and getting public-private partnerships going are some of the challenges that we face…we should have a large pool of cyber security experts, professionals in very large numbers—we are talking about millions here—to step up research and development in high-technology areas in order to make cyber security products and services and make India a manufacturing hub."

For even as the internet represents a distributed means of communication available each year to more people, states as collections of those people still have a role to play. The age of innocence is over and states are back, either through their own agency and capacity or by co-opting those technically outside their frameworks but still vulnerable to the power states wield. This is occurring irrespective of the partnerships and collaborations that seek to dress up state power with mutual consent. National sovereignty remains an issue even in the international realm of internet governance, not only because international law accords a role to governments within their own borders and with their own citizens, but also because those very citizens—often the constituents of the internet—are not simply citizens of the world but care about nationalism and their nation's sovereignty.

These competing interests and frameworks between governments, citizen users and businesses create effects on the ground and in the cloud. The double-edged sword of data nationalism is just one example; caught on the fault line between internet sovereignty and the free flow of information, many countries such as India, that have been agitating for control over their own data, are simultaneously seeking to capture the data services market. How can India and others advocate for their data interests while also wanting to make themselves net providers of data services? Markets and nations will need new norms in order to accommodate each others' needs. Ultimately, reducing the level of abstraction and technicality in these issues—which are related to wider arguments over governance, law and human rights—can make the digital sphere less a young and undefined part of international governance, and more a mature and mutually intelligible global order.

INDIA AND THE CYBERWORLD

1 Today's Decisions, Tomorrow's Terrain

Strategic Directions for India in Shaping the Future of Cyberspace

Erin English, Senior Cybersecurity Strategist,
Global Security Strategy and Diplomacy Team, Microsoft
Aaron Kleiner, Senior Cybersecurity Strategist,
Global Security Strategy and Diplomacy Team, Microsoft

India is a bellwether country in the world's march towards ubiquitous connectivity. Not only is India's rapidly growing online population demonstrative of a broader shift underway in emerging economies, but India's cyber policies are often indicative of policy trends in countries that are now coming online. For example, the Information Technology Act (IT Act) of 2000 and its subsequent amendments were among the first attempts by a large emerging economy to organise government resources and functions to address the impact of the internet.[1] Likewise, India's proposal at the 2014 Plenipotentiary Conference of the International Telecommunication Union highlighted many countries' desire for a more articulated role for governments in internet governance.[2] These policy cues provide observers with insights about where the world is headed, given that India will soon be home to the world's second largest population of internet users.[3]

Looking closely at the impact of India's new connectivity and rising global prominence, cyber security presents particularly difficult policy challenges. In some respects, India has a relatively mature cyber security policy landscape. The IT Act established roles for relevant government actors, such as the Computer Emergency Response Team – India and

* This paper reflects the authors' personal observations, and may not necessarily reflect Microsoft's views. For more information about Microsoft's perspectives on cybersecurity policy, please visit: www.microsoft.com/cybersecurity.

the Controller of Certifying Authorities. The subsequent National Cyber Security Policy and Meghraj strategies present a vision for the government's approach to cyber security and its adoption of cloud computing.[4] However, implementation of these plans has been uneven, and the government's complex operating environment makes it difficult to expect progress in the near term. Underlying these challenges is the sheer pace of growth in internet use in India, primarily on mobile devices, which itself presents security problems. New users may be less savvy about attack techniques, and mobile platforms are typically less understood by security professionals than legacy systems.

There are at least two open questions facing Indian policymakers concerned with cyberspace and cyber security. First, whether India's increasing connectivity is also raising the country's cyber security risk. Second, assuming that continued expansion of India's connectivity will proceed unimpeded, and assuming that this expansion also increases India's cyber security risk, whether there are policy strategies that maximise the internet's benefits but mitigate the new risks that it presents to governments, enterprises and consumers.

This paper aims to inform the Indian policymaking community with answers to these questions. First, India's cyber security risk is increasing, in sync with the country's connectivity. This is an entirely normal pattern that prior researchers have termed the 'Cyber Security Risk Paradox,' in which countries experience cyber security problems as their internet user base grows. Second, there is a range of policy strategies available to India as it manages a significant transition towards greater connectivity. Envisioning these strategies through the metaphorical framework of 'Peak, Plateau and Canyon,' India could implement Peak policies that have typically led to high cohesion between the government's broader societal goals and societal technological advancement, Plateau policies that maintain the current path and trend lines, or Canyon policies that tend towards isolation from the global technology ecosystem.

In summary, India's decisions will play a large part in creating the future terrain of cyberspace. Emerging economies with global aspirations will look to India for a policy template. India's direction could, in many ways, set governance trends for much of the world's online population.

India's Growth

Indians are gaining access to mobile technology and the internet in remarkable numbers. The Internet and Mobile Association of India (IAMAI) recently found that internet usage in India increased by 32 percent between October 2013 and October 2014.[5] As reported in *The Times of India,* the IAMAI projections indicate that India could surpass the US in the total number of internet users by the end of 2015. One fascinating element of India's trajectory is the rapidity of its growth. According to IAMAI, the internet user base in India took more than a decade to move from 10 million to 100 million but only three years from 100 to 200 million, and a mere year to move from 200 to 300 million users.[6]

Ten years ago, the total number of people in India with a mobile phone was just over 52 million.[7] Today, that number is within reach of 900 million, and growing at a pace above global averages.[8] The Asian Development Bank has projected that by 2015, India will be among 40 countries where more people have cellphone network access than electricity in their homes.[9] The recently announced Digital India initiative seems well timed to take advantage of this societal transformation, provided that advancements in basic infrastructure and services keep pace.

BY 2015, INDIA WILL HAVE MORE PEOPLE WITH CELLPHONE ACCESS THAN ELECTRICITY IN THEIR HOMES.

Indeed, India has acted to harness this growth and leverage its benefits. India's global leadership in IT business process management (BPM) continues to deliver significant investment in the country and services exports. According to the National Association of Software and Services Companies (NASSCOM), IT-BPM exports grew between 13 percent year-over-year in fiscal 2014.[10] NASSCOM also reports that the number of startups in India tripled from 3,000 to 9,000 between the years 2008 and 2014.[11] Looking ahead, NASSCOM's '10,000 Startups' initiative provides a runway for determined entrepreneurs to further contribute to India's success, with support from market incumbents like Microsoft.

This growth, however, has led to new risks. According to Microsoft's 'Security Intelligence Report,' India's malware infection rate exceeded the global average during 2012-2014, and the country ranked third from the bottom among G20 countries for malware infection rates, and worst among Brazil, Russia, India, China and South Africa—the BRICS nations.[12] Similarly, the IT security firm Sophos has identified India as a major source of spam, while the security firm Black Lotus Communications has noted India as a potential source for future waves of distributed denial-of-service attacks. Moreover, according to research by Ponemon Institute, organisations in India and Brazil face the highest probability of a future data breach.[13] Given the enormous operational trust that foreign companies place in their Indian partners in the IT-BPM sector, and given India's rapidly growing online population, it is especially daunting to consider the ramifications should India remain a global leader in data-breach probability.

These two forces—incredible growth in technological adoption and exploitation of the growing attack surface in India—are not necessarily at odds. Rather, they are positively correlated, at least to some degree. For a certain period in the technology growth cycle of emerging economies, they experience the Cyber Security Risk Paradox phenomenon, in which technological growth and cyber security risk travel along an upwards trajectory until a certain tipping point is reached. India may only be at the beginning of that journey.

The Cyber Security Risk Paradox

The Cyber Security Risk Paradox rests upon the hypothesis that countries experience increased malware infections as their online connectivity grows, eventually reaching a tipping point, after which increased access ceases to encourage the spread of malware and begins to reduce it. This hypothesis is rooted in the idea that countries with a developing level of technological adoption may be unprepared to secure their infrastructure commensurate with the increase in the use of computer systems, thus providing the opportunity for malware to spread unchecked.[14]

The Cyber Security Risk Paradox has been proven through econometric modelling, drawing upon 11 key indicators—or predictors—that foreshadow potential changes in global rates of malware infection. These predictors fall into one of three areas: digital access, institutional stability and economic development. The relative ability of the predictors to forecast cyber security change varies from country to country. As a rule, however, the model shows that countries with an above-average performance across these development areas can expect to see greater improvement in cyber security.

- *Digital access* measures both the quality and quantity of digital content being consumed; predictors include per capita internet use and the number of secure internet servers per million people.
- *Institutional stability* applies to a group of predictors related to national, social and human development, such as regime stability and literacy rate.
- *Economic development* relates to predictors that directly affect the creation of goods, income or business operations within the country, such as per capita GDP.

Based on the modelling of these indicators, along with Microsoft's measurement of malware infection rates reported in its 'Security Intelligence Report,' there appears to be a negative correlation in the more technologically mature countries between factors signifying maturation in technology adoption and malware prevalence, suggesting that further maturation encourages improvement in cyber security. The correlations for those same predictors are positive among some emerging economies, including India, supporting the notion that initial increases in digital access have a negative influence on cyber security in countries where technology development is less mature. However, the upside for India is that there appears to be a certain level of technology maturity at which countries develop enough technological sophistication to curb the growth of malware. Improving digital access after that point correlates with improved cyber security—the effect observed in more technologically mature countries.

India is currently travelling through the Cyber Security Risk Paradox cycle, but policymakers should not mistake the cyber security challenges that come along with technological growth as a reason to decrease investments in information and communications technology (ICT).

On the contrary, crossing the tipping point is critical to both long-term improvements in cyber security and realising the other benefits of expanding an information society. Having said that, even with the econometric model that underlies the Cyber Security Risk Paradox, it remains difficult to forecast exactly when a country reaches the tipping point, where technological adoption leads to improved security.

Looking forward, India—like most other countries—would benefit from a lightweight framework to chart its course. India's digital journey is only going to make its policy decisions more complex. Drawing from our prior work to forecast potential futures for cyberspace, we believe that a three-part framework centred on the idea of Peak, Plateau and Canyon outcomes can help policymakers sort through difficult options.

India's Strategic Options: Peak, Plateau and Canyon

India should leverage the Peak, Plateau and Canyon framework to align its broader policy initiatives with its cyber security goals. To utilise this framework, there are a number of preliminary considerations for Indian policymakers. First, the framework is future-focused and most useful when applied to long-term strategic questions that can be analysed and addressed without significant linkage to immediate developments. Next, the framework is fundamentally rooted in the notion that cyber security can be significantly influenced by policy decisions in domains that affect societal use of technology but may not have direct linkages to cyber security, such as rule of law, improvements in regulatory policy and investment in telecommunications. Finally, the framework rests upon objective analysis by policymakers of the full range of impacts that their policy choices may deliver, whether positive or negative.

The Peak, Plateau and Canyon framework was developed by Microsoft as part of its work to forecast the future of cyberspace. In its white paper 'Cyberspace 2025: Today's Decisions, Tomorrow's Terrain,' Microsoft presented the framework as a means to understand interdisciplinary relationships between policy domains through scenario-based analysis. As with its prior examination of the Cyber Security Risk Paradox, Microsoft created an econometric model—which it called the Cyber 2025 Model—to assess how cyber security might evolve from now to 2025, based on trends across various socio-economic indicators. The Cyber 2025 Model builds on historical data of 80 countries from 1990 till 2012 to create 2025 forecasts employing key indicator categories of macro-economic, socio-demographic and technology conditions. More than 100 different potential predictive indicators and thousands of indicator combinations were tested to generate the most statistically significant results.[15]

Today, we are beginning to see the emergence of Indian policy strategies and initiatives that could fall under each of these three scenarios. India's challenge will be aligning most, if not all, of its strategies and initiatives with the outcome that it most desires.

The Peak Scenario

As described in 'Cyberspace 2025: Today's Decisions, Tomorrow's Terrain,' the Peak scenario is characterised by clear, effective government policies and standards across economies, and strong collaboration between governments to support open trade and promote foreign direct investment (FDI). This is a scenario of innovation, in which ICT fulfils its potential to strengthen governance models, economies and societies. The actions of governments, businesses and societal organisations foster the widespread and rapid adoption of technology. This political, economic and social support leads to accelerated economic and technology growth as well as improved global cyber security.

For India, there are a number of initiatives underway now that would lead to a Peak outcome. The Digital India initiative is a prime example, but there are instances in other areas as well—for example, India's increasing interest in (and ability to attract) FDI. According to an analysis published in the *Washington Post* in September 2014, Prime Minister Narendra Modi's August 2014 trip to Japan secured $33 billion in new investments over a five-year timeline; the prime minister also announced that India would get new investments totalling $20 billion during his September 2014 visit to China. During the same period, the CEOs of Amazon, Facebook and Microsoft all visited India with announcements of new investments and plans to deepen their commitment to the Indian market. These impressive investment plans demonstrate confidence that India is pursuing a path that will maximise the potential of its growing connectivity.

The Plateau Scenario

The Plateau scenario is a continuation of today's trend lines, which indicate that growth is inevitable but work will be required to harness the benefits of that growth on a global level. 'Cyberspace 2025' describes the Plateau scenario as characterised by asymmetry. Political, economic and societal forces both bolster and hinder technological progress and cyber security. Some governments have inconsistent policies and standards with varied levels of stakeholder participation and international cooperation, while other governments form clusters of open trade and FDI. Some countries are able to leverage technology to advance economic and socio-economic development, while other countries are left behind technologically, unable to fulfil the potential of ICT. This fragmented and uneven approach to governance and the economy leads to a less than optimal global cyber security landscape.

In the Indian context, achieving a Plateau outcome will not necessarily require new policy steps. There are several policy pillars and initiatives in place—such as the IT Act, the National Cyber Security Policy and the Meghraj strategy—that will enable India to reap the benefits of its digital growth. However, whether these policies and initiatives can be fully implemented remains an open question. For example, the National Cyber Security Policy calls for the education of 500,000 cyber security professionals by 2018. Achievement of

this ambitious goal will not only require a significant harnessing of national resources, but of international resources as well. Likewise, while India recently raised its status under the Common Criteria Recognition Arrangement (CCRA) to become an 'authorising' member consistent with the CCRA's mutual recognition principle, the government has required domestic-only testing in other product areas (e.g., the 2012 Compulsory Registration Order). Rationalising—and perhaps reconciling—these different approaches will be an important step towards reaching the Plateau, if not the Peak outcome.

The Canyon Scenario

The Canyon scenario is characterised by obstructionist government policies and standards, protectionist stances and isolation. This significantly restricts trade and FDI and undermines relationships across industrial sectors within countries as well as between countries. In this scenario, economic and technology growth is slower, with limited adoption of ICT and deep failures in cyber security.

India's Canyon-style policies tend to centre on its drive to increase local manufacturing, and also tend to be described by the government as 'security' initiatives. The earliest iterations of the Preferential Market Access (PMA) initiative are among such examples. These early proposals essentially treated the private and public sectors as equal in the applicability of local content requirements, with limited regard for global supply chain implications. Though India ultimately determined to implement a version of the PMA that it believes is consistent with its international commitments, the resulting push-back against the earlier PMA proposals from many in the global industry demonstrates that Canyon-style policies have a fairly immediate and disruptive impact on India's key commercial relationships with global companies.

Conclusion

There is no question that in the near future, India's policy choices will be even more influential in cyberspace. As a centre of gravity in the online world, India's decisions will play a large part in creating the future terrain of cyberspace.

There is a tremendous opportunity for Indian policymakers to define the nature of India's leadership. The Cyber Security Risk Paradox provides a means to put today's cyber security challenges in context, and a basis to continue investing in IT growth even when that growth presents its own problems. Looking forward, the Peak, Plateau and Canyon framework—and the underlying Cyber 2025 model—offers a useful framework to assess and optimise policy strategies. In many ways, India's future has never been more promising. Through greater understanding of connectivity and risk, and different policy strategies to address risk and maximise the benefits of significant growth, India can create a policy template for other emerging economies.

Cyber Security

Build-up of India's National Force

2

Gabi Siboni,[1] Senior Research Fellow and Director,
Military and Strategic Affairs and Cyber Security Programs,
Institute for National Security Studies, Israel

Cyberspace creates countless opportunities alongside complex challenges. India, as a technologically advanced country with substantial online services and businesses, is highly dependent on computer communication and control systems. This is not unique to India alone, but is a global phenomenon. That is, the more that countries or organisations rely on developing technology in cyberspace to run, manage and control business operations, the greater their vulnerability and the greater the risk of severe disruption of these technologies.

Today, there is a common understanding that cyber security threats are one of the most serious challenges for national security, public safety and the economy for every nation and for the entire global society. There are innumerable examples of misuse of cyberspace. Events in recent years show that cyberspace has become an area of much activity and conflict; countries and organisations receive state support to act against other countries; others operate for reasons of intellectual property espionage and theft. Another group of active attackers are terrorists who use cyberspace to promote their own agenda, exploiting the ability to remain anonymous. Criminals and criminal organisations operate in cyberspace for money theft, blackmail and financial fraud. Finally, cyberspace accommodates ad-hoc individuals and groups of activists operating at any given moment against a common target. Correlating these developments with India's National Cyber Security Policy vision[2] requires the country to initiate a process that will transform India to a more secure place to do business in and to use services in cyberspace. Such a process will enhance India's resilience against cyber attacks and its abilities to better protect its interests. Moreover, it will help shape an open and stable cyberspace that would support India's economic development and help build India's cyber security knowledge base, skills and capabilities.

Over a year has passed since India set out its National Cyber Security Strategy. The release of the policy framework in 2013 was an important step towards securing India's cyberspace. However, there are certain areas that need further consideration for the actual implementation of the strategy.

This paper discusses conceptual pillars for the process of building a force for cyber security, which would focus on a high-level defence approach, with the aim of improving the security and resilience of national information infrastructures and services.

The Five Pillars of Building a National Cyber Security Force

The process of building a national cyber security capacity would entail long-term preparation requiring various stakeholders, projects and developments to enable a sustainable systematic and targeted force build-up. This process is a significant challenge requiring a national effort.

This model comprises of five basic pillars:

- *Formulation of national strategy in cyberspace:* This is the foundation upon which the entire process of building the force rests. This will involve drafting the nation's resources and management to improve cyberspace abilities and worldwide position.
- *Technological development of cyber security capabilities:* These are needed to allow the implementation of the strategy.
- *Development of human resources and human capital:* These are needed to allow for the effective use of developed technology within the strategy framework.
- *Definition of the organisational structure:* This will support the strategy.
- *Training and assimilation of the entire force:* This will ensure that all systems function properly and will provide the opportunity to systematically refine and develop knowledge.

National Strategy

The development of a national strategy is the initial phase of building the force and it must address two different perspectives:

- An offence strategy in cyberspace must be prepared, as India needs to respond to large-scale cyber attacks. It needs to have a clear strategy of how it would react to hostile action threatening the government, military, the health of its citizens or the country's economy. As an offence strategy has a distinct mission, it is not the focus of this article but should be discussed in a parallel process.
- A comprehensive defence approach must be developed that reflects India's cyberspace vision.

The defensive strategy needs to address the unique security protection requirements of the following groups:

- National security organisations and sensitive defence industries;
- Critical national infrastructure;
- Government services; and
- The civilian sector.

It is assumed that the first three groups are more secure and regulated and that the fourth group, the civilian population, is the most vulnerable. This group includes civilian organisations, businesses and private users; typically, this group has no guidance for cyber security, and since the entities in this group are not regulated, they are the most vulnerable to attackers, who in any case prefer to target those less protected. One can only imagine the impacts of a successful terror attack occurring against one of India's large food manufacturing plants or against a private financial organisation, or the effect of an intellectual property cyber theft from one of India's technological companies. At the same time, changes in the structure of the Indian economy and privatisation processes should sharpen the understanding that cyber security needs of the civilian sector have to be addressed with greater attention.

One of the key elements of the process of developing a cyber security strategy is the inclusion of national cyber security risk assessment, with specific focus on critical information infrastructures. Based on risk analysis, the strategy should define the minimal defensive measures to be taken in each of the pillars defined for building a national cyber security force. India needs to evaluate where it is standing and where it needs to focus its resources and investments in order to increase, in the global context, the resilience and security of its national information and communication technology assets, which support critical functions of the state. Such an evaluation needs to be done in four different areas:

- The nation's ability to have accurate early warnings of cyber security-related events;
- The nation's capabilities to prevent cyber incidents;
- The nation's competence to detect and identify security events; and
- The nation's response capabilities, which should be measured separately for early warnings and for a particular event or series of events to mitigate the situation, to take further corrective actions in relation to identified deficiencies and to prevent these events from recurring.

Alongside, there are two key phases in the development of a national cyber security strategy: Developing and executing the strategy, and evaluating and adjusting the strategy. A lifecycle approach needs to be adopted—i.e., the output of the evaluation phase should be used to maintain and adjust the strategy itself, and the national strategy should be able

to quickly respond to emerging cyber security issues and emerging threats. The strategy objectives also need to be priorities; this is of paramount importance for successful implementation and for constant improvement.

The success of the implementation of India's national cyberspace strategy relies on the remaining four pillars of building a cyberspace force.

Technology and Means

A country that leads in cyber security technology enjoys economic advantages as well as cyberspace geopolitical domination. Moreover, the application of constantly evolving defence tools is required to achieve a country's vision for cyberspace—today and in the future. It brings innovation to the protection of critical infrastructures, enhanced command and control capabilities, and high quality of intelligence, among other elements. Obviously, there are also advantages of precise and rapid attack capabilities in the realm of offence. These capabilities contribute to a nation's power, and strengthen its national security and international position.

Some of the challenges India is facing today are at the level of its cyberspace hygiene, the lack of cyber security information-sharing tools and best practice, the lack of internal cyber monitoring, and the lack of proactive cyber defence capabilities within the country's critical infrastructure.

It is important that India invest in acquiring the proper technology and means, both by internally developing new technologies and by purchasing from the private sector or allied governments. A coordinated national effort to encourage the private sector by funnelling research and development (R&D) investments to develop new cyber security-related defence tools and concepts of defence operations should be part of this phase. Investing in R&D and putting in seed money in new technological companies is one of the tools to make sure new technologies and cyber security products are synchronised with the strategy requirements. It would also serve two additional Indian objectives: Better customised products to defend itself, and the promotion of the country as an exporter of technology. For example, one of the components of India's cyberspace strategy will probably be the establishment of an integrated national Computer Emergency Response Team (CERT), as will be elaborated further on in a subsequent section. Thus, funding of R&D for dedicated early warning technologies may be required.

It is important that India should strengthen its cyber defence R&D programmes and further support and prioritise development of the cyber defence industry. The government needs to coordinate cooperation between security and defence organisations, such as military and intelligence agencies, and between high-tech R&D companies.

Development of Designated Human Resources

Human resource and human capital development, together with the technological development of tools and methods, must be fully integrated and synchronised, so as to maximally utilise all national resources for the fortification of India's cyber capabilities.

For example, a cyber security workforce needs to stay up to date with emerging risks, threats and cyber security technologies that typically require frequent knowledge acquisition and extension of studies.

Another issue to be considered is innovation in cyber security, from both the offensive and defensive perspectives, to be among the world's leaders. This can be achieved by inter-sectoral partnerships and by providing flexibility to cyber security talents to move and integrate easily between sectors like high-tech, academia, government agencies and the private sector to constantly develop skills and advance India's knowledge base for the development of future opportunities.

From a long-term perspective, it is important to define the overall cyber security workforce requirements to ensure that the country is investing in the right type of education for specific types of workforces and is keeping pace with the workforce demand.

The development of a workforce for cyber security needs to address the typical duties and skill required. In 2013, the National Institute of Standards and Technology (NIST) of the US Department of Commerce released a workforce framework[3] identifying seven cyber security workforce categories:

- *Securely Provision:* Workers are responsible for conceptualising, designing and building secure information technology (IT) systems (i.e., responsible for aspects of systems development).
- *Operate and Maintain:* Involves workers who specialise in areas of providing support, administration and maintenance, necessary to ensure effective and efficient IT system performance and security.
- *Protect and Defend:* Workers are responsible for identification, analysis and mitigation of threats to internal IT systems or networks.
- *Investigation:* Involves workers who specialise in investigation of cyber events and cyber crimes.
- *Collect and Operate:* Personnel are responsible for specialised denial and deception operations and collection of cyber security-related information that may be used to develop intelligence.
- *Analyse:* Analysts are responsible for highly specialised review and evaluation of incoming cyber security-related information to determine its usefulness for intelligence.

- *Oversight and Development:* Workers are responsible for providing leadership, management, direction and advocacy, so that individuals and organisations may effectively conduct cyber security work.

These categories, presented by the NIST, may not be fully in line with India's cyber security strategy. India should identify its professional cyber security needs in a way that would support the technological advances being encouraged in the country. This requires coordinated staff work and long-term educational planning (for all levels of education, from early schooling to advanced academia programmes) across all relevant cyber security categories mentioned above. For example, the need to develop civil cyber defence requires the academic development of designated human resources; these will fill positions in the civil defence sector in technology development, security consumer organisations, as well as the country's national regulatory bodies that will comprise the civil defence force.

Organisation: Utilising the National Potential

Most of the organisations in India have naturally developed some preoccupation with cyberspace and it is assumed that security organisations are building their own cyberspace capabilities to support their basic tasks. However, there is work to be done in two dimensions:

1. The first is the need to conduct a macro-analysis of the nation's cyber security needs, and accordingly build the nation's cyber security ecosystem and define the roles and responsibilities of the various relevant entities. A good starting point is the initiation by the Government of India of the National Critical Information Infrastructure Protection Centre, which is becoming more active and relevant. This should be followed by the establishment or further strengthening of other bodies and initiatives such as:

- The National Computer Emergency Response Team–India: This will improve national coordination of cyber incidents, and act as a focus point for international sharing of technical information and feeds on cyber security. A CERT unit also needs to include a national Security Operation Centre (SOC), which would function as a hub for monitoring the network and detecting anomalies. An SOC would also be responsible for issuing alerts to users and providing advice on best security practices. Such an entity has a great impact on the defence strategy iterative cycle—i.e., early warning, prevention, detection and response, as stated above. Establishment of a national CERT will promote India's resilience to cyber attacks and maintain its interests in cyberspace.
- National Cyber Crime Unit: This will further develop India's capabilities to combat the threat from cyber criminals. Such a unit will make India a more secure place to conduct online business.
- India also needs to consider developing initiatives that would enhance collaborations between government, industry, academia and law enforcement agencies to better coordinate efforts to reduce cyber crimes. Such collaborations will raise awareness, improve reporting and help the industry become more resilient to threats.

- Law enforcement capabilities need to be further developed to tackle cyber crime and enhance the society's confidence in conducting online business and using online services.
- Initiatives for international cooperation will promote India's interests in cyberspace. This should include cooperation with UN committees, regional (South Asia and Asia Pacific) politico-economic unions and the Commonwealth of Nations. India also needs to promote international cyber conferences. Such initiatives will help shape an open, vibrant and stable cyberspace that would support the nation's needs and the global community.
- It is advisable to establish regulators for the protection and guidance of the government ministries and authorities, and the exposed civilian sector.
- India needs to run an awareness campaign reaching out to the private sector to raise awareness of threats and to encourage business, as well as to embed effective cyber security risk management practices.

The above are a few examples of required cyber security initiatives and missions at the national level. It is highly important to plan India's cyber security organisational structure by mapping the cyber security strategy objectives. This will ensure that all activities and cyber security operations are aligned with the strategy.

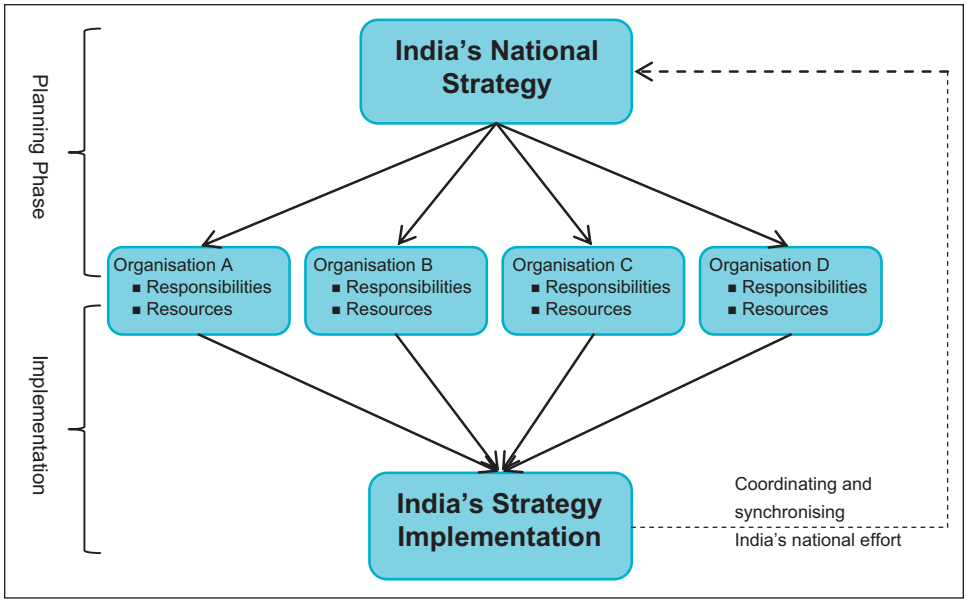
2. The second dimension is the need to define the relationships between the organisations and establish the parameters of authority of each one. This step will be the culmination of the process of building a cyber security force (see diagram on next page).

Drills, Training and Assimilation

Drills are a core component of the proposed cyber security force build-up to generate know-how and enable organisations to better prepare themselves for various scenarios. Though operational drills usually address specific scenarios (readiness for cyber attacks, IT incidents, equipment failure and more), the know-how developed as a result of these drills always exceeds the narrow limits of the specific scenario. Typically, operational drills are conducted at all levels of the organisation, up to the supreme command level. Security organisations routinely carry out training, exercises and drills. It is important to adopt the concept in the civilian sector, which is known to be the most exposed to damage caused in cyberspace.

National training programmes should be established and should focus on improving the civilian sector and the individual's knowledge of risks and vulnerabilities in cyberspace. They should also help the public learn how to deal with intrusions on their computers and devices, and encourage and promote the use of cyber security resources and tools.

In addition, there should be an annual national cyber protection exercise featuring a scenario of several cyber security incidents in a simulated environment, with clear objectives of testing escalation processes and national level coordination procedures. The exercise must challenge all pillars listed for the force build-up to regularly improve and



enhance the national response. The exercise will serve as a basis for the development of operational plans that will improve India's readiness to respond to cyber attacks.

An Overall View

The National Cyber Security Strategy will be the keystone of the national force build-up. Once this has been formulated, two main efforts need to be launched and synchronised: The development of technology and means, and the development of human resources. Those two are to be funnelled into organisations, each of which has predefined responsibilities (and authority) and is allocated required resources, such as budgets, tools and people. Drills and exercises, both in the local and the national arena, must be part of the strategy implementation. Of course, the government will need to continuously monitor and synchronise the national force build-up process, and will have to take required measures to make necessary corrections.

In July 2013, India declared its National Cyber Security Strategy. Now it is time to move to the next phase and formulate a comprehensive force build-up process. India needs to establish key elements of the planned activities over the short, intermediate and long term in support of the strategy. The strategy assessment process should be undertaken to verify progress and make adjustments as necessary, in response to changes in the technological and threat environments. This should be done on an iterative basis to make sure that the level of cyber security is constantly enhanced. Implementation of such a process could move India to the next generation of cyber security readiness and position it with leading nations in the arena of cyber security preparedness.

A Case for Leapfrogging the Digital Divide

3

Ankur Sarin, Professor, Public Systems Group,
Indian Institute of Management (Ahmedabad), India
Kavitha Ranganathan, Professor, Information Systems,
Indian Institute of Management (Ahmedabad), India

The past decade has seen tremendous strides in information and communication technologies (ICTs) which have transformed almost every sphere of our lives. However, a vast segment of the global populace is still untouched by and/or unable to leverage the benefits of digital technology, content and services. For instance, 61 percent of the world's population does not use the internet and the distribution of those not connected is unevenly distributed in the developing and developed world.[1] For example, the internet penetration in India is at a low 12.6 percent while it is above 90 percent in Denmark.[2] The terms 'digital divide' and 'digital exclusion' can describe this phenomenon: The vast difference in the availability and usage of ICTs between different regions, countries or socio-economic groups. While the existence of this divide is symptomatic of deeper socio-economic and institutional inequalities, it also threatens to accentuate and deepen these inequalities. Therefore, it is not surprising that the occurrence of 'information poverty' and its consequent debilitating effects on other dimensions of poverty are a growing concern for policymakers.[3] Indeed, most of the historical evidence on technological developments would point to this. However, we believe that ICTs differ from other technological developments in ways that might allow developing and underdeveloped countries to catch up with the more progressed societies instead of falling further behind. This way the digital divide can not only be 'leapfrogged' but also strategically leveraged by aspiring countries to catch up on several social and economic frontiers. ICTs have the potential to democratise access to and production of information and knowledge, facilitating decentralised decision-making.

