CRITICALITY ANALYSIS AND PROTECTION OF NATIONAL CRITICAL INFORMATION INFRASTRUCTURES (NCIIs)

MK SHARMA

INTRODUCTION

Current understanding of the cyber world suggests an upward trend in offensive cyber activity posing a challenge to policy-makers to develop a strategy of graded response to the disruptive and, at times, destructive cyber attacks. With the increasing likelihood of cyber attacks becoming state sponsored rather than by non-state actors, the difficulty of the sovereign governments has only increased in terms of crafting a timely, proportionate and legally acceptable counter response that is not seen by its own people as ad-hoc. While executing a discriminatory response continues to be marred by plausible deniability enjoyed by the attackers and difficulty in assessing the actual damage to National Critical Information Infrastructures (NCIIs) by the governments, there is an inevitable requirement of taking a couple of initiatives as pre-event homework by the agencies concerned. Firstly, to be able to determine the impact of an incident on the operations of all NCIIs

Wing Commander **MK Sharma** is a serving officer of Aeronautical Engineer (Electronics Branch). Presently, he is holding a staff appointment as Command Guided Weapons Maintenance Officer (CGWMO) at Headquarters Eastern Air Command. He has been on a Research Fellowship at the Centre for Air Power Studies twice and has published a book titled *Cyber Warfare: The Power of the Unseen.*

NCIIs that are otherwise physically and geographically dispersed, get interconnected and integrated through networking and information exchange, thus, the dependency amongst systems rises non-linearly.

in both the public and private domains and, secondly, to be able to arrive at a pre conceived response matrix by the government agencies, having evaluated the impact of such response across the political, economic, military and information domains. Thus, the strategy of proportionate response would have to take into consideration factors such as the level of confidence in our own cyber agencies to correctly attribute the responsibility of attack, the pragmatic and objective assessment of the impact of such attack on NCIIs, and, of course, the instruments of cyber power at the disposal of the government. As an essential first step, the task of protecting NCIIs would then have to be based on understanding the nature of NCIIs which are *prima facie* complex, interdependent, interconnected and highly distributed.

NCIIs that are otherwise physically and geographically dispersed, get interconnected and integrated through networking and information exchange, thus, the dependency amongst systems rises non-linearly. Information infrastructure is the term used to describe the totality of inter-connected computers and networks, and the essential information flowing through them.[1] Two important factors that play a role in the interdependence of NCIIs are: the rising vulnerabilities in NCIIs that could be exploited more easily by non-technical hands, and their reliance on Information and Communication Technologies (ICTs) for data gathering, fusion, processing, and dissemination for day-to-day functioning. The relationship amongst various NCIIs today is characterised by a web of multiple connections such as feedback, feed forward paths, and intricate branching topologies. A minor disruption at any point could have a rippling effect across multiple critical

1. Peter Westrin, "Critical Information Infrastructure Protection", *Information and Security* (London: Tyalor and Francis, 2001), vol 7, p. 69.

infrastructures if other functions are highly dependent on its output.[2] Thus, a renewed focus is necessitated on the vulnerabilities which are common to multiple infrastructures, leading to interdependencies.

The criticality of an information infrastructure could be looked at in many different ways. Information infrastructure is not only shared, and heterogeneous in nature depending upon the networking maturity level of the infrastructure but also evolving in terms of its role and utility interdependence among others. When we approach NCIIs' protection from the point of national security strategy, we find that not all the elements of an NCII are equally critical, thus, the protection strategy would have to be differential in nature, based on identification of the elements that are most critical. Also, when we consider protection from the point of the vulnerabilities that cut across the listed information infrastructures, the interdependencies come to the fore. What would be the second order impact on other infrastructures when a particular interdependent infrastructure is under attack? The interdependencies could arise out of the logical networking profile, functional priorities or by geographic co-location of the assets. This brings to us a new challenge of defining parameters to measure interdependencies so as to arrive at the NCIIs' protection strategy based on identification of the most critical elements that are essential for the sovereignty of the nation, or disruption of which may pose danger to life and property.

Information infrastructure is not only shared, and heterogeneous in nature depending upon the networking maturity level of the infrastructure but also evolving in terms of its role and utility interdependence among others.

The aim of this paper is to put forward a basic methodology to measure the interdependency of NCIIs using criticality analysis of infrastructures, and to propose a strategy of proportionate response to protect the NCIIs.

2. Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, " Identifying, Understanding and Analysing Critical Infrastructure Dependency", *IEEE Control Systems Magazine* (USA), vol 21, no.6, 2001, p, 14.

THEORETICAL BACKGROUND

NCIIs, Interdependence and Globalisation

The process of globalisation may be best understood with the works of Robert Keohane and Joseph Nye.[3] The multifaceted process of globalisation has lifted barriers across the states and evolved a highly comprehensive system with free flow of trade, commerce, ideas and people. The enabler for integration of economic, cultural and social factors of globalisation is ICT. As various services carried over the internet such as electronic mail, instant messaging, Voice over Internet Protocol (VoIP), electronic commerce, etc. enhanced the effectiveness and reach of the impacts of globalisation, the requirement of swift communication and trans-border data flow gradually became critical to decision-making. The rise of neo-liberalism led to changes in the patterns of interactions in global economies and new sectors such as services/financial services emerged along with the exponential growth in production, marketing and flow of goods across the borders. Moore's Law[4] predicts that bandwidth requirement would double every 18 months and the number of transistors that can be put on an integrated circuit would double every two years. This exponentially increasing demand for communication led to further research and development supported by huge investment in ICT across the globe.

The actual transmission costs have become negligible; hence, the amount of information that can be transmitted is effectively infinite. While contemporary issues of cyber attacks and piracy have brought a new set of problems, two factors, namely, the ever increasing complex interdependence of NCIIs and the emergence of non-state actors has eroded the sovereign power of the state. The decision-making process is more independent of the state today, thus, posing a number of new challenges to the security and well-being of the globalised world. However, the concept of interdependence among sectors and societies is not a novel phenomenon. In this context,

3. Robert O. Keohane and Joseph S. Nye, Jr, "Globalization: What's New? What's Not? (And So What?)", Washingtonpost.Newsweek Interactive, LLC , *Foreign Policy*, no. 118, Spring, 2000, pp. 104-119. http://www.jstor.org/stable/1149673
4. Gorden E.Moore, http://www.mooreslaw.org/. Accessed on January 15, 2016.

it may be pertinent to revisit the 1940s when globalisation of the world economy was deliberately fostered by US policy and international financial institutions for half a century post World War II. In the late 1940s, the United States sought to create an open international economy to forestall another depression and contain Communism.

NEO-REALISM AND THREATS TO NCII

The last two decades have witnessed an unprecedented dependence of individuals, organisations and nation-states on ICT and its derivative applications. It has become an integral part of planning and strategy for organisations involved in any kind of business for effective management. Nation-states have developed their infrastructures such as transportation, communication systems, banking services, e-governance, energy generation and distribution, etc. with high dependence on IT infrastructure owned by both the government and the private sector. These infrastructures have become the core of the very functioning of a modern nation-state and any disruption or destruction of these could have adverse effects on the national security. The critical infrastructure shares the IT infrastructure and employs ICTs for various management and operational processes. This dependence of a nation-state on NCIIs for its day-to-day functioning and operations has emerged as a vulnerability.

