Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG POLICY BRIEF

Crafting India's Response to State-sponsored Cyberattacks

Author

Deependra Singh Hooda

Volume VI, Issue 8

MARCH 15, 2021

Delhi Policy Group

Core 5A, 1st Floor, India Habitat Centre, Lodhi Road, New Delhi- 110003

www.delhipolicygroup.org

Delhi Policy Group
Advancing India's Rise as a Leading Power

DPG Policy Brief Vol. VI, Issue 8
March 15, 2021

ABOUT US

Founded in 1994, the Delhi Policy Group (DPG) is among India's oldest think tanks with its primary focus on strategic and international issues of critical national interest. DPG is a non-partisan institution and is independently funded by a non-profit Trust. Over past decades, DPG has established itself in both domestic and international circles and is widely recognised today among the top security think tanks of India and of Asia's major powers.

Since 2016, in keeping with India's increasing global profile, DPG has expanded its focus areas to include India's regional and global role and its policies in the Indo-Pacific. In a realist environment, DPG remains mindful of the need to align India's ambitions with matching strategies and capabilities, from diplomatic initiatives to security policy and military modernisation.

At a time of disruptive change in the global order, DPG aims to deliver research based, relevant, reliable and realist policy perspectives to an actively engaged public, both at home and abroad. DPG is deeply committed to the growth of India's national power and purpose, the security and prosperity of the people of India and India's contributions to the global public good. We remain firmly anchored within these foundational principles which have defined DPG since its inception.

Author

Lt. Gen. Deependra Singh Hooda (Retd.), PVSM, UYSM, AVSM, VSM & Bar, Senior Fellow for Military Strategy, Delhi Policy Group

The views expressed in this publication are those of the author and should not be attributed to the Delhi Policy Group as an Institution.

Cover Photograph:

This report details a cyber campaign conducted by a China-linked threat activity group, RedEcho, targeting the Indian power sector. Source: Recorded Future

Delhi Policy Group
Core 5A, 1st Floor,
India Habitat Centre,
Lodhi Road, New Delhi- 110003.
www.delhipolicygroup.org

Crafting India's Response to State-sponsored Cyberattacks

by
Deependra Singh Hooda

A recent report by Recorded Future, a U.S.-based company that tracks global cyber threats, detailed a campaign conducted by a China-linked threat activity group, RedEcho, aimed at the Indian power grid. According to the report, from mid-2020 onwards, there was a concerted targeting of 10 power sector organisations and two Indian seaports. In a subsequent interview, Christopher Ahlberg, Recorded Future's CEO and Co-Founder, stated that the Chinese hackers appeared to be active till 28 February, after which they started winding down their activities.

There was a great deal of debate whether the power outage in Mumbai in October 2020 resulted from a cyberattack, with contrasting statements from the Maharashtra and Union governments. Irrespective of whether Chinese state-sponsored hackers caused the five-hour-long power failure or not, the vulnerability of India's critical infrastructure stood exposed. Earlier, in October 2019, the Kudankulam Nuclear Power Plant had been hit by malware, though the plant's functioning had not been affected.

Cyber threats are ballooning across the world, and two recent incidents show the seriousness of the problem. The U.S. is still struggling to understand the full impact of the SolarWinds attack, likely caused by Russian hackers, that has affected at least nine government agencies and thousands of private companies. It is estimated that the U.S. government systems could take up to 18 months to recover from the attack.

On 2 March, Microsoft put out a statement that their Exchange servers had been attacked by HAFNIUM, a group assessed to be state-sponsored and operating out of China. This cyberattack has put hundreds of thousands of email accounts at risk around the globe. Even as companies scramble to secure their systems, hackers are escalating their attacks to infect as many computers as possible.

Cyber threats have many dimensions, but the greatest danger to a country's national security comes from state-sponsored attacks that target vital sectors related to infrastructure, intelligence, government, and civil society. Countries like the U.S., China, and Russia possess tremendous assets for carrying out sophisticated cyberattacks. The famous Stuxnet attack on the Iranian centrifuge facility at Natanz in 2010 was reportedly an operation involving the U.S. Central Intelligence Agency, National Security Agency (NSA), and Israel's

Unit 8200. The malware used exploited five previously unknown vulnerabilities (commonly termed zero-day exploits) and was tested on a dummy set of centrifuges. Such capability is not available with individual hackers.

In countering cyber threats from hostile states, two critical components of any nation's strategy are defending and deterring. This brief will look at some crucial aspects of cyber defence and cyber deterrence to suggest measures to strengthen India's capability.

The government's decision to set up the National Critical Information Infrastructure Protection Centre (NCIIPC) in 2014 was a much needed and positive step. The NCIIPC is mandated to provide information protection to Transport, Power and Energy, Government, Finance, Telecom, and Strategic and Public Enterprises. While the NCIIPC is doing a good job, it is perhaps time to expand our understanding of what constitutes a critical sector.