The possibility of leapfrogging the digital divide fundamentally stems from the idea that developing countries who find themselves on the wrong side of the divide do not necessarily

need to follow the digital trajectories of the West. Instead, these countries can leverage years of research and development and adopt technologies at the cutting edge[4] as per their needs and relevance. By being proactive rather than reactive, countries can also ensure that their adoption is democratic as well as relevant to their social and economic contexts, and strengthen institutions of development. While the gains to developed countries from being early adopters of various ICTs are undoubtedly significant, so are the costs of shifting to newer technology. Therefore, while path dependencies might inhibit adoption of cutting-edge technologies in the developed world, the relatively clean slate in the developing world could serve as an opportunity for these countries to 'leapfrog' and catch up via adoption of more efficient and affordable technology. The advantages of doing so are manifold, including speed, efficient technology, leaner and more flexible adaptation and sustenance.

But, despite the intuitive appeal of leapfrogging, policymakers in developing societies face the challenge of identifying appropriate technology and committing public resources to encourage and deploy it. Therefore, it becomes most necessary and useful to understand the points at which interventions might be required and relevant. Similarly, ICT innovators and solution providers have to understand factors influencing the social acceptance, relevance and usage of their technology. To these ends, we propose a framework that identifies factors likely to influence the success of interventions seeking to leverage ICTs to leapfrog. We use multiple projects from the Information and Communication Technologies for Development—i.e., ICT4D—space to illustrate aspects of the framework and use the case of one ICT venture, Eko Financials, a young start-up in India, to further illustrate the application of the framework.

ICTs and the Digital Divide

Numerous factors contribute to the digital divide: The costs of digital technology, especially if the target population is dispersed and has low paying capacity; non-literacy, since those who cannot read or write are unable to use the technology interfaces that are text based. Regulatory regimes can similarly dampen the spread of technology, worsening the digital divide. A case in point is the use of WiFi in outdoor spaces in India, which was deregulated only in 2004. Lack of connectivity and access is also a significant limiting factor that has wider social and economic ramifications, as the economic stakes are much higher if one is not able to make and take advantage of the right contacts and information.

There is no denying that these underlying capacities and capabilities of a society that lead to a digital divide demand more urgent attention than the issue of the digital divide itself. While we acknowledge that the evidence of using ICTs to create change in the factors that lead to a digital divide is mixed, that debate is outside the scope of this chapter. Instead, our starting position is that the digital divide is of consequence in and of itself and secondly, that the divide has implications for the rest of the economy as well. We focus

on characteristics that define the growth of ICTs and their implications for the value and ability of developing countries to leapfrog the divide.

The attributes of ICTs that point to the need and value for developing countries like India to commit resources to overcoming the digital divide include:

Rapidity of change: A defining characteristic of the development of ICTs is the rapidity of change and obsolescence. This implies that many of the ICTs available to developing countries today were not available when ICTs became pervasive in most of the developed world. Therefore, the capital investment needed to go down the routes developed countries did is unnecessary and avoidable.

Efficiency gains: The rapidity of change would have no implication had it not been accompanied by efficiency gains, either via reductions in cost or increased abilities (e.g., processor speeds, size of microprocessors, storage capacity). These two characteristics imply that the productivity gains from the latest ICTs might be significantly greater than those adopted earlier. While this points to the significant opportunity available to developing countries to catch up with others, it also cautions against making investments in ICT projects that might have significant start-up or fixed costs. Instead, interventions that have the ability to account for the rapidity of obsolescence should be prioritised.

Network externalities: By their nature, there are significant network externalities that characterise ICTs. This implies that the value of using any ICT depends on how many others also use it—a phone has no use if you do not have someone to call, for example. Therefore, the benefits of adopting an ICT might exceed the costs only after a critical mass of people have adopted it. However, this also implies that once a critical mass has adopted a technology, it becomes increasingly costlier to shift to another one, even if the newer technology is significantly better. This aspect of ICTs poses both a challenge and opportunity for developing countries. Developed countries may find themselves trapped with obsolete technology, simply because that is what most people are familiar with. On the other hand, developing countries may face challenges in getting a critical mass of users to adopt a technology. Secondly, given the path dependencies, the process of choosing a technology—for example, the nature and extent of government intervention—becomes critical.

Easy transferability: Unlike gains from other technologies, which are critically dependent on the hardware and actual physical transfer (of machines and such), innovations in ICTs are far more easily diffused. Further, there is a strong open source culture in ICTs that encourages the spread of innovations and overcomes problems created by traditional norms of intellectual property rights.

Intrinsically innovative: Unlike hard core technology applications, ICTs have redefined innovation in terms of inventions, rapidity, experimentation, outreach, usage, a mass

base, decentralisation and democracy. Investing in digital innovations has deconstructed the centrally managed social welfare strategies of the government and has instead put the government at the forefront of participating and contributing to the democratic development process.

A Case Study of Leapfrogging: Eko Financial Services

Eko Financial Services[5] is a young Indian start-up that uses mobile technology to bring banking to the masses. Founded in November 2007 with the mission of providing banking services to the unbanked in India, Eko uses a simple mobile phone for all front-end user transactions. Eko has tied up with at least three major Indian banks to provide basic, 'no-frills' accounts under the banking correspondent model initiated by the Reserve Bank of India (RBI). Local mom-and-pop grocery stores double up as bank branches where users can quickly create a bank account and where the store owner's phone serves as a point-of-service (POS) terminal. Eko has since garnered a large user base and most of its revenue is generated from remittances—migrant workers who send money back home to their families in rural villages. With 25 lakh (2.5 million) senders, 20 lakh (two million) receivers, and processes transactions worth five crore rupees ($50 million) every day,[6] Eko has created a strong presence in the remittances domain.

Eko's revenue model hinges on a large number of low-value transactions. Eko has successfully kept its technology costs down while simultaneously building a back-end that is immensely

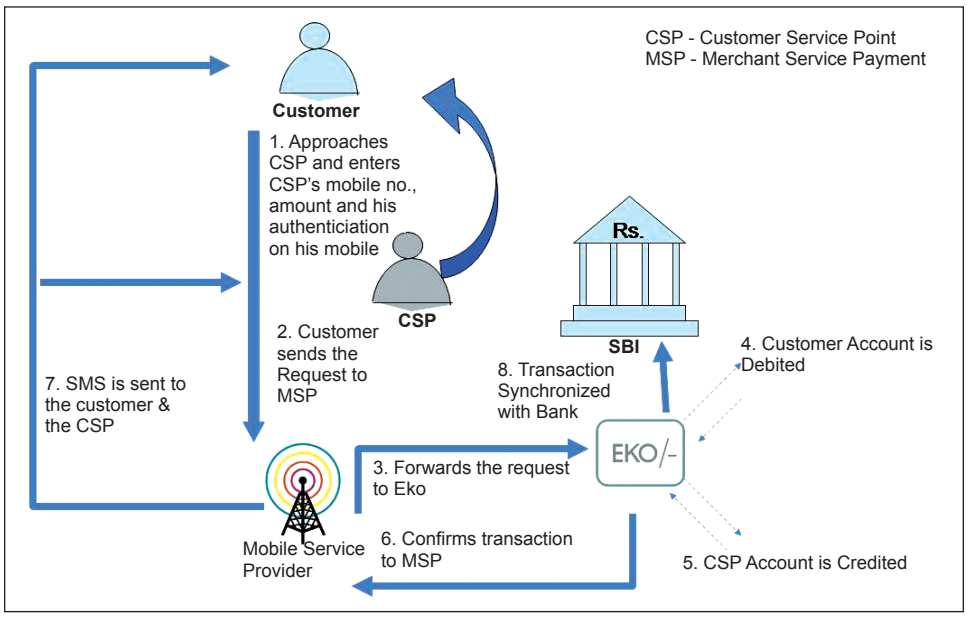


Figure 1: Eko's Model for End-to-end Process of Withdrawing Cash

scalable. This challenging task has been accomplished by leveraging not one but multiple contemporary technologies—the mobile phone, cloud computing and open source software. Figure 1 illustrates the end-to-end flow in Eko's model for a cash transaction.

By using a mobile phone to act as an automated teller machine (ATM), POS device and debit card, the costs of these additional elements have been eliminated. Eko's banking solution is called SimpliBank, which has a low-cost back-end that is embedded in a cloud system provided by Wipro (a cloud service provider in India). An existing open source software solution for microfinance, MIFOS, was selected to form the core of SimpliBank, and Eko added additional components around this core to customise it for its operations. SimpliBank effectively manages a high volume of small mobile-initiated transactions. By using cloud services for its infrastructure (data centre, storage, computer resources and security facilities), Eko could easily scale up its infrastructure as the demand for its services increases.

Factors Enabling Leapfrogging

Understanding elements that enabled Eko to reach out to underserved populations at a fraction of the cost of other institutional actors points us towards enabling conditions for ICTs to be leveraged for leapfrogging over divides in other sectors as well. In discussing Eko's case, we build on a framework developed by Steinmueller[7] in the context of leapfrogging with traditional technology. We elaborate on this framework, linking it to the Eko case as well as other examples from ICTs.

Absorptive Capacity

Absorptive capacity refers to the ability of the target audience to effectively learn and adopt the new technology. A steep learning curve is likely to dissuade users. Therefore, absorptive capacity plays a crucial role in how a new technology is perceived and accepted—the more nuanced the usage aspects, the more critical is the initial hand-holding and familiarisation process.

While absorptive capacity depends both on the audience in question and the technology being introduced, it also lends itself to external interventions. Along with the introduction of a new technology, the absorptive capacity for that technology may need to be and can be explicitly developed. This can be done through, for example, appropriate design of the user interface, training and education camps and/or education material.

In Eko's case, to ensure that the intended users (bottom of the pyramid segment) would be able to use their services easily, Eko's platform is designed to run on all basic mobile phones and does not require a Wireless Application Protocol interface or any other

additional technology. The entire interface uses Unstructured Supplementary Service Data (USSD) instead of Short Messaging Service (SMS) on GSM. The choice of USSD was made because the largely non-literate and semi-literate client base would find it easier to use the numbers and special characters that are part of USSD rather than text which would be required for SMS technology. The user interface was modelled on the prepaid recharging actions required on a mobile phone, with three easy steps. This ensured that since 90 percent of mobile subscribers in India use and are familiar with the prepaid model, Eko's interface comes across as familiar and easy to use. In addition, to make the user experience easy, Eko does not require customers to remember an account number but only a four-digit pin.

Another example of building absorptive capacity is when M-Pesa's money transfer application, a first of its kind, was introduced to rural populations in Kenya in the pilot phase. The M-Pesa team spent many hours training potential clients and newly recruited M-Pesa agents on finding and using the M-Pesa App. Even though the interface was stripped down to a very simple, SMS-based system, the initial training was crucial to jump-start usage. As narratede by Susie Lonie, M-Pesa's chief architect and project manager[8] –

> There was a great divide between people who were familiar with mobile phones, and people who were not. The former tended to pick up M-PESA quickly. For the latter group, the first chunk of any training session was taken up by explaining the concept of a menu, showing them how to find M-PESA, how to find their SMS inbox, etc.

M-Pesa's subsequent phenomenal uptake and scale-out in Kenya and beyond is well documented.[9] But it is likely that none of that could have been achieved without the upfront investments in building absorptive capacity, sometimes rather painfully "in a tin shed with the mid-day sun beating down, an enthusiastic 40-a-side soccer match going on outside, and about as many potential clients wrestling for hours to learn how to use M-PESA."[10]

Similar sensitivity to the absorptive capacity of the user population was exhibited when talking ATMs were introduced to Bolivia's indigenous regions by Prodem FFP,[11] Bolivia's self-proclaimed bank for the masses. The ATMs were carefully designed for Bolivia's poor, non-literate indigenous population and the user interface consisted of verbal cues in the local languages mixed with colour-coded buttons and pictorial displays.[12] However, despite the very intuitive user interface, Prodem ensured that each new ATM was manned by one of their staff members for the first 30 days, so that new users could be directed through their first few transactions and all customer queries and concerns could be addressed. Again, the talking ATMs were very effective and helped Prodem secure a strong foothold in rural Bolivia.[13]

One project that did not initially pay too much attention to absorptive capacity of its users is the One Laptop per Child (OLPC) project. One of the basic assumptions of the project was that children would learn to use the laptops by themselves, without any help from their teachers. Teacher training was not part of OLPC's initial plan, leading to a very bumpy start for the project.[14]

Regulatory Clarity

The leapfrogging technology is very often the latest cutting-edge technology in its domain and its adoption may be hampered by intellectual property rights, regulatory hurdles and related issues. How widely accessible a new technology is and how freely it can be disseminated will play a crucial role in its success for leapfrogging the digital divide.

Eko operates in a tricky new space which is in between a traditional financial institution, a telecom service provider and a software company. While initially there was no specific role for a company like Eko that bridged the gap between a bank and the last mile of financial inclusion, recent RBI guidelines on a new entity called a 'Business Correspondent' defined the exact space that Eko operates in. Business correspondents, as per RBI regulations, can be any third party which acts as an intermediary between a bank and the client and is allowed to collect and offer small value deposits and credit.[15] RBI subsequently relaxed norms on mobile banking and Know Your Customer requirements, which helped Eko and similar finance-related services. By creating this extra space in which innovative companies like Eko can function, the Government of India has facilitated using technologies for leapfrogging and facilitating financial inclusion.

An example of where lack of regulatory clarity impeded faster growth is the case of IEEE 802.11 wireless protocol—commonly called WiFi—ideal for creating affordable long-distance networks known as WiLD networks[16] and mesh wireless networks. However, outdoor use of WiFi was regulated in India till 2004. After deregulation, a spate of projects like the Digital Gangetic Plain[17] in the state of Uttar Pradesh and Air-Jaldi[18] in the city of Dharamsala used WiFi to create successful outdoor wireless networks.

Due to the current regulatory clarity, the Digital Empowerment Foundation has been using existing provisions, like free spectrum allocations as provided by the government that are not being otherwise utilised to provide information and media infrastructure, and reaching out to unreached communities through the Wireless for Communities intervention.[19] Globally, and in India, frequency bands in the 2.4 Ghz, 5.8 Ghz and 3.3 Ghz ranges have been kept aside as free spectrums that can be used by anyone without requiring a license or fee payment. This holds immense promise as a low-cost model to provide connectivity and access.

Complementary Capabilities

ICTs are not deployed in a vacuum. Very often their functioning is closely related to other factors. For example, a laptop is useful only if there is a reliable supply of electricity. In the context of the digital divide, the success of a technology often critically depends not only on how well the technology performs its primary function but also on whether all related/complementary capabilities have been accounted for. Some examples include the ability to withstand voltage spikes or drops and variations in the cycle frequency,[20] ability to function in temperature and humidity extremes, ability to withstand rough usage/ additional wear-and-tear and ability to deter theft.

Apart from the core technology and a mobile banking solution, Eko had to look at providing additional features and creating an ecosystem where bottom of the pyramid clients would be able to use their service. A significant barrier to financial inclusion of the poor is their lack of a legal identity. Working to get the government to relax its Know Your Customer norms so that users without proof of address could be introduced to banks by the individual manning an Eko outlet or an existing customer has helped in creating complementary capabilities for their service.

Other perceived barriers are the security and fraud concerns associated with mobile banking.

Eko has worked on multilevel authentication for its m-banking services—the phone number that acted as the bank account number, the four-digit pin and the ten-digit transaction number. Analytics provided by SimpliBank also help in detecting money laundering and fraud patterns.

In another example, the OLPC[21] project includes many of the above mentioned elements in its design of a low-cost laptop for small children in developing countries. The laptop can be charged by using a hand-crank or yo-yo that comes with it, is ruggedly built and is waterproof, and can withstand a fall as well as high temperatures. Moreover, since many rural classes are held outdoors, the laptop's display can be viewed in sunlight, using a special backlit monochrome feature. The laptop is florescent green in colour to indicate that it is a child's machine, with the hope that this decreases its usage in the black market.

Yet another example is the biometric design of Prodem ATMs. Instead of using a pin number which would have been difficult for their financially illiterate clients, Prodem ATMs identify users with their thumbprint. While this is a more foolproof solution for users potentially forgetting or misplacing their pin number, there is a danger of thieves cutting off thumbs to steal money from the ATMs. The Prodem engineers considered this point and to deter such identity theft, the biometric system has been designed to only work with hands that have blood flowing through them, rendering cut-off thumbs useless.[22]

Downstream Integration

The fourth requirement—downstream integration capabilities—encompasses market development and growth, and logistical issues of delivery of the products and services. Convincing users of the utility and reliability of a new technology can prove daunting. User buy-in is often identified as a key challenge in any technology intervention.

One of the biggest challenges for Eko was to create awareness among potential customers and win their trust. Getting customers to deposit their money at the Eko outlet was a daunting task. Eko used a multipronged approach to garner trust in its service. The customer face of Eko is the local, neighbourhood grocer (*kirana* store owner), who already has a good reputation in the vicinity and is trusted by the people there. While visiting a formal banking institution to conduct a financial transaction can be a daunting task for a poor, illiterate person, dealing with the friendly neighbourhood grocer is comparatively easier and less time consuming. Additionally, Eko has leveraged the brand awareness of the State Bank of India (SBI), a well-known government run bank. Eko's banners prominently display the SBI name and logo.

Apart for this, Eko has also held street plays and camps at multiple locations on the theme of financial inclusion, mobile banking and money transfer using Eko's services. A comic book in the local Hindi language also explains Eko's services in a fun and story-based narrative format.

A KEY ELEMENT OF LEAPFROGGING THE DIGITAL DIVIDE IS DOWNSTREAM INTEGRATION—PREFERABLY THROUGH AN INCREMENTAL APPROACH.

Another aspect of downstream integration as advocated by Surana et.al.[23] is to use an incremental, instead of a blank-slate approach, when introducing a new technology project. Given the network externalities spoken of earlier, the value of an incremental approach is amplified when introducing an ICT that aims to leapfrog and is novel and alien. An incremental approach ensures that there is already buy-in for the application or function and all the project is doing is making the delivery more efficient. On the other hand, a blank-slate approach has to first create the demand for the service—the challenges of doing so are evident from the example of the Simputer, an open hardware Linux-based handheld computer marketed as early as 2002 in India.

Designed as a low-cost alternative to a personal computer, the Simputer boasted of many innovative aspects, including a simple and natural user interface based on sight, touch and

sound. A key objective in developing the Simputer was to help bridge the digital divide with low-cost portable computing that even illiterate people would be able to use. Despite initial expectations of 50,000 units being sold, only 4,000 units were eventually sold and the project was declared a failure by the media. The main reason why intended users did not buy the Simputer was because of a lack of useful content or a standout application. In other words, the market for the product was non-existent and it was crucial to figure out content and applications that would create a market for it.[24] A blank-slate approach in this context was the main undoing of the project.

The importance of downstream integration is essential from a normative perspective as well, since it guards against paternalism. Taking steps to encourage downstream integration ensures that users adopt futuristic ICT interventions with less uncertainty about the value they are likely to derive from it. Therefore, the success of the intervention depends critically on the mutual value likely to be created both for the provider as well as users, and can be seen to be the more socially responsible option.

Conclusion

India's contribution to the development of ICTs internationally is well recognised. But much of India still awaits the benefits of ICTs that many of its citizens have helped develop. Given its relatively low resource base there is a growing consensus that, while they may not be sufficient, ICTs are going to be essential to address challenges at the scale India experiences them. In leapfrogging the digital divide, emerging economies like India can also hope to develop systems that are far more efficient, robust and less reliant on concomitant infrastructure than countries in the developed world. To do so, India will have to make careful choices regarding regulation and public expenditure. We believe the framework suggested by us can serve as a useful starting point to identify what technology could be useful to leapfrog and suitable for public support. The framework can be equally useful in identifying interventions that need to accompany different technologies to aid leapfrogging. Our work has implications not only for governments alone, but also points to factors to be kept in mind for private initiatives seeking to provide innovative ICT solutions for India's development needs.

Data Security

Challenges and Opportunities for Indian Industry*

Kamlesh Bajaj, Former CEO, Data Security Council of India
Rahul Jain, Senior Consultant, Data Security Council of India

4

All sectors of the Indian economy have benefited immensely from information and communications technology (ICT) advancements in general and the internet in particular. The indicators strongly vindicate this—the e-commerce market in India rose 88 percent in 2013 to $16 billion;[1] m-commerce is also gaining traction; as per the Reserve Bank of India data, electronic payments in India account for 48 percent of the total transactions in terms of volume and 91 percent in terms of value; the revenues of the Indian Information Technology-Business Process Management (IT-BPM) industry is currently pegged at $118 billion[2] and is expected to grow to $225 billion by 2020; according to a National Association of Software and Services Companies (NASSCOM)-Deloitte report,[3] the cloud computing market in India is expected to reach $16 billion by 2020; about 10 percent of India's 1.2 billion population—approximately 120 million people—use the internet; and the consulting firm McKinsey projects that India will overtake the United States by 2015 to claim the second highest number of internet users after China. Many other such available indicators point towards an e-transformation of the Indian economy.

One of the biggest challenges in this e-transformation is data security. To address this challenge, the Indian industry has taken proactive steps, such as adopting best practices and global standards in security, investments in the latest security technologies, allocation of skilled resources, spreading awareness among employees, focusing on IT governance and establishing internal auditing functions. All these efforts have helped in reassuring

clients, regulators and end customers, and in the process have made the industry reasonably mature in data security. However, the threat landscape is dynamic and requires organisations to keep upgrading their security programmes. New technologies and service delivery models, such as social media, big data, analytics, cloud and mobile devices, bring new security threats, vulnerabilities and risks, along with new business opportunities. Security is not a one-time activity but an ongoing journey. To continue this e-transformation, data security will continue to be one of the key enablers.

Data Security Challenges

There are several challenges that India has to address in the context of data security. In this paper we highlight only some of the key challenges that the Indian industry faces today, namely: The security workforce, cloud computing and global data flows; security standards, practices and certifications; building security intelligence through information sharing; security product development; and ICT supply chain risks.

The Security Workforce

The Indian market is already facing a shortage of skilled security professionals. The issue is not only a lack of adequate numbers but also the competency levels of professionals. The problem is not specific to the security sector but also ails other sectors of the economy, including the IT-BPM sector. As per NASSCOM, only 25 percent of graduates working in the IT field are readily employable, with only about 15 percent qualified for back-office jobs.[4] In security, the major dearth is of competent technical experts who understand how information systems work, and how to identity and mitigate security vulnerabilities. The demand for such technical experts continues to grow as increasingly more ICT is being deployed across all sectors of industry and in e-governance. Furthermore, there are some aspects of information security that pertain more to governance frameworks, processes and auditing for assurance. This is going to increase, as demands for compliance with regulations such as the Information Technology Act, 2000, and sectoral guidelines like those issued by the Reserve Bank of India and Securities and Exchange Board of India increase. All these point to the need for a security workforce with different skill sets.

The dearth of security professionals is expected to worsen in the future if the country or market does not start addressing the problem. The strategy to meet the challenge will have to be multipronged, targeted at multiple levels—entry level, vocational, formal sector, continued learning, etc. Thankfully there is cognizance of the problem, both in government and industry circles, and some solutions are under consideration. The strategy seems to be two-pronged at present, focusing on increasing numbers and building competencies. The National Cyber Security Policy anticipates the need for training more than five lakh (half a million) people in cyber security, though the implementation process is still being

finalised. The report of the Joint Working Group (JWG), set up under the aegis of the National Security Council Secretariat (NSCS), has recommended the establishment of the Institute of Cyber Security Professionals of India to train and certify professionals in cyber security. This institution will be a body similar to the Institute of Chartered Accountants. The Information Security Education and Awareness programme, running under the Department of Electronics and Information Technology (DeitY), is aimed at building capacity through the formal sector, i.e., introducing cyber security-related courses at graduate and post-graduate levels in academic institutions.

The NSDC initiative is promising and intends to leverage the PPP model for capacity building.

One of the key factors of the programmes aimed at successfully building capacity will be the alignment of the course design and industry/job requirements. The risk of a certain misalignment is higher in programmes that are run by the government with minimal industry involvement; therefore, the involvement of industry in capacity-building efforts is a must. The information security certifications available in the market today are a case in point to understand how the certifications developed by the market elsewhere in the world have found acceptability. Certifications like Certified Information Systems Auditor, Certified Information Security Manager and Certified Information Systems Security Professional are desired by many organisations, and even many government departments internationally recognise them. The success of these certifications can be attributed to the involvement of industry in the designing of the course to ensure that the course content meets the industry requirements, as well as to the efforts taken to market the certifications. In fact, all of these certifications are operated by industry, with no government role in deciding the content, training or certification (following an examination) for any of them. However, the negative side of these certifications in the Indian context is the high cost, which makes them less affordable.

Another major government initiative for skill development is the National Skill Development Corporation (NSDC), based on a public-private partnership (PPP) model. Under this initiative, Sector Skill Councils (SSCs) have been established in different sectors to develop skills specific to each sector. For the IT and IT-enabled services (ITeS) sectors, NASSCOM has taken the lead in establishing the SSC and has developed 'qualification packs' (job or skill requirements) in consultation with industry. The SSC is supported by the Data Security Council of India (DSCI). DSCI has developed qualification packs for entry level jobs in information security, even as it works with the JWG to develop industry-led certification courses with different skill-sets through the PPP programme. The IT-ITeS SSC is in the process of selecting, training and assessing partners who will train and certify aspiring candidates in line with requirements laid out in the qualification packs.

The NSDC initiative is a promising one, which intends to leverage the PPP model for capacity building. The success of this model will be instrumental in addressing the dearth of security professionals. The idea for an SSC specifically for cyber security is also being considered. DSCI also has plans to launch its own certification series—the DSCI Certified Security Professional and DSCI Certified Security Strategist. The latter certification has been identified as a need based on DSCI's interaction with security leaders in the industry, and the lack of appreciation for the role of creating a security architecture in an organisation. DSCI proposes to create and get these certifications recognised in India and abroad.

To address the dearth of information security professionals, there is room for many ideas, programmes and initiatives, and, as can be observed from the details above, different initiatives by different agencies in the government and private sector are underway or being planned. The important thing, however, will be to coordinate and collaborate among different agencies working in this area to minimise duplication of effort at the national or industry level. If the programmes and initiatives become successful, India has the human resource potential to not only fulfil its domestic requirements but also meet global needs in information security.

Cloud Computing: Cross-border Data Flows and Localisation of ICT Infrastructure

Cloud computing is increasingly becoming a new means of delivering and procuring IT services. Cloud adoption provides the opportunity to meet business requirements by leveraging the availability of cost-effective, scalable and dynamic IT resources and the expertise of the cloud service providers. Of the current worldwide spending of $3.6 trillion on IT, a significant portion could be potentially spent on procuring cloud services. According to technology consulting firm Gartner, only around $131 billion is currently being spent globally on public cloud. It has predicted that the Asia Pacific (India and Indonesia), Greater China and Latin American regions will emerge as the fastest growing markets with respect to all new public cloud spending between 2013 and 2016. A NASSCOM-Deloitte report[5] says that the Indian cloud market is expected to reach $16 billion by 2020.

Enormous opportunities exist in cloud computing that could be exploited, but at the same time, various challenges and issues have emerged that threaten its adoption. These range from technology concerns to legal and public policy obstacles. Many surveys have revealed that legal and policy-related problems in security and privacy are the major hurdles in cloud adoption. These issues[6] include geographic location of systems and servers, government imposed restrictions on cross-border data flows for privacy protection and security, difficulties for law enforcement agencies in undertaking crime investigations and capturing cyber forensics, difficulties for intelligence agencies in performing surveillance and interception in the cloud, and difficulties faced by government authorities in getting lawful access to data in the cloud.

Governments have a major role to play in solving many of these problems. The Government of India set up a Working Group at DeitY, which is chaired by Kris Gopalakrishnan,

executive co-chairman at Infosys. The key objective of the Working Group was to suggest a framework for developing a cloud policy to promote cloud adoption in India and make the country a hub for delivery of cloud services. As part of its mandate, the Working Group was also supposed to identify legal, security and privacy issues and recommend solutions. Unfortunately, after a few initial meetings, no further gatherings took place and the Working Group provided no recommendations.

The global technology architecture of the cloud and the internet are making it possible to deliver benefits and value, including elasticity, cost advantage, flexibility and user experience. However, geography-specific regulations may sometimes contradict or challenge the cloud architecture. There is a growing trust deficit in the global community vis-à-vis usage of cloud services after the Snowden revelations. Governments around the world, including the Government of India, are advocating localisation of ICT infrastructure. Such knee-jerk reactions must be avoided. There is a need to build trust and collaboration among governments and the cloud industry, and to evolve global mechanisms to facilitate cloud adoption. National concerns, especially those relating to national security, are important and must be respected by the industry. However, the solutions to challenges must be pragmatic, forward leaning and business friendly. Cloud is expected to be the next growth frontier for the IT industry, and it can only be exploited to its full potential if there is global consensus on the solutions to the issues hampering cloud adoption.

Security Standards, Practices and Certifications

Indian industry, especially the IT industry, has been enthusiastic in adopting international quality standards, such as ISO 27001 and ISO 27002. Undoubtedly these standards have been instrumental in enhancing the maturity of security programmes in Indian organisations. The certifications against international standards have found prominent mention in the responses of Indian service providers to international requests for proposal. These have helped them get business from global clients. But problems arise when organisations channel investments and resources to demonstrate compliance to such standards (e.g., extensive documentation, long checklists) instead of identifying and mitigating real risks. Organisations today need to be 'really' secure, as the threat environment in which they operate is becoming complex and dynamic, and attackers are evolving innovative techniques. In such a scenario they cannot rely on certifications alone, even though these may help provide assurance to their stakeholders. Though a standard like ISO 27001 is a good starting point for organisations to implement security measures, it is not an end in itself. When organisations operate in a vibrant, dynamic, evolving and competent environment—be it business, regulatory or a threat environment, as in the case of security—they can do better if they are able to execute long-term strategic planning in security, build security capabilities in different security disciplines, focus on protecting data, track security evolutions and identify interdependencies between different security disciplines with the objective of having an integrated approach to security.

Another major challenge is the poor participation of Indian industry in the development of international standards. Noticeably, despite being an IT powerhouse, India does not have many national standards on security or IT. As a country, we have been followers in this area rather than leaders. There are several international forums where standardisation activities take place, the most notable being the International Standards Organization (ISO). It is important to participate in the development of international standards to: (i) Protect the country's and industry's interests in the standards development process; (ii) enrich the standards through sharing of best or good practices and implementation experiences; and (iii) showcase the country's thought leadership. DSCI, as an industry body, is making efforts to address this issue. It has started to participate in the development of security and privacy standards at the ISO. Under the aegis of the Bureau of Indian Standards, it is creating awareness among businesses on security and privacy-related standards, and trying to institutionalise industry's participation in the standards development process at the ISO. Initially, DSCI is focusing on the development of cloud security and privacy-related standards, and is reaching out to industry for contributions. Industry seems to be interested in participating in such activities and hopefully, going forward, companies will nominate experts. As part of these initiatives, DSCI has also proposed to host the ISO Sub-Committee 27 (which works in the area of IT security) Working Group meetings in India in October 2015. It has also initiated efforts to increase industry's participation in the Internet Engineering Task Force forum, which is a very important platform for security product companies which sell products that depend heavily on the technical functioning of the internet.

Security Intelligence through Information Sharing

Companies in India today do not have formal mechanisms to access and share information on cyber security incidents. Given the rising number of cyber attacks against the backdrop of a worsening threat landscape, information-sharing platforms are the need of the hour. Such platforms can go a long way in providing the required situational awareness to companies to thwart attacks, curb incidents, minimise damage and improve resilience by taking preventive and reactive measures. Information sharing is required not only within the industry but between industry and government as well. For this to happen, the foundational enabler will be trust, which is difficult to establish. While leadership from the Indian Computer Emergency Response Team (CERT-IN) and the National Critical Information Infrastructure Protection Centre may be required under a legal or policy framework to establish information-sharing platforms between government and industry, industry has to take the lead for establishing these platforms for its own benefit.

One of the subgroups under the JWG constituted under the aegis of the NSCS, which was led by DSCI, had recommended the establishment of Information Sharing and Analysis Centres (ISACs) in each of the critical sectors of the economy. As part of this subgroup, DSCI invited government representatives and critical sector organisations from the telecom, banking,

financial services, energy and transportation sectors, among others, to participate in the subgroup. Solutions providers and other industry associations held several rounds of discussions to produce a report emphasising the need to establish ISACs in critical sectors. The subgroup suggested a comprehensive framework for the establishment of these ISACs in the report. The recommendations of the report were accepted by the JWG.