The neo-realist paradigm, which designates a state as the core of international politics and regards international politics as being driven by national interest, could explain the emerging threats to NCIIs, the incapacitation of which would undermine the national security. Neo-realism attempts to explain the nature of international relations by separating the state level, which Kenneth Waltz defines as composed of units, as opposed to the systems level, which is composed of structures.[5] As per the theory, states are differentiated from one another not by function but primarily by the capability to change, adopt, hold power, enhance trade and adapt to changes. The degree of dependence on NCIIs varies for different nation-

5. Suganami, Hidemi, "Understanding Man, the State, and War," *International Relations*, vol. 23, no. 3, 2009, pp. 372-388.

states depending upon their capability and capacity. The higher the degree of exposure to ICT, the more significant is the threat emanating from non-state actors as well as state sponsored actors which are targeting to exploit the vulnerabilities.

International Cooperation and NCIIs' Protection Dilemma

The underlying assumption of neo-realism designates states as seeking security and the international order renders states on their own for their survival. The ultimate state interest is in security and not power. As nation-states have realised the threats emanating from state and non-state actors to their critical information infrastructures, various security mechanisms are being devised to secure the existing systems and networks utilising technological means and growing security ties with like-minded nation-states.

As Robert Jervis points out, as anarchy and the security dilemma make cooperation seemingly impossible, nation-states face issues pertaining to the security of their national critical information infrastructures.[6] The data and configurations pertaining to critical information infrastructures is sensitive and nations refrain from sharing these details even with entrusted partners. Furthermore, nation-states are always careful of the capabilities of their adversaries in cyber space, which leads to clandestine capability development and operations. In international politics, one state's gain in security often inadvertently threatens others. The security mechanism developed by a nation may not be accurately estimated by the others and may trigger a race to gain offensive cyber capabilities which would enable a nation-state to bring down the critical information infrastructures of the adversary in the present-day network-centric environment. The nation-states having greater dependence on ICT for the functioning of their critical infrastructures are developing defensive tools to avoid any attack against their infrastructures and are considering the option to develop offensive tools to deter an adversary nation-state from targeting their vital information

6. Jervis, Robert. "A Usable Past for the Future," *Diplomatic History,* vol 16, no. 1, 1992, pp. 76-84. http://dh.oxfordjournals.org/content/16/1/76.extract

infrastructures. While most nations are developing legal frameworks to address cyber issues domestically, there is lack of international laws for cyber related issues.

NCIIs IN THE CONTEXT OF NATIONAL SECURITY

India, through the IT Act, has defined NCIIs as infrastructures critical to national security, economic security, environment, public health/ safety and continuity of governance. There is, however no universally accepted definition of national security and the strategic community remains inconclusive on the concept. Perhaps it is a dynamic concept and presently includes factors such as environment security, economic security, energy security, food security, political security, military security, etc. In other words, national security would constitute the nation-state's ability to prevent its adversaries from using force to harm its citizens, their national interest or confidence in the capability of the nation-state, maintenance of territorial and political integrity while preserving the fundamental rights of its citizens. Needless to say, information security has become an integral part of the national security construct in modern times.

Dependence of NCIIs on ICTs

Traditionally, most infrastructures vital to national security are segregated physically and geographically as National Critical Infrastructures (NCIs). However, the advent of IT and information infrastructure that has enabled greater automation in operations and control systems, and networking of assets due to computerisation, has resulted in growing convergence of the NCIs. Consequently, the information infrastructure has emerged as one of the most critical NCIs largely due to an overarching dependence of all other NCIs on it as well as for communication, information exchange and commerce.[7] While the concept of a global information infrastructure is still being deliberated, the National Information Infrastructure (NII) as defined in the Australian Defence Doctrine Publication means:

7. Peter S. Anderson, "Critical Information Infrastructure in the Information Age", in Robin Mansell, Rohan Samarajiva and Amy Mahan, eds., *Networking Knowledge for Information Societies: Institutions &Intervention* (The Netherlands: Delft University Press, 2002), p. 188.

More and more industrial processes and government functions are relying on ICTs, resulting in higher dependence and higher cyber vulnerability that adds up to the criticality of any infrastructure.

> Comprising the nation-wide telecommunications networks, computers, databases and electronic systems; it includes the internet, the public switched networks, public and private networks, cable and wireless, and satellite communications. The NII includes the information resident in the networks and systems, the applications software that allows users to manipulate, organise and digest the information; the value added services; network standards and protocols; encryption processes; and, importantly, the people who create information, develop applications and services, conduct facilities and train others to utilise its potential.[8]

In how many different ways could the dependence on ICT impact the criticality of infrastructures which are geographically dispersed but are seamlessly interconnected through continuous flow of information exchange? There could be three major elements of ICT assets embedded in a critical infrastructure: firstly, the control systems that manage, regulate and command the behaviour of the systems and processes of any infrastructure; secondly, the Supervisory Control and Data Acquisition (SCADA) that collects the real time data samples, compares with standard data and displays it at a central location for monitoring and further achieving; and, finally, the active networking element of global technology such as routers, switches, hubs, modems and firewalls that enables and controls the flow of data on the various media such as Optical Fibre Cable (OFC), coaxial cable, Wi-Fi, satellite link, etc.

More and more industrial processes and government functions are relying on ICTs, resulting in higher dependence and higher cyber vulnerability that adds up to the criticality of any infrastructure. The

8. Gary Waters, Desmond Ball and Ian Dudgeon, *Australia and Cyber-Warfare* (Canberra: ANU Press, 2008), p.61, http://epress.anu.edu.au/wp-content/uploads/2011/08/ch0420.pdf. Accessed on November 15, 2015.

natural question that, thus, arises is: does everything that uses ICT in an industry/ business become critical? Obviously, all ICT that does not contribute to core business functions does not become critical. The systems that perform real time transfer of information for decision-making, control critical processes, offline systems that are critical to operations, autonomous control systems, and the information links between important cyber assets, including Local Area Network (LAN), Wide Area Network (WAN), radio links, Virtual Private Network (VPN), satellite link are critical. All these factors are required to be weighed and calculated based on criteria of their utility.

A systemic study on defence IT and communication infrastructure would bring out a comparative criticality score that could then be normalised and averaged to get a criticality score for further comparison with other NCIIs.

For instance, if the utility of a particular IT asset is limited, the internal functioning of the infrastructure should be given less weightage than the IT asset whose utility is in the external functioning of the infrastructure and its interaction with other infrastructures, as it would be more vulnerable, and it would be more difficult to measure the impact of its failure. Such systems in the case of the defence sector would include real time online systems of decision-making communication grids, Air Defence (AD) communication networks, offline IT assets for mission planning, critical nodes between Command and Control (C2) centres and field units, data servers, Network Operation Centres (NOC), to name a few. A systemic study on defence IT and communication infrastructure would bring out a comparative criticality score that could then be normalised and averaged to get a criticality score for further comparison with other NCIIs.