In 2014, Sony Pictures was readying to release their film *The Interview*, a comedy about the North Korean leader Kim Jong-un. After the North Korean government threatened action if the film was released, hackers got into the company's network, stole and leaked emails, and grabbed five unreleased movies. Sony was forced to cancel the planned release of the film. As described in Fred Kaplan's book *Dark Territory*, there was a lot of debate within the Obama administration on whether governments have a role in responding to cyberattacks on private corporations. One view was that although a private company was targeted, this was an attack on the freedom of expression and America's way of life.

It is no longer possible to draw neat distinctions between critical infrastructure and private companies. The latest SolarWinds attack in the U.S. was not launched directly but through a software called Orion, which government agencies and companies widely used for IT management. Hackers inserted malicious codes in the updates that were sent out to all Orion users.

In February 2015, President Obama signed an executive order titled "Improving Critical Infrastructure Cybersecurity." This envisaged setting up forums where private companies could share data about hacking attempts with one another and with government agencies. In exchange, the NSA, working through the FBI, would provide top-secret tools and techniques to protect their networks. India needs to consider similar steps to expand cooperation between government agencies tasked with cybersecurity and the private IT sector.

A vital part of cyber defence is the minimising of foreign hardware and software in critical infrastructure. Countries are known to implant malware in their IT products before their export. Glenn Greenwald's book *No Place to Hide* details how NSA employees intercepted Cisco routers and implanted them with backdoors before shipping them to their original destination. Bloomberg reported in October 2018 that China's intelligence services had ordered subcontractors in China to plant malicious chips in Supermicro server motherboards bound for the U.S.

Given these practices, many countries have restricted the use of foreign products in critical networks. Beijing has banned government purchases of Microsoft Windows, Apple products, Cisco, and software from Symantec and Kaspersky Lab. On 12 March, the U.S. officially designated Chinese companies Huawei, ZTE technology, Hytera Communications, Hangzhou Hikvision Digital Technology, and Dahua Technology as threats to national security.

In India, little has been done to encourage the development of indigenous industry. In September 2020, Minister of State for Communications Sanjay Dhotre informed Parliament that more than 53 percent of the mobile network equipment of BSNL is sourced from ZTE and Huawei. This is despite Huawei having been investigated for hacking a BSNL network in 2014. There is a similar situation in the power sector. In the fiscal year 2018-19, India imported nearly Rs 71,000 crore worth of power sector equipment, of which China alone accounted for Rs 21,000 crore.

Since last year, the government has taken some important decisions. In July 2020, Power Minister R.K. Singh announced that Indian companies would require government permission to import power supply equipment and components from China. Recently, the Department of Telecommunications notified that telecom companies could use products only from trusted sources in their network and must take permission to upgrade their existing network using telecom equipment that has not been designated as a trusted product.

These decisions will give a push to indigenisation but need to be taken much further. While Chinese equipment must be targeted for replacement, offering a complete clean chit to other nations would also be wrong. In the critical sectors, the government should push for a graduated approach towards the total replacement of foreign products. This would require policy directions and, in some instances, financial support to private companies.

While we strengthen our defence against cyberattacks, we must also adopt an effective cyber deterrence strategy. The issue of cyber deterrence is hotly debated, with many arguing that this is an impractical proposition. The U.S.,

possessing the most powerful military and cyber capability globally, continues to be rocked by cyberattacks from China, Russia, Iran, and North Korea. Nuclear and conventional deterrence work because there is clarity on the adversary's capability and the costs associated with a conflict. Cyberwarfare, on the other hand, is characterised by an absence of clarity. We can never be certain about the other side's capability, and the definite attribution of cyberattacks to a state actor is difficult. In these conditions, deterrence is unlikely to succeed.

Countering this argument is the point of view that unless costs are imposed on states conducting cyberattacks, they will continue to act with impunity. It is also wrong to assume that cyberattacks can only be deterred by similar actions in cyberspace. The 2017 report of the U.S. *Department of Defense Task Force on Cyber Deterrence* states, "While offensive cyber responses are an essential part of the toolkit, the full range of military responses (symmetric or asymmetric) – as well as diplomatic, law enforcement, and economic responses – must also be considered."

On May 4, 2019 the Israel Defence Forces (IDF) carried out an airstrike in the Gaza Strip, after which the IDF tweeted, "We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work." The IDF spokesperson, Brig. Gen. Ronen Manlis said, "After dealing with the cyber dimension, the Air Force dealt with it in the physical dimension."

We could say that the power asymmetry in the Israel-Hamas relation makes this example irrelevant in a cyber situation involving two large countries. Still, it is being cited to show that there are multiple ways to respond to a cyberattack. A wholly passive and defensive cyber strategy is bound to fail because offensive cyber capabilities are today superior to the ability to defend networks.

The situation that India faces is concisely expressed by James Mulvenon, a founding member of the Cyber Conflict Studies Association, "Here's the problem – its 1946 in cyber. So we have these potent new weapons, but we don't have all the conceptual and doctrinal thinking that supports those weapons or any kind of deterrence." The danger of state-sponsored cyberattacks is now well known. It is time for India to start thinking about policies, concepts and doctrines to deal with this potent threat to national security.

***

Delhi Policy Group
Core 5A, 1st Floor,
India Habitat Centre, Lodhi Road
New Delhi - 110003
India

www.delhipolicygroup.org