5 June, 2015

In search of India's Cyber Security Doctrine

*Dr Omair Anas**

The presence of citizens, civil society, institutions, market forces and the governments, as well as their enemies from state, non-state, business and commercial entities in the real and virtual world is, by and large, of similar nature and intensity. Since the Information Communication Technology (ICT) is an ever developing domain, the technological dynamism has made the cyber nation state less predictable. Because of the sheer speed of technological innovations, that too beyond state control, threats and their responses both follow each other. Also, anonymity, occasional un-traceability and deniability are three permanent features that complicate the implementation of conventional security tools. The cyber nation states will go through, occasionally, the same process that they have gone through in the physical world. The realist state behaviour, the idealist and structural realism are already the current practices of the cyber security regimes. This article discusses how the cyber security mechanism is being evolved in response to cyber threats. Cyber threats have the potential to inflict damage very quietly on public interests as well as institutional capability of governments, business organizations and their security installations. Sometimes, they are able to create unprecedented panic and terror. A sustainable policy framework to deter such an impending threat is very much dependent on both technical as well as policy interventions.

Background

The issue of internet governance lies at the heart of cyber security as major part of internet governance is still with the United States. Amid increasing voices for multilateralism or to assign the UN a greater role in internet governance, India has not yet evolved its own strategy. Ideally, India was supposed to support greater role for the UN, but India and the US, the two major ICT players, have chosen to have bilateral understanding on the issues of internet governance without changing much of the status quo.[i] Issues of cyber crimes, cyber terrorism have also paved the way for bilateral and multilateral cooperation on internet governance. Bilateral or multilateral set-ups may prove mutually beneficial for some states, but they may not provide a sustainable cyber security environment for all states, all the time. The way China has built up its own cyber infrastructure, independent of the global arrangements, will always be a preferable way for authoritarian and centralized states, who are more concerned about foreign influence in their digital space. On the other hand, internet governance free from states' intervention as practiced in the US may not remain the same. With increase in diversity in the digital space and emerging competition from the third world entrepreneurs, American internet giants find it difficult to let them go free into their digital space. Hence, net neutrality, intellectual property regime and other restrictive measures are being introduced by none other than the very corporate sectors, which have been against states' role in regulating the digital space.

International politics, much obsessed with the Cold War fault lines, has not been able to reach any consensus either on internet governance or on cyber security measures. Many critical infrastructures, cyber businesses and financial transactions as well as major health facilities are connected with the internet. So far, governments' threat perception is not unified. If the western governments are in favour of maintaining freedom and independence of internet and freedom of speech, their respective cyber laws, Russian and Chinese concerns include the use of social media and the contents posted there and their ability to influence their politics. Major concerns for the Western governments are the security of networks and their ability to send the right information and not to be controlled by criminal networks, or state sponsored agencies. Major concerns of Chinese and Russians

as well as other regimes of authoritarian tendencies are both the governance of these networks as well as the contents being transmitted from these networks. There is gradual emergence of international understanding on governance of internet through the United Nations' Governments' Group of Experts' (GGE) recommendations. After several failures, the GGE has gradually found some common understanding on cyber security issues.

Unlike the United States, the Indian government has played an important role in introducing the cyber world to its people through public owned companies, such as TRAI. However, despite having a decisive role, Indian decision makers followed a middle path by not regulating content transmission. Also, a vibrant private participation has strengthened and diversified India's cyber world. Current questions against the government's commitment to Net Neutrality have come up mainly because of government's practising a mediator role between the consumers and the service providers. India's support to such measures will not be free from political repercussions at home, where the cyber market is at a nascent stage and such measures will create an entirely different political discourse of discrimination and exclusion of which this country has a troubled memory. Also, India's emerging cyber world is too huge and diverse to be dictated by the US model of internet governance. Political, cultural and economic sensitivities in India will always demand the Indian state to be a guarantor of free and equal access to internet, failing which the government would have to face opposition.

The growing sensitivity over India's cyber security must recognize that the United States or China or any other country where cyber security laws are successfully implemented, have a fundamentally different trajectory of ICT development. For example, the recent UN report on the development of E-Governance has made reference to India:

> The adverse impact of lack of relevant content contributes to the digital divide in two ways. First, for example, despite the fact that India had manifold increase in internet users from 5 million in 2000 to 137 million in 2012, literacy is comparatively low at 74 per cent. This means, barriers to internet access remain for over 300 million people. Secondly, of those who can access the internet, the majority cannot speak English. Unless users have some knowledge of the English language—

regardless of how good machine translators become—they will be barred from the vast reservoir of information available in the electronic world.[ii]