The critical elements of NII are defined by most nations as NCII. Section 70 of the IT (Amended) Act 2008 (Ministry of Information Technology, Government of India) defines NCII as the computer resource, the incapacitation or destruction of which shall have a debilitating impact

on the national security, economy, public health or safety.[9] In other words critical information infrastructure may be defined as a cyber-based system essential to the minimum operations of the economy and government, whose incapacitation or destruction would have a debilitating impact on the national security and the economic and social welfare of the state.[10] For India NCIIs include defence, banking finance, e-governance, chemical nuclear industry, space, energy and electricity, transportation, telecommunications, critical manufacturing, emergency and rescue services, law enforcement agencies, water suply, public health, sensitive government organisations, etc.[11]

Interdependence of NCIIs and Government's Dilemma

In the context of critical infrastructures, interdependency may be defined as a bilateral relationship between two infrastructures through which the state of each infrastructure influences, or is correlated to, the state of the other; more generally put, two infrastructures are interdependent when each is dependent on the other.[12] The interdependence of various infrastructures compounds the vulnerabilities and severity of impact in case of disruption of any element. The more complex the networks are, the more obscure it becomes to assess the risk of failure and its cascading impact on other infrastructures. In such a scenario, legitimate governments are tasked to carve out a defence and protection strategy without having credible and sufficient knowledge of the critical infrastructures and information infrastructures that are critical to healthy functioning of interdependencies. While much of the NCIIs are spread beyond pure government entities, the challenge to government agencies lies in being able to identify, understand and analyse these interdependencies that are, at times, trans-border in nature and are interlinked through complex topologies. As information

9. Ministry of Law and Justice, Government of India, " The Information Technology (Amendment) Act, 2008", http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf
10. Presidential Decision Directive on Critical Infrastructure Protection, United States, May 22, 1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm. Accessed on November 15, 2015.
11. Rinaldi, n.2, p. 14.
12. Ibid., p. 14.

infrastructure is weaved seamlessly through critical and non-critical infrastructures, segregation of critical ones is a painstaking task that requires the involvement of the owners and operators of these infrastructures in the process.[13]

Levels of Interdependencies

Interdependencies among these infrastructures may be seen broadly at five levels, namely: the hardware, the software, the information itself, the skinware (i.e. people) and the power supply.[14] While the interdependencies at the hardware level reside in computers, sensors, transmission media such as OFC, land line cables and wireless media, the transmission towers and satellites, at the software level these are evident right from the protocols, firewalls, processes and encryption level. The information level interdependencies mean the shared databases, the voice, text, imageries, and facsimile forms of information in transit. Without power supply, none of the technological benefits can realised. Some consider the Uninterrupted Power Supply (UPS) as a part of hardware but without mains supply, the UPS has a limited life. The most important of all the interdependent components of NCIIs today is at the skinware level. These constitute the people who are global citizens working for the development and maintenance of all information systems in a highly complex, distributed and interconnected way across systems, nations, sectors and entities.

For instance, the ownership and maintenance of NCIIs is shared by both the public and private sectors, thus, is subject to global competition and market forces to a certain extent. The majority of telecommunication service providers and Internet Service Providers (ISPs) for a nation today may be foreign multinational corporations using the Commercially Off The Shelf (COTS) hardware systems and software sourced from foreign Original Equipment Manufacturers (OEMs). The developers and work force for such systems may belong to any nation's private sector. Symentec Corporation,

13. "International Approaches to Critical Information Infrastructure Protection", http://www.owasp.in/talks/international-approaches-to-crotical-information-infrastructure-protection/. Accessed on November 15, 2015.
14. Rinaldi, et. al., n.2, p.63.

in its study on Critical Infrastructure Protection in 2010 depicted CII as "business and industries whose importance is such that if their cyber networks were successfully breached and disabled, it could result in a threat to national security'". The private corporations own a significant part of a nation's critical infrastructure.[15] While globalisation provides us with the ability of getting the best of products, services and manpower, it denies governments the sole ownership or control over the functioning of NCIIs. This raises the possibilities of covertly implanting of malware, back doors, Trojan horses by the adversaries for exploitation in critical times in future. This full spectrum interdependence of critical infrastructure on NCIIs coupled with their cross-border interconnectedness with other infrastructures, has given rise to new forms of vulnerabilities and threats, requiring a systemic perspective of security and resilience.

Perspectives of Interdependencies

There are challenges of coordinating the public and private sectors for equal levels of preparedness and training to respond to attacks. Interdependencies may be seen in at least four contexts:

- **Geographical:** Geographical interdependency occurs due to the spatial proximity of various elements of different infrastructures, with the possibility of a negative impact or disturbance on one, due to disruption in the other. For instance, a fire at the Indian Oil Corporation (IOC) dump will have a severe negative impact on a Bharat Sanchar Nigam Limited (BSNL) communication hub that is located in the close vicinity.
- **Physical:** Physical interdependency is a result of the dependence of one infrastructure on the material output of the other infrastructure. So it is an interdependence caused by a break in the supply chain. For instance, if coal supply to thermal power plants is disrupted due to disruption in the railways' communication and control infrastructure, the power generation would be severely impacted, or vice-versa, if the railways are denied power supply, they may not be able to deliver coal to the thermal

15. Symantec 2010 Critical Infrastructure Protection Study, http://www.slideshare.net/symantec/symantec-2010-critical-infrastructure-protection-study. Accessed on November 15, 2015.

plants. In other words, whenever a physical output of one infrastructure is used as the input of the other infrastructure for its operation, there exists a physical interdependence.

- **Cyber:** Cyber interdependencies are the most challenging ones. They occur due to information links between infrastructures. When the information passed from one infrastructure makes the other infrastructure dependent on that information, it falls under the category of cyber interdependence. Because of exponential growth in networking efforts in India, the assessment of risk due to cyber interdependency is the most challenging task facing the security agencies.
- **Logical:** Logical interdependency exists due to the logical consequence of something happening to one infrastructure on the other where there is no other type of interdependency like geographical, physical or cyber. This may be understood by the analogy of how the performance of a big blue-chip corporation impacts the stock market indices of a nation. For example, on September 15, 2008, when the Lehman brothers filed for chapter 11 bankruptcy protection with the US Bankruptcy Court in New York, it resulted in the largest drop by points in a single day since the days following 9/11 (the Dow Jones closed down just over 500 points), sending shiver waves of an ensuing recession throughout the world.[16] Furthermore, the infrastructures could be directly or indirectly connected to each other, with intersections being linear or complex among them. Thus, the complexity gives rise to a relative degree of dependencies among infrastructures.

