IJERMT
International Journal of Engineering Research & Management Technology
ISSN: 2348-4039
December-2018 Volume 5, Issue-6
Email: editor@ijermt.org
www.ijermt.org

CYBER SECURITY POLICY IN INDIA: ISSUES, CHALLENGES AND FRAMEWORK

Vipin Kumar Thakur
Research Scholar
Shri Venkateshwara University
Gajraula

Dr.Manoj Kumar
Associate Professor
Shri Venkateshwara University
Gajraula

ABSTRACT
At the most general level, cyber threats to national security span the spectrum from fears of unauthorized access to classified proprietary materials, at one end, all the way to the use of cyberspace for strategic and military purposes at the other. Within this range are increasingly complex problems that transcend more familiar ones. Terms such as "hackers" appear increasingly quaint in light of the potentially powerful disruptions posed by cyber threats. The International Telecommunication Union (ITU) completed a comparative review of state-based perspectives on cyber security and institutional responses. The review showed that threats to security and attendant damages are defined in different ways by different countries, and the response strategies differ as well. None of these or related initiatives have been integrated into an overall national security framework.
Key words: cyberspace, security

INTRODUCTION
From a national security perspective, there are three main aspects of cyber security: exploitation, defence and offense. The first involves identifying hardware and application vulnerabilities of adversarial networks to obtain critical information, a modern form of espionage. But it is not purely for passive purposes, because huge amounts of information can be "exfiltrated" and can be used to hamper military operations. The second is the building of measures to make it more difficult for attackers to degrade, disable or destroy protected networks. The third is to take initiatives to disable offensive capabilities "preventively" or "pre-emptively" that are intended for cyber attack. These offensive operations can range from playing a form of defence in peacetime to conducting full spectrum operations in wartime. This third area is especially controversial because it runs up against possible violations of national sovereignty in order to conduct "preventive" or "pre-emptive" attacks.

Advancements in information and communication technologies and their widespread use have lead to an ever-greater dependence on cyberspace and its infrastructure, which increases the vulnerabilities of societies and economies to disruptions. Policy- makers and civil society have become more and more aware of cyber risks such as cybercrime, cyber espionage and cyber terrorism, even acts of cyber war has already been diagnosed.

Many of the risks in and emanating from cyberspace can be understood as potentially systemic risks, which mean they are characterized by high uncertainty, complexity and ambiguity. In consequence, the probability and the possible damage of an event cannot be fully calculated. The sources of possible damages cannot be exactly identified and an event can have widespread effects across nations. Expert judgments of cyber risks and their possible damage differ widely. Since a strictly scientific assessment of the problem is not possible due to a lack of objective measurement, political interpretations of cyber risks weigh all the more. Actors participate in discursively structured fights for reality definitions and those definitions play an important role for legitimizing political action. Notably in the emerging field of cyber policy, discourses play a crucial role and present a highly relevant area of research.

ISSUES

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. 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. Advanced cyber threats are coming from well-organized terrorist and criminal groups, state proxies, corporate espionage and accidental system failures. 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. 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. Some of the valuable proposals in the NCSP are as follows:

- Creating a taskforce of 5,00,000 cyber security professionals in next five years.
- Providing fiscal schemes and benefits to businesses for adoption of standard security practices.
- Designating CERT-In as the national nodal agency to co-ordinate cyber security related matters and have the local (state) CERT bodies to co-ordinate at the respective levels.
- Developing a dynamic legal framework to address cyber security challenges
- Encouraging wider use of Public Key Infrastructure (PKI) for government services.
- Apart from the common theme of PPP across the cyber security initiatives, the policy frequently mentions of developing an infrastructure for evaluating and certifying trustworthy ICT security products.

India should support the idea of TCBMs (transparency and confidence building measures) as a first step towards a code of conduct or eventual cyber security convention. India must participate wholeheartedly and proactively in an international dialogue on cyber security both at inter-governmental as well at non-governmental level. Participation in cyber security discussions at academic, think tank and NGO levels will be immensely useful.