To kickstart the implementation of recommendations, the banking industry was identified for establishing the first ISAC in India. To conceptualise the idea and bring the stakeholders together, DSCI spearheaded a series of meetings with the chief information security officers of the leading banks in India, in close collaboration with the Institute of Development Research in Banking Technology (IDRBT), CERT-IN and the NSCS. These meetings helped lay down the framework for the operationalisation of the proposed ISAC. This initiative has led to the establishment of the Banking ISAC at IDRBT, Hyderabad, named the Indian Banks–Centre for Analysis of Risk and Threats (IB-CART), which was inaugurated in March 2014. IB-CART is expected to foster exchange of information on cyber attacks and cyber incidents in the banking community in India. It will be interesting to observe the success of IB-CART, as it could serve as a role model for setting up ISACs in other sectors.

Indeed, similar efforts need to be replicated across other sectors. The industry has to look beyond competition and trust issues to openly share information with peers. The government should support such efforts, as elsewhere in the world, in whatever way possible.

Security Product Development in India

India is witnessing the emergence of many information security start-ups offering very innovative security products. Approximately fifty in numbers, many of these companies are witnessing high growth rates and finding acceptance in global markets. However, they face significant challenges in the journey to transform themselves into global companies. First, like any entrepreneur in any field in India, they face difficulties in starting and sustaining a nascent business venture—in terms of lack of government support and incentives and registering intellectual property rights (especially patents), since the processes are prohibitively expensive and cumbersome. Second, they face immense competition from the already established, bigger global security companies, making their acceptance in the conservative market difficult. The Indian security market does not provide enough room for them to compete on a level playing field. In general, Indian clients want to play safe and opt for established companies and products. The government, which is a large buyer of security products and which, ironically, promotes indigenous products in the security domain, also formulates requests for proposals that present entry barriers for start-ups or small companies in terms of number of years of establishment, number of years their security products have been available and implemented, etc. Third, there is a dearth of product development skills in the country—i.e., product architecture and engineering—as the focus of the formal sector is more towards the services sector.

With the release of the National Cyber Security Policy and the JWG report on engaging with the private sector on cyber security, and their emphasis on the need to promote development of security products in the country, the ecosystem will hopefully change in favour of start-ups and the smaller, niche Indian companies in security. The key to success will be to implement the policy objectives on the ground, for which several initiatives may be required. DSCI has initiated efforts to support start-ups and small security product companies in India. It has created a platform to bring all these companies together to discuss issues and solutions, and enhance their interaction with the government to bridge the gaps. The government and industry have to come forward in experimenting with new security products from emerging companies; otherwise, there is a risk of buy-out by bigger companies or migration of entrepreneurs to countries that favour and support such start-ups. This is already occurring—in February 2014, Indian company Cyberoam Technologies was acquired by British security provider Sophos. Such a scenario, in the long term, can be unfortunate for entrepreneurship in the security field in India.

ICT Supply Chain Assurance

There is yet another area of concern—the assurance of the ICT global supply chain.[7] Given the increased dependence on global ICT products, especially in operating critical sectors, and the growing awareness of cyber risks, countries are doubting the integrity of these products, fearing that adversaries may introduce malicious codes or functions to conduct surreptitious surveillance, disrupt services or at worst, paralyse a nation. Alleviating such doubts and fears to continue benefiting from the global ICT supply chain is one of the biggest challenges the world faces in cyber security today. Some countries are trying to address this challenge by building global and national capabilities to address supply chain risks without undermining the international competiveness and legitimate trade flow; others are focusing on developing indigenous products to reduce dependence on foreign players. For Indian industry, especially those sectors that own or operate critical information infrastructure, and the Indian IT sector, which not only provides IT products and services to domestic critical sectors but also to the global market, it is very important to be aware of such concerns and participate in the development of solutions through the government, industry or trade bodies.

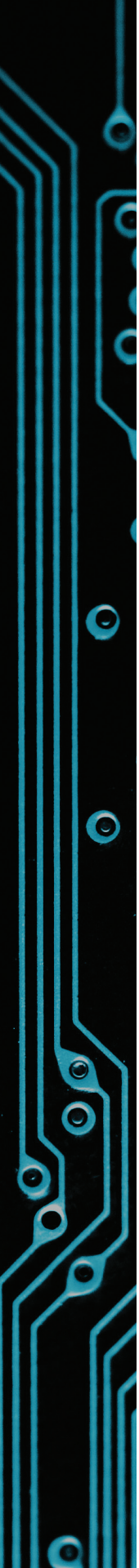
Attempts have been made by the global community to address ICT supply chain concerns through the ISO Common Criteria standards (ISO/IEC 15408), development of Collaborative Protection Profiles and the Common Criteria Recognition Arrangement (CCRA).[8] India is a member of the CCRA and was recognised as an authorising nation for IT products testing last year. This means that IT products tested in India will be accepted by the countries that are part of the CCRA arrangement. As of today, there is only one testing lab in India operated by the Standardisation Testing and Quality Certification (STQC) Directorate, a government agency under DeitY, in Kolkata. A single lab cannot address the requirements of the country. There is a need to establish a national testing and certification scheme, as envisaged in

the National Cyber Security Policy and the JWG report, under which the government and industry can come together to build the necessary IT testing infrastructure, processes, capabilities, skills, etc. Such a scheme will not only address domestic requirements but help develop an IT testing industry in India which can serve the global market.

Some positive developments after the recognition of India as an authorising nation have taken place. STQC has held some workshops to educate the Indian industry on common criteria and how to identify stakeholders who may be interested in setting up testing labs. It has also established contact with the leading industry associations and DSCI to provide industry inputs in the development of collaborative protection profiles (security requirements or specifications against which IT products are to be tested). The industry is, however, cautious in establishing testing labs, given lack of a formal government policy and uncertainty around market demand, among other factors. Interested stakeholders are not sure whether the government will mandate security testing of IT products in certain sectors like it has done in the telecom sector, or whether the mandatory testing will be based on ISO Common Criteria or any other international or domestic standard. The Department of Telecommunications, for instance, has refused to fully accept ISO Common Criteria testing for the telecom sector and is working towards prescribing additional testing requirements. Until such uncertainties are addressed, it may be difficult to convince the private sector to invest.

Conclusion

The NASSCOM-DSCI report 'Securing our Cyber Frontiers' released in April 2012 listed many policy challenges for the government, and emphasised the need for industry to scale up its efforts and work with the government to enhance cyber security in the country, especially through PPP programmes. The challenges discussed above are a partial list, and are not easy to overcome. At the same time, these challenges provide immense opportunities for Indian industry, especially the security sector. Given that data security challenges are a global concern, it is a great opportunity for India to develop the security solutions the world needs—be it security products, standards, services or security testing labs—and provide jobs to its youth. To effectively address the security challenges and harness the opportunities, there is need for enhanced industry-industry, government-government and government-industry-academia collaboration. If the required collaboration is achieved, under a robust, business-friendly and transparent policy and legal framework, security challenges can be converted into opportunities.



INTERNATIONAL COOPERATION

Espionage, Cyber Warfare and International Law

Fernanda Crespo, Intelligence Analyst, International Intelligence Unit, Fundação Getúlio Vargas, Brazil
Renato Flores, Head, International Intelligence Unit, Fundação Getúlio Vargas, Brazil

5

"Be extremely subtle even to the point of formlessness.
Be extremely mysterious even to the point of soundlessness.
Thereby you can be the director of the opponent's fate."

—Sun Tzu

The interactions between the virtual and the 'real' world have come to represent one of the most important challenges of modern society. The internet has enlarged the number and complexity of transborder relations—both commercial and political—casting doubts on the ability of traditional international law to deal with the consequent 'new' issues.

Probably more challenging than the complexities added to private relations is the impact of the creation of new technologies that are being widely used by states as tools in their international policy strategies. In this regard, some examples come to mind: The mass surveillance conducted by the US National Security Agency (NSA), exposed in 2013; the Stuxnet[1] and Flame[2] viruses, allegedly used by the US and Israel to damage and delay the Iranian nuclear programme; and more recently, the hacker attack against JPMorgan's computer network (and several other banks and financial institutions), allegedly a Russian comeback to commercial sanctions imposed by the US and the European Union in response to Russia's intervention in Ukraine.[3]

Actions like the ones described above raise several legal, security, policy, sociological and philosophical questions, to which the answers are not simple. Some of these questions are not new, but have been brought to a completely new level by the creation of the internet and the use of state-of-the-art technologies.

There have been increasing discussions on such cyber activities for the past 10-15 years, but unfortunately no consensus on the best way forward has yet been reached. The Russians have proposed a cyber weapons limitation treaty.[4] Some analysts defend an international treaty dealing with cyber conflicts and espionage as a way to increase the political cost of such practices. There has been continuous debate on issues of privacy, cyber crimes, internet governance and freedom of speech, heightened since Edward Snowden's disclosures. The truth is that finding the right balance and consensus among international players, each with an individual understanding of cyber security, is probably one of the biggest challenges of modern society.

Indeed, when it comes to the cyber world, the necessary consensus is not easily found even within one state, where the military, civil society groups, politicians and individuals feel very differently about the sensitive issues involved. In the international arena, the very definition of cyber security is often diametrically opposed among jurisdictions. While Western nations have generally promoted norms of internet freedom that require unfettered access to online information and freedom of expression, authoritarian states tend to restrict access to sources considered hostile to the regime, seeing them as a threat to national security.

In this article, we focus on the legal/policy side of the debate and try to shed some light on how modern society can better deal with the challenges that technology has come to present. We deal with issues potentially related to cyber warfare: Espionage, 'sabotage' and the use of cyberspace as a field for retaliatory measures, focusing on state actions rather than cyber attacks related to terrorist and other non-governmental groups.

We do not aspire to reach definitive conclusions but to provide some food for thought and contribute to the development of future policies.

We Need to Talk about Espionage. But do we?

When Snowden revealed that the NSA was monitoring the Brazilian president and the German chancellor's phone calls, the world was outraged. This episode and the remainder of Snowden's disclosures prompted public complaints from both leaders and states around the world.

However, cynical as this may seem, the harsh speeches against the US's 'indiscretions' were more about saving face before domestic voters than an actual outraged response.

The reality is that most nations attempt to gather foreign intelligence and participate in the 'international intelligence game'; one should not expect otherwise. The need for comprehensive and reliable information on the political, military and economic developments of friends and foes is paramount. In an increasingly complex and integrated world, cyber espionage has probably become the most important tool used by states to achieve and maintain their power and competitive edge in the international arena.

The US is not alone in this. Just to mention a few examples: China is believed to be making massive efforts to acquire American military technology, classified information and trade secrets of American companies.[5] The United Kingdom has been accused of maintaining secret listening posts operating from diplomatic buildings around the world, including from those located within the European Union.[6] According to an American report, France, Russia and Israel come in second to China in using cyber espionage against the US for economic gain.[7]

Cyber technology innovations may have facilitated data gathering incursions—after all, one does not need to be physically exposed beyond one's national borders—but they have not changed the essence of espionage.

It is interesting to note that while states may regulate intelligence gathering domestically (making it illegal), no noteworthy agreement provides for international rules for espionage during peacetime. Also, customary international law does not seem to provide much insight on the topic. In addition, there is no consensus in the existing literature on peacetime as to whether espionage constitutes a legal or illegal act. Ultimately, the tacit rule 'we spy on them, they spy on us, we try to hold them back, they try to keep us out, and everyone pretends they don't know' seems to be the only consensus found on the topic.

Again, states seek to increase and maintain their power in the international arena in the attempt to secure their very existence. To do so, they need to assess their geopolitical position, and the risks that arise from it, vis-à-vis the political, economic and military strengths of enemies and allies alike. Espionage is one of the means used to make this assessment possible.

Thus, the idea of having an agreement covering cyber (or other) espionage and preventing countries from such intelligence gathering, however well intentioned, does not seem realistic. It also seems undesirable. Espionage creates functional benefits for the international community. It enables countries to covertly monitor the actions of other nations, as well as to ensure their compliance with existing treaties, which in turn encourages countries to negotiate and agree on international rules. From this perspective, espionage may be seen as a tool to facilitate international cooperation. A treaty prohibiting espionage, besides being ineffective in practice, could prevent the development of new international norms, particularly in cases when enforcement proves difficult.

Cyber Security beyond Espionage: Is There a Role for Contemporary International Law?

Beyond espionage, the growing number of reports on government-sponsored offensive cyber programmes around the world raises other concerns. The US, Russia, China and France have recognised the development of cyber capabilities.[8] The Stuxnet and Flame malwares mentioned above are the most remarkable evidence that governments are already using cyber weapons.

There is widespread fear that hostile governments could launch computer-based attacks on critical national systems, such as telecommunications, energy distribution and financial networks, that would severely damage or disrupt public services, resulting in serious, potentially physical, harm to the population. For instance, it was reported in April 2014 that Iran unsuccessfully attempted to conduct a large-scale cyber attack on Israeli civilian communications.[9] Russia has allegedly conducted cyber attacks against Western banks, supposedly in retaliation to commercial sanctions applied in response to the Ukraine-Russia conflict, as already mentioned.

Internationalists and international lawyers are still ruminating on these new developments, trying to fit them in the body of available international law. The infiltration of borders carried out by the use of electronic means was certainly not the kind of violation that the principle of sovereignty initially envisaged.

The prohibition of the threat or use of force in international relations is the core manifestation of the principle of non-intervention. Article 2(4) of the UN Charter clearly prohibits international intervention through the use of armed force, but is silent on other forms of coercion that do not involve force. It reads: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

The UN Charter also establishes exceptions to this principle, the most relevant of which for this discussion—self-defence—is found in Article 51:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

In short, the traditional understanding of these two articles is that the prohibition of force under Article 2(4) and the complementary right to self-defence under Article 51 apply to military attacks and armed violence.[10]

Without entering into current jurisprudence discussions, it seems reasonable to expect that a cyber attack with physical consequences similar to the destruction caused by a bomb or missile would be interpreted as amounting to use of force, and therefore a breach of Article 2(4) of the UN Charter, potentially triggering a self-defence response under Article 51.

The problem becomes truly complex, however, when the cyber activity does not directly produce physical harm. Taking the case mentioned earlier, had the Iranians succeeded in tampering with the Israeli civilian communication system, which in principle would not cause human injuries or property damage, would that have constituted a breach of Article 2(4)? Could that also trigger a self-defence response from Israel?

It is not always easy to distinguish between more subtle kinds of intervention, not even in the 'real' world. Drawing the line in cyberspace is even more problematic. The unpredictable consequences of cyber attacks make analysts and policymakers question whether the rules regarding the use of force should apply to cyber attacks.

In addition to these uncertainties, the very nature of cyberspace creates practical problems related to the application of the rules on the use of force. Existing rules of war were created in completely different circumstances, when states could fairly easily identify perpetrators—i.e., they are effectively premised on the notion of clear attributability.

Here, attribution is particularly problematic considering that technology enables cyber attackers to effectively mask their trails. It is not always technically possible to determine accurately who is responsible for a cyber attack, which is further exacerbated by the jurisdictional limits of the state investigating an incident.

Empirically, even when it has been possible to locate the perpetrators, certainty with regard to the sponsors of an attack is not easily attained—at least not through methods which can be disclosed. In 2008, during the Russian invasion of Georgia, several attacks were reported against websites in the region. The US Cyber Consequences Unit revealed that although the attacks were conducted in coordination with the Russian offensive, there was no evidence of any involvement of the Russian military. In the same year, a study jointly conducted by the SecDev Group and the Citizen Lab at the University of Toronto revealed that a malware affecting devices of several pro-Tibet supporters had originated in China. The study was not conclusive whether the malware had been developed by a government agency, independent hackers or a false flag group trying to blame China.[11]

Again, being unable to identify those responsible for an attack with the necessary level of certainty—i.e., sufficiently robust to discharge one's legal burden—calls into question the practical effectiveness of such rules in cyberspace.

The failure to determine the ultimate perpetrator and sponsor of cyber attacks also has strategic implications. It hampers effective defensive or deterrent actions—because if you cannot identify the perpetrators, you cannot threaten them—and law enforcement becomes unfeasible, since it is impossible to hold the perpetrator accountable.[12] A separate but related problem is the uncertainty of causation, or how to attribute harms caused by cyber attacks.[13]

Having listed the main shortcomings of the application of current rules on the use of force to cyber attacks, it seems to us that these rules are still relevant and should indeed apply to cyber conflicts. While certainly not a perfect fit, existing international rules are extremely important to guide and limit the actions of states in cyberspace, in particular those which might cause human injuries or physical damage.

The concerns described above are not entirely new problems; the issues of attribution and causality concerning Article 2(4) arose many times during the Cold War, when antagonist states worked to conceal their participation in unconventional conflicts elsewhere. Once these conflicts were conducted through proxies, it was difficult to find consensus about even basic issues such as what occurred and on whose behalf. Evidently, achieving consensus about the correct application of jus ad bellum was not possible.[14] As accurately noted by Waxman, "such legal-factual murkiness helps explain why Article 2(4) seemed unable to address that form of conflict and why that mode of conflict offered an appealing option to the Cold War antagonists."[15]

Such "legal-factual murkiness" is similarly found today in cyber conflicts, where determining who committed the attacks and on whose behalf is an extremely uncertain task, one that is much harder than ever before. Again, like in proxy warfare, the difficulties in applying the rules on the use of force make cyber attacks an appealing weapon to some states.

Indeed, considering that a cyber attack might also constitute an efficient form of political-strategic intervention, states may be able to inflict more profound damage with a cyber weapon than they would ever cause with a traditional weapon—and most likely without being held accountable for it.

So, is that it?

Considering the fast-moving nature of technology innovations and the (technical, legal and otherwise) complexities inherent to this debate, a groundbreaking solution to the

challenges brought about by using cyberspace as an additional venue for implementing nations' international policy strategies will simply not materialise.

The analysis above shows that while international law found in the UN Charter may be helpful in dealing with cyber conflicts, the transborder and muddled nature of cyberspace renders those rules somewhat ineffective. Thus, to some, the idea of negotiating an international agreement regulating cyber conflicts—including rules on espionage, cyber weapons control, cyber attacks (in all their grades) and states' responses thereto—seems very appealing.

However, one should remember that international law is a form of cooperation and that to establish functional cooperative mechanisms such as law, certain conditions ought to be present, among which are: Relatively equal actors; high levels of trust; aligned interests; high costs of non-cooperation; matching social values and legal norms; and easy identification and punishment of free-riders and transgressors.[16] Such conditions do not seem to be found in a sufficient degree to support further international rules governing cyber conflict,[17] at least not yet.

Indeed, the ability of a state to identify threats and classify opponents' capabilities, and therefore evaluate potential gains and losses from new rules beforehand, is essential for creating the ground for an agreement. When it comes to cyber capabilities, this element is not available. Likewise, the attribution problem, as described in the previous section, provides a free pass to transgressors insofar as it prevents the imposition of any penalties or retaliatory measures, and removes any political costs that the transgressor might have had to face otherwise.[18] Compliance verification is another problem.

How and when cyber weapons are used today will influence how current and new rules are shaped.

Thus, it seems rather illogical to defend the negotiation of specific rules for the use of cyber weapons and for cyberspace as a warfare zone, when the difficulties identified in the application of current rules on the use of force—attribution, causation, compliance verification and so on—would remain.

Perhaps future cyber attacks and resulting comebacks will contribute to a fresh interpretation of Articles 2(4) and 51 of the UN Charter. Or perhaps the law of war, compliance with which depends heavily upon attributability, cannot be refined to further regulate cyber operations. Perhaps states will only be able to agree on an international framework for cyber attacks when a serious event occurs, and perhaps even then the attribution problem may remain. Perhaps, before any of this happens, technological

developments may adequately address several practical problems being faced today. The truth is that we simply do not know yet.

Countries are certainly aware that their choices on how and when they use cyber weapons today will influence how current and new rules are shaped.

In this regard, it is interesting to note that, during the implementation of Operation Olympic Games,[19] US President Barack Obama was faced with the decision of accelerating cyber attacks once the Stuxnet worm found its way out of Iran's Natanz plant. It was reported that he repeatedly expressed concerns that any acknowledgement by the US that it was using cyber weapons—even under the most careful and limited circumstances—could enable other countries, terrorists or hackers to justify their own attacks.[20]

The US also sent strong messages concerning its position on cyber attacks, stating it would respond to hostile acts in cyberspace as it would to any other threat, using all means deemed necessary, including military. This statement may support the view that the US interpretation of Article 2(4) and Article 51 of the UN Charter allows it to classify at least some cyber activities as prohibited "force" or "armed attack."

It is not surprising to see the US at the forefront of these debates. It is probably the country which has the most to gain but also the most to lose: If it is relatively stronger than others in terms of offensive capabilities, its very reliance on network information technology and globally interconnected infrastructure makes it more vulnerable.[21]

Governments are likely to view cyber threats differently. China likely perceives cyber warfare as a way of matching American military superiority and is unlikely to agree on a reading of Article 2(4) and Article 51 of the UN Charter as narrow as the US might wish. Indeed, cyberspace—a force multiplier—allows weaker states to defeat stronger ones, with relative impunity.[22] As noted by then US Air Force Chief of Staff Michael Moseley, "perhaps for the first time in the history of warfare, the ability to inflict damage and cause strategic dislocation is no longer directly proportional to capital investment, superior motivation and training, or technological prowess."[23] This fact may be particularly appealing to other countries eager to increase their leverage globally. Russia, which has ironically been calling for a cyber weapons limitation treaty, is one of the most active countries in this area and is therefore also unlikely to agree on an interpretation that would completely tie its hands. Finally, European Union member countries have shown more caution in their legal approach to the relationship between cyber attacks and the use of force than the US, a stance likely explained by the lack of common strategy among themselves.[24]

The outcome of these interactions will form the future framework for cyber attacks and cyber conflicts.

An Internet of the People, by the People, for the People

Karsten Geier, Head, Cyber Policy Coordination Staff,
Federal Foreign Office, Germany

6

In June 2014, German Foreign Minister Frank-Walter Steinmeier gave a speech on international cyber policy. Building on Abraham Lincoln's famous phrase, he proposed an "internet of the people, by the people, for the people."

Foreign Minister Steinmeier called for an internet "of the people," i.e., a decentralised global commodity. Second, he argued that the internet should remain an internet "by the people," a multistakeholder space. Third was the call for an internet "for the people." The internet has already radically changed our lives. But the changes brought about by the internet will accelerate even more in the future. Take industry, for example: We are now at the start of Industry 4.0. However, internet "for the people" means something else too: Equal opportunities in the digital sphere. If we do not succeed, if the internet is closed off to some, is state-controlled or simply unaffordable, tomorrow's world will be even more unequal than today's. This, the foreign minister said, must not be allowed to happen.

The internet has become too important, the repercussions of 'cyber' in the real world too resounding to be put in danger. McKinsey estimates that the internet contributes 20 percent to the GDP in advanced industrial countries—three quarters of this contribution being in the traditional, non-IT economy. Consider also the importance of social media: One-third of all people in Germany are on Facebook, and Germany is among the top ten countries in terms of Twitter usage. Figures are similar or higher in other advanced industrialised economies.

The internet has become so important that one might seriously discuss the question of whether internet access has become a human right.

The internet has incredible potential. It can help increase economic growth and innovation, foster freedom of expression as well as access to information and ideas, and enable democratic participation in a knowledge society. Cyber technology has introduced a new dynamic into the relationship between the state, society and the private sector.

Individuals enjoy the same universal human rights 'offline' as 'online.' This includes the right to privacy, as the UN General Assembly unanimously confirmed in December 2013. This issue has proven to be particularly thorny. One part of the discussion comes down to the question whether states have the right to collect unlimited electronic data on individuals and to insist that the business community—i.e., private IT service providers—assist in doing so.

The European Court of Justice (ECJ), in its 8 April 2014 decision on the European Data Retention Directive, has laid down some important markers. These apply to the retention and use of personal data, but the underlying principles have wider implications. The Court made clear that within its jurisdiction—the 28 member states of the European Union—the retention of personal data, when it is wide ranging and seriously interfering with fundamental rights, needs to be sufficiently circumscribed to ensure that interference is limited to only what is strictly necessary. The ECJ has stated that full compliance with the requirements of data protection and security, carried out on the basis of European Union law, is an essential component of the protection of individuals. This limits the transfer of personal data beyond the confines of the European Union, a provision of tremendous importance for the future of international data flows.

Another part of the debate addresses a different, yet related set of questions that arise when discussing the collection, storage, processing and analysis of big data by private companies. Some firms associated with the use of big data are facing critical questions regarding whether they respect individuals' privacy rights. Unless clients are satisfied with the answers, these firms' businesses may suffer.

The internet offers tremendous potential. At the same time, it presents dangers and opportunities for abuse.

Cyber crime springs to mind. A recent study published by the Center for International Security Studies estimated that the US lost about $100 billion to cyber crime and economic espionage last year; Germany was second with losses of $60 billion, and China followed with $45 billion. In both the US and China, these losses represent about 0.6 percent of their economies, while Germany's loss accounts for 1.6 percent. Yet there is a huge controversy regarding how to respond. The members of the Council of Europe and 17 other states, from Argentina to the US, have agreed on a Convention on Cybercrime. It is open for others to sign.

From an international security perspective as well, the internet creates new, substantial challenges. Numerous states are pursuing military cyber capabilities. Military experts assume that cyber action forms part of any contemporary and future war-fighting effort. They classify cyberspace as an operational domain, comparable to maritime, air or outer space. We may not welcome this development, but the genie is out of the bottle. The challenge now is to make it do our bidding.

Traditional political-military strategies predate the existence of the internet. During the Cold War, the opposing parties built their defence on the idea that the best defence is to deter an enemy state from attacking. There is a corollary: In the event of a failure of deterrence, an adversary should be denied the success of his or her action. Deterrence and denial require that the consequences of any attack be clearly and credibly communicated to a potential adversary. This may not hold in cyberspace, with perpetrators showing great skill in hiding or confusing their targets, using botnets, convoluted routings, delayed messaging and other techniques. They may not even be states. It has recently become possible, in individual cases and with considerable effort, to trace the origins of an attack in cyberspace to specific buildings, if not to specific computers or individuals. However, the effort required, the limits on forensic capabilities and the absence of cooperation and collaboration between nations mean that uncertainty about the origin of hostile cyber action is a characteristic of cyber incidents. This makes it impossible for states to threaten negative consequences of such action with any degree of certainty and credibility. Under such circumstances, deterrence may not work. Denial—raising the cost of an attack so as to make a success worthless—is equally difficult, since our hardware is designed for functionality, not security. Current security software is normally unable to identify specially developed malware. It seems practically impossible to run security-critical applications solely by using security-certified software and hardware. Added to this is Moore's Law, according to which processing speeds double roughly every eighteen months, which in security terms translates as follows: Today's impenetrable protection will quickly become an insufficient shield every year and a half.

What about the thought, much cherished by some post-Cold War theorists of international relations, that 'mutual entanglement' can build stability? Entanglement supposes that states cannot go to war when their domestic societies are intertwined through cultural, social and economic ties. If this were true, the internet should be a great international stabiliser. However, the empirical data on this is ambiguous—Germany, in 1914, had strong historical, economic and social ties, even close dynastic links, to Great Britain and Russia, but this did not prevent the outbreak of World War I. On the other hand, 'mutual entanglement' has worked extremely well in Western Europe after World War II and in most of Central Europe since 1990.

If political-military strategies fail to account for cyber capabilities, so does traditional arms control. The 1968 Nuclear Non-Proliferation Treaty differentiates between five nuclear

powers and those signatory states that do not have nuclear weapons. By comparison, it seems next to impossible to negotiate an arms control or even disarmament treaty for 'cyber weapons,' given the potentially unlimited number of actors that can procure computer malware. Also consider the difficulty of defining a 'cyber weapon' in the first place. For some, this might be computer malware which allows an intrusion into another party's computer system, either with the purpose of conducting cyber espionage or for cyber sabotage. Others prefer talking about 'information weapons,' a much wider term that covers the capacity to threaten, destroy or otherwise affect individuals, society, the state and their interests. A common understanding of what we are talking about remains elusive.

Three scenarios for cyber conflict may be worth exploring: (1) All-out cyber war; (2) the limited use of cyber capabilities as part of a larger war-fighting effort; and (3) an international military crisis developing from a cyber action.

1. All-out cyber war

The idea that a cyber attack could cripple a country's military force, economy and communication, defeating it without a shot, may hold some attraction. Could this be a 'humane' war? Even if this were the case—and this is up for debate—all-out cyber war seems unlikely at present. The term 'cyber war' is inadequate. It conjures up a misleading picture of the threat situation in cyberspace, and of the possible countermeasures. In Germany's opinion, 'cyber war,' just like the traditional notion of war, implies severity, immediacy, measurability of effects, military character, state involvement and presumptive legitimacy. We have yet to see any use of cyber capabilities that would match these characteristics. For the foreseeable future, cyberspace will not be the exclusive environment of any conflict that might be qualified as war(fare).

2. Limited use of cyber capabilities as part of a larger war-fighting effort

A more likely scenario may be the limited use of cyber capabilities as part of a larger war-fighting effort. Cyber attacks, in combination with conventional means of conflict, can pose a substantial threat, for which we must prepare.

All countries today rely on modern information and communication technology (ICT), albeit to a varying extent. Even where the military duplicates civilian infrastructure, for instance by using its own communications network without a link to the internet, ICT plays a role—in the 'internet of things,' Web 3.0 machines rely on ICT to work. And even if a military should forego such machines, proceeding, for example, without satellite communication and GPS, the underlying civilian economy can no longer be expected to function without using modern ICT. This is why cyber action must be expected to form part of any future war-fighting effort.

3. Military crisis developing from a cyber incident

The dependence of the modern world on ICT carries another danger. Cyber incidents can escalate into 'real-life' conflict. Consider the following scenario: A country is in a tense political situation. Relations with a neighbouring state are strained. All of a sudden, the main telephone and internet provider becomes victim of a software bug. Nobody can make phone calls, there are no e-mails. With electronic communications down, the banking system collapses. News websites cannot be reached, there are no functional mass media outlets. Government, economy and also security services are paralysed. The situation deteriorates: Trains no longer run, airplanes cannot fly, the power grid collapses, sanitation breaks down, food becomes scarce… All because of a little, hard-to-detect piece of malware. Who planted it? For what reason? Suspicions run high that the less friendly neighbour perpetrated a cyber attack. How to respond? Is this a case where the attacked state may use its right to self-defence? The danger of escalation is evident.

Cyber capabilities make offence easy, while defence is difficult: Cyber attacks can be terribly hard to detect, and it is difficult, if not impossible, to know who is behind them. This establishes an incentive to attack, introducing a degree of uncertainty in international relations, which has the potential to be extremely destabilising. To counter this instability, there are a few things we can do. We can try to agree on rules for responsible state behaviour in cyberspace, and we can engage in transparency and confidence-building measures.

International Rules for Responsible State Behaviour in Cyberspace

Building on an international consensus that international law, and in particular the UN Charter, is applicable to cyberspace and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible information and communication environment, the UN General Assembly has mandated a Group of Governmental Experts to study, with a view to promoting common understandings, how international law applies to the use of information and communication technologies by states. Germany is among the Group's 20 members, along with other European partners such as Estonia, France, Spain and the United Kingdom. We are glad to be cooperating with China, the US and Russia, as well as colleagues from other interested states such as Israel, Malaysia and South Korea. The Group does not need to write a new 'cyber law.' Its mandate is challenging enough as it stands.

It would be useful, for instance, if all agreed that a state is authorised, under international law, to respond to hostile cyber action with the use of force. The UN Charter says, in Article 51, that states have the inherent right to self-defence in the event of an armed attack. But what about hostile cyber action? In Germany's opinion, this depends on the scale and effects: If a state finds itself the target of a cyber operation with effects comparable to an armed attack—be they cyber-to-cyber or cyber-to-kinetics—it may exercise its right to self-defence.

Cyber action is not limited to cyberspace. It can cross domains and create real damage in the physical world. This raises new questions: Are there cyber acts that would be unacceptable under humanitarian law? Take actions that could have excessive consequences on the civilian population, such as attacks on certain critical infrastructure, nuclear power plants or hospitals. They may well be inadmissible under the general rules of international law aimed at protecting civilians from the indiscriminate effects of weapons and combatants from unnecessary suffering.

Are there elements of cyberspace that should be immune from hostile action? An attack on critical internet infrastructure, such as underwater cables or main exchange servers, could have far-reaching effects on global communications, going well beyond the confines of a local or regional conflict. Are states obligated to protect critical information infrastructure?

We may not even need to go all the way to the law on armed conflict. There may well be a whole other set of norms, notably on cyber operations, below the threshold of an armed attack, worth discussing:

- Are states allowed to tolerate or even conduct economic espionage by electronic means?
- What limits does an individual's right to personal privacy set on foreign data surveillance?
- Analogous to the law of the sea, where anybody is obliged to provide assistance to a vessel in distress, is there an obligation to help in case of a cyber emergency?

Confidence-building Measures

The Organization for Security and Co-operation in Europe (OSCE) has recently made important progress in this field. It agreed on a set of measures to reduce the risks of misperception, escalation and conflict that may stem from the use of ICT. OSCE-participating states have agreed, inter alia, on the following voluntary steps:

- Providing their national views on various aspects of national and transnational threats to and in the use of ICT;
- Facilitating cooperation among the competent national bodies and exchanging information;
- Holding consultations in order to reduce 1) the risks of misperception and 2) the possible emergence of political or military tension or conflict that may stem from the use of ICT;
- Sharing information on measures they have taken to ensure an open, interoperable, secure and reliable internet, and on their national organisation; strategies; policies and programmes;

- Using the OSCE as a platform for dialogue, exchange of best practices, awareness raising and information on capacity building;
- Nominating contact points; and
- Providing a list of relevant national terminology.

It is encouraging that the implementation of these confidence-building measures has begun, in a serious and workmanlike fashion, regardless of the political turbulence that has been shaking Europe in recent months. National experts regularly discuss information exchanged and explore further confidence-building measures. In fact, Germany and Switzerland have recently proposed some ideas for concrete, confidence-building steps.

The OSCE may inspire similar work in other regional organisations. Germany is already engaging with other regional institutions, such as the Union of South American Nations, the Organization of American States and the Association of South East Asian Nations Regional Forum, to support their work on enhancing cyber stability. We are looking forward to deepening and widening this engagement, and we think the European Union would be well advised to intensify such efforts too.

In conclusion, the internet offers tremendous opportunities for economic growth, for scientific exchange and innovation, for societies and politics worldwide. At the same time, the internet introduces new risks to international security. These need to be managed. Exploring how international law—principles, norms, treaties and rules of procedure—applies to cyber security, and agreeing to confidence and security-building measures, particularly in regional organisations, may help.

State security in the digital world is an issue in which there is ample room for international cooperation. If we keep an open mind and if we engage in new formats of exchange and interaction, we may truly arrive at an internet of the people, by the people, for the people.

Protecting the Global Internet through MLAT Reform*

Jonah Force Hill, Adjunct Fellow, Strategic Technologies Program,
Center for Strategic & International Studies, USA

7

In addition to igniting a vigorous debate about the nature of surveillance and intelligence collection online, the 2013 Edward Snowden disclosures also brought with them a renewed focus on questions of law enforcement in the digital age. As criminals (and their victims) increasingly go online to communicate and store information, law enforcement officials are correspondingly seeking ever-greater access to online data as part of their criminal investigations and prosecutions. But in today's global data environment, where data moves instantaneously and without consideration of national boundaries, and where information is increasingly stored on servers around the world, law enforcement officials are finding that retrieving critical information is a vastly more challenging undertaking than in the pre-digital era. The globalisation of data has blurred lines of jurisdiction and rendered the methods and procedures formerly used to obtain evidence largely ineffective.

Law enforcement's difficulty with accessing information thought to be essential to investigations and prosecutions is already causing international conflicts. National governments, tech firms and the legal community are all seeking to reconcile data globalisation with the often-competing demands of national sovereignty, citizen privacy, corporate responsibility and the need to preserve a robust criminal justice system—and all under the watchful eyes of an international public still profoundly wary of government overreach in a post-Snowden world. Governments and technology firms are finding

* This piece is a longer and more comprehensive version of the article titled "Problematic Alternatives: MLAT Reform for the Digital Age" in the Harvard Law School National Security Journal dated January 28, 2015 (http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/).

themselves stuck between multiple rocks and hard places, unable to satisfy all these competing demands and obligations.

Luckily, the problem is not intractable and the foundations for amelioration are already in place. The key lies in reform of the Mutual Legal Assistance Treaty (MLAT) process, the system of bilateral and multilateral agreements by which nation-states commit to assisting one another in criminal investigations and prosecutions. Today, the MLAT system is deeply dysfunctional. Responses to MLAT requests for information are often abysmally slow; many of the requests are denied or only partially remedied due to confusion over the rules governing data. Consequently, governments are finding that they cannot count on the MLAT system as an effective means of acquiring digital information for their criminal cases and are beginning to consider alternatives. Those alternatives, however, run the risks of damaging international cooperation on criminal justice issues and of fragmenting the global internet ecosystem. It is thus critical that governments urgently—yet thoughtfully—reform the MLAT system, before the alternatives to MLATs become the norm.

MLATs

Unlike cooperation on national security intelligence (including cooperation concerning threats of international terrorism), which has tended to be negotiated clandestinely through national security agencies, state-to-state cooperation on more conventional law enforcement matters is generally formalised within the context of treaties (some of which are public and some secret). MLATs are perhaps the most important agreements for law enforcement and the most widely used mechanism by which law enforcement officials formally request foreign assistance in domestic criminal investigations and prosecutions. MLATs tend to be drafted broadly to allow for cooperation and assistance on the widest range of law enforcement issues and needs, such as locating and extraditing individuals, freezing assets, requesting searches and seizures, and taking testimony.[1] They have proven to be an effective tool in combating transnational crime, such as money laundering and human trafficking,[2] and for prosecuting criminals who attempt to evade domestic law enforcement by operating abroad.

In recent years, however, with the emergence of globalised data, the MLAT system has struggled to keep pace. The number of MLAT requests has skyrocketed and the matters they concern have become vastly more complex. The system has become deeply strained. In the United States, to illustrate, the Department of Justice (DoJ) estimates that over the past decade the "number of MLAT requests for assistance from foreign authorities has increased by nearly 60 percent, and the number of requests for computer records has increased ten-fold."[3] Further adding to the strain, many of today's MLATs were drafted prior to the era of globalised data and thus fail to address many of the core questions

of data jurisdiction (for instance, how should data held overseas by a subsidiary of a domestic parent company be treated?). Perhaps most significantly, many MLATs do not effectively address the fundamental concern of privacy versus law enforcement's need for evidence: Frequently, MLATs do not specify what constitutes 'protected data' or under what conditions 'content' differs from 'meta-data' for the purposes of information sharing.[4]

This upsurge in the number of MLAT requests, and the concomitant rise in the legal uncertainties of those requests with regard to privacy and data protection regulations, has caused a significant slowdown of the MLAT process. The President's Review Group on Intelligence and Communication Technologies (the independent review board tasked by President Obama with assessing US intelligence collection practices following Snowden) has estimated that, for MLAT requests in the US, the average time required from request to delivery is today roughly 10 months, and can sometimes take years.[5] MLAT requests of other countries for information from the US government are similarly drawn out, and can often take far longer. For law enforcement officials with urgent information needs, such delays are simply unacceptable. Unsurprisingly, impatient prosecutors are looking for alternatives to the MLAT process for access to digital information. However, those prosecutors, and the governments that they serve, must be mindful of the potential long-term consequences of those alternatives, particularly adverse consequences to the functioning of the internet itself.

Microsoft vs. The United States

One prominent example of this frustration with the MLAT system can be seen in the ongoing court case between the US DoJ and Microsoft Corporation. The DoJ is seeking information contained in a Microsoft Outlook account based in Ireland for a federal criminal investigation in the Southern District of New York. Instead of pursuing that account through an MLAT request directed to the relevant authorities in Ireland, as would have been the practice in prior years before the globalisation of data, federal prosecutors have sought the issuance of a warrant[6] directing Microsoft to produce information from the account directly. Microsoft has challenged the warrant, but the District Court (after substantial briefing, including amicus briefs submitted by other large internet companies) sustained the issuance, and now Microsoft is appealing the ruling before the Court of Appeals for the Second Circuit.[7]

The DoJ has made a fundamental policy choice in this case: To seek a warrant and to not go through the formal MLAT treaty process. One can reasonably discern that the government's decision to bypass the process was based in large part on concerns about the efficacy of the MLAT system and the potential for a drawn-out waiting period before prosecutors would get their evidence. Indeed, in its brief to the District Court in support of the warrant, the government argued,

> In contrast to an SCA [Stored Communications Act] warrant [the statutory form of warrant issued], which can be served upon a provider immediately upon issuance by a judge, an MLAT request typically takes months to process, with the turnaround time varying widely based on the foreign country's willingness to cooperate, the law enforcement resources it has to spare for outside requests for assistance, and the procedural idiosyncrasies of the country's legal system.[8]

Similar doubts about the MLAT process were expressed in the Federal Magistrate ruling in support of the government's issuance of the warrant. The Federal Magistrate, in its rejection of Microsoft's request to vacate, noted that the "slow and laborious" procedures of the MLAT placed such a "substantial" burden on the government as to necessitate the use of other means of retrieval.[9] In other words, the government, the Federal Magistrate and the District Court that ultimately rejected Microsoft's appeal all agreed that the MLAT did not offer a satisfactory means of obtaining evidence, and that the warrant was a necessary alternative, notwithstanding concerns of extraterritoriality.[10]

Microsoft's challenge is premised on the legal assertion that the SCA warrant used by the government does not allow for extraterritorial searches, but beyond the strictly legal questions involved, two important policy considerations are central to its position. Firstly, like virtually all major American technology companies, Microsoft is still dealing with the perception, post-Snowden, that US tech firms have been complicit in—or at least overly submissive to—NSA intelligence collection programmes, and thus cannot be trusted to protect foreign customers from US government overreach. Tech firms like Microsoft continue to worry that this concern is leading to lost contracts and could cause foreign governments to adopt legislation that could limit American access to foreign markets. Undoubtedly, Microsoft's decision to challenge the DoJ reflects the desire to be seen as maintaining a degree of independence from the US government, and as a protector of the rights and privacy of the company's non-American customers.[11]

Secondly, and perhaps even more importantly, beyond the perceptional issues, Microsoft also recognised that the US government circumvention of the MLAT process was setting a troubling precedent concerning the United States government's ability to demand data stored abroad in the future. Microsoft argues that the government is attempting to treat data stored abroad as it treats data stored in the US. The DoJ, Microsoft argues, is essentially

MICROSOFT V. THE UNITED STATES SHOWS IN THE STARKEST LIGHT THAT MLATS ARE INADEQUATE TO LAW ENFORCEMENT IN THE DIGITAL AGE.

claiming that its right to access to the former should be no less than its right to access to the latter (reading the government's briefs, this is not an unfair characterisation). In so doing, Microsoft contends, the DoJ is dramatically expanding its reach into foreign states, which have their own laws concerning access to digital information stored within their borders. Thus, Microsoft insists, the government's actions are subjecting American firms with data stored abroad to multiple and potentially contradictory data protection rules. And given the push by nations around the world—and within Europe, most critically—to update domestic data protection laws in ways that diverge significantly from US rules, forced compliance with multiple and inconsistent discovery and disclosure requirements could result in an endless stream of legal battles for tech firms operating abroad, perhaps even forcing US companies to pull out of certain overseas markets entirely.[12]

While the government and Microsoft await a ruling of the Court of Appeals on whether or not prosecutors may obtain access to data stored abroad by means of a warrant, the parties, as well as other stakeholders, need to acknowledge that the government has a legitimate interest in obtaining this information for its criminal investigations, and that Microsoft has equally compelling reasons to resist providing information to the United States in potential violation of privacy or data protection laws of other countries in which it does business. It was this potential for international investigatory conflicts that spawned the MLAT system in the first place. Yet this case has arisen precisely because the government has concluded—probably rightly—that MLAT would not meet its needs. Thus, *Microsoft v. The United States* shows in the starkest light that MLATs are inadequate to law enforcement in the digital era.

The Rest of the World vs. MLATs

Naturally, the US is not the only government encountering problems with MLATs. The Brazilian government, for instance, has similarly been frustrated by extended delays in the MLAT system, importantly pertaining to its request for information from Google's servers in the US for use in several cases pending before the Brazilian Supreme Court.[13] Similarly, India has often invoked the US-India MLAT to request that the other party serve summonses upon Google, as well as on Facebook, Twitter and others, for failing to prevent the dissemination of online speech prohibited under Indian law. Those requests have repeatedly been rejected due to American civil liberties sensibilities.[14]

Yet there are asymmetries between the US government frustration with the MLAT process and non-American frustration. American tech firms still maintain the lion's share of the global data storage marketplace. When Brazilians, Indians or others find that they, like the Americans, are unable to get the data they want in a timely manner, they too, in theory, can issue a direct subpoena or warrant under their domestic laws, but unlike the Americans, they generally have to issue those direct requests to a subsidiary which may not 'possess' the desired information. Even if the parent/subsidiary problem does not arise, the fact

remains that those governments have less influence over the American parent company than the US government. There is surely no doubt that if there are conflicting jurisdictional requirements, the great American tech companies will in all likelihood abide by the laws and requirements of their country and not risk all of the sanctions that could be imposed upon them by their government.

This asymmetry, together with the overwhelming domination of American technology firms in the internet economy and the international uproar over the Snowden revelations, understandably creates an unacceptable status quo for non-American governments. Legislatures and regulators around the world are now consequently considering adopting new legal regimes that would either keep data local or that would establish local jurisdiction over all citizen data no matter where it sits.[15] Germany, for example, is considering server and data localisation as part of a new internet security law;[16] in Brazil, the Internal Revenue Service announced its Declaratory Act #7 in October 2014 that would impose a 50 percent tax on all tech companies holding data overseas.[17] Among the effects of these laws would be a mitigation of some of the asymmetry by allowing for discovery of information directly from the subsidiary in the same manner as the DoJ demanded in the Microsoft case.

However, both of these two approaches—localisation and jurisdictional expansion—are deeply problematic for a number of reasons. First, forcing companies to hold data domestically (or to insist that only domestic firms operate domestically) likely brings up costs for internet users and small businesses, could retard technological innovation and the internet's 'generativity,' and will reduce the ability of firms to aggregate services and data analytics through cloud services. Equally important, localisation policies will likely degrade data security for the countries considering them, making censorship and surveillance easier for domestic governments (and perhaps even foreign governments) to achieve. Additionally, as was explained above, rules establishing jurisdiction over all citizen data, no matter where it resides, subjects companies to multiple and oftentimes competing jurisdictions and authorities. These overlapping and potentially conflicting jurisdictions put tremendous strain on firms: If they are unable to develop services or business models that comport with all the various legal requirements, they may be forced to leave certain markets entirely. For users and small businesses that rely on the low cost and efficiencies offered by the large internet companies, the loss of access to them or their services can present a significant hardship. Under either of these scenarios, internet companies suffer, internet users suffer, and privacy and internet freedom may suffer as well.

Recommendations

The US DoJ's recourse to warrants to obtain data stored abroad, and localisation schemes by other countries to keep data from the Americans are both potentially harmful to a robust and free internet, and both could be rendered unnecessary if nations were to adopt

reforms to the MLAT system. Below are proposed five such reforms, two of which can be implemented in short order, while three others will require longer-term commitments by national executives and legislatures.

1. Provide additional funding for processing MLAT requests

Timeline: Immediately

One of the primary causes of MLAT backlogs is insufficient resources for processing requests. At home, the US must be prepared to spend more money to make MLATs work for legitimate foreign law enforcement. Recently, the American government has made a down-payment on this necessary new funding. The DoJ requested and Congress funded an extra $24.1 million exclusively for MLAT processing. With these new funds for the 2015 financial year, the DoJ will hire 168 new staffers, including 85 attorneys, and supplement MLAT assistance within the US Attorneys' offices and the Federal Bureau of Investigation. This new staffing, the DoJ predicts, "will reduce backlog, and cut its response time by half by the end of 2015; it hopes to respond to legally sufficient requests in a matter of weeks."[18] But this is still not enough, as increasingly more MLAT requests will come in as criminal prosecutions increasingly focus on digital evidence.

The US is also entitled to expect other countries to spend more to expedite their responses to American requests. Realistically, other nations must recognise that American prosecutors will adopt the type of warrant procedures utilised in *Microsoft v. United States* if their MLAT requests gather dust on the desks of employees of foreign justice ministries.

2. Issue unilateral guidelines on direct requests for extraterritorial data, and importantly, require authorities to make "first use" of the MLAT process before resorting to other means of acquiring information

Timeline: Immediately

Governments around the world should issue unilateral self-binding guidelines to limit prosecutorial authority to bypass an applicable MLAT and to compel the production of email and other electronics records stored outside their own jurisdiction. As Phillip Reitinger has observed, there is precedent in the US for this type of unilateral restraint. He points out that "Section 279(b) of the Criminal Resource Manual requires that prosecutors obtain the approval of Justice's Office of International Affairs before issuing a subpoena for records located abroad."[19] Not every matter of evidence production needs the same degree of self-limitation; limitations can be flexibly applied to the range of evidence requests. As Reitinger suggests, a warrant, which is an especially intrusive procedure because no prior notice to the target of the investigation is provided, might require a higher standard of self-limitation than would a subpoena, where prior notice is customarily given. Similarly,

when the information sought from abroad is particularly sensitive (political or financial information perhaps) governments ought to be more willing to use MLAT procedures in preference to any unilateral discovery mechanisms. Further, once the MLAT process is expedited, governments ought to consider instituting a "first use" constraint, requiring that law enforcement agencies try in good faith to use the MLAT process prior to pursuing direct access. A "first use" constraint is of course likely to be politically palatable only among nations that adopt parallel reciprocal procedures.

3. Streamline the MLAT process

Timeline: Medium Term

The lack of resources is not the sole cause of delays in the MLAT system. Indeed, the process itself by which MLATs are approved or denied needs reform and streamlining. Importantly, as of today, there is no online submission form for MLAT requests. MLATs must either be submitted by paper or by email to relevant authorities in a slow and cumbersome process. Accordingly, all nations participating in the MLAT system should create an online submission form and guide for MLATs. An online system would allow requests to be sorted and prioritised, based on topic, and would even send automated responses in those instances when a request is wholly uncontroversial. Second, as the President's Review Group has noted, the current MLAT process contains multiple, oftentimes redundant, reviews for requests. In the US, for instance, the DoJ Office of International Affairs and the US Attorney's office must conduct separate independent reviews. These types of redundancies should be re-evaluated for efficacy and necessity.

4. Companies should adopt industry-wide policies on how to interpret domestic and international law with respect to requests for data for law enforcement purposes

Timeline: Medium Term

To avoid confusion and inconsistencies among companies and governments, the major technology and internet firms ought to seek industry-wide consensus on how to interpret national and international law with respect to data collection from law enforcement authorities (again, as distinct from requests sent by intelligence agencies, which present a far more challenging topic). The technology policy advocacy group Access has suggested that the tech industry should publicly explain their "interpretation of the law and the way in which they exercise their discretion as to when, how, and under what conditions user information is provided."[20] This industry-wide statement will not necessarily alter the way in which governments seek to access data, but it will give law enforcement a sense of the types of requests that will be challenged versus the types of requests that are broadly seen as appropriate, and will thus avoid unnecessary legal and political confrontations.

5. Renegotiate existing bilateral and multilateral MLATs to explicitly cover modes of communication associated with evolving networks and services

Timeline: Long Term

As mentioned above, innovation in the tech sector and the globalisation of data infrastructure has enormously complicated former notions of jurisdiction. Nevertheless, agreement can be reached on key terms and principles in a sufficiently broad way as to avoid bottlenecks in the MLAT process. These key terms and principles must be incorporated into updated MLAT agreements. To ensure that these agreements keep pace with changing technologies, however, matters dealing with data issues between and among treaty parties ought to be revisited frequently within multinational working groups. This will ensure that the MLAT procedures in place are still relevant. For example, as data sharding architectures (the process of partitioning data into pieces and dispersing it across multiple databases, oftentimes situated on servers located around the globe) or database caching (storing databases as temporary cache files) become increasingly prevalent, governments may need to revisit notions of data 'location,' data 'type,' 'personally identifiable information,' etc., within their respective treaties.

Streamlining and expediting the MLAT system will not, and should not, do away with all direct government demands for data from companies. MLATs are not the sole legitimate way governments can access data. Through the exercise of a country's police power, prosecutors will do what is permissible under their legal systems to obtain evidence. There will always be instances under which the urgent need for information will supersede the objective of maintaining international comity. Moreover, there will be times when no MLAT is useful because the information sought cannot be found in any specific jurisdiction, such as when sophisticated criminals store information, or components of information, in multiple locales. But because the MLAT regime will not always work, and because now it is not working well at all, does not mean that it cannot be a valuable tool for law enforcement that is both efficient and consistent with evolving notions of privacy.

Reform of the MLAT system is of tremendous importance for the future of the global internet. If left unreformed, or if reform is handled irresponsibly and without an understanding of consequences to the internet as a whole, law enforcement and jurisdictional battles among and between governments and technology firms could place yet another strain on the already stressed global internet system. In contrast, developing updated and efficient MLATs could pay enormous dividends, not only for law enforcement as it faces enormous international challenges, but also by serving as confidence-building measures as sovereign nations take on the task of resolving other, even more difficult, global internet policy challenges.

Network Diplomacy in Digital Networks

Patryk Pawlak, Senior Analyst, European Union Institute for Security Studies, France

8

With a larger share of the world's population gaining access to information and communication technologies, digital networks have become the backbone of social, economic and political life for millions of people across the world. At the same time, the international community struggles to find a consensus on norms that would preserve this digital environment as open and secure. This process is framed by the complexity of risks in the digital space on the one hand, and cultural or institutional context in specific countries or regions on the other. The fight against cyber crime is a good example of how different frameworks emerge and coexist, creating layers of competing—and sometimes complementary—sets of norms. The task is even more complicated given the diversity of interests (i.e., the fight against cyber crime, the rollout of e-government programmes, confidence building) and values (i.e., protecting freedom of expression, sovereignty over decisions concerning cyberspace, human development) represented within this increasingly dense global 'network of networks.'

Consequently, winning a global 'struggle over ideas' becomes a challenge for all actors—governments, private sectors and civil society—that wish to shape the future of the digital world. As Joseph Nye argues, the world nowadays is no longer about whose army wins but whose story wins. In this context, the ongoing struggles related to the fight against cyber crime, cyber security or internet governance are part of a larger global shift, whereby concepts like sovereignty, freedom of expression and responsibility are being used to draw mental borderlines in an increasingly connected world. With other regions gaining ground as hubs of global trade and business, and emerging economies becoming incubators of innovative ideas and technologies, it is clear that very few future challenges can be resolved by a group of developed countries alone. On the contrary, in a world where the centres of gravity are increasingly shifting away from them, they often need to defend their standpoints or convince others to follow their lead.

Marketplace of Ideas

The number of contenders at the global marketplace of norms is growing. While the debate about the shift in global power may seem rather vague, the trends in the distribution of digital resources across the world show a clear shift from the developed to the developing world. The Boston Consulting Group estimates that the internet economy in G20 countries will grow by eight percent each year for the next five years, while in developing countries this figure is expected to be almost double. In 2010, the BRICS group of countries accounted for 13 percent of global demand with spending of about 328 billion euro, or $360 billion, on Information and Communication Technology (ICT).[1] "China became the world's largest producer of ICT products, with exports of ICT increasing fourfold between 2004 and 2008."[2] Entities like Naspers (a South African global platform operator) and Alibaba (a group of internet-based e-commerce businesses headquartered in Hangzhou) are already among the biggest internet companies in the world.

These developments have encouraged BRICS countries to become global players rather than mere users of ICT goods and services. The Thekwini Declaration adopted at the BRICS Summit in Durban in March 2013 stated that "it's important to contribute to and participate in a peaceful, secure, and open cyberspace," and that emphasis on "security in the use of Information and Communications Technology through universally accepted norms, standards and practices is of paramount importance." Later, China's Foreign Minister Yang Jiechi said that the country is opposed to "turning cyberspace into another battlefield, or using the internet as a new tool to interfere in other countries' internal affairs."[3]

As this shift is taking place, it is expected that the discussion about norms in cyberspace, defined as standards of appropriate behaviour, will also accelerate. Four debates in particular are of great importance:

Fighting cyber crime: Adopted in 2001, the Council of Europe Convention on Cybercrime established the foundations for international cooperation beyond Europe. However, there is also a large group of countries that pursue similar objectives outside of the Convention. The Fortaleza Declaration adopted at the Sixth BRICS Summit expresses the commitment to seek independent and common initiatives, as well as the elaboration of a common strategy at the international level. Regional groupings like the Commonwealth, the Organization of American States or the Association of Southeast Asian Nations are also implementing their own capacity-building programmes. The Commonwealth Model Law on Computer and Computer-related Crime, for instance, provides guidance on language for the implementation of the Convention in the Commonwealth but does not include provisions on computer-related offences or provisions on international cooperation, although the Harare Scheme relating to Mutual Assistance in Criminal Matters might be interpreted as an element of international cooperation. In 2013 China and Russia, with support from Brazil, made proposals at the UN to clarify the mandate for the UN Office on

Drugs and Crime to continue discussions on cyber crime and possible new legal responses to it. The basic premise behind this idea was to investigate ways to strengthen the UN Crime Prevention and Criminal Justice Programme.

The right to privacy: A debate about privacy and freedom in cyberspace became particularly vivid after the revelations of the secret surveillance programmes being carried out by the US. Speaking at the 68th session of the UN General Assembly, Brazilian President Dilma Rousseff stated that ICT should not become the new battlefield between states and called for increasing the UN's role in preventing cyberspace from becoming a 'weapon of war.' Consequently, Brazil proposed a number of initiatives to that effect. In 2013, together with Germany, Brazil put forward a draft resolution on the right to privacy in the digital age. In 2014, Brazil launched informal consultation at the UN for resolutions on effective measures to enhance the protection, security and safety of diplomatic missions, which includes some clauses on cyber security.

Internet governance: The most pronounced division lines probably persist with regard to the future governance of the internet. A group composed of liberal democracies (including European Union countries and the US) maintains that the multistakeholder approach comprising governments, the private sector and civil society should continue to provide the basis for internet governance. In contrast, certain countries dubbed as 'cyber-sovereignty' advocates (including China and Russia) lobby for more governmental control over cyberspace. This debate was particularly heated at the World Conference on International Telecommunications in Dubai in 2012 and was picked up again in April 2014 at the NETmundial meeting in São Paolo. Russia, Cuba and India have clearly distanced themselves from the outcome of the latter, which presented a slight departure from a state-centric discourse. China, Russia, Tajikistan and Uzbekistan also insisted on a mention that follow-up deliberations should take place "within the United Nations framework"[4] while the US, Australia and several European nations reaffirmed their support for a body not dominated by governments.[5]

ICTs and international security: Russia introduced a draft UN resolution warning against the creation of information technology weapons and the threat of information wars as early as 1998. The proposal was largely rejected by Washington and other Western democracies that viewed it as an attempt to curb freedom of speech and suppress opposition by legally restricting the flow of information online. After the failed attempt of the first Group of Governmental Experts (GGE) to build consensus, the second GGE (2010) focused more on norms for development, confidence-building measures (CBMs) and capacity building in developing countries. In September 2011, Russia and China (together with Tajikistan and Uzbekistan) proposed an International Code of Conduct for Information Security, and Russia's resolution started becoming increasingly popular among other countries like Belarus, Myanmar, China, Cuba, Turkmenistan, Vietnam and Zimbabwe. A significant effort was also undertaken under the auspices of the Organization for Security and Co-

operation in Europe (OSCE) in 2012 aimed at preventing a cyber war. It was not approved after Russia refused to sign the conclusion and instead advocated a universal cyber convention that would codify reasonable standards of state behaviour. Eventually in 2013, the Permanent Council of the Organisation for Economic Co-operation and Development adopted Decision 1106 on the initial set of OSCE CBMs to reduce the risks of conflict stemming from the use of ICT.

Building Trust by Limiting Uncertainty

Closing the gap between different approaches and reaching an agreement on norms regulating behaviour in a digital environment is difficult without trust between actors and confidence in the effectiveness of the international system. Part of the problem stems from the uncertainty and lack of conceptual clarity that 'cyber' brings to global conversations. Therefore, changing the language from abstract and technical concepts towards the rule of law, good governance and human rights might be a good starting point to reduce complexity. For instance, often-recalled examples of cyber terrorism are at best an illustration of the link between terrorism and cyber crime, the limits of freedom of expression online, the protection of privacy, coordination of activities across jurisdictions or the rule of law. The problems with defining a challenge often translate into misguided policy responses.

Numerous examples of events that have taken place might serve as a point of departure for further debate. One of the dilemmas concerns the discussion about cyber terrorism as opposed to incitement to crime or hate speech through the use of the internet. The question is relevant as it bears implications for discussion on proportionate and necessary responses. In April 2014, Israeli government websites were victims of the planned distributed denial-of-service attack dubbed *Op Israel*, the aim of which was to "hack, deface, hijack, database leak, admin takeover, and DNS terminate the Israeli cyberspace by any means necessary."[6] In 2012, panicked Indian northeasterners fled their homes as a consequence of calls for Muslims to attack them spread over the internet and through mass SMS messages on mobile phones. In the latter case, the Government of India blocked some 250 websites. However, this ban was successively extended to journalists' Twitter accounts and news stories by local and foreign media organisations critical of the government, some of which parodied then Prime Minister Manmohan Singh. These types of restrictions are particularly problematic as there are no objective rules for assessing what is offensive and what the benchmarks should be for deciding when the imposition of limitations on freedom of speech is justified.

Recently, the Government of China has also launched a series of diplomatic demarches signalling interest in discussing cyber terrorism with its international partners. In September 2014, at the UN Security Council Summit on Terrorism, the Minister of Foreign Affairs of China Wang Yi stated that "social media has become a battlefield for

terrorist and extremist groups to instigate their ideology, a tool to plot terrorist attacks and a platform to recruit terrorists"[7] and that the international community should take appropriate measures "to stop the use of social media to spread extremist ideas, especially the releasing of audio and video materials of violence and terror. Internet companies and operators should exercise self-discipline. To this end, it is imperative to formulate as soon as possible a code of conduct for the global cyber industry."[8] Such statements, of course, are open to broad interpretation and could potentially result in targeting innocent populations or political opponents who are inconvenient for those in power. Nevertheless, a debate on applicable norms in such cases is concerned more with access to justice, rights of the accused, freedom of speech, etc. rather than cyber issues as such.

Finally, governments themselves have become exploiters of new technologies in order to pursue their own political ends, which calls into question norms underpinning their relationship with citizens and other actors like the private sector or non-governmental organisations. In Egypt, for instance, the government significantly limited access to Facebook, Yahoo and Google during the anti-government demonstrations. Similarly, during the presidential elections in Turkey, Prime Minister Recep Tayyip Erdogan ordered a ban on Twitter, which the Constitutional Court subsequently deemed "illegal, arbitrary and a serious restriction on the right to obtain information."[9] Similar attitudes adopted by governments around the world have encountered a rather negative reception among private companies whose reputations have been significantly shattered in relation to the US National Security Agency (NSA) scandals. In addition, tools like the DaVinci Remote Control System—a so-called 'legal surveillance' tool—give governments the means to monitor encrypted files and emails, Skype and other Voice-over-IP or chat communication.

Building Consensus through Network Diplomacy

Several reports on global governance highlight the shift towards a world shaped by different centres of gravity and coalitions of the willing. In such a networked world, power is measured by the strength of ties between actors and translates into the capacity to make ideas dominant within the network diplomacy, relying on economic, diplomatic or other instruments.

The debates about norms in cyberspace are no different. While many countries have their own vision of the future—as the examples mentioned above illustrate—hardly any of them enjoy the legitimacy or the position that would allow them to influence the outcome. The global standing of the US was shaken by the revelations of NSA surveillance programmes and press reports about its offensive operations around the world. The Golden Shield Project and expanding cyber espionage by the Chinese government or government-affiliated groups point to a larger state involvement in cyberspace. Consequently, network diplomacy becomes the only way for those countries to achieve their desired outcome.

The first strategy to increase network power is through leading by example. The mistrust in states' behaviour in the digital environment fits within a broader crisis of trust in the international system as observed today. Distrust among competing nations is fuelled by disagreements over interpretation and selective enforcement of existing norms shaping interstate relations. The best example of this climate is the response of the international community to the conflict in Libya and the subsequent lack of action in Syria. Therefore, rather than talking about cyber norms in abstract terms, the discussion should focus on how the cyber domain fits within frameworks of existing international rules and how to better implement the latter.