Interdependencies and Failure Types

In order to calculate interdependencies based on geographical location, physical characteristics, cyber or logical, these could be segregated in a two-pronged approach of dependency, based on the type of relationship, namely, linear or complex. When this is extrapolated on the failure types in ascending order of severity such as dampening, distributed, cascading

16. MK Sharma, *Cyber Warfare: The Power of the Unseen* (New Delhi: KW Publishers Ltd, 2012), ch 1, p.35..

or escalating, it would give the required interdependency and failure impact scale. As is understandable, the failure could range from just the dampening effect on an infrastructure to a distributed impact on other interconnected infrastructures to a further severe cascading impact on several infrastructures as the second order or third order impact, and the impact could also be escalating in the physical domain with multi-sector disruptions in more severe cases.

Table 1: Interdependencies and Failure Types Weightage Matrix

	Geographical		Physical		Cyber		Logical	
	Linear	Complex	Linear	Complex	Linear	Complex	Linear	Complex
Dampening	1	2	3	4	5	6	7	8
Distributed	2	3	4	5	6	7	8	9
Cascading	3	4	5	6	7	8	9	10
Escalating	4	5	6	7	8	9	10	11

The proposed metrics tool is based on the comparative degree of the complexity of the relationship and relative difficulty in assessing the impact. IT assets are geographically well dispersed so are given least weightage. The cyber relationship of dependence is considered more complex than physical dependence and weighed accordingly. And logical dependence is given the highest weightage due to the high difficulty levels of assessing the impact of logical relationships. By the same premise, dampening, distributed, cascading and escalating effects have been weighed in an ascending order.

Criticality Analysis of NCIIs

As some would ask, while the defence sector is one of the NCIIs, does mundane information like about a troop's game in the evening fall into the critical information category, thereby to be provided topmost protection? How does one decide what element of the whole infrastructure is more critical than the others? How does one go about assessing the comparative criticality of multiple NCIIs? The rationale behind criticality analysis is based on the argument that if everything is equally critical, then everything will be recovered at the same time, but the recovery time could be lengthier. Similarly, a criticality analysis yielding different levels of criticality will

yield varying recovery times, with the most important information assets being recovered first and the least important potentially last. The approach to NCII protection is multifaceted and should be bottom up, with individual organisations of NCIIs at the bottom and nodal government agencies at the top. The criticality analysis of the NCII has to begin at the organisational level, followed by the sector, and then the national level.

While it is amply clear that the concept of criticality is a complex function of multiple parameters, one of the many ways to evaluate the relative criticality within NCIIs could be through collecting and synthesising on all the defined criteria like redundancy, threshold MTTR (Mean Time To Restore), impact severity, probability, impact type, interdependency and IT dependency in order to arrive at relative rankings of criteria through a mathematical series of iterations.

For instance, at the **moment of failure** at a given time, the criticality of a particular infrastructure could be far higher than its perceived value. These factors are difficult to be taken into consideration. **Redundancy** play an important part in evaluating criticality: if the system has built-in redundancy, its disruption will not impact the process. In other words, a system without an alternative is both critical and vulnerable. **Mean Time To Restore** (MTTR) is the time required by any hardware/software to get repaired or human element to get restored functionalities. Thus, the higher the MTTR, the higher is the criticality of the infrastructure. This brings the issue of maintainability and training to the fore.

Similarly, the **degree of impact or severity** of any asset or service in the NCII will have a proportionate contribution to criticality. The impact of the severity could be allocated on the basis of percentage of population or service that would be affected if a particular asset is disrupted or made unavailable. Also, along with high severity, a higher **probability** of disruption or unavailability would make that asset more critical. This is akin to risk assessment where the chances of failure are combined with an estimation of the negative impact, and it requires highly specialised people to calculate this. These complex interrelations, established due to a multitude of logical, physical and electronic inter-connections through

Considering the vast scope of NCII protection, and keeping in view the threats and vulnerabilities, its protection is a strategic challenge requiring joint efforts from the government, the private sector and the economy at large.

which a vast amount of intricate feedback, and feed forward information travels among various elements of the infrastructures, create interdependencies. While the infrastructures that are increasingly cyber dependent would have a high degree of **cyber interdependence** within that system, on the other hand, infrastructures with a high degree of geographical and physical interdependence would have a higher impact on the other dependent infrastructures, thus, should be considered more critical. Furthermore, the impact type could be defined based on the factors a nation considers while defining NCII, which are generally concerned with the impact on the health, security, economic or social well being of people.

MAPPING THE THREAT LANDSCAPE TO NCIIs

Analysis of Threat to NCIIs

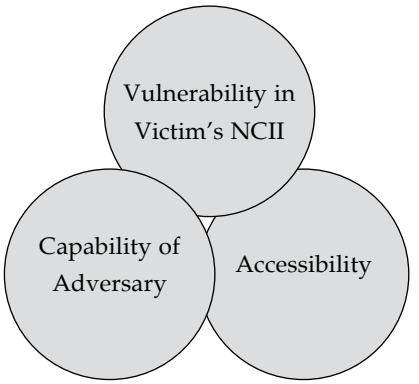
The NCIIs constitute a wide array of assets and service, from information systems, to data and associated assets that facilitate, equipment and personnel. Considering the vast scope of NCII protection, and keeping in view the threats and vulnerabilities, its protection is a strategic challenge requiring joint efforts from the government, the private sector and the economy at large. The organisations (governmental and private) across the globe face attacks of varied nature on their systems and infrastructure, primarily for the following purposes:

- **Exploitation Purposes:** The case of Ghost Net was the first of its kind where the virus was used for economic and political espionage purposes. The virus was capable of identity theft and designed to target government IT systems.

- **Disruption Purposes:** The Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks or spams generated using botnets are mainly used to disrupt the services or functions and the legitimate users are denied access to the service. The malware Stuxnet was found to be targeting the disruption of the Iranian nuclear programme.
- **Destruction Purposes:** This scenario has not yet materialised (except for the Stuxnet attack on the nuclear facility of Iran at Natanz that destroyed the centrifuges by overspeeding the convertors) but, given the increasing pervasiveness of ICT in all critical infrastructures of nations, it cannot be ruled out in future conflicts. The attacks on infrastructure vary in terms of nature, capability and targeted system. A variety of attacks that could be launched include targeted scanning, probing and exploration of networks and IT infrastructure, large scale defacement and semantic attacks on websites, malicious code attacks (i.e. virus, worm, Trojans, botnets), identity theft attacks, large scale spoofing, DoS and DDoS attacks, Domain Name Server (DNS) attacks, application level attacks and router level attacks.
- The possible targets for such attacks would obviously constitute cyber assets such as sensitive and critical information infrastructure, infrastructure of data centres and network operation infrastructure, routers, switches, database and Domain Name Servers (DNS), web portals, and satellite network communication systems. Furthermore, the SCADA systems, centralised and distributed control systems of the organisation, database administration, individual users, including senior executives and officials would also be prime targets for such attacks by adversaries.

The possible targets for such attacks would obviously constitute cyber assets such as sensitive and critical information infrastructure, infrastructure of data centres and network operation infrastructure, routers, switches, database and Domain Name Servers (DNS), web portals, and satellite network communication systems.

