Cultivating India's Cyber Defense Strategy

NOVEMBER, 5TH, 2019 | 16:00 to 20:00

INDIAN ISLAMIC CENTRE
87-88, Lodhi Road, Lodhi Gardens, Lodhi Estate,
New Delhi, Delhi 110003

Information Communication Technologies (ICTs) are woven into every aspect of life in the twenty-first century. In India, individuals, government institutions, and the private sector increasingly rely on cyberspace for discharging economic, social, and political functions. However, as both states and non-state actors alike continue to engage in the weaponization and exploitation of cyberspace for reaping strategic dividend, India needs a strategy that secures its digital frontiers. As India firms up its cyber security strategy in 2020, critical discourse on response, detection, and publication of incidents, and governance of vulnerabilities, exploitation, and disclosure is certainly the need of the hour.

Recently, the Kudankulam Nuclear Power Plant in Tamil Nadu is suspected to have fallen victim to a potentially disastrous cyber attack. In September 2019, Kaspersky Labs published their report on the DTrack remote administration trojan, which is suspected to have been operated by Lazarus APT. After initially refuting claims made by security researchers, the Nuclear Power Corporation of India Limited has finally confirmed an incident. The reason for the initial denial remains unknown, and the consequences of India's defense posturing need to be re-examined.

Undoubtedly, India's defense posturing needs to adopt multilateral cooperation underscored by robust technical readiness. The question is "What does the Indian government need, at the technical, legal, and policy levels, to achieve this readiness?"

The Centre for Internet & Society invites you to a roundtable discussion that identifies critical vectors in this debate, and hashes out next steps for a robust cyber defense agenda.

Format: Chatham House Rules. 5-7 minute opening interventions by lead discussants in each session followed by open discussion by all stakeholders.

AGENDA

16:00 - 16:15 Arrivals and Tea/Coffee

16:15 - 17:00 Setting the Scene: Pukhraj Singh

17:05 - 18:15 **Session 1: Building India's cyber defences - vulnerabilities, exploits and cyber attacks/weapons**

Speaker: Gunjan Chawla (CCG), Udbhav Tiwari (Mozilla), Karan Saini (CIS)

18:15 - 18:30 High Tea

18:30 - 19:30 **Session 2: Future of norms setting processes in cyberspace and India's strategic interests**

Speakers: Arun Mohan Sukumar (ORF), Dr. Karthik Nachiappan (NUS), Arindrajit Basu (CIS)

19:30 - 20:00 **Discussion on Next Steps and Closing**

Setting the Scene

This session will attempt to take stock of the key actors, threat vectors and thought processes prevailing within the cyber defense ecosystem in India. Till the announcement of the Defense Cyber Agency earlier this year, there was no dedicated body in the military responsible for combating cyber threats from external adversaries. A patchwork of other bodies reporting to various nodal authorities exist, as summarised in the link here.

Key questions we hope discussants might answer are:

1. Is there emerging doctrinal thought in the military, or wings of the government, on India's strategic posturing?
2. Is there sufficient co-ordination among the various entities responsible for India's cyber defense?
3. How can India continue to improve its response to cyber threats?

Key Readings:

1. Nidhi Singh, "India's New Cyber Defense Agency" (CCG NLUD, May 10, 2019).
2. VIF Task Force " Credible Cyber Deterrence in Armed Forces of India".
3. Arun Mohan Sukumar, The Case for Cyber and Cyber-Physical Weapons: India's Grand Strategy and Diplomatic Goals, ORF Special Report No 15, (2016).
4. Arun Mohan Sukumar and Col. R.K. Sharma, The Cyber Command: Upgrading India's National Security Architecture, ORF Special Report No 9, (2016).
5. Anand V and Saikat Datta,"Cyberattack scare dogs india's nuclear plants" (Asia Times, October 30th, 2019)

Session 1: Building India's cyber defences - vulnerabilities, exploits and cyber-attacks/weapons

The presence of security vulnerabilities and flaws in any type of digital technology is virtually unavoidable. While there are a wide array of best practices which can be adopted in an effort

to minimise the presence of security vulnerabilities, adherence to best practices and standards still cannot act as an "end-all" to, or eliminate entirely, the prevalence of security vulnerabilities or flaws within a particular system or technology.

States increasingly rely on the edge provided by discovering and exploiting security vulnerabilities in software and hardware components for intelligence gathering, and for achieving "the continuation of politics by other means." As global infrastructure becomes increasingly digitized, it becomes important to address the strategies and ways in which states engage with vulnerability exploitation. Key questions in this discussion include:

1. What is the difference between cyber weapons, cyber physical weapons, and vulnerabilities?
2. Is there an adequate framework for the governance of vulnerabilities exploitation by the government? Is the Vulnerabilities Equities Process (VEP) developed by other countries a workable model?

States, however, are by no means the only actors involved in this space. Vulnerabilities are discovered individually by both malevolent hackers, as well as those who undertake their exploratory research in good faith. Given the recent push for digitization of the governance infrastructure in India, it becomes important to ensure a proper framework through which outside parties (i.e., security researchers) are able to report any discovered security flaws to the Government. The questions which arise from existing frameworks and processes include:

1. What hurdles do hackers face when disclosing vulnerabilities to the Government, and in engaging in security research?
2. How can the existing frameworks for voluntary vulnerability reporting and disclosure be improved?
3. Is the present legislative framework conducive to a vibrant culture for security researchers and hackers?

Key Readings:

1. Disclosing vulnerabilities to the Government:
2. Karan Saini, Pranesh Prakash, Elonnai Hickok, "Improving the Process for Disclosing Vulnerabilities to the Government of India" (Centre for Internet & Society, March 20, 2019)

Session 2: Future of norms setting processes in cyberspace and India's strategic interests

Global norms formulation processes are back on in full swing with a rejuvenated United Nations Group of Governmental Experts (UN-GGE), now in its sixth iteration, and an Open Ended Working Group (OEWG) set up at the behest of a Russian sponsored resolution in cyberspace. Private actors are getting in on the game too. The key role by Microsoft in charting out the CyberSecurity Tech Accords, Paris Call for Trust and Security in Cyberspace, and its most recent initiative, the Cyber Peace Institute, must be commended. However, the success of its entrepreneurship relies on how well it can work both with multilateral mechanisms under the aegis of the United Nations, and multi-stakeholder fora such as the Global Commission on Stability in Cyberspace.

However, several technical experts continue to believe that the unique characteristics and unpredictability of cyberspace render them ungovernable by the existing standards of International Humanitarian Law. For the most part, India has remained silent when engaging with these processes and on the applicability of international law or norms for responsible state behaviour. We hope this session will discuss:

1. The strategic value of International Law in cyberspace and what India's positioning should be
2. How can multilateral cooperation aid India's cyber readiness?
3. The role of the private sector in cyber defense/strategic offense

Key Readings:

1. Arindrajit Basu and Elonnai Hickok (2018) "Cyberspace and External Affairs: A memorandum for India"
2. Arindrajit Basu and Elonnai Hickok (2018), "Conceptualizing an International Security architecture for cyberspace" (Global Commission on Stability of Cyberspace)
3. Pukhraj Singh, ' A Death Knell for the International Norms of Cyber Conflict" (Modern Warfare Institute, Aug 8,2019)
4. Arindrajit Basu and Karan Saini, "Setting International Norms of Cyber Conflict is Hard but that doesn't mean we should stop trying" (Modern War Institute, Sep 30,2019)