Another important carrier of change is capacity building, in cyberspace understood as efforts to develop and strengthen human, institutional and organisational resources at the national and international levels. While the ultimate objective of the process is to improve security—motivated either by self-interest to minimise the risk of external threat or by more ideological aspirations like enhancing human development—capacity building is also a tool of network diplomacy. The promotion of the Budapest Convention on Cybercrime and its adoption in different parts of the world illustrates this point. The Council of Europe, with financial support from the European Union, provides capacity-building assistance to fight cyber crime. Support to improve the legal framework, train law enforcement agents or build forensic capabilities, among others, is offered to countries that join the Convention or express the intention to do so in the future. This type of conditionality is supposed to ensure that any beneficiary is also subscribing to the rule of law and human rights and therefore to spread the normative agenda underpinning the Convention.

Finally, network diplomacy can be exercised through CBMs. In 1988, the UN Disarmament Commission presented guidelines for CBMs aimed at preventing military confrontation (intended or by accident) through reducing or even eliminating "the causes of mistrust, fear, misunderstanding and miscalculation with regard to relevant military activities and intentions of other States."[10] By engaging in dialogue, countries that do not necessarily share the same understanding of the world gain a better insight into each other's worldviews, build relationships and eventually gather political capital they can use to advance their ideas. In the absence of an overarching legal framework for cyberspace and given the existing differences between major players, the challenge of designing a generally acceptable catalogue of CBMs for cyberspace becomes starker. Some countries have therefore opted for establishing bilateral channels. The US and European Union nations have established cyber dialogues with each other, and also with China, in order to discuss potential security cooperation and further discussions on international norms of state behaviour in cyberspace.

The ongoing cyber-related debates have already resulted in a varied global geometry driven by a group of pioneers. The challenge for any actor with global ambitions is therefore to create and maintain ties with those who influence or play an important role in relevant networks.

GLOBAL INTERNET GOVERNANCE

Sovereignty will Reshape Internet Governance

James Lewis, Director and Senior Fellow, Strategic Technologies Program,
Center for Strategic & International Studies, USA

9

The political landscape of the internet has changed dramatically in the last few years. Two factors explain this. The first is that the internet has become a global infrastructure serving millions of users around the world. This brings new actors who demand a voice in how it is run and structured. The second is that governments have realised that far from being a global commons, there are borders in cyberspace and they can exercise sovereign control. Cyberspace rests entirely upon a tangible physical foundation. The internet is the product of agreements and contracts among business entities. There is no part of cyberspace that is not owned by someone who is subject to sovereign control. These changed perceptions about the importance of cyberspace and the nature of sovereignty create political forces that will reshape internet governance. It will continue to be a multistakeholder model, but with changed roles and responsibilities.

Governance involves understandings and expectations that guide behaviour and a framework for relations that provides a degree of predictability in interactions in security, trade and politics. Cyberspace is still an undefined element in the framework of relationships that govern relations among countries and the relationships between one country and the citizens of another. Governance of the internet and cyberspace is a new and important aspect for inter-state relations. There are sharp differences among blocs of nations over the nature of sovereignty and universal rights, the fundamental nature of the internet and America's global role.

As governments extend sovereign control into their national networks, they are increasingly uncomfortable with playing only a limited role in ensuring stability and security for an

essential global infrastructure upon which their economies depend and which has become the source of new and dangerous threats. Governments seek to expand their control in cyberspace because it impinges on many of their primary responsibilities. The risk is that their pursuit of greater control will damage both the economic and social benefits of cyberspace.

This expansion of sovereign control creates concerns that it will diminish a 'free and open internet.' As with any complex international issue, there is no simple way to address these concerns. It is clear that some countries hope to use the expansion of sovereign control to restrict access to information and to provide commercial advantage to their national companies. Their vision of the next generation of internet governance —to i) reduce the political risk that unrestricted access to information creates for some countries and ii) use a politicised governance process to gain commercial advantage—would create new constraints on transborder information flows. If these trends dominate, the internet will be damaged and global growth slowed.

Governments seek to expand their control in cyberspace because it impinges on many of their primary responsibilities, but the risk of this pursuit damages the economic and social benefits of cyberspace.

At the same time, assertions that the current governance model must be preserved if we are to maintain a 'free and open' internet face two problems. First, there is increasing foreign scepticism about the slogan and a belief that 'free and open' is actually a defence of the status quo. More importantly, there is no binding international obligation or commitment to a free and open internet, nor is it clear that every country has the same definition of 'multistakeholder' and 'open' or the same ideas on the role of government, the private sector, civil society and the UN. The mix of trade, security and political issues, combined with a vibrant non-governmental discussion, make the task of finding a way forward complicated and the pace slow.

The multistakeholder model was based on optimistic millennial expectations about the future of global politics, and the internet was created when the idea of globalisation was at its most powerful. The internet now serves a global population, with different values and different expectations about cultural norms, the role of government and economics. These new participants are not persuaded by assertions used by the incumbent internet community that the ideas of the 1990s have continued relevance to the internet's governance structure.

Governments, companies and non-governmental organisations have an equal say in decision-making in the current multistakeholder model, where governments are in fact at a disadvantage. This is intentional. The multistakeholder model was an experiment in global, non-Westphalian governance that grew out of the millennial expectations of the 1990s of a global community with shared political and cultural values replacing disappearing borders and a shrinking government role. The internet of that time, largely American, appeared to be an ideal test bed for a new mechanism for governance.

As the population of internet users has expanded beyond the US and Europe, the current model does not adequately represent the global user base. The current multistakeholder model is not truly representative of the global population of internet users, and this undercuts its legitimacy and authority. The global user base has created new requirements for representation, accountability and legitimacy. National governments, in this regard, have a greater claim to legitimacy in representing their populations than self-selecting elites, and it is likely that any new system of internet governance will be driven to rely more on nation-states as the legitimate representatives of the internet user population. The chief miscalculation in the thinking of the 1990s was that informal communal mechanisms could replace the formal governance institutions laboriously developed since the 19th century.

Economic and Commercial Implications of Change

One objection to a changed multistakeholder model is that it will erode the free and open internet, damage the economic benefits of the cyber space or lead to Balkanization. There is an understandable fear that moving from the original governance structure will damage the internet. Balkanization, however, is unlikely, as no country will knowingly give up the economic advantages of global connectivity.

Instead, countries will put in place rules and technologies that let them better enforce their laws on their national networks, and most will do it in a way that is consistent with their international obligations on security, trade and rights. The greater danger is not Balkanization, but incompatibility, as nations impose different and often conflicting requirements on global services that interfere with cross-border data flows and obstruct efficient communication in a range of business processes. Even when countries share political values, the rules for data localisation, data protection and privacy can be incompatible, given the lack of coordination and agreed principles. The risk from increased sovereignty is not fragmentation but inefficiency.

Regulatory frameworks for localisation, privacy and data protection are evolving rapidly, but most governments take a national approach that undervalues connectivity. For example, a former senior Indian official recently stated at a conference that India would impose new data localisation rules to keep data in India, but would also seek to make India

a global leader in providing cyber security services. These two positions are incompatible. Cyber security services require data to flow rapidly across borders, the complete opposite of localisation. There needs to be a clearer recognition that badly designed rules of localisation and sovereignty will damage economic growth, nationally and globally.

The risk of damage to innovation from a modified governance structure is also overstated. The assertion that the multistakeholder governance model is crucial for maintaining the free and open internet that drives global innovation is open to question, the most important being the assertion that an open and free internet produces economic growth and innovation. An initial review of data on internet freedom suggests that while access to the internet and broadband services creates economic growth, particularly in developing countries, the political conditions for access have little effect provided any restraints do not interfere with commercial activity.

Growth and innovation are complex activities with many factors contributing to how well a nation performs. The internet is one of these factors. Everything else being equal, a nation with a 'free and open internet' would outperform a nation with a closed internet, but national regulations and their enforcement, infrastructure, human capital and access to investment all play a more important role in determining growth and innovation. The salient counter-example is China—the internet is far from free and open and yet its growth has exceeded that of countries with more liberal policies for decades. While in the long term political restrictions on internet content harm a nation's ability to innovate, in the near term they need not be an obstacle to development.

Non-Western audiences hear 'free and open' as code for continued American dominance. The status quo is believed to favour American companies, and this is attributed to various American plots and devices to control the internet in ways that give it an economic advantage. The alternate explanation, that American companies are more innovative and offer better technology, is distasteful, even though it better explains the situation. If governance changes in a neutral way (e.g., one that does not use politics to favour another nation's companies), American firms are likely to still play a leading role.

When we look at other global, social infrastructures such as finance, transportation or trade, they are also complex and involve many actors and mechanisms for coordination. Internet governance will follow the same path. It would be inefficient and damaging to seek a global treaty on governing the internet. Nor can the International Telecommunication Union (ITU) serve as the governing body for cyberspace. Just as we do not use the ITU for trade, human rights, law enforcement or security matters, its role in internet issues should be similarly constrained. What we are likely to see, in the absence of a new approach to coordination, are actions by different governments to establish rules and penalties for behaviour on the internet. This will aggregate into a new governance framework, but it will also produce an increasing number of discordant sovereign controls.

The extension of government authority is appropriate for some functions—governments are responsible for protecting their citizens and upholding the law—and not for others. 'Free and open' also means an absence of centralised control over the internet and its content, technology and structure. This means that the software, standards and protocols that run the internet are not set by government policy. The benefits of letting the private sector create technology are intuitively apparent, but the issue is complicated by concerns over American hegemony and a desire in some countries to seek a competitive advantage for domestic companies.

Political Implications of Cyberspace Sovereignty

We are in a moment of immense transition in inter-state relations. In crude terms, Europe is in decline while Asia rises. The US, though still powerful, appears befuddled, while powerful non-Western nations demand a larger voice in the global institutions created after World War II. A few of these new powers go further and challenge those institutions themselves, as well as the concept of universal rights and institutions that supplant national prerogatives. The international 'system' is in flux.

Part of the reason for this is that the internet has created immense political forces that challenge governments in every country. It has changed citizen expectations of how governments should operate, something all nations will need to take into account. Citizens everywhere now expect a bigger voice and more insight into what their governments are doing. Old models of government-citizen interaction are under pressure to evolve. This political force applies equally to internet governance. The requirements for transparency, accountability and participation are different and greater. Just as the current governance structure was a 1990s experiment, it is time to develop new experiments in global participation and coordination.

JUST AS THE CURRENT GOVERNANCE STRUCTURE WAS A 1990s EXPERIMENT, IT IS TIME TO DEVELOP NEW EXPERIMENTS IN GLOBAL PARTICIPATION AND COORDINATION.

The internet makes it infinitely easier to send ideas across borders. Ideas are not weapons, but the internet creates immense political risk for countries that fear political change or have difficulty in managing it. A foreign website can host material that a country finds objectionable, and efforts to block it will not always work. National controls are inadequate

for stopping digital samizdat, since the rules countries impose on their national networks lack extraterritorial reach. Authoritarian regimes, for whom the internet is an existential threat, will try to reshape, restrict and possibly divide the global network.

The idea of sovereignty is itself in flux. Before 1945, sovereignty meant that whatever nations did within their borders was their own business and no one should interfere with their internal affairs. This led to global war. After the war, nations adopted universal protections for human rights. They did this because states that do not respect the rights of their citizens will also not respect the rights of neighbouring countries. Universal rights increase international stability, but a few nations openly oppose these universal commitments, and elites in some other non-Western countries question them as part of a larger scepticism about the international structure created after World War II.

The pressure to change internet governance gives authoritarian regimes an opportunity to buttress national controls by winning international agreement to restrict extraterritorial data flows. We are facing a messy, global debate to define the boundaries between sovereign control, extraterritorial networks and universal rights, but there is a global expectation that nations will respect their commitments to universal rights in any new governance system. Key nations like India and Brazil endorse free speech and other democratic values. Russia, China and a few others would like to use this debate to see universal rights narrowed and the older idea of sovereignty restored. They will continue to use the UN and the ITU as vehicles for advancing a competing vision of cyberspace. This competing vision runs contrary to the powerful political forces that the internet has unleashed—the precedent is the political effect of the Helsinki Accords, which empowered dissent—and the future will be one of greater participation and transparency. No matter how good the system of national political controls—and Russia has the best in the world—they can only delay change, not stop it.

The existing multistakeholder model faces scepticism in other countries, but this does not mean endorsement of the Russian and Chinese alternative. Most nations are in the position of 'fence-sitters,' still deciding which approach best serves their larger interest in development and economic growth. What is needed is a new and persuasive narrative to retain support for an internet that respects universal human rights and policies for open and equitable markets. Brazil's NETmundial showed that there is support for a new approach to governance that can accommodate new political forces while expanding economic opportunity and respect for individual rights. This is not a guaranteed outcome and democracies need to move beyond the slogans of the 1990s as internet governance is reshaped.

A new approach must recognise and define state responsibilities while respecting the diversity of national cultures and resurgent non-Western voices, but this does not entail a derogation of universal rights nor should it create new obstacles to trade or obstruct

agreement on the safer operation of the world's most critical global infrastructures. The goal for the international community is to define a nexus of norms, rules and institutions, both formal and informal, which will guide cyber interactions within and among societies and produce a safer and more stable environment. Rebuilding governance will take time, as it involves disaggregating tasks, creating new multilateral decision-making mechanisms and building broad consensus.

Accepting that governments have the right to control their national networks consistent with their international obligations creates an immense shift in the nature of governance. It shifts the focus of the governance discussion to international agreements among states as the foundation for a secure and stable cyberspace. As a first step, it would be useful for nations to agree to general principles for stability and for responsible state behaviour in cyberspace. Drawing on the precedent of principles that underpin other global infrastructures, the basis for a new approach to governance would require commitments to:

- Regularly consult on international changes that affect cyberspace and cyber security.
- Cooperate in developing and applying measures to increase stability and security in cyberspace.
- Prevent and end cyberspace practices that are agreed to be harmful to global prosperity and stability.
- Avoid actions that could threaten the stable operation of the internet or other cyber networks and the critical infrastructures that depend upon them.
- Protect the data of individuals and companies consistent with national laws and international obligations.
- Assist each other to overcome short-term difficulties in securing networks and responding to cyber incidents.

A new governance structure will need to be more accountable and more representative than the current system if it is to be perceived as legitimate. The best outcome would preserve a decentralised, 'multistakeholder' approach, but with redefined roles for each 'stakeholder' and with better mechanisms. We are likely to still see multiple organisations responsible for different technical and policy issues, some private, some governmental, but in an environment where decisions are determined more by governments and less by the current informal and non-governmental processes. The most likely result will be a system changed in ways that expand the role of governments and shrink the role of civil society organisations. The goal is a single, global network that avoids inefficiencies and still creates opportunities.

A simple test for change is to ask if any change improves governance (by increasing transparency, accountability or increasing representation) without damaging connectivity or universal rights. The Internet Corporation for Assigned Names and Numbers (ICANN), for example, is a lightning rod for criticism but actually performs well. Those who wish to

replace it need to demonstrate that any alternative would perform as well or better. This is not to say that modifications to ICANN are not needed, but to date no such replacement that does less harm than good has been identified. New proposals for governance will need to accommodate Western insistence that any change must 'do no harm' to the internet. There are bounds—commercial, technological and political—that shape and define any mandate for change.

The transition in governance poses challenges in a complex global political and technological environment. The interest of newly powerful nations will play an important role. The internet itself is in transition, politically and technologically. The future internet will blend autonomous devices, massive data sets and a mobile, cloud infrastructure. The extension of national sovereignty to the internet means that nations are creating their own rules for their national networks—for data localisation, privacy, acquisitions and security. All governments are extending sovereign control and they will eventually need to agree on how to cooperate in doing this. How they exercise their newfound jurisdiction will reshape global connectivity.

A Fork in the Road to the Future of Global Internet Governance

Examining the Making and Implications of the NETmundial Initiative*

Parminder Jeet Singh, Executive Director, IT for Change, India

10

It is customary in television debates to get two persons with completely opposed views engaging in a polarised discussion. Many are critical of this method as tending to suffocate the more nuanced views that may fall in between. They rightly claim that it serves to dumb down politics. At another level, however, a time comes in politics when any responsible political actor has to make a clear choice, as the path forward forks between two ways that are mutually exclusive and lead towards two fundamentally different political futures. Global internet governance stands at such a fork today. One path is of a continued evolution of our democratic institutions of governance—however drastic such evolutionary changes may today need to be—while keeping within the larger norms of democracy. The other fundamentally different path is to make a clean departure, and declare democracy inadequate to the scale and complexity of human organisation at the global level, especially in today's networked society. The focus, in this case, shifts towards seeking what are considered 'pragmatic solutions' to global problems, which would involve political, economic, technical and social elites running the world on the basis of some general conceptions of 'good governance,' including sporadic consultations with 'important groups' or 'stakeholders' that are considered relevant by such elites. The accountability of this system, it is claimed, will be ensured from the transparency and intense communicability that characterises a hyper-networked world, which would ensure a basic level of 'openness.'

Internet governance (IG) is indeed a very new field, as the manner in which the internet is impacting on social systems and structures and transforming them is highly complex, and also very unpredictable. There is so much to know and learn about before one can act decisively. On the other hand, the clock is fast winding down for decisive political action as the internet's architecture is getting concretised, increasingly towards a centralisation of power rather than its decentralisation, as was hoped for. As the dominant architecture is 'normalised' and a considerable amount of economic, social and political investment gets made in it, it will soon be too late to do much about it. The time for political action is therefore *now*. This is a major dilemma facing political actors in the global IG space.

A lot of mainstream actors have become so deeply immersed in exploring and discussing issues, at the cost of doing anything at all about them, that a major vacuum with regard to actual political action is being witnessed, especially at the global level. The global IG meetings and conferences circuit is unbelievably intense, and every few weeks the same faces seem to turn up in different parts of the world. Meanwhile, many actors propose setting up new information platforms and observatories as the real way forward—for instance, the proposed European Union Global Internet Policy Observatory—with numerous issues-mapping exercises occurring over the last few years, and still new ones being developed. At least two or three commissions have been set up to provide 'an authoritative recipe' for moving forward. Interestingly, these commissions are often set up and/or backed by those who gain the most from the status quo, which makes it unsurprising that their reports seem to contain further complexities rather than clear paths for the much-needed political action to address the myriad global public policy issues related to the internet. Much of the conference circuit is similarly propped up by actors from the Global North in general and by those entrenched in the status quo in particular, effectively giving rise to a US-centric global IG regime, corporates included. This puts a question mark on the neutrality of the knowledge that is delivered by these forums on what is one of the most hotly contested geopolitical subjects today. It is further increasingly unclear whether the overall effort is to move things forward politically, or to stall any such movement in favour of the status quo.

With a number of important policy events lined up, especially the 10-year high-level review of the World Summit on the Information Society (WSIS), 2015 could be a key year for concrete action. Alternatively, the year could end up being remembered for missed

'EQUAL-FOOTING MULTISTAKEHOLDERISM': THE SOLUTION OF STATUS QUOISTS, WHERE GOVERNMENT AND NON-GOVERNMENT ACTORS HAVE EQUAL ROLES IN DEVELOPING POLICY.

opportunities. Serious political actors must step back at this stage from the ever-faster revolving IG circus with its undeniable charms, and take some time to think dispassionately about the real needs, importance and urgency of global and national public policy issues related to the internet. This is even more so for actors from the Global South, who are increasingly being set up and co-opted into new geo-digital structures that are expected to leave them even more supplicant. The alternative is for these actors to take internet politics firmly into their hands, instead of being led by the nose as at present. It is in this regard that one speaks of a fork in the IG road, about which a clear and firm political decision will have to made, especially by the Global South.

How the Global Political and Corporate Elite are Taking Control

The political fork that is discussed here first appeared around 2010, and can be said to have taken a very clear shape with the recently launched NETmundial Initiative (NMI), which is led by the World Economic Forum (WEF) and the Internet Corporation for Assigned Names and Numbers (ICANN). The one good thing—perhaps the only one—about the new NMI is that it has provided a clear contour to, and a symbol for, a post-democratic world order. If the involved political actors still turn a blind eye to it, history might judge it as complicity. To put this historic political juncture in context, some key elements of the recent history of global internet governance are very briefly revisited below.

The Working Group on Internet Governance (WGIG), set up after the first phase of the WSIS, was the first important milestone for IG at the global stage. Its report was a remarkably sound document and still stands its ground today. Even though it had members from different stakeholder groups, its conceptions and outcomes were thoroughly democratic. The report described key public policy issues in the IG space while also laying out the respective roles and responsibilities of different stakeholders in this regard. Public policy was clearly to be a governmental responsibility, with other stakeholders contributing inputs to it. It also put forward the option of four institutional models for addressing both technical and public policy requirements with regard to the internet at the global level.

The outcome documents of the second phase of the WSIS, held in Tunis in 2005, took liberally from the WGIG report. In terms of actual institutional development, the Tunis Agenda mandated the establishment of a policy dialogue space in the form of the Internet Governance Forum (IGF), but left the issues of oversight of technical administration of the internet and internet-related public policies for further discussions within a place-holder concept of 'enhanced cooperation.' The Tunis Agenda represented a real and good compromise, and was spoken of highly by all parties in the following years. The pro status quo groups[1] were happy with a broad and somewhat diffuse definition adopted for internet governance, and an implicit admission that the existing structure of technical and administrative management of the internet was working well and need not change.

Although during the WSIS they had strongly opposed the proposal for establishing the IGF, status quoist groups quickly began to take control of it as they realised that developing country governments, except for Brazil, and for some time initially China, lacked the time and energy, and perhaps also the ability, to employ the complex and time-consuming processes of the IGF to press their claims and priorities.

It was towards the WSIS plus-five review that developing countries began to get vocal about the lack of any progress on institutional evolution related to public policies, as was required under the 'enhanced cooperation' mandate. It was at the 2008 IGF in Hyderabad, India, that Brazil first brought the issue of 'enhanced cooperation' to the IGF as a main session, against considerable resistance from status quoist groups. At this time, India did not appear to be too interested in the subject. But things began to heat up when, in 2010, India, Brazil and South Africa—the IBSA grouping—came together to make a joint statement on the issue, seeking a UN-based platform for addressing pressing internet-related public policy issues.[2]

The status quoist groups had until then dismissed any mention of 'enhanced cooperation' by claiming that it was a meaningless term that was used in the final WSIS negotiations to dexterously cover up the gaps between different positions. It was always a non-starter, dead on arrival, and there was no point flogging it any further. But when confronted by developing country demands to begin work on this mandate of the Tunis Agenda, they came up with a novel response. They claimed that 'enhanced cooperation' was well and happening at the IGF. Later, they began to claim that the IGF was an appropriate place for global coordination on internet-related public policies, and no other institution was needed for this purpose. Interestingly, such a claim was accompanied by simultaneous efforts to decrease or altogether remove the UN administrative oversight of the IGF. These groups refused to consider proposals for stable core UN funding for the IGF, and have been active in developing private funding for it. At its annual meeting in Baku in 2012, there was even an attempt by the Multistakeholder Advisory Group of the IGF to choose its own chair instead of one nominated by the United Nations. On the other hand, many of the concerned status quoist actors remained mindful of the fact that the IGF was after all a UN institution and would always be subject to its oversight and directions in some form or another. It would be difficult to ever fully negate this fact; thus, the status quoists considered wise to not put all their eggs in the IGF basket.

In 2010, the WEF revealed its Global Redesign Initiative, which presented a new vision of global governance. Multistakeholder governance was now no longer about consultations by governments with other stakeholders but involved co-development of policy, with an equal role claimed for non-government stakeholders and governments. WEF's Global Agenda Council on the Future of the Internet declared that such a multistakeholder institution with an equal role for all stakeholders is certainly the most appropriate one for dealing with internet-related public policy issues. As the WEF was working on these documents, one began to hear the reverberations of these radical, and certainly anti-democratic (i.e.

'post-democratic,') proposals in the form of a new formulation in IG discussions—'equal-footing multistakeholderism.' The WEF's rather ambitious blueprint was evidently being introduced and tested out in all earnestness in the virgin IG space.

However, it was becoming increasingly difficult for status quoist parties to argue that there were no significant global internet-related public policy issues to be dealt with. Consequently, around 2012, a somewhat deliberately inadequate term—'orphan issues'—began to be bandied about in the IG discourse. The term referred, somewhat grudgingly, to such global policy issues that were indeed impossible to deny any more and which did not have any existing institutional home. And then, all at once, in the middle of 2013 the Snowden revelations considerably raised the stakes, making the 'no action needed' position even more implausible and difficult to defend.

Greatly miffed with the US National Security Agency's surveillance of its president and other key targets, Brazil declared that it would seek a new UN-based institutional architecture for global internet governance, which sent alarm bells ringing all over. With India sticking to its earlier position for a new UN-based body, this coming together of the views of two leading developing countries could have potentially gathered cascading support for democratising global governance of the internet in a highly charged post-Snowden environment. An 'admission' of the need to do something about the 'orphan issues' was central to the overture that ICANN's CEO made to the Brazilian president in late 2013, almost certainly at the behest of the US. In response, Brazil agreed to host a conference on this subject, which was then quickly taken control of by ICANN.

The NETmundial meeting in São Paulo in April 2014 produced a problematic format to deal with global governance issues, where global corporates sat at the outcome-drafting table ensuring that their narrow commercial interests were protected and promoted. They were, for instance, able to introduce controversial intellectual property-related text into the document. ICANN, on the other hand, ensured that nothing normative was mentioned with regard to the process of transition of its oversight. Ignoring these major drawbacks, most non-governmental actors present at the meeting seemed delighted simply with the fact that a new format was produced, and in their mind, legitimised, for 'equal-footing multistakeholder' development of global normative texts. In this context, they appeared to be willing to turn a blind eye to the grave problems with the event's processes, and the fact that it was largely controlled by the status quo powers.[3]

The NETmundial outcome could still be considered to be relatively harmless if it was to be just another conference declaration that had no formal status. The problem, however, is that the status quoist groups project this outcome as a kind of new constitutional document for global governance of the internet. Never mind the fact that not only was this document not supported by many governments, a very large group of civil society actors, present on the floor when the document was adopted, opposed it, and issued a statement to the

effect. (Many of the civil society actors involved later withdrew this opposition, apparently because they so greatly liked the new format that promised them seats at the global policy table.) A false claim of universal support for the São Paulo NETmundial meeting began to be employed to legitimise and further shape a new global IG order.

In order to preserve the 'gains' from the NETmundial meeting and build on them towards a new post-democratic global IG order, a need was felt to set up some kind of formal and enduring global organisation or forum. This is what led ICANN's CEO to approach the WEF, that veritable seat of the global elite, and the NMI was launched. Although elitist, a relatively positive feature of the WEF is that it is certainly seen as a more global forum. Developing a new initiative around it does mitigate the perception of the US centricity of the current regime, which the status quoists felt was hurting their image the most. Facing some early resistance to their initiative, ICANN and the WEF co-opted the Brazilian Internet Steering Committee as a third partner to try and give the NMI a more acceptable look. But the window-dressing nature of this new addition was not lost on most observers.

This new initiative is clearly set to be 'the' place for finding multistakeholder 'solutions' to global internet problems, including and especially those that are traditionally considered matters of public policy. It therefore anticipates and is presented as the alternative to any other possible new globally democratic institutions that may be demanded for addressing global internet-related public policy issues. The NMI website has this to say about what is meant by seeking IG 'solutions,' which is a thinly disguised formulation for stepping into the area of public policy:[4]

> Internet governance solutions may be policy models, standards, specifications, or best practices and are produced by the Distributed Governance Groups. Solutions may be adopted voluntarily, or when necessary, formalized through other means such as social conventions, regulations, directives, contracts, and/or other agreements. Solutions for non-technical Internet governance issues are urgently needed to address the growing number of issues ranging from cyber-security to user privacy.

The website makes it further clear that the NMI is not just a policy dialogue, or a platform for taking inputs for policymaking, for the kind of tasks that the IGF is identified with. The purpose here is to take the dialogic outcomes from institutions like the IGF towards actual policies, camouflaged under the term 'solutions.'

> Through its work the NETmundial Initiative focuses resources to formulate solutions for the emerging issues identified through the multistakeholder dialogues at the IGF and other relevant fora.

In the eyes of its protagonists, the NMI evidently fulfils the role of the institutional mechanism that the Tunis Agenda codenamed 'enhanced cooperation,' which was to deal with global

internet-related public policies. Later UN resolutions identified the complementarity between the IGF as a policy dialogue forum, and 'enhanced cooperation' as the site for actual development of public policies. The above quote from its website shows how the NMI arrogates to itself this complementarity with the IGF, and thus also clearly the global policy development role in the IG space. Wolfgang Kleinwachter, an academic advocating civil society's support for the NMI, has stressed the complementarity of the IGF and the NETmundial process.[5] If there is still a veil over whether the NMI is supposed to be 'the' global forum for addressing key existing and emerging internet-related public policy issues, it is too thin to be of any significance other than to those who are rather too willing to be beguiled by it.

Democratic or Post-democratic Governance—A Choice has to be Made NOW

As the global political and economic elite develop their own captive global IG mechanism, the process has been accompanied by a systematic deriding of UN-based venues and possibilities, and a withdrawal from them. There is space here to only briefly touch upon this rather well-planned and well-executed strategy. After the first few years of showing great respect to the WGIG report and the Tunis Agenda, such deference begun to disappear among the status quoists around 2010 when the new elite-based model of global IG started to be given shape. The WGIG report, which interestingly was of a multistakeholder authorship, was completely banished from the discourse. The Tunis Agenda began to be spoken of as a relic from the past that hindered forward movement rather than enabled it, so much so that some actors, like the Indian government, had to struggle to get even a simple reference to the Tunis Agenda inserted in the São Paulo NETmundial Statement. The major sticking point for status quoists regarding these WSIS documents is the text about the respective roles in public policy development for governments and non-governmental actors. It went fully against the new post-democratic formulation of equal-footing multistakeholderism that was proposed as the new governance model extending also to actual public policymaking where corporate actors were to sit and vote at the same level as governments in global public policy matters.

It was with great difficulty that in 2012 developing countries managed to get a UN Working Group to look into the unfulfilled 'enhanced cooperation' mandate of the Tunis Agenda. However, in the face of a complete refusal to consider any kind of substantial institutional evolution by developed country governments, as well as big business, the technical community and most of the involved civil society, this Working Group could not come up with any recommendations, as it was required to. It is symptomatic of the changed times that while 10 years ago the WGIG could both map public policy issues and come up with four alternative institutional models, this new Working Group could not even attain that level of outcome. This clearly evidences a path of regression rather than progress as far as any possibilities within the UN system are concerned. Even the public policy mapping exercise that this new Working Group conducted, on which work was recently finalised by the secretariat of the UN Commission on Science and Technology for

An NMI-like global multistakeholder body may very well be the path adopted, where elites make deals among themselves.

Development, has been refused admittance by developed countries as an official document for the proceedings of the Commission and the WSIS plus-10 review. It is important to recognise the significance of the emergence of an alternative global IG paradigm and process in the name of NETmundial, over the year 2014, against the backdrop of a simultaneous withdrawal from the UN Working Group tasked precisely with developing recommendations for institutional evolution in the global IG space.

Any serious proposal for a new UN body modelled on the best global participatory practices to deal with global internet-related public polices, as was presented by India to the UN General Assembly in 2011, is met with significant propaganda of it being an effort to control the internet. Very interestingly, the same actors who oppose such a forum at the global level—developed country governments, global businesses, the technical community and many major civil society actors—fully engage with the Organisation for Economic Co-operation and Development's internet policy body, which is inter-governmental, and has exactly the same design and level of participation for non-governmental actors as the body that India proposed at the UN level. Inter-governmentalism at home and multistakeholderism abroad is a strange recipe—but perhaps it is an understandable one when the real motive is to resist any meaningful global governance of the internet that could place global normative or policy checks on the march of internet-assisted global political and economic domination by actors largely based in the US.[6]

At the same time that proposals for any new globally-democratic bodies or forums to deal with internet-related policy issues are blocked, the existing ones like the International Telecommunication Union (ITU), whose mandate comes closest to a possible internet-related role, are also not allowed to take up internet-related matters. This is quite a paradox. In what was clearly an ideological battle at the World Conference on International Telecommunication, the possibility of a mere mention of the word 'internet' in the new International Telecommunication Regulations was strongly resisted. Global governance of the internet had to be fully kept away from any globally democratic body. At the recent ITU Plenipotentiary meeting, developing countries repeatedly proposed text to mandate the ITU to look into issues of privacy and data protection—among the most important global policy issues today—but this was not accepted by developed countries, global businesses, the technical community, and also, something that one needs to keep mentioning with great regret, some major civil society groups engaged in IG area. The justification for such a stand was simply that the ITU is not the appropriate institution to govern these and other internet-related public policy issues. But then if not the ITU, the question is: Which

institution is the appropriate one to handle such issues, given that the same actors also block the possibility for any new UN-based, or otherwise globally democratic, body for such a purpose? The NMI has begun to provide the answer: It would be an NMI-like global multistakeholder body, where the elites make deals among themselves in the name of efficient and expertise based 'management' of the global internet.

