Patching the gaps in India's cybersecurity

Pranesh Prakash   Arindrajit Basu

2021-03-06

The Hindu

Abstract

Doctrinal clarity and institutional coherence are essential for a robust cybersecurity posture

Doctrinal clarity and institutional coherence are essential for a robust cybersecurity posture

On Sunday, February 28, there was a sensational report in *The New York Times*, *China appears to warn India: push too hard and the lights could go out*, based on investigations by a United States-based cybersecurity firm. It raised the possibility that the power outage in Mumbai, on October 13, 2020, could have been the result of an attack by a Chinese state-sponsored group. Maharashtra's Home Minister acknowledged that a report by the Maharashtra Cyber Cell showed that the grid failure was potentially the result of "cyber sabotage". Meanwhile, the Union Power Ministry denied that the grid failure was linked to any cybersecurity incident, and blamed human error for it. We cannot say who is right since not enough information is available in the public domain. And therein lies the rub.

While Maharashtra's Home Minister has promised to table the report in the Assembly, this would be the first time, to our knowledge, that a cybersecurity incident has been discussed this openly by government officials.

India has been a target earlier

India has been attacked by suspected Chinese state-sponsored groups multiple times in the past. In 2009, a suspected cyber espionage network dubbed GhostNet was found to be targeting, amongst others, the Tibetan government in exile in India, and many Indian embassies. By pursuing the leads from that discovery, researchers found what they dubbed the Shadow Network, a vast cyberespionage operation which extensively targeted Indian entities, including military establishments, news publications, and even the National Security Council Secretariat itself, with clear evidence that confidential documents had been accessed by the attackers. In response to a question raised in Parliament, the then Minister Sachin Pilot noted an investigation was under way. There were a number of subsequent attacks that targeted India, including Stuxnet, which had also taken down nuclear reactors in Iran; Suckfly, which targeted not just government but also private entities including a firm that provided tech support to the National Stock Exchange; and Dtrack which first targeted Indian banks, and later the Kudankulam nuclear power plant (Tamil Nadu) in 2019. However, neither the report from the Shadow Network investigation, nor any other, has ever been tabled in Parliament, nor even a redacted version made public. Even when parliamentarians have raised serious questions, the government's responses have only been perfunctory. Appraising lawmakers of the scale and depth of the damage wrought is critical to enabling meaningful public discussions and crafting a robust response. Further, doing so will enable the government to be able to own the narrative around these incidents.

On a side note, while there is much evidence to show that Chinese state-sponsored groups were responsible for many of these attacks, Chinese cybersecurity agencies have also helped the security community in dismantling the infrastructure behind some of these attacks. And it must also be remembered that documents released by WikiLeaks show that groups such as the Central Intelligence Agency's UMBRAGE project have advanced capabilities of misdirecting attribution to another nation-state ("false flag attacks") by leaving behind false "fingerprints" for investigators to find. Given this, questions of attribution are always murky when it comes to cyber attacks — necessitating a robust institutional posture and political acumen in publicly dealing with these issues.

Institutional security

Over the past two decades, India has made a significant effort at crafting institutional machinery focusing on cyber resilience spanning several government entities. The Prime Minister's Office includes within it several cyber portfolios. Among these are the National Security Council, usually chaired by the National Security Adviser (NSA), and plays a key role in shaping India's cyber policy ecosystem. The NSA also chairs the National Information Board, which is meant to be the apex body for cross-ministry coordination on cybersecurity policymaking. The National Critical Information Infrastructure Protection Centre established under the National Technical Research Organisation in January 2014 was mandated to facilitate the protection of critical information infrastructure. In 2015, the Prime Minister established the office of the National Cyber Security Coordinator who advises the Prime Minister on strategic cybersecurity issues.

India's Computer Emergency Response Team (CERT-In), which is the nodal entity responding to various cybersecurity threats to non-critical infrastructure comes under the Ministry of Electronics and Information Technology (MEITY). The Ministry of Defence has recently upgraded the Defence Information Assurance and Research Agency to establish the Defence Cyber Agency, a tri-service command of the Indian armed forces to coordinate and control joint cyber operations, and craft India's cyber doctrine. Finally, the Ministry of Home Affairs oversees multiple similarly-named "coordination centres" that focus on law enforcement efforts to address cybercrime, espionage and terrorism, while the Ministry of External Affairs coordinates India's cyber diplomacy push — both bilaterally with other countries, and at international fora like the United Nations.

This institutional framework, while seeking to create an ‘all of government’ approach to countering and mitigating cybersecurity threats at the national level, has also resulted in concerns around effective coordination, overlapping responsibilities and lack of clear institutional boundaries and accountability. This needs to be clarified in India’s National Cyber Security Strategy, which has been drafted by the NSC — a much-needed update to the National Cyber Security Policy 2013 — but is yet to be released. Ensuring coherence and coordination between these different actors should be its primary goal.

Doctrine on cyber conflicts

India is also yet to clearly articulate a doctrine that holistically captures its approach to cyber conflict, either for conducting offensive cyber operations, or the extent and scope of countermeasures against cyber attacks. While reports indicate that India too engages in targeted cyber-attacks, the rules of engagement for that too are unclear. This is unlike India’s approach to other global security regimes. For example, the ‘No First Use’ nuclear posture has been critical in preventing a nuclear armageddon in a region fraught by political and military tensions, and continues to further India’s global reputation as a responsible nuclear state.

Is it fair to argue that ‘cyber’ is different? Could secrecy and ambiguity surrounding a nation’s doctrine and capabilities provide a tactical advantage when engaging in cyber operations? This is hardly the case in today’s increasingly unstable geopolitical scenario. The existing asymmetry in capabilities does not currently favour India. The absence of a credible cyber deterrence strategy means that states and non-state actors alike remain incentivised to undertake low-scale cyber operations for a variety of purposes — espionage, cyber crime, and even the disruption of critical information infrastructure.

Define the red lines

The same argument must be made for India’s contribution to global regimes crafting norms for responsible state behaviour in cyberspace. India has been an active participant at processes within the First Committee of the United Nations General Assembly dealing with issues of disarmament and international security. While the Indian delegation has made public some of their intervention, India’s long-term strategic thinking on core issues of debate at these fora remains relatively unknown, barring a few statements by public officials, including Shivshankar Menon and Arvind Gupta. A key opportunity herein is a precise articulation of how international law applies to cyberspace, which could mould the global governance debate to further India’s strategic interests and capabilities. In particular, this should include positioning on not just non-binding norms but also legal obligations on ‘red lines’ with respect to cyberspace-targets that should be considered illegitimate due to their significance for human life, such as health-care systems, electricity grids, water supply, and financial systems.

Clearer strategy and greater transparency are the need of the hour to improve

India's cybersecurity posture. To better detect and counter threats from both state actors and their proxies as well as online criminals, improved coordination is needed between the government and the private sector, as well as within the government itself — and at the national and State levels. A clear public posture on cyber defence and warfare boosts citizen confidence, helps build trust among allies, and clearly signals intent to potential adversaries, thus enabling a more stable and secure cyber ecosystem.

Pranesh Prakash was a co-founder of the Centre for Internet and Society, and is an affiliated fellow at Yale Law School's Information Society Project. Arindrajit Basu is Research Lead at the Centre for Internet and Society