DEFENDING INDIA'S CRITICAL INFORMATION INFRASTRUCTURE

THE DEVELOPMENT AND ROLE OF THE NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTRE (NCIIPC)

SAIKAT DATTA
INTERNET DEMOCRACY PROJECT

With the establishment of the National Critical Information Infrastructure Protection Centre (NCIIPC) in 2014, India has taken an important measure towards strengthening its cybersecurity. But while the establishment of NCIIPC as such is a positive step forward, several shortcomings mark, however, its implementation.

In this paper, I will first briefly outline the origin and development of NCIIPC and will then go on to critically examine three challenges or limitations in particular: NCIIPC's command and control structure; fallacies in the framework that was used to rank sectors in order of criticality; and the absence of sector-specific guidelines and standard operating procedures (SoPs). As we will see, each of these contributes to important vulnerabilities remaining in India's critical information infrastructure (CII).

NCIIPC's Origin and Development

In 2008, in recognition of the rise in cyber vulnerabilities, threats and attacks as well as the emergence of new threats, India's Information Technology Act was reworked with the aim of establishing a national cybersecurity policy framework. Among the significant amendment made, several touched on the protection of India's CII. Through an amendment to section 70, the Act now defined CII as

> those facilities, systems or functions whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation.

In addition, section 70A was introduced, which laid down the mandate for the creation of a new agency to protect sectors designated as critical information infrastructure (CII). Under sub section (1) the amended clause stated that the

> Government may, by notification published in the Official Gazette, designate any organisation of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.

The mandate for the proposed agency was framed under sub section (2), stating that the

> national nodal agency designated under sub-section (1) shall be responsible for all measures including Research & Development relating to protection of Critical Information Infrastructure.

While those changes were made in 2008, the Gazette Notification by the Government of India came, however, only on January 16, 2014 – a good six years after the IT Act had been amended. It designated the National Critical Information Infrastructure Protection Centre (NCIIPC) as the national nodal agency for critical information infrastructure protection.[1]

• 1. Ministry of Communications and Information Technology, Department of Electronics and Information Technology, Notification. *The Gazette of India,* New Delhi, 16 January 2014, http://deity.gov.in/sites/upload_files/dit/files/S_O_18%28E%29.pdf.

In particular, NCIIPC's 'mission' has been defined as follows:

> to take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction, through coherent coordination, synergy and raising information security awareness among all stakeholders.

and this with a vision 'to facilitate safe, secure and resilient Information Infrastructure for Critical Sectors of the Nation'[2] (see Box 1 for NCIIPC's charter).

Box 1: NCIIPC's Charter

1. Develop mechanism to facilitate identification of CII, protection of CII through risk management and ensuring compliance of NCIIPC policies, guidelines, advisories/alerts, etc. by CIIs.

2. Lead and coordinate national programs and policies on Critical Information Infrastructure.

3. Establish national and international linkages / initiatives for the protection of CII, including R&D

4. Promote Indigenous Research and Development (R&D) relating to protection of Critical Information Infrastructure including Modelling and Simulation of Complex CII, development of CIIP tools and Threat Scenarios.

5. Develop mechanism to facilitate sharing of information on Information Security Breaches, incidents, cyberattacks, espionage, etc. among CII stake holders as well as with NCIIPC.

6. Facilitate thematic workshops and Information Security Awareness and Training Programme through PPP.

7. Facilitate capacity building towards creation of highly skilled manpower through Engaging Premier Institutes like IISC, NITs, etc. as well as private/non-government Partners working on CIIP.

8. Develop capability for real time warning system and facilitate sharing of information on emerging threats, cyberattacks, vulnerabilities, etc. with CIIs.

9. Establish sectoral CERTs to deal with critical sector specific issues.

Source: NCIIPC (2013). *Guidelines for the Protection of Critical Information Infrastructure, Version 1.0, June 2013*. New Delhi: NCIIPC, p. 6, http://perry4law.org/cecsrdi/wp-content/uploads/2013/12/Guidelines-For-Protection-Of-National-Critical-Information-Infrastructure.pdf.

• 2. Please see the NCIIPC Digital Repository: https://nciipc.gov.in/.

Limitation 1: Including All Relevant Stakeholders

What are some of the limitations that NCIIPC has had to work with or around during its period of existence so far? A first one has to do with the institution's command and control structure.

When it was founded, NCIIPC was placed under the National Technical Research Organisation (NTRO),[3] a technical intelligence agency created as part of India's security architecture reforms in the aftermath of the Kargil war with Pakistan.[4] NTRO sought to incorporate and consolidate all the technical intelligence capabilities under one roof and deploy them for defensive and offensive operations.