Fig 1: Cyber Attack Convergence



Attack Convergence

The real threat to a system arises when the vulnerability, accessibility of the system and capability of the adversary to mount an attack converge (Fig 1). Vulnerability could be an identified weakness, an attack on which could be decisive. It could arise out of an inadequate security procedure or a weakness due to failure to follow proper security processes designed to prevent unauthorised access. The physical parts also become vulnerable such as the fibre optic cable or radio/microwave transmission towers. It may be a product of interdependence and complexity or a product of the time required to repair the infrastructure or reinstate operational availability/ business continuity. Therefore, undoubtedly, the critical components that significantly affect functionality and require extended time to repair or replace become the preferred targets for adversaries. Towards achieving the attack capability, the accessibility by the adversary is mainly through breach of information assurance. The target could be either the elements of information assurance, the component of hardware or software, the information, the people who operate and maintain it or the power supply, or it may be a combination of all these.

Furthermore, cyber threats can be unintentional or intentional. Unintentional threats can be caused by software upgrades or maintenance procedures that inadvertently disrupt systems. Intentional threats include both targeted and untargeted attacks from a variety of sources, including

criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists.[17] Nations use cyber tools as part of their information gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrines, programmes, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of citizens across the country. Terrorists seek to destroy, incapacitate, or exploit critical infrastructure in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence.[18]

APPROACHES TO NCIIs PROTECTION

Defence-in-Depth Approach

The attack surface includes three primary constituents; network, software and skinware (human beings). The security architecture encompassing the in-depth architecture needs to address these interrelated considerations. While on the **networks attack surface**, the attack will often be delivered via a network (tunnels or network attacks), a **software attack surface**, with a primary focus on web applications, focusses on the union of the code, interfaces, services, protocols, and practices available to all users, with a strong focus on what is accessible to unauthenticated users. The **human attack surface** considers social engineering, errors, trusted insider, death and disease (human factor). Being able to clearly identify an organisation's attack surface is critically important to developing a threat vector-based defence-in-depth architecture. The techniques or best practices developed and adopted by an organisation to reduce the attack surface are: reduce the amount of running code, reduce access to entry points by untrusted

17. Gregory C. Wilshusen, "Cyber Security Challenges in Securing the Electricity Grid", United States Government Accountability Office (Testimony Before the Committee on Energy and Natural Resources, U.S. Senate), July 17, 2012, n. GAO-12-926T, p. 7, see http://www.gao.gov/assets/600/592508.pdf. Accessed on January 24, 2013.
18. Ibid., p. 8.

users, reduce privilege to limit damage potential, anonymous code paths, reduce attack surface early; and measuring the attack surface. There are five primary architectural approaches to achieving defence-in-depth: uniform protection, protected enclaves, threat vector analysis, information-centric protection, and role-based access control.[19]

The process of infrastructure defence should first identify the assets to be protected, assign a priority to the identified assets so that the most critical assets from a business continuity perspective could be worked upon first. Later, the strategy employs brainstorming sessions to find out the possible and probable ways the threat could get access to the critical assets. The last exercise would be to figure out how to place controls on the vectors to prevent the threat from crossing the vulnerability. The adversary exploits the vulnerabilities and possesses a definitive motive which varies according to the actors such as national governments, terrorists, hactivists, industrial espionage, or organised crime. The medium adopted by the adversary is the threat vector which could vary from a mobile to a cloud or a portable memory drive or a human.

Multi-Layered Criticality Assessment Approach

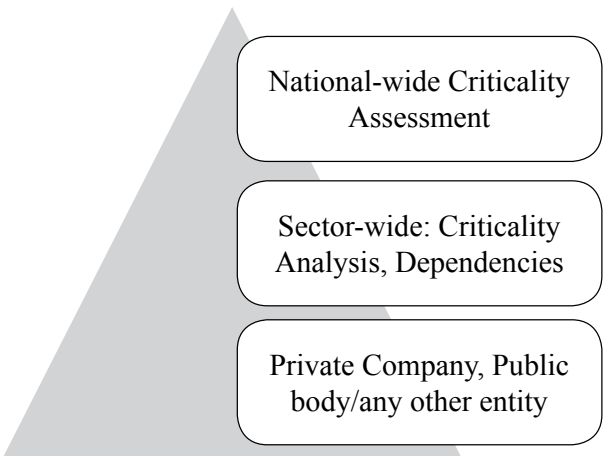
The approach to protection of critical information infrastructures could be divided into three layers[20]:

- **Layer 1:** The basic concern of any organisation (private company, public body or any other entity) is to protect its own business operations, ICT assets and systems, from security threats. This layer forms the base of the pyramid and the exercise is carried out in a comprehensive manner by all the organisations which are part of the critical infrastructure of a nation state.

19. Stephen Northcutt, "The Uniform Method of Protection to Achieve Defence-in-Depth", *SANS Technology Institute Security Laboratory*, February 26, 2007, see, http://www.sans.edu/research/security-laboratory/article/367. Accessed on July 23, 2012.
20. Marianthi Theoharidou, Panayiotis Kotzanikolaou and Dimitris Gritzalis, "A Multi-layer Criticality Assessment Methodology Based on Interdependencies", *Computers & Security* (USA), 2010, pp. 12-14, see http://oplab.im.ntu.edu.tw/download/98/0615/20100615_A%20multi-layer%20Criticality%20Assessment%20methodology%20based%20on%20interdependencies.pdf. Accessed on July 25, 2012.

- **Layer 2:** The scope of a sector-wide criticality analysis involves all the organisations that are members of the sector. An identified individual sector is analysed in detail during a sector-wide criticality analysis and dependencies with other sectors are also examined. The data collected from Layer 1 is utilised to draw inferences for the Layer 2 sectors.
- **Layer 3:** This execution is carried out by a national body (e.g. a government) which is interested in protecting the entire critical infrastructure. A nationwide criticality assessment needs to analyse security threats that are outside the scope of a single sector, but which pose an impact for the whole society. The summation of criticality analysis at the national level is conducted at this layer.

Fig 2: Three-Tier Approach for Criticality Assessment



The bottom up approach begins with an individual organisation, and the data generated by the bottom layer is used as an input for the upper layer. The scope of different layers lies with different actors, with the government and policy institutions at the top. The policy measures flow from top to bottom. The adopted CII protection strategy and practices identified by the top layer percolate to the subordinate layers and the implementation takes place at the individual constituents level of the critical infrastructure protection architecture.