Despite differences in perceptions, some measure of agreement can be achieved more easily on some issues than on others. For instance, everyone agrees that cyber crime and cyber terrorism pose a major threat to individuals, states and societies. It should therefore be easier to agree on cooperation measures to deal with these threats. A number of UNSC resolutions on terrorism can be made applicable to cyber terrorism and cyber crime as well. India should be proactive in building a consensus on how to deal with cyber crime and cyber terrorism.

India can propose that the principles of the UN Charter:maintenance of international peace and security, international cooperation, universalism of human rights, etc.: should form the basis of rules of the road, code of conduct or CBMs in cyber space. Thus any new ideas that are proposed in the context of cyber space must first be checked for validity against norms mentioned in the UN Charter. Where there are ambiguities and disagreements, further discussion and dialogue must be held to remove them or formulate new approaches.

A great deal of discussion has been held at various UN forums, World Summits on Information Security and numerous technical forums on information security and cyber security. It would be useful to collate principles, which have been enunciated at these gatherings. True, these are mostly declaratory in nature but they do reflect a measure of consensus. For instance, most countries would agree that the digital divide should be bridged, capacities should be built, cooperation among law enforcement agencies should be promoted, technical cooperation should be encouraged, etc. Thus there are a number of ideas on which a considerable amount of agreement exists. India can examine such ideas, which can form the basis of TCBMs in cyber space.

Many cyber securities related projects are managed by Indian security and intelligence agencies without any parliamentary approval and oversight. The intelligence infrastructure of India needs

transparency and reforms. Without this cyber immunity cannot be granted to these agencies. India must also reconcile civil liberties and national security requirements while protecting Indian cyberspace. The ultimate solution is to formulate a techno legal framework that can safeguard Indian cyberspace in the best possible manner.

CHALLENGES

Some of the important cyber security challenges that nations are overall grappling with are enumerated below:

- ICTs are largely owned and operated by the private sector in most countries. The private sector thus has to directly protect, or be involved in the protection, of this infrastructure
- Addressing network security requires a public-private partnership as well as international cooperation and norms
- It is important to create mechanisms for intelligence and information sharing
- Governments must develop a comprehensive frame- work to ensure coordinated responses and recovery after a significant incident or threat. This must include a definition of the roles and responsibilities of each player in the PPP
- Nations must specify the roles of government and industry even as they identify incentives for businesses that implement best practices and standards
- Insider threats must be assessed. Background checks of employees in an organisation are essential
- Create a predictable legal regime for dealing with cyber crimes, storage and retention of cyber forensics data, and international cooperation across jurisdictions to track cyber criminals

The national security community is wrestling with several tough problems, which will take considerable time and effort to resolve. These include:

1. ***Declaratory policy****:* The Government has no official policy publicly communicating what it would or would not do in the event of a major cyber attack against Defense forces, command and control systems, electric power grids, financial networks, or other elements of military power or critical infrastructure. Should there be a declaratory policy and, if so, what should it stipulate? For example, should we define categories of "major cyber attack" that are unacceptable, so-called "red lines," that would likely trigger a major retaliatory response?

2. ***Deterrence policy****:* Much of the nuclear age has been marked by refinements of deterrence policy crafted to influence adversarial behaviour in irregular, conventional and even nuclear war. Are these concepts applicable to the cyber domain where attribution of the attack is often difficult to ascertain and the range of cyber attack damage can be from the trivial (e.g., slowing email receipt) to the profound (e.g., disabling the nation's military early warning systems)?

3**. *Authorities & Responsibilities****:* If cyber attacks against defense forces or critical infrastructure originates abroad, a response to them would almost surely involve violation of the sovereignty of the state where the attack originated. What is the legal basis to conduct such operations? Moreover, there is a huge time lag between obtaining appropriate legal authorities (measured often in weeks or months) and the need for national security forces to respond effectively (measured at times in minutes or hours). How can this time lag be most effectively bridged?