While it has not been clearly explained why the task of protecting CII fell upon an intelligence agency, it was speculated that since cyberspace fell within NTRO's charter, the agency was deemed fit to oversee NCIIPC's functioning.

However, protecting CII is a shared responsibility, with a major role for the private sector. This means that there is a need to create joint structures and SoPs to effectively deal with threats and exigencies, as and when they occur.

A designated intelligence agency will have several issues with sharing of its SoPs or of information that could jeopardise its other ongoing operations, and therefore, it could be restricted in effectively carrying out its CII tasks. The same challenges also prevent the agency from naturally taking a full-fledged multistakeholder route, the need for which is inherent in a CII framework since many of the designated critical sectors lie in the private domain. In other countries, the protection of critical information infrastructure is situated with a civilian agency that works openly and without the restrictions natural to an intelligence organisation. In the U.S. the responsibility lies with the Department of Homeland Security, along with sector-specific departments.

It has to be recognised, however, that NCIIPC does acknowledge the role of other stakeholders, with the draft framework stating that 'protection of CII involves a multi stakeholder approach'.[5] This draft framework, currently under discussion, recognises five principle stakeholders in particular: the CII owner; service providers to the CII; NCIIPC; the Indian Computer Emergency Response Team (CERT-IN); and law enforcement agencies.

Although this may still fall short of the commonly accepted norm of a multistakeholder approach, it does indicate a gradual recognition of the new realities of Internet governance, despite India's traditional emphasis on a multilateral approach, especially with regard to security issues.[6]

• 3. Ministry of Communications and Information Technology, Department of Electronics and Information Technology, Notification: Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013. *The Gazette of India*, New Delhi, 16 January 2014, http://deity.gov.in/sites/upload_files/dit/files/GSR_19%28E%29.pdf.

• 4. Chen, Liu Chuen (2015). What you should be knowing about the Kargil war. *India Today*, 26 July 26, http://indiatoday.intoday.in/story/kargil-war-vijay-diwas-facts/1/454125.html.

• 5. NCIIPC (n.d). *Draft on Framework for Protection of Critical Information Infrastructure.* New Delhi: NCIIPC, pp. 1-2. This document is currently under development by NCIIPC, and was forwarded to stakeholders for comments and suggestions in 2015.

• 6. For more on this, see Datta, Saikat (2016). *Cybersecurity, Internet Governance and India's Foreign Policy: Historical Antecedents.* New Delhi: Internet Democracy Project, https://internetdemocracy.in/reports/cybersecurity-ig-ifp-saikat-datta/.

Limitation 2: Fallacies in the Criticality Framework

A second limitation has to do with the framework that was used to rank sectors in order of criticality.

The sectors that have been designated as critical are defence; banking and financial sector; ICT and telecommunication; transportation; power; energy; the Ministries of Home Affairs, External Affairs and Heavy Industries; and Niti Ayog (the erstwhile Planning Commission).[7]

The sectors were chosen on the basis of a combination of factors,[8] with the understanding that the list would be revised and updated periodically. These factors were:

1. **Functionality:** 'set of functions, procedure and or capabilities associated with a system or with its constituent parts. It may be viewed at two levels- Functional Uniqueness and Functional Dependency'.
2. **Criticality Scale:** 'availably [sic], access, delivery and consummation of essential services'.
3. **Degree of Complementarities:** 'Failure of one system has potential to shut down other Critical Information Infrastructure relatively quickly in a cascading manner'.
4. **Political, Economic, Social and Strategic Values**: 'what is held important for political stability, economic prosperity, fraternity, unity and integrity of the nation'.
5. **Time Duration**: 'significance in the identification and categorization of CII. The same system may or may not be critical for all the time. Systems or their constituent needs to be identified in their alignment with period'.

In addition, a matrix was created to rank the different sectors in their order of importance, by mapping the number of interdependencies each sector had. The higher the number of interdependencies of a sector, the higher its criticality rating would be.[9] Using this interdependency map, NCIIPC designated the power sector as the most critical one.