The fork in the road to the future of the global governance of the internet is thus very clear. It lies between the possibilities and evolution of our democratic governance institutions on the one side, and new post-democratic forms based on an engagement among the global elites on the other. It can hardly be clearer. This is therefore one of those crunch times when every political actor must correspondingly make a clear choice of one or the other path. Going with the elitist model is one way, and making patchwork improvement to it—in terms of greater transparency and selection of non-governmental nominees by respective communities, for example—does not change its basic nature of serving elite interests. It perhaps makes it simply more dangerous by 'band-aiding' its superficial problems. The other path at this fork is to clearly reject this post-democratic enterprise in favour of evolving and innovating solutions within our democratic institutions and norms that are designed to serve the public interest. This of course does not mean accepting the grave defects in the existing UN mechanisms, just as for instance in India, keeping our faith in the current basic democratic institutional model, as it exists nationally, does not mean we are blind to its multiple shortcomings, or that we will give up on addressing them. After all, the IGF has been a remarkable innovation within the UN system. We can evolve a similarly innovative mechanism that can effectively address global internet-related public policies, which is democratic in its basic architecture, while adopting the best contemporary practices of openness and participation, many of which have uniquely evolved in the global IG space.

This primary choice, between an evolutionary democratic path and a post-democratic elites-based governance model, frames and logically precedes other engagements and activities in the global IG space. It is said that in politics, not doing anything itself is a political choice. Not to urgently address this key framework political issue or dichotomy could by default mean giving explicit or implicit consent to what today is the dominant wave in the IG space—that of derision and withdrawal from the UN-based and other globally democratic forums, and investment into post-democratic models of governance where global 'solutions' or policies are negotiated and decided among the political, economic and social elites. We must not 'un-see' the direction the IG discourse is taking and keep our attention narrowly fixed on the other myriad activities and engagements in the IG area.

The choice that the various political actors make at this historic fork in the road will determine the appropriate political alliances and strategies for them. It is time that the IG world shake off the deep obstinacy that has come to characterise it, the key result of which has been a complete policy paralysis in this most important of policy areas that impacts all social sectors.

Evolving with our Stakeholders

ICANN's Programme of Inclusion and Improvement

Yu-Chuang Kuek, Vice President and Managing Director – Asia Pacific, ICANN

In 1998 when the Internet Corporation for Assigned Names and Numbers (ICANN) was formed, four percent of the world's population was online, with half of those users in the US alone. By 2013, 35 percent of the world's population was online, with almost half of those users to be found in Asia. Looking ahead, the Boston Consulting Group predicts that by 2016, the internet economy will have expanded to $4.2 trillion in the G20 economies. If such an internet economy were a national economy, it would rank as one of the world's top five, behind only those of the US, China, Japan and India, and ahead of that of Germany.

This is staggering growth by any metric, and ICANN is proud to have played a central role in that growth and in making sure that throughout, and in spite of ongoing exponential growth, the internet has continued to work. ICANN's role in coordinating the Domain Name System is a key aspect of what makes the system work, with one authoritative root, a secure, stable, resilient and interoperable network (or network of networks), and a track record that boasts of not a single shutdown of the Domain Name System.

This is a track record of which we are proud, but also one that humbles us. In our short 16-year history, ICANN has continuously refined and improved its model to meet expanded adoption of the internet and shifting demographic realities of global internet usage. As such, ICANN's relevance from the very outset has stemmed from a culture of continuous self-improvement—actively soliciting feedback and involving as many stakeholders as possible so that we can refine the model and address shortcomings. This is exemplified

> *ICANN's Five-Year Strategic Plan, based on seven specific tracks, was developed to globalise the Corporation and localise our relevance.*

by the work of ICANN's Accountability and Transparency Review Team process, which has completed two rounds of reviews since 2009. Such a mindset of continuous self-improvement has also resulted in palpable changes in the way we work. This can be seen by the growth of our original headquarters in Los Angeles into three global hubs to include operational functions in Istanbul and Singapore. The ongoing work on the Internet Assigned Numbers Authority stewardship transition marks yet another milestone in our developmental journey.

It is in this context that ICANN's Five-Year Strategic Plan was developed to globalise the Corporation and to localise our relevance. ICANN is committed to our global, diverse and ever-expanding community. Globalisation is critical to how we operate, and a top strategic priority for the 2015 financial year and beyond. With the groundwork laid, we are now accelerating that vision over the next three years, and it is this framework that is discussed in this paper.

Globalisation and Localisation: The Programme

ICANN is excited to have a new programme meant to help the organisation globalise, while simultaneously making our processes and stakeholder experiences ever-more localised. This programme, initially previewed by ICANN President and CEO Fadi Chehadé at the opening ceremony of the ICANN 50 meeting in London, has now been further refined and defined into the seven tracks described below.

Global Sensitivity

The internet today has become a global resource across continents and within communities, dominated by no one region and country and supporting a multistakeholder group of interests. Recognising this, ICANN has begun to update practices so that staff are even better positioned than they are now to engage with our multilocal communities, thus making ICANN more locally relevant, while as a whole remaining globally vibrant.

The objective here is to ensure structured coordination of ICANN's internal technical and operational resources, and institutionalise a mindset of continuous improvement.

Global Stakeholder Service Channels

To improve the usefulness of responses to the community, our stakeholder service channels are being revamped to ensure a uniform global experience. Contracted parties, volunteers and members of the broader stakeholder community will get the same consistent experience when making queries and providing feedback to ICANN, be it by telephone, email or other service support systems, no matter where they are. The process is starting with the six UN languages, but, where practical, the aim is to accommodate local time zones and local language needs.

To date ICANN's main enquiry line has been in Los Angeles and has included ticketing capability. Now the Asia Pacific hub, along with Beijing and Seoul, provide phone and email customer support channels, and a pilot is being explored with the Global Domains Division team to increase service channels and improve the customer service experience. This includes the development of a multilingual call centre capable of servicing global queries.

Local Contracts and Payments

In addition to globalising ICANN's representation and service support, we are also working to 'localise' certain key functions. The goal is for global hubs to have the ability to contract with stakeholders in select local jurisdictions and enable engagement centres to receive payments in local currency. This is important for a number of reasons.

First, by contracting in local law and making local payment options available through any of our global hubs, we could increase community flexibility by providing localised solutions to communities outside the US. Second, by providing greater choice to companies outside the US that contract with us, we can strive to simplify business processes and lower operational costs for our constituents, speeding up our responsiveness to stakeholders. This is intended to help level the playing field globally and in so doing, allow for the further development of the domain name industry in emerging markets. Third, the diversification of ICANN functions across hub and engagement offices helps further integrate our activities into the regional and local communities.

It is worth noting though that as we move forward with these developments, these steps increase the legal, financial and operational risks and complexity for ICANN, and are therefore developments to be proceeded with thoughtfully and after careful evaluation.

Community-driven Language Localisation

Operating in a multicultural and multilingual world, accessible content is of utmost importance to us. We have therefore already put a great deal of effort into translating core

ICANN content into the most representative languages, including the six UN languages. To extend this beyond the most commonly used languages and increase stakeholder access to ICANN materials, we have begun a community-driven language localisation track, complementing the work of our in-house language services department.

Under this approach ICANN will partner with local communities in bringing awareness-building and public education content back to local platforms; as such, the project complements and builds upon the existing pool of official translations. The programme is being piloted out of ICANN's Asia Pacific hub and learnings will be shared at a global level.

Our aim is to partner with the community to service any local language, depending on need. Ultimately it is all about ensuring that content is accessible to local communities in local languages.

Hubs and Touch-points Engagement

This strategic initiative needs to be understood at three levels. First, ICANN's strategy to create three global hubs—in Los Angeles, Singapore and Istanbul—has allowed us to better engage stakeholders globally and has ensured improved time-zone support. The staff members on the ground have local language capability and cultural understanding to share developments with, and collect feedback from, local stakeholders within the geography and time zones of the community. The hubs now remain responsible for ICANN's core work. In particular, ICANN is expanding and growing the Singapore and Istanbul hubs.

Second, engagement centres are being established to provide bridges to communities in a range of countries. The criteria for adding a new engagement centre depends upon the strategic value of each addition to ICANN, the costs involved and whether the new communities are better served because of these additions.

Third, there is the possibility of strategic partnerships and Memorandums of Understanding with the community to build 'touch-points' across selected regions. This will provide a larger ICANN engagement footprint to interact with and serve the global community. Such an initiative also better integrates ICANN's work with that of our community partners. This programme dovetails with the work being done to localise select ICANN functions such as contracts and payments.

Decentralised Functions

ICANN's internal operational functions, such as finance, human resources (HR) management, information technology (IT) and legal functions, are all relatively centralised

today. Decentralising these functions allows ICANN to operate globally in a more efficient, responsive, representative and possibly more cost-effective way.

It will also bring new capabilities to the regions. For example, having an HR manager on the ground allows us to better understand the local labour markets so that we hire the appropriate talent to better serve that local community, enabling ICANN to scale globally. In addition, it means that we better understand the local environment, and can provide constant time-zone coverage. Decentralised IT functionality allows for new capabilities such as webinars being conducted in the region, while decentralised finance and legal functions improve in-country support.

For the community, registry and registrar service managers and contractual compliance team members based in the Istanbul and Singapore hubs mean that user needs are better met in local time zones, cultures and languages.

Expansion of Policy Outreach Channels

ICANN policy channels have been robustly built for global participation, with meetings held around the world in a systematic fashion to be as inclusive as possible. Remote participation is always available, and fellowships are provided on a regular basis to help with travel expenses of candidates from geographies with challenging financial conditions.

Nevertheless, we believe this effort needs to be further extended by collecting policy input at platforms outside the traditional ICANN platform to allow greater inclusion of the wider end-user community. This will position ICANN as an 'easy partner' for interactions, by overcoming geographical, cultural and technological barriers.

Under this track ICANN will provide policy updates at non-ICANN platforms to raise awareness and solicit views. The outcomes in this case are for clear, effective and predictable policy development and decision-making processes that enable greater inclusion of diverse global stakeholders, and evolved processes that allow under-represented countries and communities to identify and pursue relevant topics. The result is implementable ICANN policies and advice.

As the domain name space expands with the number of internet users coming online, and as the multilingual internet touches more and more communities, it is important to evolve policy together with these stakeholders, as well as understand the way they use the internet.

This plan is not exhaustive and may continue to evolve, due to community feedback and needs.

Transitioning to the Next Stage of Development

Why is this transitional programme important? By the time ICANN's Five-Year Strategic Plan is complete, it is estimated that 63 percent of the world's population will be online, many of whom will not use Latin keyboards. This growth brings more users, more expectations and more dependency. But even more importantly, the fact that so many are banking on future economies, on cloud computing and the Internet of Things is a vote of confidence in the work that must continue to be done effectively.

That so many people and businesses around the world now take the internet for granted, while not knowing what ICANN is, we take as validation of the work being done. But it is also validation of the need for a culture of continuous self-improvement, and is justification for the changes now being driven through and the implementation programme outlined in detail above.

The above brings us to the unique strengths of the multistakeholder model, the need for ongoing and expansive inclusiveness and the requirements to continue to open ourselves up to outside challenges, critiques and constructive engagement. This is the only way in which ICANN will continue and adapt over time, and the only currently apparent model for the internet to be able to remain open, scalable and robust. And it is in this context that we look to now extend our engagement with India.

India and Next Steps

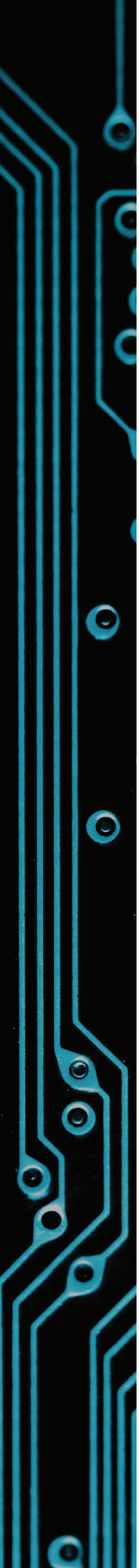
ICANN has long been a beneficiary of wisdom coming from India. An active participant in the Governmental Advisory Committee, India also contributed a board member to ICANN. But within an expansive and inclusive framework, the question is: What can be done next to promote access and usage?

We share the same optimism about the internet's future with Prime Minister Modi's Digital India agenda. The Digital India plan has set a target of providing broadband connectivity to 250,000 villages (India had 641,000 villages according to the 2011 Census) and making as many schools WiFi-enabled by 2019. The overall target of the mission is to make 1,000,000 people digitally literate by end-2015.

The Digital India project also aims to ensure that government services are available to citizens electronically and to help people gain benefits from the latest information and communication technology (ICT). Under the Digital India programme, all central government ministries and departments will come up with their individual projects that can be delivered to the public using ICT in the areas of health services, education, judicial services, and so on. There are nine pillars under the Digital India programme:

Broadband highways, everywhere mobile connectivity, Public Internet Access Programme, e-Governance, e-Kranti (which aims to provide electronic delivery of services), information for all, electronics manufacturing, IT for Jobs and early harvest programmes.

These are the kinds of overall economic and socially beneficial programmes that we expect to see and work with governments to support. ICANN's relevance stems from its continuous self-improvement in collaboration with its stakeholders. We invite India to work with us and to actively shape the future of internet governance both for India and for the regional and global communities.



PRIVACY AND SECURITY

Security and Privacy in Mobile Health

Siddharth Verma, Managing Director, Corazon Systems, Australia

Clinicians and patients are adopting mobile technologies faster than providers can protect security and privacy. The mobile device is well and truly front and centre. It is time to play catch-up.

To understand the impact the humble smartphone has had on the health industry, it is worth taking a step back in time to appreciate its meteoric growth, one of pandemic proportions. The IBM Simon Personal Communicator was a forerunner of the modern smartphone. It went on sale on 16 August 1994, and combined mobile phone technology with a wide range of computing features. While it was not called a smartphone back then, it had several features we see today—a calendar, facility to take notes and send email messages—and combined all of this with a cell phone. It had a stylus, a green LCD screen (similar in size to an iPhone 4) and a battery life of about five hours (something a lot of mobile users can relate to even today).

Twenty years later, as mobile technology advances and expands, it is changing the way healthcare is delivered around the globe. According to the International Telecommunication Union, six billion people, or 87 percent of the world, had mobile subscriptions by the end of 2011, up from 5.4 billion in 2010. Of the one-third of the global population using the internet, 62 percent are residents of the developing world. In the last fiscal quarter of 2011 alone, 180 million new mobile subscribers were registered, reflecting the rate of the near-exponential growth in this sector.[1] In India alone, the market for mobile health interventions will be worth $557 million by 2017.[2] Under a project run by Johns Hopkins University, over 850 female fieldworkers in rural Bangladesh had gone, in less than a decade, from being completely disconnected, to owning and using a personal mobile phone to connect with family, friends and co-workers.[3] The growth of mobile devices and their reach is astronomical.

As states Alain Labrique:

> Mobile technologies are also rejuvenating the domain of telemedicine and electronic health (e-health), which were previously largely 'tethered' systems, focused on facility-based recordkeeping, supply chain monitoring and sometimes decision support. Mobile technologies serve to 'untether' these systems from their facilities. They widen the reach and versatility of the e-health infrastructure to support front-line healthcare workers where and when they need access to patient information, while also allowing them to contribute to clinical records from the field.[4]

Specifically regarding mobile health, "[s]ince the start of 2013, more than $750 million in venture capital has been invested in companies that do everything from turning your smartphone into a blood pressure gauge to snapping medical-quality images of the inner ear. Apple, Samsung, Qualcomm, Microsoft and other corporate giants are creating mobile health products and investing in start-ups."[5]

Both Apple and Google can lay claim to over one million applications being available from their respective app stores. Apple CEO Tim Cook announced that over 60 billion applications had been downloaded till October 2013 (compared to 30 billion downloads during the same period last year). Sundar Pichai of Google announced in July 2013 that Android users had downloaded over 50 billion applications till date. Microsoft, while a distant third in this race, is moving fast with over 300,000 applications and counting.

However, while the mobile healthcare industry undergoes significant growth, it is not bereft of poorly designed or unsecured applications. As per a 2012 PwC report, "[o]f the 100,000-plus mobile health applications available for smartphones, very few have been downloaded more than 500 times." Furthermore, less than one-third of people who downloaded such an application continued to use it.[6]

There is also the question of security. One of the primary requirements of healthcare is protecting the information of the patient. A personal health record is sensitive information that is worth a lot of money in cyberspace. However, an unregulated market, teeming with information-hungry consumers with an almost fatalistic addiction to 'sharing' freely is a

AN UNREGULATED MARKET, TEEMING WITH INFORMATION-HUNGRY CONSUMERS WITH AN ALMOST FATALISTIC ADDICTION TO 'SHARING' FREELY IS A RECIPE FOR DISASTER.

recipe for disaster. Moreover, how are these apps safeguarding and using data provided by the user?

Mobile health apps are ubiquitous. There are applications to count calories, measure heart rate, document sleep patterns, analyse blood sugar and even monitor moods for signs of depression. A recent study reveals that there are about 100,000 varieties of inexpensive and easy to use mobile health apps available in the market, and all indications point to huge growth in the near future.[7]

The mobile industry tracker Research2Guidance predicts that by 2017 half the world's 3.4 billion-plus smart phone users will have downloaded health apps. But have we realised what happens to the sensitive data consumers enter into these apps? Most of the apps do not deliver the medical miracles they promise; rather, they share that data with advertisers and other third parties without the user's knowledge. With a huge growth in health apps, the privacy of important medical data has become a reason of concern.

The Privacy Rights Clearinghouse released a study funded by California Consumer Protection Foundation showing the potential privacy risks of mobile fitness and health apps.[8] The study evaluated 43 such apps (paid and free) on both Google Play and Apple's App Store to determine potential risks to important health data being collected, transmitted and stored using these apps.

	Free Apps	Paid Apps
App has a link to website privacy policy	43%	25%
Notifies users privacy policy doesn't apply to 3rd party links	48%	25%
Notifies users that personal information made public is not protected	57%	15%
Shares users generated PII data with advertisers	43%	5%
Uses anonymised data (non PII) for analytics	70%	70%
Contact information – developers details mentioned in privacy policy	57%	100%
Can opt out of developer / vendor sharing data with 3rd parties	57%	30%

Information courtesy privacyrights.org

This study unveiled many security loopholes in the usage and storage of sensitive health information collected by mobile medical apps. In addition, according to the report, only 13 percent of free apps and 10 percent of paid apps encrypt all data connections and transmissions between the app and the developer's website. The biggest difference between paid apps and free apps was likely the fact that 43 percent of free apps shared user-generated personally identifiable information (PII) with advertisers, while only five percent of paid apps did the same.

The US Health Insurance Portability and Accountability Act (HIPAA), which limits who can see and receive a person's health information, instructs doctors, insurers and pharmacies to keep electronic health records confidential, unless the user explicitly gives permission to share them. However, certain mobile health app developers are not obliged to follow such regulations if the data is not being used by a covered entity, such as a physician, hospital or health plan. The apps often send clear and unencrypted data without the user's knowledge and consent. Some apps even share the user's location and other personal details with advertisers and third-party companies within few minutes of the mobile device being turned on, again often without the knowledge of the user. Less than half of the free apps have privacy policies in place and only half of those who had privacy policies described the app's technical processes accurately. Due to unencrypted connection during data transmission and unprotected data storage, apps end up exposing sensitive data to everyone in the network—a huge privacy risk.

Despite all the hype and promised benefits, m-health is plagued with more challenges and misconceptions than opportunities. Questions around perception, interoperability, open standards, privacy, security, trust and suitability still cloud the conversation.

Perception

What is m-health? While a simple question, it sparks a range of different answers. To general mobile phone users, m-health is measuring their steps, calories burnt, dietary intake, etc. To patients suffering from chronic diseases (such as diabetes), m-health means using a mobile device to measure blood sugar levels and exercise patterns. To nurses or community health workers, m-health is the ability to provide care to their patients by using mobile devices as a tool. Finally, to a clinician, m-health is the ability to access electronic medical records through mobile devices.

While all of these are very valid and specific uses of m-health, the typical mobile user often has a skewed view of what m-health is in reality. In this chain of users there is a natural progression from being a healthy individual to someone who eventually becomes a part of the healthcare cycle. The same user in some instances becomes a patient who will need to interact with a nurse, community health worker, clinician and occasionally the hospital.

A user's perception and expectation of what m-health is will change as he/she progresses through the system.

Interoperability

It is predicted that by 2017 there will be more mobile phones than people on this planet.[9] Interoperability will "enable the exchange of data among systems in common formats, the use of common protocols and ultimately the ability to work together. [It] is a critical issue for m-health, because patients may have multiple clinical needs and conditions at one time and will interact with the health systems via multiple points, providers and professionals."[10]

Open Standards

Interoperability and open standards go hand in hand. 'Open standards' means that standards are publicly available. Information about a standard's use and application is available, there are no fees for its use and the standard was developed using a consensus process. Currently multiple 'standards' exist in m-health. We already have the Health Level Seven (HL7) that

> refers to a set of rules that govern how healthcare systems exchange information with each other. SNOMED CT is a coded taxonomy which is used to define healthcare information concepts (e.g., to define diseases, findings, procedures, and so on). However, although both examples have been developed by non-profit organizations, neither is yet freely available for use.[11]

Open standards are particularly important for equity in m-health. These standards must explicitly define how and what application developers can program into their solutions, what level of compliance and security needs to be adhered to. There is a need for either a regional or global governing body that applies and oversees adherence to standards.

Privacy and Security

The rapidly growing "i" generation is sharing personal information freely and frequently. Most consumers, when asked about the importance of privacy of their personal information, always rank it high up in the list, but disregard the fact that they are doing the exact opposite when sharing personal information on social media. It is scary to think how most consumers fail against their own lofty expectations of privacy. However, it is unfair to expect the average consumer to be an ideal role model. On the other hand, large organisations and corporates that provide such solutions play an equally important role in ensuring that the circle of privacy and security is not breached. Designing systems that are interoperable, adherence to common standards, good system design that is built on the foundation of security and privacy—these are the bare minimum requirements

to safeguard privacy. The consumers will play with what is given to them. Therefore, as businesses working to earn and grow, they equally need to take social responsibility and good citizenship seriously while designing solutions.

Bring your own device (BYOD) is becoming the norm at hospitals. Almost 85 percent of hospitals allow their staff to connect their personal devices to the hospital network. What security measures are in place for when this occurs? About 69 percent of clinicians use mobile devices to check their patients' medical records. How secure are these devices? As more mobile devices enter the healthcare system, the potential threat to sensitive medical records increases exponentially. In 2014, almost 40 percent of health organisations reported a criminal attack, up from 20 percent in 2010.[12]

The top three concerns for healthcare organisations in 2014 are reportedly employee negligence (75 percent), public cloud services (41 percent) and mobile device security (40 percent).[13] What compounds the matter further is the risk of consequences and visibility. With the HIPAA in the US and the Australian Privacy Principles in Australia, organisations have to report any such breaches. Public shaming has far greater impact than the threat of a financial penalty. In healthcare, it is all about trust.

Trust—the Hippocratic Oath

Gone are the days when medicine was only practised face to face with a direct physician-patient interaction. With e-health, tele-health and m-health, the lines are blurred, the boundaries have been pushed out. Corporate enterprises such as Google, Facebook, Microsoft and Apple are now becoming custodians of sensitive and personal information. When did this change happen? Who gave them permission to collect and store such information? What is this information being used for? Who will this information be shared with? As patients, we trust our healthcare professionals to keep our information safely and securely. However, with this new breed of m-health solution providers, where does the balance of trust sit? It is time for such organisations to reach out to the consumer and build that trust and demonstrate that the information is secure.

Suitability

Most m-health applications either do not reach the right audience, or they do not deliver the promised result. For example, a diet-tracking and calorie-counting mobile app quite possibly has a much greater use for an obese person than someone who has a natural disposition to lead a healthy and active life. Mobile health, while possessing the immense power of reaching out to the masses, has to reach out to the right audience if it is to act as a solution.

In the recent Ebola outbreak in Nigeria, healthcare workers used m-health quite effectively—a spectacular success story where the World Health Organization recently

declared Nigeria, Africa's most populous country, to be Ebola-free within 42 days. A real-time reporting app on the Android platform was supposedly instrumental in reducing the reporting time of Ebola infections by 75 percent so that help reached much quicker, helping curtail the infection.[14]

This highlights the fact that there are some significant opportunities when it comes to m-health.

Opportunities

Mobile devices provide many benefits to medical, nursing and allied health practitioners and their patients. The average Medicare patient in the US with one chronic condition sees seven doctors in a year. For a patient over the age of 65, with more than one disease, the number of doctors, therapists and social health workers increases significantly.

While most developed countries have electronic health records, hospitals and clinics to provide coordinated care, a large part of the improvement and preservation happens outside the four walls of these establishments. This is where m-health can play an important part. Mobile technology can be used to provide the day-to-day continuum of healthcare plans.

However, for this to deliver the promised benefits, m-health needs an ecosystem of workflow. When wearable (like Fitbit) or mobile devices (like the iPhone app) capture and regurgitate valuable information, an expert should be able to view and analyse the information. This poses another challenge: It requires a shift in the workflow of the healthcare workers. Will they be able to handle the change and the increased workload?

We also need to look beyond just mobile or smart phones.

The Future of M-health

It is reported that by 2020 there will be over 50 billion devices connected to the internet.[15] Many of these will be connected to the healthcare network—Google Glass, wearable devices such as Fitbit, Jawbone and Nike Fuelband, smart watches (iWatch, Galaxy Gear), wearable medical devices such as insulin pumps, blood glucose monitors and halter monitors. The future of healthcare will have m-health at its very core. It is going to be a game changer. The entire health ecosystem will have to adapt.

If the horse has not yet bolted, it is about to.

It is fair to say that m-health is now an integral part of the healthcare system. While it promises some significant benefits to one and all, it does carry heavy baggage in the form

of privacy and security concerns. Lack of governance and regulatory guidelines relating to mobile devices in medical workplaces is still a concern. Privacy and security issues in healthcare contexts are of particular concern to all stakeholders because of the sensitive nature of the data stored on the many mobile devices. The development of apps is also ad hoc and frequently undertaken without input or critical appraisal by end users,[16] often delivering solutions that do not deliver the expected function.

Use of best practices in the domain of m-health need to adopted into the education itself of healthcare professionals, and classes must incorporate all the necessary knowledge, skills and attitudes required for professional health practices.[17]

Last but not the least, as question Fernando and Lindley, "[i]n the case of an adverse event, who precisely is responsible: the app developer, the individual clinician user, the healthcare provider organisation or the government regulators?"[18] In other words, where does the buck stop?

Security: Privacy, Transparency and Technology

Sunil Abraham, Executive Director, Centre for Internet and Society, India
Elonnai Hickok, Programme Manager, Internet Governance,
Centre for Internet and Society, India
Tarun Krishnakumar, Research Volunteer,
Centre for Internet and Society, India

The Centre for Internet and Society (CIS) has been involved in privacy and data protection research for the last five years. It has participated as a member of the Justice A.P. Shah Committee, which has influenced the draft Privacy Bill being authored by the Department of Personnel and Training. It has organised 11 multistakeholder roundtables across India over the last two years to discuss a shadow Privacy Bill drafted by CIS with the participation of privacy commissioners and data protection authorities from Europe and Canada.

Our centre's work on privacy was considered incomplete by some stakeholders because of a lack of focus in the area of cyber security and therefore we have initiated research on it from this year onwards. In this article, we have undertaken a preliminary examination of the theoretical relationships between the national security imperative and privacy, transparency and technology.

Security and Privacy

Daniel J. Solove has identified the tension between security and privacy as a false dichotomy: "Security and privacy often clash, but there need not be a zero-sum tradeoff."[1] Further unpacking this false dichotomy, Bruce Schneier says, "There is no security without privacy. And liberty requires both security and privacy."[2] Effectively, it could be said that

privacy is a precondition for security, just as security is a precondition for privacy. A secure information system cannot be designed without guaranteeing the privacy of its authentication factors, and it is not possible to guarantee privacy of authentication factors without having confidence in the security of the system. Often policymakers talk about a balance between the privacy and security imperatives—in other words a zero-sum game. Balancing these imperatives is a foolhardy approach, as it simultaneously undermines both imperatives. Balancing privacy and security should instead be framed as an optimisation problem. Indeed, during a time when oversight mechanisms have failed even in so-called democratic states, the regulatory power of technology[3] should be seen as an increasingly key ingredient to the solution of that optimisation problem.

Data retention is required in most jurisdictions for law enforcement, intelligence and military purposes. Here are three examples of how security and privacy can be optimised when it comes to Internet Service Provider (ISP) or telecom operator logs:

1. Data Retention: We propose that the office of the Privacy Commissioner generate a cryptographic key pair for each internet user and give one key to the ISP / telecom operator. This key would be used to encrypt logs, thereby preventing unauthorised access. Once there is executive or judicial authorisation, the Privacy Commissioner could hand over the second key to the authorised agency. There could even be an emergency procedure and the keys could be automatically collected by concerned agencies from the Privacy Commissioner. This will need to be accompanied by a policy that criminalises the possession of unencrypted logs by ISP and telecom operators.

2. Privacy-Protective Surveillance: Ann Cavoukian and Khaled El Emam[4] have proposed combining intelligent agents, homomorphic encryption and probabilistic graphical models to provide "a positive-sum, 'win–win' alternative to current counter-terrorism surveillance systems." They propose limiting collection of data to "significant" transactions or events that could be associated with terrorist-related activities, limiting analysis to wholly encrypted data, which then does not just result in "discovering more patterns and relationships without an understanding of their context" but rather "intelligent information—information selectively gathered and placed into an appropriate context to produce actual knowledge." Since fully homomorphic encryption may be unfeasible in real-world systems, they have proposed use of partially homomorphic encryption. But experts such as Prof. John Mallery from MIT are also working on solutions based on fully homomorphic encryption.

3. Fishing Expedition Design: Madan Oberoi, Pramod Jagtap, Anupam Joshi, Tim Finin and Lalana Kagal have proposed a standard[5] that could be adopted by authorised agencies, telecom operators and ISPs. Instead of giving authorised agencies complete access to logs, they propose a format for database queries, which could be sent to the telecom operator or ISP by authorised agencies. The telecom operator or ISP would then process the query, and anonymise/obfuscate the result-set in an automated fashion based on applicable privacy

policies/regulation. Authorised agencies would then hone in on a subset of the result-set that they would like with personal identifiers intact; this smaller result set would then be shared with the authorised agencies.

An optimisation approach to resolving the false dichotomy between privacy and security will not allow for a total surveillance regime as pursued by the US administration. Total surveillance brings with it the 'honey pot' problem: If all the meta-data and payload data of citizens is being harvested and stored, then the data store will become a single point of failure and will become another target for attack. The next Snowden may not have honourable intentions and might decamp with this 'honey pot' itself, which would have disastrous consequences.

If total surveillance will completely undermine the national security imperative, what then should be the optimal level of surveillance in a population? The answer depends upon the existing security situation. If this is represented on a graph with security on the y-axis and the proportion of the population under surveillance on the x-axis, the benefits of surveillance could be represented by an inverted hockey-stick curve. To begin with, there would already be some degree of security. As a small subset of the population is brought under surveillance, security would increase till an optimum level is reached, after which, enhancing the number of people under surveillance would not result in any security pay-off. Instead, unnecessary surveillance would diminish security as it would introduce all sorts of new vulnerabilities. Depending on the existing security situation, the head of the hockey-stick curve might be bigger or smaller. To use a gastronomic analogy, optimal surveillance is like salt in cooking—necessary in small quantities but counter-productive even if slightly in excess.

In India the designers of surveillance projects have fortunately rejected the total surveillance paradigm. For example, the objective of the National Intelligence Grid (NATGRID) is to streamline and automate targeted surveillance; it is introducing technological safeguards that will allow express combinations of result-sets from 22 databases to be made available to 12 authorised agencies. This is not to say that the design of the NATGRID cannot be improved.