Numerically, India is far ahead of many countries in terms of the number of smart phones and use of English language. But the per capita coverage of ICT is still poor. Also, despite having been world's second largest English speaking country (226 million), ICT penetration into remote areas requires the use of regional languages. What is important to note is that this gap is greatly responsible for India's success prospects for e-commerce, which, despite having progressed well, is considered disappointingly slow.[iii] The ITU report 2014 on ICT development in many Asian countries highlights a significant and persistent urban-rural digital divide.[iv] India remains at 129 place in World ICT Development Index along with other South Asian countries below India, except Maldives and Bhutan, which stand above India. In terms of India's ICT penetration, it is far behind many developing countries, leaving majority of its population excluded from ICT connectivity. This has direct impact on India's economic growth and inclusion of the common people into it. If the majority of India's population is excluded from ICT and the majority of ICT users are not aware of secure use of ICT tools, it is still too early to project the enormity of cyber security challenges for a billion internet users.

India's cyber security must be based on two parallel objectives; first, inclusion of larger population into the ICT fold and accessibility of ICT in local languages; second, educating these users about secure use of ICT. India's failure to provide high speed internet and local language information to its rural areas has hampered its health, literacy, education and banking sectors, which could have performed well, had there been better ICT development. Not only in terms of citizens' access to ICTs, but there is growing pressure from the private sector to end net neutrality as well as put strict intellectual property regime on which the Indian political discourse is deeply divided. Any policy discourse must be based on the recognition of West's asymmetrical technological edge.

India's Cyber Vulnerabilities

In the circle of national security policy making, criminal hacking, terrorist networks, nation-states conducting espionage, threats to critical infrastructures or services are the

most important security concerns. Among the most seriously assessed cyber attacks on Indian interests are the espionage campaign by GhostNet, Chinese espionage activities [against DRDO in March 2012 and Indian Navy's Eastern Command in June 2012] and

attack on Indira Gandhi International Airport network. It has always been difficult to trace the origin of a cyber threat and cyber crime. A report by Symantec says that India ranks second in social media scams and third in Asia for ransomware attacks and sixth in being the most bot-infected country. Thirty-four per cent of cyber attacks in India were targeted at small businesses.[v]

India's response to cyber security concerns is still in evolution. The National Critical Information Infrastructure Protection project was approved by the UPA government under the NTRO. However, the new government has introduced a new body, the National Cyber Coordination Centre (NCCC) to coordinate between intelligence and cyber response agencies, such as the Intelligence Bureau (IB) and the Indian Computer Emergency Response Team (CERT-IN). [vi] The first legislation to regulate Information Technology was the IT Act 2000. But more serious and elaborate policy making started only in recent years with the publication of the first ever National Cyber Security Policy in July 2011. This policy document relies on private public partnership to evolve a strong cyber specialist workforce in the next five years. Also, the introduction of National Cyber Coordination Centre, National Critical Information Infrastructure Protection Centre (NCIIP), the Computer Emergency Response Team of India (CERT-In) are in line with India's evolving cyber security measures. Lack of coordination between different agencies, such as the CERT-IN, National Information Security Assurance Program (NISAP) and National Information Centre (NIC) has affected India's ability to take a swift response to any cyber attack. Threats originating from state and non-state hostiles are aimed at our critical infrastructures as well as financial and public networks as the history of attacks suggests. Because of anonymity and high deniability in cases of cyber attacks, the most important area of security is the identification of potential threats from any part of the world. That needs collaboration with the states where a potential threat may originate from state or non state hostiles. Once a cyber threat has passed into the security sensitive network, there is not much to do except to minimise the damage. This collaboration involves many

complicated issues, such as data sovereignty, jurisdiction and territorial claims in the digital space. As of now, India has been part of Government Group of Experts, under the aegis of the United Nations and also a member of 24/7 Network of Contacts for High-Tech Crime of the G-8.

Existing Cyber Security Models

There are three models under discussion these days. The so called realist model advocates that India should stay away from any strong multilateral mechanism and should evolve its own cyber deterrence. The Chinese-Russian model is more problematic as it advocates for a strong multilateral framework, which allows member states to have final opinion with regard to internet governance in their countries, but, at the same time, these countries are secretly developing cyber armies. The last model is to involve all stakeholders, namely the governments, service providers, consumers and the civil society. None of these models have succeeded so far in evolving a common understanding on how to respond to a cyber attack.

After two Government's Group of Experts meetings, in which India is an important member, differences over cyber security issues and, more specifically, their implications on national security and military affairs have found some common understanding among the member states. The 2013 GGE has recognized that international law, including the principles of the law of state responsibility, fully apply to state behaviour in cyberspace.[vii] More importantly, the group has underlined the important role of the private sector and civil society. Though India has also agreed to the GGE's principle agreement on a role for government and private sector as well, India has greater scope for an independent cyber security policy that looks into the interests of its internet users, safeguards its critical infrastructure and prevents any externally originating threat to it. Efficacy of multilateral mechanism is more in the field of predicting and assessing cyber security concerns, but not in the case of immediate cyber security threats.