4. ***Guarantees of Civil liberties****:* Cyber security presents a major tension between the policy and legal communities. Given the difficulty in attributing the origins of cyber attacks, and the possibility that some of these attacks could originate in India or by our citizens, how do we formulate effective policies that still guarantee the civil liberties of our citizens? Under what circumstances would it be justified for the government to monitor the cyber communications of its citizens or, if necessary, to degrade or disable these systems? And who and how should these activities be monitored?

FRAMEWORK

The growth of IT sector in India has been fuelled by equally impressive growth in telecommunication infrastructure. The world is moving towards converged networks being referred as 'Next Generation Networks (NGN)'. In the coming decade the NGN is likely to replace the legacy networks. This upcoming national information infrastructure would be marriage of IT and telecommunication infrastructure with various regulatory and security challenges that need careful scrutiny.

As our investments in ICT infrastructure grow our vulnerability to damage by natural disasters or through attacks by insurgents/terrorists with objective to immobilize and paralyze day-to-day activities of the nation is becoming real. Such damage would cause short and long term setback to economy. We have many lessons from US initiative to secure our cyber system, while planning and implementing India's ICT infrastructure. Natural or insurgency/terrorist induced disaster increases pressure on available ICT systems exponentially to facilitate coordination between various agencies like fire brigade, medical services, police, media and civil administration.

It is proposed that the existing and planned ICT infrastructure of the nation, both in public and private domain be analyzed by a group of experts under aegis of NDMA to suggest suitable operational arrangements to minimize their vulnerability to perceived attacks by inimical elements and natural disasters. This would entail rigorous technical analysis of current and emerging wireless and wired ICT systems. The expert group should find and recommend suitable mix of redundancies in the critical ICT systems supporting the governance structure of the nation. The focused analysis of the vulnerabilities and their protection, would lead to recommendations that would avoid duplication of effort and, therefore, economical at national level. The notion that disasters can be completely brought under control by technological and scientific capabilities alone would be too presumptuous. The most sacrosanct component in any such venture is participation from all stakeholders to ensure an appropriate solution for the welfare of humanity.

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'. 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).
Joshi & Nair (2011) enumerate some of the major concerns regarding the current framework.

1. ***Reporting and Ownership***: Is there a clearly defined entity within the Government of India that owns cyber security as a subject? Many of the security provisions outlined in the draft are theoretically impeccable, but unless the document addresses the critical elements of ownership, mandate and empowerment, issues of the past will continue and there will be a disconnect between our intent and our capability. The draft does not provide any clarification on this fundamental ownership ambiguity. It is important that a single body be identified to own cyber-security in India, be adequately staffed and have the mandate to enforce policy, as required. The responsible entity ought to be clearly identified and its governance responsibilities, mandate and reporting structure need to be clearly spelled out.

2. ***Staffing and Resources***: The draft envisages an ambitious project, which can only be successful if it has full commitment at the highest levels of the government, adequate and well-qualified resources, buy-in from central/ state-level entities and private sector, and adequate funding, all of which need to be sustainable over time. The document does not provide any details about these issues.

3. ***Orphan Policy:*** Cyber security cannot be considered in a silo. Cyber security – the business of safeguarding a country's networking and technology infrastructure, and electronic information – is a subset of national security and a cyber security policy must be congruent to a national security policy. However, as India does not have a national security policy, the cyber security policy identified in the draft is effectively a "policy orphan." As a result, significant gaps could exist between this policy document and what different ministries, departments and agencies assume might be India's national security goals and priorities. While we agree that this is not something that can be remedied at one go, the orphaned nature of the cyber security policy should be recognised and its implication studied and understood.

4. ***Information Lifecycle Control***: While the draft does well to design adequate controls over some "states" of information, it is advisable to consider the entire "information lifecycle" and design appropriate controls. This encompasses the creation, processing, storing, transmitting/ receiving and deleting of information. Further, it is important to consider both technical controls (which the draft discusses well) and non-technical controls (which appear in limited form in the draft), because electronic information can be breached with or without the aid of technology. For example, social engineering attacks such as phishing and pretexting, and other malicious activities such as dumpster diving cannot be addressed purely through technical controls. Training and awareness programs are far more critical than pure technical controls in some states of the information lifecycle.