Security and Transparency

There are two views on security and transparency: One, security via obscurity as advocated by vendors of proprietary software, and two, security via transparency as advocated by free/open source software (FOSS) advocates and entrepreneurs. Over the last two decades, public and industry opinion has swung towards security via transparency. This is based on the Linus rule that "given enough eyeballs, all bugs are shallow." But does this mean that transparency is a necessary and sufficient condition? Unfortunately not, and therefore it is not necessarily true that FOSS and open standards will be more secure than proprietary

> *Optimal surveillance is like salt in cooking—necessary in small quantities but counter-productive even if slightly in excess.*

software and proprietary standards. The recent detection of the Heartbleed[6] security bug in Open SSL,[7] causing situations where more data can be read than should be allowed, and Snowden's revelations about the compromise of some open cryptographic standards (which depend on elliptic curves), developed by the US National Institute of Standards and Technology, are stark examples.[8]

At the same time, however, open standards and FOSS are crucial to maintaining the balance of power in information societies, as civil society and the general public are able to resist the powers of authoritarian governments and rogue corporations using cryptographic technology. These technologies allow for anonymous speech, pseudonymous speech, private communication, online anonymity and circumvention of surveillance and censorship. For the media, these technologies enable anonymity of sources and the protection of whistle-blowers—all phenomena that are critical to the functioning of a robust and open democratic society. But these very same technologies are also required by states and by the private sector for a variety of purposes—national security, e-commerce, e-banking, protection of all forms of intellectual property, and services that depend on confidentiality, such as legal or medical services.

In order words, all governments, with the exception of the US government, have common cause with civil society, media and the general public when it comes to increasing the security of open standards and FOSS. Unfortunately, this can be quite an expensive task because the re-securing of open cryptographic standards depends on mathematicians. Of late, mathematical research outputs that can be militarised are no longer available in the public domain because the biggest employers of mathematicians worldwide today are the US military and intelligence agencies. If other governments invest a few billion dollars through mechanisms like Knowledge Ecology International's proposed World Trade Organization agreement on the supply of knowledge as a public good, we would be able to internationalise participation in standard-setting organisations and provide market incentives for greater scrutiny of cryptographic standards and patching of vulnerabilities of FOSS. This would go a long way in addressing the trust deficit that exists on the internet today.

Security and Technology

A techno-utopian understanding of security assumes that more technology, more recent technology and more complex technology will necessarily lead to better security outcomes.

This is because the security discourse is dominated by vendors with sales targets who do not present a balanced or accurate picture of the technologies that they are selling. This has resulted in state agencies and the general public having an exaggerated understanding of the capabilities of surveillance technologies that is more aligned with Hollywood movies than everyday reality.

More Technology

Increasing the number of x-ray machines or full-body scanners at airports by a factor of ten or hundred will make the airport less secure unless human oversight is similarly increased. Even with increased human oversight, all that has been accomplished is an increase in the potential locations that can be compromised. The process of hardening a server usually involves stopping non-essential services and removing non-essential software. This reduces the software that should be subject to audit, continuously monitored for vulnerabilities and patched as soon as possible. Audits, ongoing monitoring and patching all cost time and money and therefore, for governments with limited budgets, any additional unnecessary technology should be seen as a drain on the security budget. Like with the airport example, even when it comes to a single server on the internet, it is clear that, from a security perspective, more technology without a proper functionality and security justification is counter-productive. To reiterate, throwing increasingly more technology at a problem does not make things more secure; rather, it results in a proliferation of vulnerabilities.

Latest Technology

Reports that a number of state security agencies are contemplating returning to typewriters for sensitive communications in the wake of Snowden's revelations makes it clear that some older technologies are harder to compromise in comparison to modern technology.[9] Between iris- and fingerprint-based biometric authentication, logically, it would be easier for a criminal to harvest images of irises or authentication factors in bulk fashion using a high resolution camera fitted with a zoom lens in a public location, in comparison to mass lifting of fingerprints.

Complex Technology

Fifteen years ago, Bruce Schneier said, "The worst enemy of security is complexity. This has been true since the beginning of computers, and it's likely to be true for the foreseeable future."[10] This is because complexity increases fragility; every feature is also a potential source of vulnerabilities and failures. The simpler Indian electronic machines used until the 2014 elections are far more secure than the Diebold voting machines used in the 2004 US presidential elections. Similarly when it comes to authentication, a pin number is harder to beat without user-conscious cooperation in comparison to iris- or fingerprint-based biometric authentication.

In the following section of the paper we have identified five threat scenarios[11] relevant to India and identified solutions based on our theoretical framing above.

Threat Scenarios and Possible Solutions

Hacking the NIC Certifying Authority

One of the critical functions served by the National Informatics Centre (NIC) is as a Certifying Authority (CA).[12] In this capacity, the NIC issues digital certificates that authenticate web services and allow for the secure exchange of information online.[13] Operating systems and browsers maintain lists of trusted CA root certificates as a means of easily verifying authentic certificates. India's Controller of Certifying Authority's certificates issued are included in the Microsoft Root list and recognised by the majority of programmes running on Windows, including Internet Explorer and Chrome.[14] In 2014, the NIC CA's infrastructure was compromised, and digital certificates were issued in NIC's name without its knowledge.[15] Reports indicate that NIC did not "have an appropriate monitoring and tracking system in place to detect such intrusions immediately."[16]

The implication is that websites could masquerade as another domain using the fake certificates. Personal data of users can be intercepted or accessed by third parties by the masquerading website. The breach also rendered web servers and websites of government bodies vulnerable to attack, and end users were no longer sure that data on these websites was accurate and had not been tampered with.[17] The NIC CA was forced to revoke all 250,000 SSL Server Certificates issued until that date[18] and is no longer issuing digital certificates for the time being.[19]

Public key pinning is a means through which websites can specify which certifying authorities have issued certificates for that site. Public key pinning can prevent man-in-the-middle attacks due to fake digital certificates.[20] Certificate Transparency allows anyone to check whether a certificate has been properly issued, seeing as certifying authorities must publicly publish information about the digital certificates that they have issued. Though this approach does not prevent fake digital certificates from being issued, it can allow for quick detection of misuse.[21]

'Logic Bomb' against Airports

Passenger operations in New Delhi's Indira Gandhi International Airport depend on a centralised operating system known as the Common User Passenger Processing System (CUPPS). The system integrates numerous critical functions such as the arrival and departure times of flights, and manages the reservation system and check-in schedules.[22]

In 2011, a logic bomb attack was remotely launched against the system to introduce malicious code into the CUPPS software. The attack disabled the CUPPS operating system, forcing a number of check-in counters to shut down completely, while others reverted to manual check-in, resulting in over 50 delayed flights. Investigations revealed that the attack was launched by three disgruntled employees who had assisted in the installation of the CUPPS system at the New Delhi Airport.[23] Although in this case the impact of the attack was limited to flight delay, experts speculate that the attack was meant to take down the entire system. The disruption and damage resulting from the shutdown of an entire airport would be extensive.

Adoption of open hardware and FOSS is one strategy to avoid and mitigate the risk of such vulnerabilities. The use of devices that embrace the concept of open hardware and software specifications must be encouraged, as this helps the FOSS community to be vigilant in detecting and reporting design deviations and investigate into probable vulnerabilities.

Attack on Critical Infrastructure

The Nuclear Power Corporation of India encounters and prevents numerous cyber attacks every day.[24] The best known example of a successful nuclear plant hack is the Stuxnet worm that thwarted the operation of an Iranian nuclear enrichment complex and set back the country's nuclear programme.[25]

The worm had the ability to spread over the network and would activate when a specific configuration of systems was encountered[26] and connected to one or more Siemens programmable logic controllers.[27] The worm was suspected to have been initially introduced through an infected USB drive into one of the controller computers by an insider, thus crossing the air gap.[28] The worm used information that it gathered to take control of normal industrial processes (to discreetly speed up centrifuges, in the present case), leaving the operators of the plant unaware that they were being attacked. This incident demonstrates how an attack vector introduced into the general internet can be used to target specific system configurations. When the target of a successful attack is a sector as critical and secured as a nuclear complex, the implications for a country's security and infrastructure are potentially grave.

Security audits and other transparency measures to identify vulnerabilities are critical in sensitive sectors. Incentive schemes such as prizes, contracts and grants may be evolved for the private sector and academia to identify vulnerabilities in the infrastructure of critical resources to enable/promote security auditing of infrastructure.

Micro Level: Chip Attacks

Semiconductor devices are ubiquitous in electronic devices. The US, Japan, Taiwan, Singapore, Korea and China are the primary countries hosting manufacturing hubs

of these devices. India currently does not produce semiconductors, and depends on imported chips. This dependence on foreign semiconductor technology can result in the import and use of compromised or fraudulent chips by critical sectors in India. For example, hardware Trojans, which may be used to access personal information and content on a device, may be inserted into the chip. Such breaches/transgressions can render equipment in critical sectors vulnerable to attack and threaten national security.[29]

Indigenous production of critical technologies and the development of manpower and infrastructure to support these activities are needed. The Government of India has taken a number of steps towards this. For example, in 2013, the Government of India approved the building of two Semiconductor Wafer Fabrication (FAB) manufacturing facilities[30] and as of January 2014, India was seeking to establish its first semiconductor characterisation lab in Bangalore.[31]

Macro Level: Telecom and Network Switches

The possibility of foreign equipment containing vulnerabilities and backdoors that are built into its software and hardware gives rise to concerns that India's telecom and network infrastructure is vulnerable to being hacked and accessed by foreign governments (or non-state actors) through the use of spyware and malware that exploit such vulnerabilities.

In 2013, some firms, including ZTE and Huawei, were barred by the Indian government from participating in a bid to supply technology for the development of its National Optic Network project due to security concerns.[32] Similar concerns have resulted in the Indian government holding back the conferment of 'domestic manufacturer' status on both these firms.[33]

Following reports that Chinese firms were responsible for transnational cyber attacks designed to steal confidential data from overseas targets, there have been moves to establish laboratories to test imported telecom equipment in India.[34] Despite these steps,

SECURITY PRACTITIONERS AND POLICYMAKERS NEED TO AVOID THE ZERO-SUM FRAMING PREVALENT IN POPULAR DISCOURSE REGARDING SECURITY VIS-A-VIS PRIVACY, TRANSPARENCY AND TECHNOLOGY.

in a February 2014 incident the state-owned telecommunication company Bharat Sanchar Nigam Ltd's network was hacked, allegedly by Huawei.[35] A successful hack of the telecom infrastructure could result in massive disruption in internet and telecommunications services. Large-scale surveillance and espionage by foreign actors would also become possible, placing, among others, both governmental secrets and individuals personal information at risk.

While India cannot afford to impose a general ban on the import of foreign telecommunications equipment, a number of steps can be taken to address the risk of inbuilt security vulnerabilities. Common International Criteria for security audits could be evolved by states to ensure compliance of products with international norms and practices. While India has already established common criteria evaluation centres,[36] the government monopoly over the testing function has resulted in only three products being tested so far. A Code Escrow Regime could be set up where manufacturers would be asked to deposit source code with the Government of India for security audits and verification. The source code could be compared with the shipped software to detect inbuilt vulnerabilities.

Conclusion

Cyber security cannot be enhanced without a proper understanding of the relationship between security and other national imperatives such as privacy, transparency and technology. This paper has provided an initial sketch of those relationships, but sustained theoretical and empirical research is required in India so that security practitioners and policymakers avoid the zero-sum framing prevalent in popular discourse and take on the hard task of solving the optimisation problem by shifting policy, market and technological levers simultaneously. These solutions must then be applied in multiple contexts or scenarios to determine how they should be customised to provide maximum security bang for the buck.

Looking Ahead

The Shifting Digital Pivot

Time for Smart Multilateralism*

Samir Saran, Chair, CyFy and Vice President,
Observer Research Foundation, India
Mahima Kaul, Head of Cyber and Media Initiative,
Observer Research Foundation, India

As a decentralised and multistakeholder global internet governance system becomes institutionalised, countries like India need to build strategies to successfully navigate the ecosystem to achieve their national goals. Pursuing a policy of 'smart multilateralism'—which is a mixed bouquet of bilateral, multilateral and multistakeholder arrangements—suits India's goals to carve a niche role for itself and achieve Indian exceptionalism in cyberspace.

It is difficult to capture the shifting power centres and discourse of global internet governance in a single sentence, paragraph or even paper. The number of countries actively engaging in this debate is increasing at a steady pace, as is the number of stakeholders. Countries like India, at the periphery of these discussions although crucial to their outcomes, are actively strategising on how to engage with a decentralised and largely multistakeholder global system that does not simply rely on the state as the key interlocutor for its citizens. Who should the state engage with, and how? Which are the focus areas where the state should take the lead, and in which layers of internet governance should it rely on 'digital ambassadors' from academia, civil society, the private sector and

* For shorter articles written on the subject, see Samir Saran, "A Time to Lead," The Indian Express, April 16, 2015, http://indianexpress.com/article/opinion/columns/a-time-to-lead/ and Mahima Kaul, "Global Internet Governance: India's Search for a New Paradigm," Global Policy Journal Blog, September 30, 2014, http://www.globalpolicyjournal.com/blog/30/09/2014/global-internet-governance-indias-search-new-paradigm.

activist groups to further its national goals? How must it decide these national goals, at a time when internet governance itself is being redefined? How must the state go about creating a pool of digital ambassadors to pursue these goals?

In this paper, we examine why and how sovereignty is slowly being redefined in the global internet governance ecosystem, and suggest that adopting a strategy of 'smart multilateralism' is the best way forward for India to carve out a niche role for itself and secure Indian exceptionalism in cyberspace.

Competing Agendas: The New Normal

The network of networks is not only expanding with every new device connected to the internet, but is today a resource as valuable in non-material terms as it is in material terms. This growth of the global cyberspace, and by extension the cyber economy, is adding $450 billion to the global GDP every year according to McKinsey Global Institute's report 'Global Flows in a Digital Age.'[1] It argues that the flow of goods, services and finance reached $26 trillion in 2012, or 36 percent of global GDP, 1.5 times the level in 1990. This is expected to increase to $85 trillion by 2025, three times the value in 2012. Underneath these figures is the need for data and communication to flow freely—'connectedness.' The lack of real world tariffs and barriers has allowed the emerging economies to participate and profit from the world economy. India is currently ranked at 30, jumping 16 spots from the previous year, in McKinsey Global Institute's Connectedness Index 2012.[2]

The clear benefits of this new 'connectedness' have allowed corporations to earn the trust of large sections of civil society. The rise of social media has also given the consumer-citizen a voice, which is exercised vigorously. A loss of confidence in public institutions across the world has bolstered these trends. The Snowden revelations[3] were a watershed moment in internet history, eroding credibility in traditional powers like the US government and opening the door for new players—other governments, businesses and civil society alike—to assume a central role in managing the internet. NETmundial, the international internet governance conference hosted by the Brazilian government soon after the Snowden revelations, is one example. It demonstrated the collective weight of civil society, and both national governments and corporations have had to pay heed to it.

Take, for example, the letter written by Cisco chief executive officer John Chambers to US President Barack Obama,[4] warning that America's technological leadership will be impaired if a fragmented internet is the result of the Snowden revelations about mass surveillance by the US government. Similar misapprehensions surfaced across the world, particularly when countries like Brazil, Germany and even India reacted strongly to the news, to the extent of considering data localisation.[5] Further, Germany has announced it is ending its long-running

contract with Verizon communications in 2015 over concerns that it is legally required to hand over certain information to the US National Security Agency (NSA).[6]

US technology companies have begun to feel the consequences, as people around the world have begun to shun them for fear of their close relationship with the US NSA. Various research has pinned losses of US technology corporations over the next few years anywhere from $35 billion to $180 billion.[7] Companies like IBM and Microsoft have plans to build data centres across the globe to pre-empt any economic damage they may suffer due to the political damage that has accrued post-Snowden.[8] Big multinational companies like Microsoft admit that there is now a 'value shift' across the global cyber market, one that the incumbents need to familiarise themselves with.[9] This is of particular significance, since US soft diplomacy is often carried out through its corporations, which have become assets to them in places where the American government is unpopular.

On its part, the US government seeks to back a decentralised, multistakeholder internet governance ecosystem at the global level. Currently, the transition proposed by the Internet Corporation for Assigned Names and Numbers (ICANN) away from US government oversight to a new, non-governmental, multistakeholder body is underway. By encouraging this transition, the US government hopes to regain some of its lost credibility and also establish the current ecosystem as the dominant and stable alternative to a traditional UN-based system or a US-controlled one. And while this new system certainly accommodates the growing legitimacy of many different groups and their competing interest, it does leave sovereign countries in a dilemma. How can they best leverage the current system to achieve their goals?

Sovereignty Redefined

Following the International Telecommunications Union's plenipotentiary[10] meeting in Busan, South Korea, in 2014, the official who led the United States' delegation wrote a blog called 'The Busan Consensus.'[11] The title of this blog reveals as much as its content does. Today, the US's preferred option for global internet governance decision-making is consensus-driven, where no single party has a veto over the process. This a direct reference to shedding the decision-making structures the UN offers, which have traditionally been a one-country-one-vote system. It may be instructive to add here that the NETmundial Outcome Statement was drafted by the multistakeholder community through a consensus-based process, and is the reason why it has global acceptability across a majority of stakeholders. For its part, 'The Busan Consensus' also notes with satisfaction that the International Telecommunication Union (ITU), a body under the auspices of the United Nations, is not going to become a platform to discuss internet public policy issues.

The victory is not a small one. This goal had been outlined quite clearly almost two years before the Busan meeting took place, and US diplomats and envoys travelled the world

building consensus on the issue. The ITU resolutions are binding on countries in a way NETmundial is not. It was this gigantic effort made by the US that helped defeat India's own draft resolution at the ITU plenipotentiary. India had made two suggestions: The first was that the ITU, a UN-led multilateral body, could absorb some key roles related to the critical functions of the internet because, according to the Indian proposal, the internet cannot be separated from telecommunications. The second suggestion built on the premise that regulating telecommunications is the sovereign right of states, and therefore, some features of internet governance would naturally fit into an expanded mandate of the ITU.

This final outcome might seem to be paradoxical at first glance. A move to keep global internet public policy discussions away from a platform where only sovereign countries have a vote is at the same time being claimed as a victory by a sovereign country in its quest to settle global internet governance mechanisms. The fact is that 'The Busan Consensus' certainly reads as an affirmation of US dominance, but it is in service of perpetuating the 'multistakeholder' consensus-based internet governance model that is currently the global system employed to discuss internet public policy issues. If this sounds confusing, it is because it certainly is. The current internet governance ecosystem can best be described as decentralised, with a number of platforms which range from multilateral to multistakeholder, that are each suited to discuss only particular aspects of internet governance.

IT WOULD BE A MISTAKE TO ASSUME THAT THE VALUE OF SOVEREIGNTY HAS DIMINISHED IN THIS NEW DYNAMIC ECOSYSTEM, WHICH CAN BEST BE DESCRIBED AS DECENTRALISED.

What the US and some other countries have understood clearly is that governance of the internet—an entity which means different things to different stakeholders—cannot be regulated in a centralised manner. The old legacy institutions of the UN no longer carry the same weight they used to, and today are often sidelined by agreements in smaller multilateral groupings or bilateral agreements, and multistakeholder meetings.

This is how internet governance works: Those looking to regulate the internet's technical working flock to ICANN, where engineers, diplomats, business leaders and civil society sit together, while at other forums like the Group of Governmental Experts constituted under the UN to discuss norms of state behaviour in cyberspace, only top government officials take a place at the table. Other meetings, like the Internet Governance Forum, are highly anticipated by civil society, governments and business, but produce non-binding outcomes which only carry moral weight in the internet governance world.

It would be a mistake to assume that the value of sovereignty has diminished in this new dynamic ecosystem. If anything, it has expanded to include participants in the pursuit of sovereign goals by including new stakeholders who are crucial for the growth and security of the internet ecosystem. Businesses, which predominantly own the physical infrastructure the internet is built on, and who run companies which are driving the growth of internet traffic, need to be accommodated in this discussion along with end users, civil society and the technical community, without whom innovative growth is not possible. Therefore, regulating porous digital borders from attacks, protecting the data and privacy of citizens, negotiating and helping to develop technical standards on which the internet is run, and inculcating a system of trust in this network of networks cannot be conducted on a single platform.

The nation-state must be smart and understand that consensus building with multiple stakeholders, including like-minded countries, has become the backbone on which this system is being built. Countries with big diplomatic corps and mature internet industries and civil society movements have been early adopters of the system. They are using the system to keep decision-making open and malleable, especially when it concerns core functions. Other, smaller countries have adopted issues of immediate importance to them—for example, building consensus on the norms of cyberspace—in order to build a safer cyberspace where they do not come under attack from larger powers. Emerging economies have much to gain by consensus building and some are certainly dipping their toes in the system.

For India, the assertion of sovereignty must straddle both worlds: One where governments are looking for a place in the critical resource management of the internet, and the other where other stakeholders are equally invested in the success of this enterprise and need to be accommodated in this high-stakes debate. India too must, as it is doing slowly, embrace this new digital complex. A country which has 300 million internet users (with the 'next billion' yet to be connected to the internet), large scale e-governance projects underway, an innovative and growing e-commerce market already generating sales of $16 billion in 2014, and is especially vulnerable to cyber threats given its scale and low-cost-low-security devices, has a unique set of issues it needs to address. The scale of India's net population, the variety of services it seeks to supply and its social imperatives make India's position special. Indian exceptionalism needs to be fulfilled in the internet era. What the country imperatively needs next is a strategy for the road ahead.

Smart Multilateralism

It is an unlikely scenario that India will carry the weight of a billion people in a single vote on a common platform like the UN. Such a situation is not desirable either. India cannot and should not have the same weight in internet discussions as countries with small internet

populations and even smaller economies. It should take the lead in carving out rules of the road that are beneficial to the healthy growth of India's cyberspace. The underlying question being asked here is: What is the best suitable platform for negotiations in order to achieve a positive result? Traditional multilateralism has to be tweaked to become 'smart multilateralism': The state must take the lead in core strategic areas of concern at platforms best suited to these discussions, while relying on other stakeholders to take the lead in other contemporary forums and institutions where the state has less sway and acceptability.

Smart multilateralism can be divided into four broad pillars. The first would be for India to institutionalise its exceptionalism through bilateral agreements with like-minded and relevant partners. Already there is momentum in India's relationships with key countries, which can be strengthened further. In fact, bilateral agreements between countries can lead to changes in international arrangements and laws at the highest level. Take for example how the India-US nuclear deal, borne of a bilateral arrangement, is compelling the UN to change its rigid architecture. India was one of 23 founding members of the multilateral General Agreement on Tariffs and Trade arrangement, raising developing country concerns at the grouping which later grew to become the World Trade Organization, a body that today boasts of 123 signatory countries. India has far greater weight and participation at the G20 and even greater significance at the BRICS. This is because the former was a focused group created to respond to a specific economic task at hand, while the latter was made in response to an infirmity in the global governance system. Contrast this to India's single vote—and not even a veto—at the UN. India could create a rule-making body—a new 'Digital 20'—which could have members who are equally invested in the system. The key to success would lie in choosing the right partners, whose influence would be proportional to their 'buy-in' and stakes. This right mix of partners with real-world influence could come together to agree on digital norms and rules for the 21st century.

The second would be to engage with opportunities for rule making and norm shaping outside the UN. The state-led London process is one such avenue. The ICANN transition process is another. There are plenty of smaller gatherings, such as technical meetings, regional forums and high-level meetings organised by academic institutions and think-tanks, which help steer public policy thought in specific directions. These must be leveraged after careful selection. At the same time, one must add that there is still space for norm making within the UN system, most notably through the Group of Governmental Experts, which looks at shaping norms of state behaviour in cyberspace, and through interventions at the World Summit on the Information Society review meetings.

The third broad pillar to pursue is the creation of a platform that would manage and shape the discourse on managing the digital world. This is admittedly easier said than done, as the internet governance ecosystem is dotted with overlapping conferences in all

parts of the world. However, not all attempts to create a platform have been successful. The recent example of a lukewarm response to the NETmundial Initiative spearheaded by ICANN, Brazil and the World Economic Forum comes to mind. Volunteers at ICANN too have complained of process fatigue. However, meetings which can take a fresh and honest look at problems from new perspectives are needed if the decentralised ecosystem is to work, and this gives emerging economies an advantage. Given that the next four billion to come online are going to be from their countries—reflecting a digital pivot to Asia—conversations crucial to the growth, freedom and security of these regions have automatically become pressing. Often, gatherings in the developing world do not reflect these concerns accurately, paying lip service to concepts like the 'digital divide' and 'capacity building' as they discuss issues important to emerging economies, such as intellectual property rights and a possible cyber arms race. This is where a country like India, representing all spectrums of the digital society—the uber-connected, the recently-connected and the completely unconnected—can present a legitimate platform to hold discussions on pertinent digital debates. Weight must be given to the platform by having the Prime Minister chair it, with the Minister for Communications and Information Technology co-convening, and it must give equal weight to the views of non-governmental stakeholders as it does to the government.

> ***India and 'smart multilateralism'—institutionalise its exceptionalism, engage in rule-making processes outside the UN, create a platform to shape the discourse and discuss digital economy.***

Finally, the fourth pillar must entail creating a robust multisectoral debate on the digital economy. India has already shown very positive first steps with the overwhelming response to the question of network neutrality. This engagement must be encouraged so that the resulting digital society is shaped by the concerns, suggestions and goals of the domestic stakeholders, to be then exported to global forums. One only need to look at the intermediary liability protections offered in the US's domestic Digital Millennium Copyright Act of 1998 to understand how civil liberties groups, corporations and academics have successfully managed to fight for similar protections the world over. Not only have the European Union and other countries accepted this, Indian civil society groups too have taken up the cause of intermediary liability, drawing inspiration from what they see as successful examples like the US digital copyright act. A robust domestic debate will encourage an acknowledgement of India's own larger goals in the global sphere, and allow it to rely on its digital ambassadors to pursue a positive agenda at platforms where the state has little influence or space.

Conclusion

Ultimately, there is no escaping the reality of our times. The decentralised, multistakeholder model of internet governance has broad global acceptance, even as its exact form is being worked out. The experiment at ICANN, i.e., handing over oversight of critical functions to a multistakeholder body, is an example of how this global governance system is being operationalised. Many countries around the world have openly declared their support for the multistakeholder system, including the US, the UK, the Netherlands and Brazil. Others are still learning to straddle the new system.

This is where the second reality comes into play. States will increasingly manipulate digital spaces to their advantage, and this control and manipulations will be managed through third parties, including corporations, civil society, scientists and academia. The strength of this will lie in domestic multistakeholder processes that will allow these different actors to work towards a common long-term vision of the internet, even as short-term goals may differ. The states which will succeed in meeting their broader internet policy goals in this age of 'smart multilateralism' will be the ones who are able to create strong partnerships with non-state stakeholders.

At the start of 2015, India's Minister for Communications and Information Technology was famously quoted as saying that "India will decide on its internet governance model which will be consistent with the role private players play in the spread of internet and the pre-eminent role played by government in public welfare… to come up with a broad framework, we will need to consult various stakeholders."[12] This must also be the blueprint for India's approach towards international internet governance. The objective, therefore, for India to pursue must be "how to retain agency with the government while leveraging the creative capacities outside."[13]

NOTES

1

1 "Information Technology Act, 2000," Government of India, June 9, 2000 and "Information Technology (Amendments) Act, 2008," Government of India, February 5, 2009, http://deity.gov.in/content/cyber-laws.

2 "Draft New Resolution, ITU's role in Improving Network Functionalities for Evincing Trust and Confidence in IP based Telecom Networks," International Telecommunications Union, 2014, http://www.itu.int/net4/proposals/PP14/Submission.aspx?Language=English&Proposal=15338.

3 "Executive Summary of Internet in India 2014," Internet and Mobile Association of India, 2014, http://www.iamai.in/rsh_pay.aspx?rid=4hjkHu7GsUU=.

4 "National Cyber Security Policy 2013," Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India, 2013, http://deity.gov.in/content/national-cyber-security-policy-2013-1 and "Government of India's GI Cloud (Meghraj) Strategic Direction Paper," Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India, 2013, http://deity.gov.in/sites/upload_files/dit/files/GI-Cloud%20Strategic%20Direction%20Report%281%29.pdf.

5 "Executive Summary of Internet in India 2014."

6 Ibid.

7 "World Telecommunications/IT Database," International Telecommunication Union, 2014, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

8 Ibid.

9 "Innovative Asia: Advancing the Knowledge-Based Economy, The Next Policy Agenda," Asian Development Bank, 2014, http://adb.org/sites/default/files/pub/2014/innovative-asia-knowledge-based-economy.pdf.

10 "India IT-BPM Exports," NASSCOM, 2014, http://www.nasscom.in/india-itbpm-exports.

11 "India Start-up Ecosystem," NASSCOM, 2014, http://www.nasscom.in/india-startup-ecosystem.

12 "Security Intelligence Report, Volume 17," Microsoft, 2014, http://www.microsoft.com/en-us/download/details.aspx?id=44937.

13 "2014 Cost of Data Breach Study: Global Analysis," Ponemon Institute, 2014, http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis.

14 "The Cybersecurity Risk Paradox: Impact of Social, Economic, Political, and Technological Forces on Rates of Malware," Microsoft, 2014, http://download.microsoft.com/download/E/1/8/E18A8FBB-7BA6-48BD-97D2-9CD32A71B434/Cybersecurity-Risk-Paradox.pdf.

15 "Cyberspace 2025: Today's Decisions, Tomorrow's Terrain," Microsoft, 2014, www.cyberspace2025.com.

2

1 The author wishes to thank Mrs. Hadas Klein, Cyber Forum Manager at the Cyber Security Program, INSS, for her assistance in researching and writing this article.

2 Drafted by the Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India. The full version can be found at http://deity.gov.in/content/national-cyber-security-policy-2013-1.

3 The National Cybersecurity Workforce, National Initiative for Cybersecurity Education (NICE), 2013, http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing.pdf.

3

1 "World Telecommunication/ICT Indicators database," International Telecommunication Union. http://www.itu.int/en/ITU-D/Statistics/Pages/publications/wtid.aspx.

2 "Measuring the Information Society 2013," International Telecommunication Union, https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf.

3 Pippa Norris, *Digital divide: Civic Engagement, Information Poverty, and the Internet Worldwide* (New York: Cambridge University Press, 2001).

4 W.E. Steinmueller, "ICTs and the possibilities for leapfrogging by developing countries," *International Labour Review* 140, no. 2 (2001), pp. 193-210 and K. Ranganathan, "Leapfrogging the Digital Divide: Myth or Reality for Emerging Regions?," *International Journal of Information Communication Technologies and Human Development* 3, no. 4 (2011), pp. 17-30, 34.

5 K. Ranganathan and A. Kapoor, "EKO – The Mobile Phone as a Financial Identity," *Asian Case Research Journal* 18, no. 1 (2014), pp.143-173.

6 Deepa Krishnan, "A banking, money transfer service for immigrant workers," Moneycontrol, April 9, 2013, http://www.moneycontrol.com/sme-stepup/news/aninnovative_technology_platform_to_provide_banklike_service_to_lowwage_workers-849597.html.

7 Steinmueller, "ICTs and the possibilities for leapfrogging by developing countries."

8 Nick Hughes and Susie Lonie, "M-PESA: Mobile Money for the 'Unbanked' Turning Cellphones into 24-Hour Tellers in Kenya," *Innovations: Technology, Governance, Globalization* 2, no. 1-2, pp. 63-81 (April 2007).

9 "Why does Kenya lead the world in mobile money?," *The Economist*, May 27, 2013, http://www.economist.com/blogs/economist-explains/2013/05/economist-explains-18 and William Jack and Tavneet Suri, "Mobile Money: The Economics of M-PESA," National Bureau of Economic Research Working Paper 16721, January 2011.

10 Hughes and Lonie, "M-PESA: Mobile Money for the 'Unbanked.'"

11 Roberto Hernandez and Yerina Mugica, "What Works: Prodem FFP's Multilingual Smart ATMs for Micro Finance," World Resources Institute Case Study, 2003, http://www.wri.org/sites/default/files/pdf/dd_prodem.pdf.

12 Gautam Ivatury, "Harnessing technology to transform financial services for the poor," *Small Enterprise Development* 15, no. 4, pp. 25-30 (December 2004).

13 Eduardo Bazoberry, "The Bolivian Experience of the Prodem Private Financial Fund S.A." (case study presented at Paving the Way Forward for Rural Finance: An International Conference on Best Practices, Washington, D.C., June 2-4, 2003), http://pdf.usaid.gov/pdf_docs/PNADF040.pdf.

14 Michael Trucano, "Evaluating One Laptop Per Child (OLPC) in Peru," EduTech: A World Bank Blog on ICT use in Education, February 23, 2012, http://blogs.worldbank.org/edutech/olpc-peru2.