While there was sound logic to the approach, basing the criticality ranking merely on an interdependency map has, however, had its limitations. A typical risk assessment framework also takes into account other factors that may prove critical to mapping vulnerabilities and criticality, such the intent of a possible attacker and the timing of the attack – and for good reason. Consider the following example. The power sector depends upon the energy sector. Defence and national war fighting capabilities also depend on the energy sector. Without energy,

• 7. NCIIPC, op. cit., pp. 2-3. Most of these – including the defence, finance, power, transport and communications sectors – were also already mentioned in NCIIPC (2013). *Guidelines for the Protection of Critical Information Infrastructure, Version 1.0, June 2013*. New Delhi: NCIIPC, p. 1, http://perry4law.org/cecsrdi/wp-content/uploads/2013/12/Guidelines-For-Protection-Of-National-Critical-Information-Infrastructure.pdf. For a history of the guidelines, see Singh, Shalini (2013). NSA Puts Cybersecurity Initiative on Fast Track. *The Hindu*, 20 July, http://www.thehindu.com/news/national/nsa-puts-cyber-security-initiative-on-fast-track/article4933077.ece.
• 8. NCIIPC (2013). *Guidelines for the Protection of Critical Information Infrastructure, Version 1.0, June 2013*, pp. 7-8.
• 9. Comment by Munish Sharma, IDSA, at a CII workshop in Delhi, on 4 November 2015. Mr. Sharma was part of the NCIIPC team that designed the CII interdependency map.

both power and defence would be severely compromised. Chances, thus, are that, in the prelude to an attack on a sovereign nation, a possible enemy might prioritise focusing its limited resources on attacking the energy sector, rather than the power sector, despite the latter's greater number of interdependencies. This is because the impact of disruption of the energy sector on the nation's ability to defend itself would likely be much greater.

Similarly, in the event of a war, a forward air force base may still be able to function without power supply, using backup generators on conventional fuel. However, a cyberattack on its mission computers and radar coverage could have a far more debilitating effect on its combat-readiness, even though the energy sector has a far smaller number of interdependencies than the power sector.

A comprehensive risk assessment, thus, also needed to factor in intent, capability and timing of the intended attack. Merely mapping the number of interdependences was not sufficient.

Indeed, whatever their number of interdependencies, sectors such as defence will remain prime targets, as has been amply demonstrated in the past. While mapping vulnerabilities and their criticalities, it is imperative to note that cyberspace is 'unique in that it is manmade, recent and subject to even more rapid technological changes than other domains'. Moreover, as Nye argues, 'the barriers to entry in the cyber domain are so low that non-state actors and small states can play significant roles at low levels of cost'. This has proven to be a game-changer and brings a paradigm shift in the nature of threats and vulnerabilities to critical systems and programmes (see also box 2).

Box 2: Continued importance of the defence sector – an illustration

The cyberattack on the Joint Strike Fighter programme of the United States in late 2006 is a classic example of the paradigm shift in the nature of threats and vulnerabilities that cyberspace has brought with it. A 337-billion-US dollar programme was deeply compromised when hackers believed to be based out of China carried out a Computer Network Exploitation (CNE) attack, pulling out massive amounts of classified data that was estimated to be worth billions of dollars and of critical strategic value. The attack took place, not on the Pentagon, as was first suspected, but on the weakly-defended systems of Lockheed Martin, a private defence contractor that was designing the aircraft. While the attack came from non-state actors in China, it couldn't be attributed to an act of the Chinese state. Such scenarios highlight that the defence sector will continue to be highly critical and a prime target of attacks, even if its interdependencies might be fewer than of sectors such as power and energy.

Source: Harris, Shane (2014). *@War: The Rise of Cyber Warfare.* London: Headline Publishing Group.

The NCIIPC guidelines from 2013 acknowledge that 'time duration' is critical to mapping CIIs, and there is a stated aim to review each sector periodically. And indeed, some adjustments seem to have been made after the circulation of the draft framework in 2015; for example, following criticisms, the current list of critical sectors that is shown on the NCIIPC website[11] is somewhat different from the earlier one. Changes include the absorption of the power sector in the energy sector.

• 10. Nye, Joseph (2010). Cyber Power. Cambridge, MA, Harvard Kennedy School, Belfer Center for Science and International Affairs, Harvard Kennedy School, May, p. 4, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.
• 11. Please see the list under 'Sectors' on https://nciipc.gov.in/.

However, the original guidelines have not been systematically reviewed or re-written so far,[12] and whatever changes have been there seem to have been made in an ad hoc manner: they have not substantively and systematically impacted overall processes in NCIIPC.

Perhaps, the hiatus can be attributed to the delay between legislation and implementation: while the mandate for NCIIPC was laid down in 2008 through the amendment of the IT Act 2000, the guidelines were initially created in 2012 and then released in 2013.[13] The gazette notification for creating the NCIIPC came quite a bit later: it was issued in January 2014, much after the guidelines had already been accepted and released by the Government of India. Usually, an organisation is created before it issues guidelines, to ensure continuity. Moreover, in this case, since the guidelines were created by a team of external experts, there was a break with the team that would eventually man the organisation and evolve its methodology to protect CII. Perhaps these factors could be a possible reason for the delayed evaluation of the CII protection framework, and it continues to be a work in progress.

Limitation 3: Sector-Specific Guidelines and SoPs

A final important deficiency in the current CII framework is the absence of sector-specific guidelines and SoPs in the event of a cyberthreat or attack. The creation of sector-specific plans (SPP) ensures the development of 'a trusted relationship and true partnership between the government and the industry',[14] by setting several goals for industry and government to be achieved within a time-bound framework (for an example, see box 3 on p. 7). While the general guidelines have laid down a preliminary road map, the sectors identified by it are yet to evolve their specific charters. This creates a major vulnerability that is yet to be addressed.[15]

Currently, NCIIPC follows a framework of conducting a 'vulnerability/threat/risk' analysis (V/T/R analysis) for mapping the level of vulnerability of each designated sector during 'steady state operations', or the routine operations of an installation that follow a regular schedule.[16]

Based on the V/T/R analysis, NCIIPC carries out a control configuration audit and brings in change management to mitigate any vulnerabilities. The audit maps the various controlling nodes of the sector's 'operational technology' (OT) or 'supervisory control data acquisition' (SCADA) systems that are critical to running automated plant operations in large-scale industrial plants. This audit of the control systems helps NCIIPC to map out various vulnerabilities such as the logical and physical separation of OT/SCADA systems

• 12. Comment by Munish Sharma, IDSA, at a CII workshop in Delhi, on 4 November 2015.
• 13. See Singh, *Op. Cit.*
• 14. US Department of Homeland Security and US Department of Energy (2010). *Energy-Sector Specific Plan: An Annexe to the National Infrastructure Protection Plan 2010*. Washington DC: US Departments of Homeland Security and Energy, p. i.
• 15. Datta, Saikat (2015). The Deadly New Age War. *The Hindu*, 23 June, http://www.thehindu.com/opinion/op-ed/the-deadly-new-age-war/article7342982.ece.
• 16. Presentation on NCIIPC methodology by Director, NCIIPC at a CII workshop held in Delhi on November 4, 2015.

Box 3: Example:
Goals of the US Energy Sector SPP

The goals of the U.S. energy sector SPP are as follows:

1. *Information sharing and communication: Build real-time situational awareness of risks, threats and attacks.*
2. *Ensure security: Use risk management principles to implement comprehensive counter measures that enhance preparedness, security and resilience.*
3. *Coordination and planning: Conduct emergency, disaster and continuity of business planning, define roles and responsibilities, and understand key sector interdependencies and collaborate with other sectors.*
4. *Public confidence: Strengthen confidence in the sector's ability to manage risks and implement effective counter-measures.*

Source: US Department of Homeland Security and US Department of Energy (2010). *Energy-Sector Specific Plan: An Annexe to the National Infrastructure Protection Plan 2010*. Washington DC: US Departments of Homeland Security & Energy, p. 2.

from the Internet and other information security measures that can significantly reduce risks and the threat of cyberattacks. While NCIIPC has so far approached the banking and power sectors for its initial projects, it is yet to look at the other sectors at this time.

Conclusion

The establishment of NCIIPC is a significant milestone in the strengthening of cybersecurity in India. In 2000, when the IT Act was being drafted, cybersecurity was not even mentioned. The first recognition of cybersecurity from a statutory perspective comes only in 2008, when the IT Act is amended and further clarified, including by introducing CII as key sectors to protect. With the establishment of NCIIPC in 2014, an institution is now finally in place to implement this mission.

As I have discussed in this paper, it may, however, currently be considerably hampered in doing so effectively for three reasons. The first is that its location within an intelligence agency makes it difficult to fully adopt the multistakeholder approach that the protection of CII really calls for. The second is that the criticalities framework that was used depends too much on sectors' interdependencies, while ignoring the importance of the intent, capability and timing of intended attacks in its risk assessment. As a consequence, sectors with lower interdependencies but high strategic value, such as defence, might not be given their full due. The third is that there has been a delay in the development of sector-specific guidelines and SoPs, leaving major vulnerabilities unaddressed.

If cybersecurity has been identified by the Indian government as a major concern in the twenty first century, CII has to be the corner stone of any related security policy. It is therefore essential that the challenges discussed here are not merely addressed, but that this is done with the urgency and comprehensive attention that this crucial building block of India's cybersecurity framework requires.