Cyber Terrorism

'Cyber terrorism' is the convergence of terrorism and cyber space. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

Further, to qualify as cyber terrorism, an attack should result in violence against persons or property or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism depending upon their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

Cyber-terrorism can also be understood as "the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population." A hostile nation or group could exploit these vulnerabilities to penetrate a poorly secured computer network and disrupt or even shut down critical functions. Some Examples:

Middle East Tension Sparks Cyber Attacks

With the Middle East Conflict at a very heated moment between bordering countries Pro-Palestinian and Pro-Israel Cyber Groups have been launching an offensive against websites and mail services used by the political sectors the opposing groups show support for. The attacks had been reported by the NIPC (National Infrastructure Protection Center) in October of 2000 to U.S. Officials. The attacks were a volley of email floods, DoS attacks, and ping flooding of such sites as the Israel Foreign Ministry, Israeli Defense Forces, and in reverse, sites that belonged to groups such as Hamas and Hezbollah.

Pakistan/India Conflict

As tensions between the neighboring regions of India and Pakistan over Kashmir grew over time, Pro-Pakistan cyber-terrorists and recruited hackers began to target India's Internet Community. Just prior to and after the September 11 attacks, it is believed that the sympathizers of Pakistan (which also included members of the Al Qaeda Organisation) began their spread of propaganda and attacks against Indian Internet based communities. Groups such as G-Force and Doctor Nuker have defaced or disrupted service to several major entities in India such as the Zee TV Network, The India Institute of Science and the Bhabha Atomic Research Center which all have political ties.

ISIS

Recent activities of ISIS in Middle East and series of videos released by them are potential cyber terrors. They are using Cyber space for their propaganda and for influencing vulnerable people to join ISIS. It is threat to the world and the way they are growing needs global cooperation to check them before they create havoc.

Cyber Crime

The Internet is an increasingly attractive hunting ground for criminals, activists and terrorists motivated to make money, be noticed, cause disruption or even bring down corporations and governments through online attacks.

Today's cybercriminals primarily operate out of the former Soviet states. They are highly skilled and equipped with very modern tools, they often use 21st century tools to take on 20th century systems. In 2014, we saw cybercriminals demonstrating a higher degree of collaboration amongst themselves and a degree of technical competency that caught many large organisations unawares.

The Future of Cyber politics

Given the rapid growth of Internet users, the increased complexity of managing cyberspace, and the record of governments' control or denial of access, it is reasonable to consider potential trajectories of international relations and their cyber politics.

Efforts to differentiate among alternative cyber futures are based on one key assumption: that the traditional real systems of interactions, power, and influence will shape the contours of cyberspace in the future. Technological decisions, alternative Internet architectures, and different modes of governance of cyberspace and management system will follow accordingly.

For conceptual purposes, two trajectories or dimensions are drawn to provide an internally consistent frame of reference. One pertains to the dominant principle underlying authority and decision, namely, state sovereignty versus private authority. The other relates to modes of international behaviour, that is, conflict and violence versus cooperation and collaboration. Jointly they provide the criteria and dimensions to identify alternative futures. On this basis, Choucri (2012) presents four generic but very different models of the future of cyber politics with the understanding that these are model at best and are not intended to be specific predictions. The purpose is to signal possibilities and potentials, given the many facets of cyber politics.

The first model is a future anchored in high sovereign control over cyber venues in the context of a high level of international conflict and violence. This model future is the *garrison cyber system*, in respectful memory of Harold Lasswell, who first coined the term "garrison state" and outlined its critical features more than sixty years ago. Countries like Saudi Arabia, Myanmar, North Korea, and China may become candidates.

The second model of cyber futures proposes a world of high conflict and violence worldwide in the absence of sovereign control or any centralized authority. This model future is known as *cyber anarchy*. This is a world where private order dominates, with no overarching authority or forms of governance and no constraints on the activities of actors or agents. In many ways, this future approximates the proverbial Hobbesian state of nature, the war of all against all.

The third cyber future issues from international cooperation and coordination in a world dominated by non-state actors, agents, and entities. This is a "hands-off" future in which only the minimum coordination necessary for core Internet and other cyber operations is put in place. This model is being called as the *global cyber commons.* Civil society, local and global, would be the main supporters and constituencies of this model.

The fourth model of cyber futures is a world managed by sovereign states and characterized by a high degree of international cooperation and collaboration. This future is termed as the *cyber grand bargain* to high- light collaborative management, bargaining, and negotiations. This future is an extension:with refinements and alterations:of the original vision of the Internet, as well as the current cyber system and its management. The United States, the European Union, and other political democracies may potentially be supportive of such a future and help realize it. Each model is based on different normative underpinnings, different assumptions about international relations and different expectations about interactions among decision entities.

Such visions of cyber futures must be understood only as model types, that is, representing central tendencies, anchored in fundamentally different parameters of politics in any context. The development of any one of these cyber futures will necessarily involve alterations, additions, or extensions of the current infrastructure and managerial systems. It is important to recognize the transformative functions of social demands and technological innovation. At the same time, the close connection of technology and society requires the recognition of the growing politicization of cyberspace, reinforced by continued lateral realignments among actors, and agents, interests and influences, worldwide.

Conclusion

The construction of cyberspace and the expansion of access and participation have led to new ambiguities and uncertainties and created new challenges to theory, policy, and practice for both the traditional kinetic and the cyber domains. We have come to the end of an era for tradition and convention in international relations. The salience of cyberspace is recognized worldwide. It is now an integral feature of the world we live in and of the interactions within and across sovereign states. With growing access to cyberspace, objective factors may assume their own subjectivities. With little consensus over the nature of prevailing "truths," we can expect more rather than less international contentions over matters of jurisdiction, legitimacy, authority, and accountability. With various government initiatives on national security, like the National Grid, designed as an NW of 21 available databases across government and private agencies and meant to help flag potential terrorist threats and also the Aadhar programme, for issuing unique identity numbers, there have arisen serious concerns about privacy as personal data are compiled in central databases and accessed by the various government agencies. It is essential that proper amendments or necessary laws like a separate data protection/privacy legislation be put in place to safeguard against the misuse of such personal information and protect individual privacy.

Similarly, there need to be put in place proper legislative as well as procedural measures to ensure that the freedom of expression guaranteed under Article 19 of the Constitution is not compromised at the altar of national security.

REFERENCES

1. David Bainbridge, Encyclopaedia of information technology law, Universal Law Publishing Co. Pvt. Ltd., Delhi, 2018.
2. Faye Fangfei Wang, Internet jurisdiction and choice of law, Cambridge University Press, New York, 2015.
3. Graham J.H. Smith, Internet law and regulation, Sweet & Maxwell, London, 2018.
4. Myra Williamson, Terrorism, War and International Law: the Legality of the Use of Force against Afghanistan in 2001, Ashgate Publishing. United Kingdom, 2009.
5. N. Wiener, Cybernetics or Control and Communication in the Animal and the Machine, The Technology Press John Wiley & Sons, Inc., New York, 1948.
6. Peter K. Smith (ed.) & Georges Steffgen, (ed.), Cyberbullying through the new media, Psychology Press, East Sussex, 2018.

7. Peter Lilley, Hacked, Attacked and Abused, Biddles Ltd., Guildford and Kings Lynn, UK 2015.
8. Rasita Anand. Cyber Security Policy in India, Ph.D. Thesis, Central University of Gujrat, Gandhinagar, 2015.
9. Tim Paul Kevan and Paul Mcgrath, Encyclopaedia of information technology law: e-mail, the internet and law essential knowledge for safer surfing, Universal Law Publishing, New Delhi, 2015.
10. Vakul Sharma, Information Technology: Law and Practice, Universal Law Publication Co., New Delhi, 2012.
11. Verinder Grover, Encyclopaedia of International Terrorism, Deep & Deep Publications, Delhi, Vol. 2, 2014.