15 "[Economy] Banking Business Correspondents Agents (BCA): Meaning, functions, Financial Inclusion, Swabhimaan, Common Service Centres (CSC)," Mrunal, http://mrunal.org/2013/01/economy-banking-business-correspondents-agents-bca-meaning-functions-financial-inclusion-swabhimaan-common-service-centres-csc.html.

16 Rabin Patra et al, "WiLdnet: design and implementation of high performance wifi based long distance networks" in *Proceedings of the 4th USENIX conference on Networked systems design & implementation* (Berkeley, CA, USA: USENIX Association, 2007), http://tier.cs.berkeley.edu/docs/wireless/wild_multihop.pdf.
17 Sonesh Surana et al, "Deploying a Rural Wireless Telemedicine System: Experiences in Sustainability," *Computer* 41, no. 6 (2008).
18 Himanshu Kakkar, "Himalayan Effort," Outlook, September 3, 2011, http://business.outlookindia.com/article_v3.aspx?artid=278077.
19 "Wireless For Communities (W4C) - Background & Concept," Wireless for Communities/Digital Empowerment Foundation, http://wforc.defindia.org/background-concept/.
20 Surana et al, "Deploying a Rural Wireless Telemedicine System."
21 Tekla S. Perry, "The Laptop Crusade," IEEE Spectrum, April 1, 2007, http://spectrum.ieee.org/computing/hardware/the-laptop-crusade.
22 Robert Katz, "From Prodem to Pragati - ATMs for the Poor," Worldchanging, December 4, 2006, http://www.worldchanging.com/archives/005493.html.
23 Surana et al, "Deploying a Rural Wireless Telemedicine System."
24 Rodrigo Fonseca and Joyojeet Pal, "Bringing devices to the masses: a comparative study of the Brazilian Computador Popular and the Indian Simputer" (presentation at the South Asia Conference, UC Berkeley, December 2003), http://tier.cs.berkeley.edu/docs/fonseca-pal-simputer.pdf.

4

1 "India's e-commerce market rose 88% in 2013: Survey," *The Economic Times*, December 30, 2013, http://articles.economictimes.indiatimes.com/2013-12-30/news/45711192_1_e-commerce-market-online-shoppers-survey.
2 "India IT-BPM Overview," NASSCOM, http://www.nasscom.in/indian-itbpo-industry.
3 "Decontsructing the "Cloud": The New Growth Frontier for Indian IT_BPO Sector," NASSCOM/Deloitte, 2012.
4 Harsimran Julka and Pankaj Mishra, "Only 25% IT graduates readily employable: NASSCOM," *The Economic Times*, April 7, 2011, http://articles.economictimes.indiatimes.com/2011-04-07/news/29392668_1_engineering-colleges-employability-study-nasscom.
5 "Deconstructing the 'Cloud'."
6 Data Security Council of India, "Legal and Policy Issues in Cloud Computing" (discussion paper based on DSCI-BSA Workshop, New Delhi, 2013), http://www.dsci.in/node/1486.
7 "Securing Our Cyber Frontiers," NASSCOM-DSCI Cyber Security Advisory Group Report, March 2012, https://www.dsci.in/sites/default/files/NASSCOM-DSCI%20Cyber%20Security%20Advisory%20Group%20(CSAG)%20Report.pdf.
8 "About the Common Criteria," Common Criteria Recognition Arrangement, https://www.commoncriteriaportal.org/ccra/.

5

1 Stuxnet is a computer worm that infected Programmable Logic Controllers manufactured by Siemens, responsible for the automation of mechanical engines and industrial processes. It is believed that the worm was created by the US military with assistance from Israel and scientists at Siemens, with the objective of tampering with Iran's nuclear programme. The effect

of the worm caused Iranian centrifuges in the Natanz plant to turn more rapidly or slowly than appropriate, without the system detecting and reporting the problem. According to some US and Israeli officials, Stuxnet delayed Iran's nuclear programme for several years. The worm eventually found its way out of Natanz and infected computers around the world.

2 Flame is a highly sophisticated piece of malware designed primarily to spy on the users of infected computers. It is able to steal data, record audio via a microphone and also download information of Bluetooth-enabled devices. Like Stuxnet, Flame is believed to have been created by the US and Israel to be used against Iran's nuclear programme. The worm attacked the computers of Iranian officials. It is believed that Flame had been operating as early as March 2010, but was only discovered in 2012.

3 The JPMorgan Chase computer network was recently attacked by hackers who gained entry to dozens of the bank's servers. It is believed that several other banks and financial institutions were also affected. Given the level of sophistication of the attack, investigators believe it may have involved some coordination or assistance from a foreign government. Based on the architecture of the malware, investigators suspect the attack was carried out by Russians or East Europeans.

4 See John Markoff and Andrew W. Kramer, "In Shift, U.S. Talks to Russia on Internet Security," *The New York Times,* December 12, 2009, www.nytimes.com/2009/12/13/science/13cyber.html?_r=1.

5 See, for example, Mark Clayton, "US indicts five in China's secret 'Unit 61398' for cyber-spying on US firms," *Christian Science Monitor*, May 19, 2014, http://www.csmonitor.com/World/Security-Watch/Cyber-Conflict-Monitor/2014/0519/US-indicts-five-in-China-s-secret-Unit-61398-for-cyber-spying-on-US-firms-video and Jonathan Kaiman, "China reacts furiously to US cyber-espionage charges," *The Guardian*, May 20, 2014, http://www.theguardian.com/world/2014/may/20/china-reacts-furiously-us-cyber-espionage-charges.

6 See Duncan Campbell, Cahal Milmo, Kim Sengupta, Nigel Morris and Tony Patterson, "Revealed: Britain's 'secret listening post in the heart of Berlin,'" *The Independent*, November 5, 2013, http://www.independent.co.uk/news/uk/home-news/revealed-britains-secret-listening-post-in-the-heart-of-berlin-8921548.html.

7 See Adam Rawnsley, "Espionage? Moi?," Foreign Policy, July 2, 2013, http://www.foreignpolicy.com/articles/2013/07/01/espionage_moi_france.

8 David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0 and Christopher C. Joyner and Catherine Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework," *European Journal of International Law* 12, no. 5 (2001).

9 See Yaakov Lappin, "Iran attempted large-scale cyber-attack on Israel, senior security source says," *The Jerusalem Post*, August 17, 2014, http://www.jpost.com/Arab-Israeli-Conflict/Iran-attempted-large-scale-cyber-attack-on-Israel-senior-security-source-says-371339.

10 Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *Yale Journal of International Law* 36, no. 421 (2011).

11 Jonathan Solomon, "Cyberdeterrence between Nation-States Plausible Strategy or a Pipe Dream?," *Strategic Studies Quarterly* 5, no.1 (Spring 2011), http://www.au.af.mil/au/ssq/2011/spring/solomon.pdf.

12 Waxman, "Cyber-Attacks and the Use of Force."

13 Ibid.

14 Ibid.

15 Ibid.

16 See Michael J. Glennon, "The Dark Future of International Cyber Regulation," *Journal of National Security Law and Policy* 6, no. 563 (2013).

17 Ibid.

18 Ibid.

19 Operation Olympic Games was a covert campaign of sabotage by means of cyber disruption, directed at Iranian nuclear facilities, allegedly by the United States and Israel. One of its elements

was the malware Stuxnet (see Note 1).

20 Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran" and Joyner and Lotrionte, "Information Warfare as International Coercion."

21 Waxman, "Cyber-Attacks and the Use of the Force."

22 Mary McEvoy Manjikian, "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik," *International Studies Quarterly* 54 (2010).

23 T. Michael Moseley, "The Nation's Guardians: America's 21st Century Air Force," Chief of Staff of the US Air Force White Paper, December 29, 2007, http://www.dtic.mil/dtic/tr/fulltext/u2/a477488.pdf.

24 Manjikian, "From Global Villages."

7

1 Hon. Virginia M. Kendal and T. Markus Funk, "The Role of Mutual Legal Assistance Treaties in Obtaining Foreign Evidence," The American Bar Association, Litigation 40, no. 2 (October 2014), http://www.americanbar.org/content/dam/aba/events/criminal_justice/CSR_MLAT_LetterRogatory.authcheckdam.pdf; see also, T. Markus Funk, "Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges," Federal Judicial Center, 2014, http://www.fjc.gov/public/pdf.nsf/lookup/mlat-lr-guide-funk-fjc-2014.pdf/$file/mlat-lr-guide-funk-fjc-2014.pdf.

2 "UNODC promotes regional extradition and mutual legal assistance network," United Nations Office on Drugs and Crime, July 30, 2013, https://www.unodc.org/southeastasiaandpacific/en/2013/07/mla-workshop/story.html.

3 "US Department of Justice FY 2015 Budget Request: Mutual Legal Assistance Treaty Process Reform," US Department of Justice, June 13, 2014, http://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf.

4 For a comprehensive compilation of MLATs, see https://mlat.info/mlat-index.

5 "Liberty and Security in a Changing World," The President's Review Group on Communications and Technologies, December 12, 2013, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

6 Warrant Issued by the U.S. District Court for the Southern District of New York, 13 Mag 2814, https://www.eff.org/files/2014/06/12/microsoft_search_warrant.pdf.

7 Steve Lohr, "Microsoft Protests Order to Disclose Email Stored Abroad," *The New York Times*, June 30, 2014, http://www.nytimes.com/2014/06/11/technology/microsoft-protests-order-for-email-stored-abroad.html?_r=0.

8 Preet Bharara, Serrin Tuerner and Justin Anderson, U.S. Attorneys, "Government's brief in support of the magistrate judge's decision to uphold a warrant ordering Microsoft to disclose records within its custody and control. In the matter of a warrant to search a certain email account controlled and maintained by Microsoft Corporation," 13 Mag 2814, July 9, 2014, http://cdn.arstechnica.net/wp-content/uploads/2014/07/federalbrief-microsoftcase.pdf.

9 "Microsoft Ireland Case: Can a US Warrant Compel a US Provider to Disclose Data Stored Abroad?," Center for Democracy and Technology, July 30, 2014, https://cdt.org/insight/microsoft-ireland-case-can-a-us-warrant-compel-a-us-provider-to-disclose-data-stored-abroad/.

10 Ibid.

11 Microsoft even formally noted this concern it its initial objection. See, "Microsoft's Objections to the Magistrate's Order Denying Microsoft's Motion to Vacate in Part a Search Warrant Seeking Customer Information Located Outside the United States. In the matter of a warrant to search a certain email account controlled and maintained by Microsoft Corporation," 13 Mag 2814, June 6, 2014, https://www.eff.org/files/2014/06/12/microsofts_objections_to_the_magistrates_opinion.pdf.

12 AT&T, "Memorandum of Law of Amicus Curaie AT&T Corp. in Support of Microsoft Corporation.

In the matter of a warrant to search a certain email account controlled and maintained by Microsoft Corporation," 13 Mag 2814, June 11, 2014, https://www.eff.org/document/att-amicus-brief-support-microsoft.

13 Over a year has passed and the request has yet to be resolved. See Rebecca Blumenstein, "Brazil's Rousseff Pressures U.S. on Data Collection," *The Wall Street Journal*, January 25, 2014, http://online.wsj.com/news/articles/SB10001424052702304632204579341183665708524.

14 "MLATs and International Cooperation for Law Enforcement Purposes," Presentation of the Centre for Internet and Society, Bangalore, http://cis-india.org/internet-governance/blog/presentation-on-mlats.pdf.

15 These policies are a result of issues other than just questions of jurisdiction for law enforcement – the post-Snowden political environment clearly weighs heavily on the decision – but the inability of local law enforcement to get the data they needs is undoubtedly playing its part. See Jonah Force Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers," Lawfare Research Paper Series 2, no. 3 (21 July 2014), http://www.lawfareblog.com/wp-content/uploads/2014/07/Lawfare-Research-Paper-Series-Vol2No3.pdf.

16 Ibid.

17 Felipe Dreher, "Governocrava 50% de imposto em serviços de DC prestados do exterior," Computer World Brazil, October 22, 2014, http://computerworld.com.br/negocios/2014/10/22/governo-crava-50-de-imposto-em-servicos-de-dc-prestados-do-exterior/ and Mais essa: governo impõe taxa de 50% em imposto para DataCenter no exterior," Tech Mundo, October 22, 2014, http://www.tecmundo.com.br/economia/64833-governo-impoe-taxa-50-imposto-datacenter-exterior.htm.

18 U.S. Department of Justice FY 2015 Budget Request.

19 Phil Reitinger, "When good law is bad policy," Federal Times Blog, October 24, 2014, http://www.federaltimes.com/article/20141024/BLG04/310240014/Justice-Department-demand-documents-stored-abroad-good-law-bad-policy.

20 "Discussion paper - What are the solutions to the 'MLAT problem'?," Access, https://mlat.info/policy-analysis-docs/discussion-paper-what-are-the-solutions-to-the-mlat-problem.

8

1 European Information Observatory Report 2011.

2 Jean Paul Simon, "The ICT Landscape in BRICS Countries: Brazil, India, China," European Commission's Institute for Prospective Technological Studies (IPTS), September 2011, http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=4619.

3 Terril Yue Jones, "China says willing to discuss cyber security with the US," Reuters, March 12, 2013, http://www.reuters.com/article/2013/03/12/us-usa-china-cybersecurity-idUSBRE92A0XO20130312.

4 "Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General," Item 93 on the provisional agenda, 66th Session, UN General Assembly, September 14, 2011, http://content.netmundial.br/files/67.pdf.

5 Leo Kelion, "Future of the internet debated at NetMundial in Brazil," BBC, April 23, 2014, http://www.bbc.com/news/technology-27108869.

6 "Anonymous - Opisrael 07.04.2014 [AnonSec & AnonGhost]," Youtube video, 2:33, message issued by hacker group Anonymous, Posted by "Fiwer Sec," April 7, 2014, https://www.youtube.com/watch?v=4Wu00-Bk39w.

7 "Working Together to Address the New Threat of Terrorism," Statement by H.E. Wang Yi, Chinese Minister of Foreign Affairs at the UN Security Council Summit on Terrorism, September 24, 2014, http://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1195235.shtml.

8 Ibid.
9 Ceylan Yeginsu, "Turkey Lifts Twitter Ban After Court Calls It Illegal," *The New York Times,* April 3, 2014, http://www.nytimes.com/2014/04/04/world/middleeast/turkey-lifts-ban-on-twitter.html?_r=0.
10 "Special Report of the Disarmament Commission to The General Assembly at its Third Special Session Devoted to Disarmament," Fifteenth Special Session A/S-15/3, United Nations General Assembly, May 28, 1998, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/S-15/3(SUPP)&Lang=E.

10

1 The term, as used in this paper, applies to those actors who are largely happy with the status quo regime of the global IG, with or without minor changes.
2 This joint IBSA statement was made at the consultation on 'enhanced cooperation' organised by the UN in New York in December 2010.
3 The NETmundial meeting was specifically called to address the changed global perceptions with regard to IG issues after the Snowden revelations. It is paradoxical, therefore, that the meeting outcomes have been most celebrated by the very powers whose wrongful practices were exposed by the revelations: the US government and the global internet companies. This fact gives a useful clue as to who exercised control over the NETmundial meeting.
4 There is some semantic and political trickery involved here, whereby between policy dialogue/inputs and actual policy making (in the old political style) is interposed a new layer of developing a set of policy models that would be NMI's primary task. Is it obvious that the power invested behind such policy models will be so much, which is the whole point of the prior dialogue and deals amongst the elite, that such models would become *de facto* public policy.
5 Wolfgang Kleinwachter, "NetMundial: Watershed in Internet Policy Making?" in *Beyond NetMundial: The Roadmap to Institutional Improvements to the Global Internet Governance Ecosystem,* eds. Willaim J. Drake and Monroe Price (Philadelphia: University of Pennsylvania, 2014).
6 As to why European actors acquiesce to these efforts or, even more strangely, why major global civil society networks involved in the IG space do not stand up to them, can be very briefly summed up thus: European actors face the dilemma of how to configure the IG geopolitics within their traditional geopolitical and geo-economic alliance with the US, and the reason for the latter group lies in a complex phenomenon of an emergence of a new global middle class that is becoming globally politically articulate – the IG space being an early experiment. This latter class is so distraught with their national polities that they are willing, however grudgingly, to be soft on US's geopolitical and geo-economic unipolarity.

12

1 "The World in 2011: ICT Facts and Figures," ICT Data and Statistics Division, Telecommunication Development Bureau, International Telecommunication Union, 2011, https://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf.
2 Siddharth Vishwanath et al, "Touching lives through mobile health: Assessment of the global market opportunity," PricewaterhouseCoopers India, February 2012, https://www.pwc.in/en_IN/in/assets/pdfs/publications-2012/touching-lives-through-mobile-health-february-2012.pdf.

3 See Christen Brownlee, "mHealth – Can You Hear Me Now?," Johns Hopkins Public Health Magazine, Special Issue, 2012, http://magazine.jhsph.edu/2012/technology/_pdf/jhsph_se_tech_2012_mag_features.pdf.
4 Alain Labrique, "The future with mHealth," Devex, June 19, 2012, https://www.devex.com/news/the-future-with-mhealth-78481.
5 Nanette Byrnes, "Mobile Health's Growing Pains," MIT Technology Review, July 21, 2014, http://www.technologyreview.com/news/529031/mobile-healths-growing-pains/.
6 Ibid.
7 Ibid.
8 "Fact Sheet 39 - Mobile Health and Fitness Apps: What Are the Privacy Risks?," Privacy Rights Clearinghouse, December 1, 2014, https://www.privacyrights.org/mobile-health-and-fitness-apps-what-are-privacy-risks.
9 "Traffic and Market Report: on the pulse of the networked society," Ericsson, June 2012, http://www.ericsson.com/res/docs/2012/traffic_and_market_report_june_2012.pdf.
10 "A Reality Checkpoint for Mobile Health: Three Challenges to Overcome," PLOS Med, February 2013, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3582561/.
11 Ibid.
12 "Fourth Annual Benchmark Study on Patient Privacy & Data Security," Ponemon Institute LLC, March 2014, https://www2.idexpertscorp.com/resources/single/fourth-annual-benchmark-study-on-patient-privacy-and-data-security/r-general.
13 Ibid.
14 Yinka Ibukun, "Nigeria Uses Android App With Facebook to Beat Ebola," Bloomberg News, October 8, 2014, http://www.bloomberg.com/news/articles/2014-10-07/nigeria-uses-android-app-with-facebook-to-beat-ebola.
15 "Internet of Things in Logistics," DHL Trend Research & Cisco Consulting Services, 2015, http://www.dhl.com/content/dam/Local_Images/g0/New_aboutus/innovation/DHLTrendReport_Internet_of_things.pdf.
16 Juanita Isabelle Fernando and Jennifer Lindley, "Being Smart: Challenges in the Use of Mobile Applications in Clinical Settings," *European Journal of Public Health*, November 2013, http://www.researchgate.net/publication/259239044_Being_Smart_Challenges_in_the_Use_of_Mobile_Applications_in_Clinical_Settings.
17 Ibid.
18 Ibid. .

13

1 Daniel J. Solove, Chapter 1 in *Nothing to Hide: The False Tradeoff between Privacy and Security* (Yale University Press: 2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1827982.
2 Bruce Schneier, "What our Top Spy doesn't get: Security and Privacy aren't Opposites," Wired, January 24, 2008, http://archive.wired.com/politics/security commentary/security matters/2008/01/securitymatters_0124 and Bruce Schneier, "Security vs. Privacy," Schneier on Security, January 29, 2008, https://www.schneier.com/blog/archives/2008/01/security_vs_pri.html.
3 There are four sources of power in internet governance: Market power exerted by private sector organisations; regulatory power exerted by states; technical power exerted by anyone who has access to certain categories of technology, such as cryptography; and finally, the power of public pressure sporadically mobilised by civil society. A technically sound encryption standard, if employed by an ordinary citizen, cannot be compromised using the power of the market or the regulatory power of states or public pressure by civil society. In that sense, technology can be used to regulate state and market behaviour.

4 Ann Cavoukian and Khaled El Emam, "Introducing Privacy-Protective Surveillance: Achieving Privacy and Effective Counter-Terrorism," Information & Privacy Commisioner, September 2013, Ontario, Canada, http://www.privacybydesign.ca/content/uploads/2013/12/pps.pdf.

5 Madan Oberoi, Pramod Jagtap, Anupam Joshi, Tim Finin and Lalana Kagal, "Information Integration and Analysis: A Semantic Approach to Privacy"(presented at the third IEEE International Conference on Information Privacy, Security, Risk and Trust, Boston, USA, October 2011), ebiquity.umbc.edu/_file_directory_/papers/578.pdf.

6 Bruce Byfield, "Does Heartbleed disprove 'Open Source is Safer'?," Datamation, April 14, 2014, http://www.datamation.com/open-source/does-heartbleed-disprove-open-source-is-safer-1.html.

7 "Cybersecurity Program should be more transparent, protect privacy," Centre for Democracy and Technology Insights, March 20, 2009, https://cdt.org/insight/cybersecurity-program-should-be-more-transparent-protect-privacy/#1.

8 "Cracked Credibility," *The Economist*, September 14, 2013, http://www.economist.com/news/international/21586296-be-safe-internet-needs-reliable-encryption-standards-software-and.

9 Miriam Elder, "Russian guard service reverts to typewriters after NSA leaks," *The Guardian*, July 11, 2013, www.theguardian.com/world/2013/jul/11/russia-reverts-paper-nsa-leaks and Philip Oltermann, "Germany 'may revert to typewriters' to counter hi-tech espionage," *The Guardian*, July 15, 2014, www.theguardian.com/world/2014/jul/15/germany-typewriters-espionage-nsa-spying-surveillance.

10 Bruce Schneier, "A Plea for Simplicity," Schneier on Security, November 19, 1999, https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html.

11 With inputs from Pranesh Prakash of the Centre for Internet and Society and Sharathchandra Ramakrishnan of Srishti School of Art, Technology and Design.

12 "Frequently Asked Questions," Controller of Certifying Authorities, Department of Electronics and Information Technology, Government of India, http://cca.gov.in/cca/index.php?q=faq-page#n41.

13 National Informatics Centre Homepage, Government of India, http://www.nic.in/node/41.

14 Adam Langley, "Maintaining Digital Certificate Security," Google Security Blog, July 8, 2014, http://googleonlinesecurity.blogspot.in/2014/07/maintaining-digital-certificate-security.html.

15 This is similar to the kind of attack carried out against DigiNotar, a Dutch certificate authority. See: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1246&context=jss.

16 R. Ramachandran, "Digital Disaster," *Frontline*, August 22, 2014, http://www.frontline.in/the-nation/digital-disaster/article6275366.ece.

17 Ibid.

18 "NIC's digital certification unit hacked," *Deccan Herald*, July 16, 2014, http://www.deccanherald.com/content/420148/archives.php.

19 National Informatics Centre Certifying Authority Homepage, Government of India, http://nicca.nic.in//.

20 Mozilla Wiki, "Public Key Pinning," https://wiki.mozilla.org/SecurityEngineering/Public_Key_Pinning.

21 "Certificate Transparency - The quick detection of fraudulent digital certificates," Ascertia, August 11, 2014, http://www.ascertiaIndira.com/blogs/pki/2014/08/11/certificate-transparency-the-quick-detection-of-fraudulent-digital-certificates.

22 "Indira Gandhi International Airport (DEL/VIDP) Terminal 3, India," Airport Technology.com, http://www.airport-technology.com/projects/indira-gandhi-international-airport-terminal-3/.

23 "How techies used logic bomb to cripple Delhi Airport," Rediff, November 21, 2011, http://www.rediff.com/news/report/how-techies-used-logic-bomb-to-cripple-delhi-airport/20111121htm.

24 Manu Kaushik and Pierre Mario Fitter, "Beware of the bugs," *Business Today*, February 17, 2013, http://businesstoday.intoday.in/story/india-cyber-security-at-risk/1/191786.html.

25 "Stuxnet 'hit' Iran nuclear plants," BBC, November 22, 2010, http://www.bbc.com/news/technology-11809827.
26 In this case, systems using Microsoft Windows and running Siemens Step7 software were targeted.
27 Jonathan Fildes, "Stuxnet worm 'targeted high-value Iranian assets'," BBC, September 23, 2010, http://www.bbc.com/news/technology-11388018.
28 Farhad Manjoo, "Don't Stick it in: The dangers of USB drives," Slate, October 5, 2010, http://www.slate.com/articles/technology/technology/2010/10/dont_stick_it_in.html.
29 Ibid.
30 "IBM invests in new $5bn chip fab in India, so is chip sale off?," ElectronicsWeekly, February 14, 2014, http://www.electronicsweekly.com/news/business/ibm-invests-new-5bn-chip-fab-india-chip-sale-2014-02/.
31 NT Balanarayan, "Cabinet Approves Creation of Two Semiconductor Fabrication Units," Medianama, February 17, 2014, http://articles.economictimes.indiatimes.com/2014-02-04/news/47004737_1_indian-electronics-special-incentive-package-scheme-semiconductor-association.
32 Jamie Yap, "India bars foreign vendors from national broadband initiative," ZD Net, January 21, 2013, http://www.zdnet.com/in/india-bars-foreign-vendors-from-national-broadband-initiative-7000010055/.
33 Kevin Kwang, "India holds back domestic-maker status for Huawei, ZTE," ZD Net, February 6, 2013, http://www.zdnet.com/in/india-holds-back-domestic-maker-status-for-huawei-zte-7000010887/. Also see "Huawei, ZTE await domestic-maker tag," *The Hindu*, February 5, 2013, http://www.thehindu.com/business/companies/huawei-zte-await-domesticmaker-tag/article4382888.ece.
34 Ellyne Phneah, "Huawei, ZTE under probe by Indian government," ZD Net, May 10, 2013, http://www.zdnet.com/in/huawei-zte-under-probe-by-indian-government-7000015185/.
35 Devidutta Tripathy, "India investigates report of Huawei hacking state carrier network," Reuters, February 6, 2014, http://www.reuters.com/article/2014/02/06/us-india-huawei-hacking-idUSBREA150QK20140206.
36 "Products Certified," Common Criteria Portal of India, http://www.commoncriteria-india.gov.in/Pages/ProductsCertified.aspx.

14

1 James Manyika et al, "Global Flows in a Digital Age," McKinsey Global Institute, April 2014, http://www.mckinsey.com/insights/globalization/global_flows_in_a_digital_age.
2 Ibid.
3 In June 2013, Edward Snowden, a contractor working with the US National Security Agency (NSA), leaked classified documents to several media outlets around the world. The first batch of documents published revealed mass surveillance practiced by the NSA and other security agencies within the USA through programmes like PRISM and Boundless Informant. Later leaks revealed varying degrees of collusion with US agencies by foreign security agencies and private companies. Data was collected directly from fibre optic cables and through information sharing systems. As he leaked the documents, Snowden fled first to Hong Kong and then to Russia, where he remains.
4 Arik Hesseldahl, "In Letter to Obama, Cisco CEO Complains About NSA Allegations," Re/code, May 18, 2014, http://recode.net/2014/05/18/in-letter-to-obama-cisco-ceo-complains-about-nsa-allegations/.
5 Jonah Force Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," Lawfare Research Paper Series 2, no. 3 (21 July 2014),http://www.lawfareblog.com/wp-content/uploads/2014/07/Lawfare-Research-Paper-

Series-Vol2No3.pdf.

6 Kristin Bent, "German Government Ends Contract With Verizon Over U.S. Spying Concerns," CRN, June 27, 2014, http://www.crn.com/news/networking/300073273/german-government-ends-contract-with-verizon-over-u-s-spying-concerns.htm.

7 Claire Cain Miller, "Revelations of NSA spying cost US tech companies," *The New York Times,* March 21, 2014, http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=0.

8 Ibid.

9 Aaron Kleiner, "Rethinking the Cyber Global Market," Panel discussion at CyFy 2014: The India Conference on Cyber Security and Internet Governance, New Delhi, October 15-17, 2014, http://orfonline.com/cms/sites/orfonline/html/events/video61.html.

10 The ITU Plenipotentiary Conference is the top policymaking body and supreme organ of the International Telecommunication Union. It is a meeting of ITU Member States and is held every four years. Plenipotentiary conferences adopt the underlying policies of the organisation, determine its structures and activities, establish the financial plan for the organisation and revise the Constitution and Convention when needed. They set the ITU's general policies, adopt four-year strategic and financial plans, and elect the senior management team of the organisation, the members of Council and the members of the Radio Regulations Board. The Plenipot is the key event at which ITU member states decide on the future role of the organisation, and determine the ITU's position on issues such as convergence, telephone tariffs, the internet, universal service and electronic commerce.

11 Daniel Sepulveda, "The Busan Consensus," U.S. Department of State Official Blog, November 10, 2014, http://blogs.state.gov/stories/2014/11/10/busan-consensus#sthash.wXvaFuVV.dpuf.

12 "India's Internet Governance Model to Balance Public & Private Interests", *The Huffington Post,* January 1, 2015, http://www.huffingtonpost.in/2015/01/16/india-internet-governance_n_6486234.html.

13 Samir Saran, "A Time to Lead", *The Indian Express,* April 16, 2015, http://indianexpress.com/article/opinion/columns/a-time-to-lead/.

List of Acronyms

ATM	Automated Teller Machine
BPM	Business Process Management
BRICS	Brazil, Russia, India, China and South Africa
CBM	Confidence-building measures
CCRA	Common Criteria Recognition Arrangement
CERT	Computer Emergency Response Team
CERT-IN	Computer Emergency Response Team – India
CIS	Centre for Internet & Society
DeitY	Department of Electronics and Information Technology
DoJ	Department of Justice, US
DSCI	Data Security Council of India
ECJ	European Court of Justice
FDI	Foreign Direct Investment
FOSS	Free and open-source software
GGE	Group of Governmental Experts
IAMAI	Internet and Mobile Association of India
IB-CART	Indian Banks – Centre for Analysis of Risk and Threats
IBSA	India, Brazil and South Africa
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technology
IDRBT	Institute of Development Research in Banking Technology
IG	Internet Governance
IGF	Internet Governance Forum
ISAC	Information Sharing and Analysis Centre
ISO	International Standards Organization
ISP	Internet Service Provider
IT	Information Technology
ITes	IT-enabled services
ITU	International Telecommunication Union
JWG	Joint Working Group

MLAT	Mutual Legal Assistance Treaty
NASSCOM	National Association of Software and Services Companies
NATGRID	National Intelligence Grid
NIST	National Institute of Standards and Technology, US
NMI	NETmundial Initiative
NSA	National Security Agency, US
NSCS	National Security Council Secretariat
NSDC	National Skill Development Corporation
OLPC	One Laptop per Child
OSCE	Organization for Security and Co-operation in Europe
PMA	Preferential Market Access
POS	Point of sale
PPP	Public-private partnership
RBI	Reserve Bank of India
SBI	State Bank of India
SMS	Short Messaging Service
SOC	Security Operation Centre
SSC	Sector Skill Councils
STQC	Standardisation Testing and Quality Certification
USSD	Unstructured Supplementary Service Data
WEF	World Economic Forum
WGIG	Working Group on Internet Governance
WSIS	World Summit on the Information Society

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

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

WITH THE INCREASING INTEGRATION OF THE INTERNET IN ALL ASPECTS OF GLOBAL LIFE, OLD TENSIONS AND CONCERNS ABOUT NATIONAL SECURITY, SOVEREIGNTY AND GLOBAL GOVERNANCE AMONG OTHERS ARE BEING EXAMINED IN A NEW LIGHT. TO EXPLORE THESE ISSUES, THE THIRD VOLUME OF THE GP-ORF SERIES FEATURES PAPERS FROM PRACTITIONERS OF CYBER SECURITY AND INTERNET GOVERNANCE ACROSS THE WORLD, INCLUDING THOSE IN BUSINESS, ACADEMIA, CIVIL SOCIETY AND GOVERNMENT. IT EXPLORES THE IMPLICATIONS OF A CHANGING DIGITAL WORLD IN FOUR KEY AREAS OF THOUGHT: INDIA AND THE CYBERWORLD, INTERNATIONAL COOPERATION, GLOBAL INTERNET GOVERNANCE AND PRIVACY AND SECURITY. THE CYFY JOURNAL *DIGITAL DEBATES* IS AN INTEGRAL PART OF CYFY: THE INDIA CONFERENCE ON CYBER SECURITY AND INTERNET GOVERNANCE, THE ANNUAL INTERNET POLICY CONFERENCE ORGANISED BY THE OBSERVER RESEARCH FOUNDATION. CYFY 2014 WAS HELD FROM 15-17 OCTOBER IN NEW DELHI, INDIA.