Identification of Critical Asset Elements

Assets are the key enabler in the functioning of an organisation. Some of the assets are critical to the key business functions and processes. While building a defence against failures and attacks, it is imperative to identify the critical assets. Given below are the critical asset elements and their description, which helps identify the critical assets[21]:

Table 2: Critical Asset Elements and Description

Critical Asset Elements	Description
Personnel	Staff, management, and executives necessary to plan, organise, acquire, deliver, support, and monitor mission-related services, information systems, and facilities. This may include groups and individuals external to the organisation who are involved in the fulfilment of the organisation's mission. Security management personnel are also included.
Automated Information and Control Systems	All electronic and telecommunications equipment, hardware, and software (operating systems, communications, and application packages), counter-measures, and/or safeguards that are part of, or support, critical assets.
Non-Automated Information and Control Systems	All other systems, internal and external, that are part of or support critical assets (for example, paper archives, personnel and accounting procedures, publications).
Data	All data (in electronic and printed form) and other information that are part of, or support critical assets. These include numbers, characters, images, or other means of storing information in forms that can be: (1) assessed by a human; or (2) input into a computer, stored and processed there, or transmitted digitally.
Facilities and Equipment	All facilities and equipment that form part of, or support, critical assets, especially those that house and support Information Technology (IT) assets.

Best Practices as a Protection Strategy

If IT network management follows good practices, 85 percent of cyber

21. Critical Infrastructure Assurance Office of the US Department of Commerce, "Practices for Securing Critical Information Assets", p. 19, see http://www.infragard.net/library/pdfs/securing_critical_assets.pdf. Accessed on July 25, 2012.

attacks may be prevented.[22] Good practices have emerged as a prominent strategy to thwart attacks against IT networks and reduce the attack surface. The best practices could be moulded into six wide categories and further described as the following:

Table 3: Description of Best Practices as NCII Protection Strategy

Protection Strategies - Best Practices	Description
Redundancy	Operation centre Communication systems, lines Access possibilities
Degradation Modes	Alternative processes Separation of control areas
Collaboration	With public authorities Within sector (e.g. mutual assistance, facilities)
Tightened Access Control	Detailed, restrictive user access management concepts Application of special technologies (e.g. IRIS-Scan)
Early Warning	CERT - sector specific, national, regional, international networks specific security messages (e.g. validation of principles, alerts, warnings)
Training, Exercises	Complexity (communication, coordination) Extension (local, department, company) Sector specific (national, international) Frequency (planned, started, regularly, weekly, yearly)

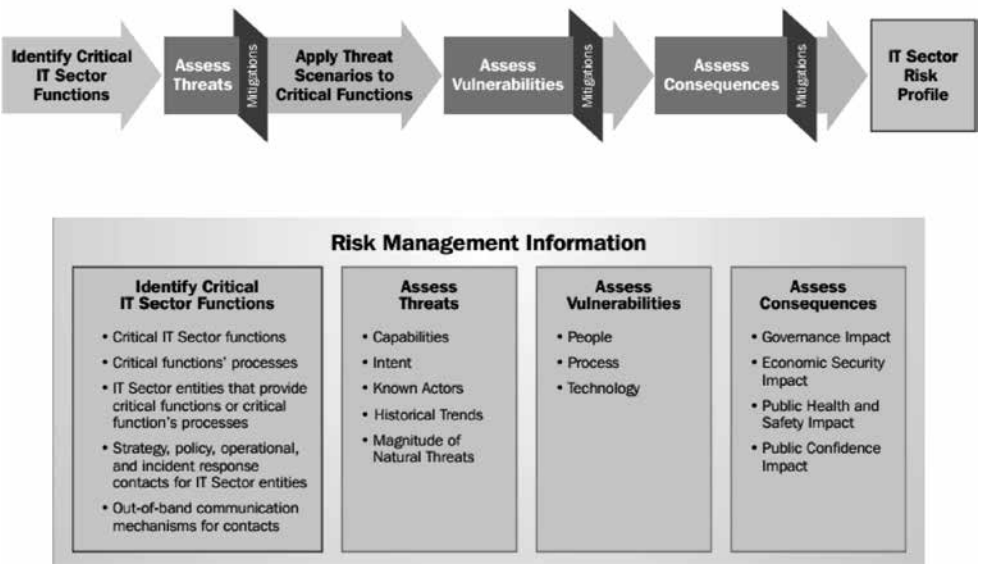
Crisis Management and Business Continuity Plan Approach

Risk is defined as the probability that a threat will cross vulnerability. Risk is hard to calculate, but a rough idea could be generated by considering the attack surface, the exposure, and the reachable and exploitable vulnerabilities. In other terms, risk is a functional analysis of the level of threat, the degree of vulnerability and the impact. Impact and threat are constant and beyond control, while vulnerability can be reduced. The means of risk reduction could be integrated in the network architecture such as firewall usage; network segregation; management controls, ranging from planning to risk assessment; operational controls,

22. "Senate Panel: 80 Percent of Cyber Attacks Preventable", see http://www.wired.com/threatlevel/2009/11/cyber-attacks-preventable/. Accessed on July 26, 2012.

for instance, personnel security, contingency planning, configuration management; technical controls, such as authentication, access control, systems and communication protection.

Fig 3: Risk Management and Assessment Process Flow and Information
(Source: U.S. Department of Homeland Security)



A crisis is defined as a significant threat to operations that can have negative consequences if not handled properly. In crisis management, the threat is the potential damage a crisis can inflict on an organisation, its stakeholders, and an industry. A crisis can create three related threats: public safety, financial loss, and reputation loss[23]. A crisis management plan is designed to provide guidelines for a practical communications system that is adaptable for any crisis situation. It is part of an overall safety and emergency preparedness plan and a standard part of the overall strategic planning process.[24]

23. "Crisis Management Plan", *e-Governance Bulletin from Gujarat Informatics Ltd.*, vol. 7, no. 7, 2010, pp. 1-5, see http://www.gujaratinformatics.com/pdf/Crisis%20Management%20Plan.pdf. Accessed on July 7, 2012.
24. "A Guide to Developing Crisis Management Plans", NTA's Market Development Council, March 2000, p. 1, see http://www.ntaonline.com/includes/media/docs/crisis-mgm-plan-020703.pdf. Accessed on July 26, 2012.

The business continuity planning is a proactive action plan to prevent or manage the consequences of a disruption, and mitigate the impacts on the core business functions. It could include all possible threats and catastrophic events of natural disasters such as floods / earthquakes as well as man-made acts of terrorism and sabotage. The effect of being closed for business, however temporarily, will cost the organisation monetary loss. The expense isn't limited to the immediate problem of restoring services or production – there's the lost time, ruined stock, ongoing costs of rebuilding confidence in the customer base and potentially amongst shareholders, plus the knock-on effects such as an increase in insurance premiums. A comprehensive business continuity plan covers the safety of data and information in the case of outages due to hardware or network failures. As the businesses are becoming heavily dependent on IT infrastructures, there is constant risk to continued availability, reliability, and recoverability of resources. The dependency on information processing and telecommunications for automated information systems can seriously impact the performance during disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire) from a variety of sources such as natural disasters to terrorists actions, and even cyber crime.

The crisis management plan for countering cyber attacks and cyber terrorism outlines a framework for dealing with cyber related incidents. The plan needs a coordinated, multi-disciplinary and broad approach for rapid identification, information exchange, swift response and remedial actions to mitigate and recover from malicious cyber related incidents impacting critical processes and assets.

A cyber related incident of national significance may take any form: an organised cyber attack, an uncontrolled activity such as a computer virus or worms or any malicious software code, a national disaster with significant cyber consequences, or other related incidents capable of causing extensive damage to critical infrastructure or key assets. Large scale cyber incidents may overwhelm corporate resources and services by disrupting the functioning of critical information systems and can have a cascading effect on other business institutions and the government. The strategy for

The organisations operating critical information infrastructure have been advised to implement information security management practices based on the International Standard ISO 27001.

crisis management at organisational level is divided into four stages:

Pre and Post-Incident Preparation

This phase involves establishing and training an incident response team and acquiring the necessary tools and resources for incident analysis and response.

- **Detection and Analysis:** Detection is necessary to alert the organisation whenever incidents occur. Identification of the attack type, scope and vectors and then implementation of the appropriate controls to contain the attack and quarantine any compromised host is done during this phase.
- **Containment and Mitigation:** Strategies and procedures for containing the incident have to be predetermined to limit continued impact.
- **Post Incident Activity:** This phase would involve a follow-up for each incident, for technology upgrade, future use and to document lessons learnt. Also to create a formal chronology of events and create the monetary estimate of the amount of damage caused in terms of any loss of software and files, hardware damage, and staffing cost.

India's Cyber Security Institutions: A Review: The Government of India has formulated a crisis management plan for countering cyber attacks and cyber terrorism for implementation by all ministries / departments of central government, state governments and their organisations and critical sectors. The organisations operating critical information infrastructure have been advised to implement information security management practices based on the International Standard ISO 27001.[25] Such practices are being adopted by information security agencies and governments across the globe, while being integrated with policy for CII protection.

25. Press Information Bureau, Government of India, "Crisis Management Plan for Cyber Attacks", May 6, 2010, see http://pib.nic.in/newsite/erelease.aspx?relid=61597. Accessed on July 26, 2012.

India has elevated its response to protect the CII in the recent years. The legal framework to address the threats emanating from cyber space, especially cyber terrorism to the CII was developed in the amendment made in 2008 to the Information Technology (IT) Act, 2000. The response includes addressing the need to develop defence against, as well as to create an emergency response for, cyber attacks. Section 66F of the IT Act (Amendment), 2008, identifies cyber terrorism to be a threat to CII as it could be used to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people. The computer resources might be used to conduct actions leading to the death of, or injuries to, persons, or damage to, or destruction of, property or damage or disruption of supplies or services essential to the life of the community or adversely affect the CII.[26] Section 70A of the Act designates an organisation of the government as the national nodal agency responsible for all measures including Research and Development (R&D) relating to protection of CII. This responsibility was given to the National Critical Information Infrastructure Protection Centre (NCIIPC), established under the aegis of the National Technical Research Organisation (NTRO) in December 2012.[27]

The computer resources might be used to conduct actions leading to the death of, or injuries to, persons, or damage to, or destruction of, property or damage or disruption of supplies or services essential to the life of the community or adversely affect the CII.

In this role, the NCIIPC will have the responsibility of identifying threats in advance and monitoring the cyber space of the critical assets on a real-time basis. There is a division of responsibility between the NCIIPC and Indian Computer Emergency Response Team (CERT-IN).The NCIIPC will only look after absolutely critical sectors[28] that have a high threat perception

26. n.9.
27. Ibid., pp. 28-29.
28. These sectors have been identified as energy (power, coal, oil and natural gas), transportation (railways and civil aviation), banking and finance, telecom, defence, space, law enforcement and security.

coupled with greater dependence on ICT, while the other sectors will be with CERT-IN.[29] The mandatory requirement for critical sector organisations and ministries is to appoint a Chief Information Security Officer (CISO) as the point of contact for all interactions with the NCIIPC. The CII protection strategy of India is moving towards a collaborative model where the private sector is part of the initiatives taken by the government. In such a move, a joint working group with representatives of industry associations to bring out guidelines for the protection of critical information infrastructure in India is being set up by the NCIIPC.

TOWARDS DEVELOPING A STRATEGY OF PROPORTIONATE RESPONSE

Attribution: A Priori to Execute Proportionate Response

One of the most crucial elements towards development of proportionate response is the attribution capability of the nation. The severity of the response would depend on the degree of accuracy and surety that could be attributed to a cyber attack. For instance, even for a severe cyber attack, if the level of attribution is low, the authorities may choose a restricted response, though the capability for a full-fledged counter may exist. Alternately, in a similar scenario of low level of attribution, the authorities may choose a low value target for counter-attack to avoid escalation and international criticism whereas the incident may have been demanding a full scale counter-attack against a high value target. Furthermore, in some situations where the there is no verifiable evidence for the source of the attack, the policy-makers might be forced to take no action. Such is the importance of the attribution capability in delivering a proportionate response. The next most important aspect for implementation of this strategy is analysis of the impact of a cyber attack on any NCII which has been dealt with in some detail earlier in the article. Also, one doesn't need to overemphasise the fact that the range of responses available to the government to exercise against a cyber attack are not limited to action in cyber space alone; they

29. Ibid., pp. 28-29.

could include anything from diplomatic arm-twisting, economic strangulation to a military strike, with their own associated risks, of course.

It is important to clarify that the proposed response matrix is more appropriate for tackling the state sponsored cyber attacks, and for the cyber disruptions or destruction perpetrated by individuals or cyber criminal groups not supported by the states, the law enforcement actions would be more appropriate.

Primacy of Covert Operations

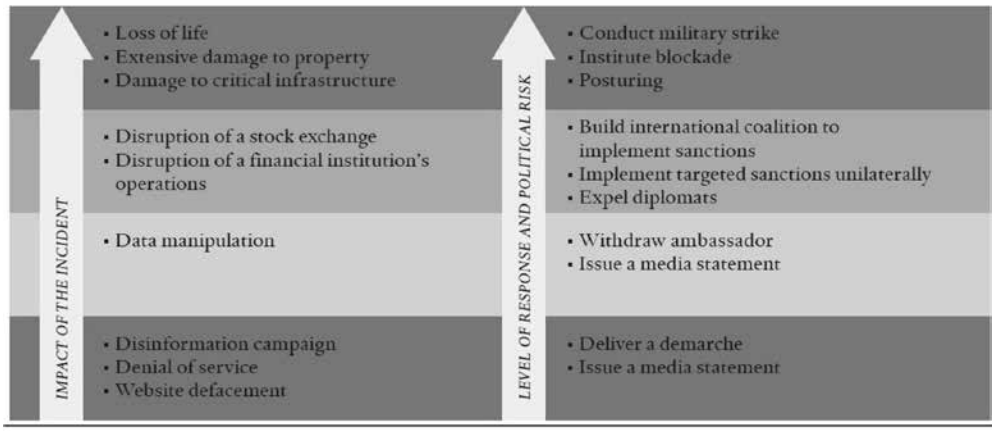
In most instances, the cyber response would be delivered by covert means but the more important question that remains is whether we have the payload developed and designed specifically for the designated target. Developing such custom cyber payloads entails prior understanding of the target and a lot of espionage to pinpoint the security gaps in the target surface. It took years to develop the Stuxnet, based on a particular model number of the convertors manufactured by Siemens and then to develop the ability to write a code within the code in the programme of the SCADA system. The primacy of covertness also emanates from the fact that cyber weapons are not reusable, thus, an overt response may deny reuse of the weapon on other target surfaces, besides exposing nation-states to international condemnation. Also any kind of outsourcing of such cyber attacks through patriotic hackers or non-state actors comes at the cost of losing out on the command and control function in such responses, in case a state wants to exercise a strategic pause to allow a diplomatic solution to take place during the conflict. Therefore, decision-makers would like to retain C2 on all levers of power, including covert operations in the cyber domain. Towards this, we need to develop a response framework proportionate to the impact factor of a cyber attack on any NCII beforehand. While in the event of an actual attack, the response would be specific to the incident, the framework so developed would act as a basic guiding vector for the policy-makers to consider the response options of applying various levers of state power for various levels of cyber incident escalations at a glance.