International collaboration on cyber security is an unavoidable option. No country, in isolation, can ensure its complete security from cyber threats, no matter how advanced a technology they develop. In the time of a neo-liberal global economy, transnational

financial flows, mostly outside of states purview, face many cyber threats. Critical installations, financial, security and infrastructural, are also integrated with each other. The Indian economy is also becoming an IT driven economy. Much of the governments' international cooperation on cyber security is being defined in terms of long established principles of the United Nations, which require member states to comply with the prohibition of the use of force and respect territorial sovereignty and the principle of settling disputes by peaceful means, as the last three reports of GGEs have recommended.[viii]

However, it is a fact that transnational cyber security is not a limitless option. Everything cannot be achieved through a transnational or a global cyber security regime in the same way as physical security is not achievable by relying much on international institutions. In view of the diversity in the origin and variety of cyber threats, a diverse range of responses are undertaken by various governments and non government institutions. For example, the Indo-US cooperation on cyber security is not free from mutual mistrusts and reservations. The National Security Agency (NSA) of the USA has developed some notoriety because of the Snowden episode.

In 2007, Estonia became the first country to face cyber attacks on its critical infrastructure that warranted NATO's help to protect Estonia. Estonia has now evolved its own cyber security strategy, which has made considerable progress in addressing its security. The Estonian Information System Authority (Riigi Infosüsteemi Ame) (RIA) has been assigned to lead its major security policy work with the Department of Critical Information Infrastructure Protection (hereinafter CIIP), Critical Information Infrastructure (CII), the Police and Border Guard Board (PBGB), the Estonian Defence League's Cyber Unit (EDL CU), and finally the Information Technology Foundation for Education (HITSA). Along with these domestic bodies, Estonia is actively engaged with regional and international cyber security policy making. The four years goal of the Estonian Cyber Security Strategy 2014-2017 defines its objective as "to increase cyber security capabilities and raise the population's awareness of cyber threats, thereby ensuring continued confidence in cyberspace." One of the major goals of its strategy is also ensuring alternative solutions for important services. The development of cyber capabilities and cross-sectoral activities are the most distinctive features. If Estonia and other European

countries are evolving a cooperative cyber security policy, countries like China and Russia have been accused of developing a cyber military, majority of whom are the most skilled hackers. [ix]

Options for India

The cyber security discourse in India has widely discussed domestic cyber security regime, as well as international collaboration along with partnership with stakeholders from various sectors. The domestic cyber security regime requires not only legislation, but also education and training on cyber security, particularly among the newly included masses in the digital space, who are generally trapped by disguised messages and links. Cyber security requires not only a secure and worm-resistant network, but also diversity and multiplicity of networks on threat so that the damage can be minimised if not stopped completely. Unlike the American consumers, Indian consumers are the least protected and often exploited. Only the American model or reliance on market forces to define cyber governance or only bilateral cyber security arrangements may not provide all the answers that India's nascent cyber sphere requires. The Japanese cyber security can be referred to as the one, which is trying to find a balance between all stakeholders 'without creating excessive state control'.[x] Japan has internationally promoted its own initiatives, such as PRACTICE (Proactive Response against Cyber-attacks through International Collaborative Exchange) and TSUBAME (International Network Traffic Monitoring Project).

Policy Framework

India's cyber security policy must respond to multiple challenges that it faces in the cyber world. India's economic growth, as important as the cyber security, is dependent on popular access to the ICTs. Second, India's e-Governance, though these are developing extraordinarily, are still limited within a small community of net users, thanks to many reasons including the non responsive e-Governance. Third, India's ever increasing number of internet users is largely untrained and unaware of cyber threats and security responses. Both Russia and China or the Western countries have performed well in these aspects. Given the fact that India has the ability to evolve its own independent mechanism, it should evolve its cyber security policy in response to its specific challenges. By investing more

resources in universalizing ICTs, cyber training programs and cyber security research and development, India can evolve an effective national cyber security and also support the international community. It is recommended that India's cyber security strategy should be in response to: i) understanding the nature of problem and ii) understanding the nature of cyber threats.