Proportionate Response Framework

One such framework depicting different possible cyber incident impact and policy options based on the principle of proportionality, as proposed by Tobias Feakin,[30] is shown below in Fig 4. The range of cyber incidents in the ascending order of severity are plotted from simple website defacement at the bottom to loss of life at the top and against each of them are the possible levels of proportionate responses ranging from issuing a media statement at the bottom to a kinetic military response on the top of the spectrum. As is evident, there are inherent political and legal risks associated with each decision taken by the policy-makers as we go up the level of response options. At this juncture, it is important to clarify that the proposed response matrix is more appropriate for tackling the state sponsored cyber attacks, and for the cyber disruptions or destruction perpetrated by individuals or cyber criminal groups not supported by the states, the law enforcement actions would be more appropriate. This only reiterates the cruciality of developing a more matured attribution mechanism within our country.

30. Tobais Feakin, "Developing a Proportionate Response to a Cyber Incident", Australian Strategic Policy Institute, Council on Foreign Relations Press, Australia, August 2015, http://www.cfr.org/cybersecurity/developing-proportionate-response-cyber-incident/p36927?cid=nlc-publications-publications_quarterly-fall_2015-link32-20151109&sp_mid=50037808&sp_rid=Z29uZGVlemFAZ21haWwuY29tS0.

Fig 4: Proportionate Response Matrix to Escalating State-Sponsored Cyber Incidents



In Defence of Proportionate Response

Whenever a serious cyber attack is reported, there is always public pressure on the government to take a disproportionate retaliatory response to deter any future recurrence but good international relations wisdom suggests that the country take only a proportionate measure necessary to defeat / nullify any ensuing cyber attack or disruption. Such approach inherently arrests the escalation from the victim country's side, in terms of scale, scope, duration and intensity. In fact, proportionality of response is good old statecraft practised as a tool of maintaining international relations in all domains, be it expulsion of diplomats for skirmishes on the borders or imposing economic sanctions for more serious incidents. A proportionate response also gives a country the upper hand to garner international support to punish or isolate the attacking nation.

As depicted in Fig 6, while a simple web defacement may warrant only a public denouncement, for loss of data of an NCII through exfiltration by state sponsored cyber means, the proportionate response might even be up to expulsion of diplomats, if the disruption impacts the economy of the country. When the impact of a cyber incident is such that it affects the economy adversely, there is a range of proportionate response options,

When the impact of a cyber incident is such that it affects the economy adversely, there is a range of proportionate response options, including diplomatic pressure, freezing of financial transactions of the individual in the source country, and imposing international sanctions.

including diplomatic pressure, freezing of financial transactions of the individual in the source country, and imposing international sanctions. Military posturing or military action is envisaged as a proportionate response only when the cyber attack causes physical damage to the people and property of the nation.

The Limitations of the Proposed Framework

For such a framework to become more pragmatic, the criticality analysis of NCII would have to be more rigorous and objective. It demands involvement of the public and private stakeholders in NCII, from the operator level to the top decision-making level in the process of developing a more comprehensive response framework. On the one hand, the policy-makers would need inputs from the analysis of criticality in determining the adverse impact of a cyber incident on the functioning of a particular NCII and cascading impact on other NCIIs, and, on the other hand, they would have to weigh the impact of choosing a response option on international relations, on our standing, and on military operations in a highly dynamic and complex decision-making environment. It would demand continuous evaluation damage to our NCIIs by the cyber attack and also continuous evaluation of the risk associated with different response options. The proposed response matrix is but rudimentary at its best for deciding the course of action, however, it could certainly act as a initial point for broad reference in order to arrive at the best course of action as assessed in the light of many other factors presenting themselves during a crisis.

CONCLUSION

NCIIs are characterised by interdependence, interconnectedness, distributedness and complexity. Any kind of cyber disruption or attack

could lead to a cascading impact on other sectors and loss of sensitive and strategic data, thereby, jeopardising national security. While India has taken some remarkable steps at the national level in recent years, protection of the NCIIs is an arduous endeavour that demands simultaneous efforts at the individual organisation, sector, national, regional and international levels.

Not all the communication/network of an identified NCII, is equally critical, thus, it requires an objective analysis of the relative criticality of various elements based on mathematical modelling of the severity of impact by different types of attacks. Such differentiation would allow policy-makers the options of a proportionate response in a given situation. However, when undertaking criticality analysis of NCIIs, there would be constraints in the form of technical, practical and financial feasibility for both public and private stakeholders due to its inherent criss-cross spread among individual organisations cutting across industry sectors and eventually converging at the national level.

The criticality analysis should begin by identifying the parameters of criticality based upon different industry sectors which are part of the NCII. While Redundancy, Threshold Mean Time To Restore (MTTR), impact severity/degree, probability, impact type, interdependency, and ICT dependency are major indicators for analysis of criticality, two parameters, namely, impact severity and impact are considered to have high significance while computing criticality of an asset.

A defence-in-depth methodology needs to understand and analyse the interconnected, interrelated and highly interdependent nature of the Critical Infrastructure (CI) and the information infrastructure. The protection strategy then would have to address the technological, policy and legal dimensions. The emerging challenge before nation-states is to develop a deep understanding of implications of the policy framework and technological implementation as well as to find the right balance between offensive and defensive capabilities.

The strategy should be divided into three layers with a bottom-up approach which begins with an individual organisation. The data generated by the bottom layer is used as an input for the upper layer. The sector-wide

and national level protection strategy should be built at the middle and top layers respectively. The policy implementation should be a top-down process where the adopted NCII protection strategy and practices identified by the top layer percolate to the subordinate layers and the implementation would take place at the individual constituents of the critical infrastructure protection architecture.

Best practices should be an integral part of the strategy, followed with stringent implementation and verification mechanisms. This would reduce the attack surface significantly. The assessment of NCII threats and vulnerabilities, identification of critical processes and assets, adoption of best practices, adherence to guidelines and real-time response to cyber attacks on any of the NCII sectors will help India develop safe, secure and resilient information infrastructure for critical sectors of the nation.