Understanding the Nature of Problem

1. India's cyber space, once accessible to all, will be the most diverse, dynamic and volatile cyber space full of regional, ethnic, religious, sectarian, linguistic and class sensitivities as well as opportunities.
2. India is facing huge digital deficit where only limited population has access to internet and internet based services. The limited accessibility to internet is because of poverty, lack of services in Hindi and other regional language, and lack of computer education in rural areas.
3. Though India is the fastest growing cyber space, it is also the least trained for the cyber security issues. That makes India's cyber security vulnerable to both domestically and externally originating threats.
4. To protect its citizens from any cyber crime, fraud, theft or terrorism, it is the responsibility of the state and, hence, the state's role in defining security of common users will remain important.
5. Private sector still holds much control over internet, but it does not share much responsibility of cyber security for both citizens and the state.
6. India's national security has been facing immense threats from global terrorism, organized criminal networks, as well as often hostile neighbours and their proxies. Their use of cyber space against India is proven by their past activities.

Understanding the Nature of Cyber Threats

1. Past cyber attacks suggest that terrorist and criminal groups are acquiring or being supplied medium and advanced cyber capability to achieve their goals. The existence of cyber terrorism and cyber military hostile to India's cyber space is a reality.

2. Majority of cyber threats can be easily averted by a little training and technical support. There is lack of training and technical mechanism to restrict these normal cyber threats.
3. Advanced cyber threats are coming from well organized terrorist and criminal groups, state proxies, corporate espionage and accidental system failures.
4. Within Indian governance, both state and central government and their partners share responsibility to protect the cyber space, but private and corporate sectors are yet to have a well defined role to protect the interests of their consumers.
5. A large chunk of cyber crimes are about financial transactions, breach of privacy or sexual harassment. As of now, the Indian police system has failed to evolve its cyber version to control these crimes.

Policy Framework

1. For general cyber threats, inclusion of compulsory cyber security training in all human resource development programs will create a broad base of cyber capable netizens. Also, the inclusion of larger population into the cyber world will create a capable citizenry.
2. A universal and responsive e-Governance will enhance people's participation in the cyber world and will make them responsible citizens of the cyber state as well. In absence of cyber citizens, the cyber state will remain irrelevant for common interests.
3. The financial crimes, in which consumers are affected, should be resolved through a mix of state-market mechanism so that the responsibility of market is fixed.
4. For cyber crimes against national security, a diverse approach, which includes bilateral, multilateral, multi-sectoral engagement, will be helpful. However, the much required thing is to invest in research and development of cyber capabilities, which can identify potential security threats, neutralise them and keep India's cyber nation-state safe and secure.
5. For international collaboration, independent internet governance under the aegis of the UN will help in containing the dominance of Western countries, particularly the United States. The GGE's gradual success suggests that a multilateral mechanism is possible in which member states' sovereignty will be more respectable.

6. India's cyber doctrine should be based on the objectives of development and deterrence. With more than half the population without internet, India's development goals will remain compromised. Cyber empowerment of rural and local bodies as well as individuals, particularly women and protection of their cyber rights, will help develop cyber capability for a safe and secure cyber space for all. The cyber security doctrine based on development and deterrence is absent from current cyber security discourse.

Dr. Omair Anas is Research Fellow at the Indian Council of World A ffairs.

---

[i] Indo-US Cyber Security Forum (IUSCSF) set up in 2001.

[ii] United Nations, "United Nations E-Government Survey 2014: E-GOVERNMENT for the Future We Want" http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf p. 132, (Accessed on 15 May 2015).

[iii] Mahajan, Ambika Choudhary, E-Commerce Industry in India: $6 Billion by 2015 with Disappointing Slow Growth! http://dazeinfo.com/2014/10/20/ecommerce-india-6-billion-industry-2015-disppointing-slow-growth/, (Accessed on 15 May 2015).

[iv] International Telecom Union, Measuring the Information Society Report 2014, Page 1, http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf, (Accessed on 10 May 2015).

[v] *Business Standard*, "India Ranked 2nd in Cyber Attacks through Social Media in 2014, 23 April 2015 http://www.business-standard.com/article/technology/india-ranked-2nd-in-cyber-attacks-through-social-media-in-2014-115042200643_1.html, (Accessed on 10 May 2015).

[vi] *The Hindustan Times*, "Centre to Shield India from Cyber Attacks Proposed", 17 August 2014 http://www.hindustantimes.com/india-news/rs-950-crore-centre-to-shield-india-from-cyber-attacks-proposed/article1-1252849.aspx, (Accessed on 10 May 2015).

[vii] Detlev Wolter, "The UN Takes a Big Step Forward on Cyber Security", September 4 2013. http://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity, (Accessed on 10 May 2015).

[viii] Article 51, UN Charter passed by the UN Group of Governmental Experts (GGE).

[ix] *The Guardian*, "Chinese Army Hackers are the Tip of the Cyber Warfare Iceberg", 23 February 2013 http://www.theguardian.com/technology/2013/feb/23/mandiant-unit-61398-china-hacking, (Accessed on 10 May 2015).

[x] International Strategy on Cybersecurity Cooperation - j-initiative for Cybersecurity, http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf