Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG POLICY BRIEF

Towards a Cyber Deterrence Strategy for India

Author

Deependra Singh Hooda

Volume VI, Issue 19

JULY 14, 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 19
July 14, 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 Photographs:

Photo 1, Source: Shutter Stock
Photo 2, Source: Security Today

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

Towards a Cyber Deterrence Strategy for India

By
Deependra Singh Hooda

Contents

Towards a Cyber Deterrence Strategy for India

by
Deependra Singh Hooda

Introduction

In 2013, Thomas Rid wrote a book titled *Cyber War Will Not Take Place.* He argued that an "offensive act has to meet certain criteria in order to qualify as an act of war: it has to be instrumental; it has to be political; and, most crucially, it has to be violent, or at least potentially violent." He stated that "there is no cyber offense that meets all three criteria."[1]

Many of the points made by Rid remain theoretically relevant today, but our understanding of the nature of cyber threats has changed. Whether a cyber war takes place or not, offensive cyber-attacks are increasingly being viewed as a danger to national security. This does not mean that there is now total clarity in responding to these threats, only that the exploitation of cyberspace is reaching levels that endanger vital national interests.

Deterring threats instead of fighting damaging wars has been a constant strategic aim through the ages. Deterrence is the practice of discouraging or restraining someone—in world politics, usually a nation-state—from taking unwanted actions, such as an armed attack.[2] In modern warfare, nuclear deterrence theory attracted a great deal of scholarly attention during the Cold War due to the need to avoid a destructive nuclear war. Conventional deterrence was considered more difficult to achieve than nuclear deterrence because while nuclear weapons have a clearly defined end result, the outcome of conventional battles is uncertain. Nevertheless, conventional deterrence is still considered an essential element of national strategies.

We are now facing cyber threats, which remain below the threshold of war fighting but are a serious danger to national security. Faced with this, can cyber deterrence be considered a feasible strategy? What type of cyber threats can be deterred? What should be the components of a cyber deterrence strategy for India? This paper will attempt to answer some of these questions.

Defining the Cyber Threats to be Deterred

Cyber threats can take numerous forms, from malware, phishing, identity theft, denial of service, ransomware to espionage and disruption of a nation's critical infrastructure. Unfortunately, it is virtually impossible to deter all kinds of

threats, and in crafting a national strategy for cyber deterrence, there must be a clearly focused approach.

The first step is to define the cyber threats that would pose a threat to national security. This could include attacks on critical infrastructure like telecommunications, power, transportation, etc.; attacks that compromise the integrity of crucial data; and attempts to cause loss of confidence in the government or disrupt social harmony. For example, the 2019 cyber attack on the Kudankulam Nuclear Power Plant and the recent cyber intrusions by the Chinese state-sponsored group *RedEcho* into the Indian power sector would certainly classify as threats to national security.

A national response must be aimed primarily at state-sponsored attacks, whether carried out directly or through state proxies. We have to accept the reality that individual criminal hackers cannot be effectively deterred, and it would be wasteful to adopt a 'whack-a-mole' approach against all cyber attacks. States are the more rational actors in international politics, and a cost and benefits strategy is easier to apply against them than to a group of terrorists or cyber criminals.

Cyber espionage is a difficult area. Spying is an ancient and acceptable practice pursued by all countries, and it is hard to condemn a state for espionage. However, some distinctions are now sought to be made. Theft of intellectual property, particularly in the fields of defence and high technology, is considered an activity that breaches the norms of traditional espionage.

A 2017 report of the U.S. Department of Defense Task Force on Cyber Deterrence defines theft of intellectual property as "Costly Cyber Intrusions" that constitute "unacceptable actions."[3] China is known to be heavily engaged in intellectual property theft. It is estimated that this theft is causing the U.S. industry losses in the range of $180 billion to as high as $540 billion per year.[4] Theft of intellectual property must not be treated as part of espionage but as a threat requiring a robust national response.

Another area requiring deliberation is whether the government's response should also extend to serious cyber attacks on civilian commercial companies outside the purview of critical infrastructure. In 2014, North Korean hackers forced Sony Pictures to cancel the release of their comedy *The Interview,* which depicted the assassination of the North Korean leader, Kim Jong-un. This kicked off a debate within the Obama administration on "what role *should* government play in responding to cyber attacks on citizens or private corporations?"[5]

The usual response of governments is that private companies must take care of their own cybersecurity. However, the state cannot completely disassociate itself from the commercial sector. The Sony Pictures hack was seen as an attack on the freedom of expression, and President Obama announced that the U.S. government would "respond proportionally."[6] There are no simple answers on how the government-private corporation cyber deterrence model would work. A delicate balance would have to be struck so that the government does not overstretch itself while private companies ignore their cybersecurity and become dependent on the government to bail them out in the event of cyber attacks.

The Challenges of Cyber Deterrence

A deterrence strategy depends on the ability of a state to restrain an opponent by threats, coercion, or incentive. There is a great deal of debate on whether the nature of threats in cyberspace can actually be deterred and whether we are considering applying a strategy that works well in the nuclear domain to an entirely different type of threat. Some of the challenges to the idea of cyber deterrence are discussed here.

Attribution is perhaps the biggest challenge. Nations must be clear about the identity of the perpetrator of a cyber attack so that their counter actions are not misdirected. This is not easy because locations can be spoofed, identities hidden, and the nature of cyberspace ensures that attacks can be launched from any geographical location. In addition, false flags could be used to deceive or misguide attempts to identify the attackers. The 2018 Winter Olympic Games opening ceremony in South Korea was hit by a cyber attack that resulted in the official website being taken offline for 12 hours. *The Washington Post,* quoting intelligence officials, reported that the hacking was done by Russian spies who tried to make it look as if North Korea conducted the intrusion.[7]

Even if hacking groups are identified as belonging to a particular country, it is often not possible to prove that they are state-sponsored. Where the fingerprint of a state is found, there could be a reluctance to openly declare this because it could compromise intelligence operations. However, any hesitation to respond would weaken both credibility and deterrence.

Another challenge to cyber deterrence is the uncertainty of the effect. Nuclear deterrence worked because the capabilities of each side were known, as was the destructive potential of atomic weapons. National cyber capabilities are zealously guarded, and there is no certainty about how a cyber response would impact the adversary.

There is also the danger of unintended collateral damage. A joint U.S.-Israeli cyber attack on the Iranian Uranium enrichment facility at Natanz started in 2009. Although the malware, now known as Stuxnet, was designed to affect only the Siemens supervisory control and data acquisition systems at Natanz, it spread beyond its intended target. It is estimated that Stuxnet infected more than 200,000 computers around the world.[8] NotPetya, considered the most devastating cyberweapon, is widely assessed as having been launched by a Russian state group called Sandworm. While it primarily targeted Ukraine, NotPetya disrupted businesses and supply chains worldwide, causing approximately $10 billion in damage.[9] These considerations surrounding uncertainty of effect could sometimes delay decisions on taking cyber deterrence actions.

Deterrence is a strategy based on the threat of use of force and fails if force is actually applied. Fischerkeller and Harknett contend that cyber deterrence is not a credible strategy because cyberspace is perpetually contested. They write, "The combination of interconnectedness and constant contact with cyberspace's ever-changing character... encourages operational persistence in order to secure and leverage critical data and data flows." They suggest that "in operational reality, operational persistence/engagement (not operational restraint)" is the "appropriate strategic choice."[10]

'Cyber persistence 'as defined by Fischerkeller and Harknett, is "a strategy based upon the use of cyber operations, activities and actions (as opposed to the threat of force) to generate through persistent operational contact (as opposed to avoiding contact) continuous tactical, operational, and strategic advantage in cyberspace".[11] They feel that this will "allow greater freedom of manoeuvre to impose tactical friction and strategic costs." Whether cyber persistence can also be considered a component of deterrence is open to interpretation.

Notwithstanding these challenges, the absence of a clear deterrence strategy could result in continuing cyber attacks from hostile players with impunity. According to Indian government data presented in the Parliament, nearly 1.16 million cases of cyber attacks were reported in 2020, up almost three times from 2019 and more than 20 times compared to 2016.[12] This trend is likely to continue.

In crafting a cyber deterrence strategy, India will have to start almost from scratch. A 2013 Cyber Security Policy exists (and is now being updated), but it is a set of general guidelines.[13] A cyber deterrence strategy will have to lay down a specific action plan to respond primarily to state-sponsored attacks that threaten national security.

Components of a Cyber Deterrence Strategy

There are two fundamental approaches to deterrence – denial and punishment. This part of the paper looks at how these approaches could be applied in the Indian context, particularly considering India's current cyber power capability and its shortfalls.[14] This reality has to be a major consideration in preparing a strategy.

Cyber deterrence by denial means the hardening of our critical information infrastructure to the extent that the adversary feels that attacking such systems will yield little results. It is a well-known fact that today attacks in cyberspace have a distinctive edge over defensive measure. Despite this, protection of networks, redundancy in systems, use of trusted equipment, and defending forward could mitigate some of the weaknesses of cyber defence.

The first step is to reduce our vulnerabilities in the existing critical networks by replacing foreign hardware and software with indigenous solutions. India claims to be an Information Technology power, but this potential remains to be exploited. More than 50 per cent of the state-run BSNL's equipment is sourced from Chinese companies.[15] Incidentally, BSNL also has a strategic alliance with and shares resources with the Indian Army.[16] The Indian Air Force Network (AFNET), which links command and control centres, sensors, aircraft bases, and missile squadrons, was rolled out in 2010 with the support of BSNL, HCL Infosystems, and CISCO.

Dependence on foreign companies raises severe doubts about India's ability to defend critical infrastructure. Numerous policies have been floated on self-reliance, but their implementation has often been criticised. In June 2021, the Ministry of Finance issued a letter exempting firms having transfer of technology pacts with countries sharing a land border with India (e.g., China) from mandatory registration. After security concerns were raised, the order was put on hold.[17]

Deterrence by denial also encompasses defending forward by proactively seeking out potential threats, regular assessments of critical networks to see whether they have been penetrated, speedy threat mitigation, and improved intelligence collection. Government agencies, including the military, must be able to harness the best cyber-talent in the country, unencumbered by bureaucratic processes.

India must also work to improve its cyber attribution capabilities. As brought out earlier, one of the biggest challenges to cyber deterrence is the difficulty of attribution. This will require a collective effort by all intelligence agencies and

the development of advanced competencies in cyber forensics. The system of sharing information about cyber attacks must also be improved. In the case of the *RedEcho* hacking of the power sector, the Maharashtra state police were informed of the threat in November 2020. However, the National Critical Information Infrastructure Protection Centre (NCIIPC) only alerted the Ministry of Power on 12 February 2021.[18] Attribution becomes difficult if all sources of information are not pooled together.

Deterrence by punishment seeks to prevent an adversary from carrying out unacceptable acts by the threat of imposing high costs. It must be clearly communicated that cyber attacks which threaten national security will *always* be responded to. And this response is not necessarily restricted to actions in cyberspace but includes military, economic, diplomatic, and legal action.

On May 4, 2019, the Israel Defence Forces (IDF) carried out an airstrike against a building in the Gaza Strip that housed a Hamas cyber unit. The IDF spokesperson said, "After dealing with the cyber dimension, the Air Force dealt with it in the physical dimension."[19] On June 23, *The Washington Post* reported that the U.S. Cyber Command had launched an "offensive cyber strike that disabled Iranian computer systems used to plan attacks on oil tankers in the Persian Gulf." The cyber strike was carried out in retaliation to Iran's alleged attacks on two oil tankers in the Gulf of Oman earlier in June.[20]

The first a kinetic response to cyber threats, and the second a cyber response to a kinetic threat, show that deterrence by punishment should not be looked at only as a cyber vs. cyber contest.

It could be said that threats against a strong power like China could lead to an escalation. This is true, but escalation impacts both sides, and for any deterrence to work, the capability to carry out the threat must be believable. It must also be noted that we are talking about serious threats to national security and not routine cyber intrusions. The absence of a response will only invite further attacks and lead to a more significant crisis that could have been averted if credible action was taken in the first instance.

While deterrence by punishment includes all instruments of government power, India also needs to build up its offensive cyber capability. According to the 'National Cyber Power Index' report published by the Belfer Center of Harvard Kennedy School, India ranks 27th in cyber offence among the 29 countries surveyed.[21] This is primarily because not much is publicly known about India's capability in this field. The general impression is that "India has developed relatively advanced offensive cyber capabilities focused on Pakistan."[22] It now needs to focus on China, given the growing tensions

between the two countries and recent reports of Chinese-backed intrusions in India's power sector, defence industry, and telecommunications.[23]

Preparing and Executing the Cyber Deterrence Strategy

Does India need to articulate a formal cyber deterrence strategy? It could be said that cyber capabilities are highly secret, and therefore any strategy discussing their use should not be put out in the public domain. However, communications and signalling are essential elements of deterrence. If an adversary is neither clear about our red lines nor the cost that his actions will invite, deterrence will fail. One of the reasons that India is rated poorly in cyber power is because it is shy about declaring its capabilities and intentions.[24]

The responsibility for preparing the draft of India's cyber deterrence strategy should be entrusted to the military. Any such strategy deals with serious threats to national security posed by external forces, and the institution most equipped to deal with external threats is the military. Inputs will have to be taken from other agencies, and the strategy could eventually emanate from the Prime Minister's Office, but the lead will have to be taken by the military. The strategy should comprise a whole-of-government approach that is tailored to specific adversaries. Deterring Pakistan and China will require completely different tactics.

Similarly, the execution of the cyber deterrence strategy should be coordinated by the military. The military will have to synchronise the defensive efforts with the NCIIPC and the offensive efforts with other government ministries. The ultimate instrument of deterrence is military power, which is why the responsibility for the execution of cyber deterrence should be primarily entrusted to the military, with the ultimate authority resting with the Prime Minister.

This will require the empowerment of the Defence Cyber Agency (DCA), which was raised after an inordinately long wait in 2019.[25] While the primary responsibility of the DCA will be military cyber operations, it must play a more prominent role in shaping the national cyber strategy. One of the three focus areas of the U.S. Cyber Command is "strengthening our nation's ability to withstand and respond to cyber attack".[26] If the DCA is given an appropriate mandate, it could contribute significantly to India's cybersecurity.

Conclusion

There are numerous challenges to deterrence in cyberspace, but that should not prevent us from holding hostile actors accountable for their actions. India's

national will to resolutely respond to threats to national security must be clearly communicated through an articulated cyber deterrence strategy. The DCA should be tasked to prepare this strategy in concert with other government agencies.

Deterrence is a combination of communication, credibility, and capability. Downplaying serious incidents, a reluctance to act, and capability weaknesses in cyber power could have serious consequences. A national cyber deterrence strategy may not be a complete solution to combating state-sponsored cyber attacks, but it is undoubtedly a vital cog and also the need of the hour.

***

[1] Rid, Thomas. *Cyber War Will Not Take Place*. 1st edition. Oxford ; New York: Oxford University Press, 2013.

[2] Mazarr, Michael J. "Understanding Deterrence," April 19, 2018. https://www.rand.org/pubs/perspectives/PE295.html.

[3] Department of Defense, Defense Science Board. "Task Force on Cyber Deterrence." https://dsb.cto.mil/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf

[4] Jones, Jeff. "Confronting China's Efforts to Steal Defense Information." Belfer Center for Science and International Affairs. Accessed June 30, 2021. https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information.

[5] Kaplan, Fred. *Dark Territory: The Secret History of Cyber War*. Reprint edition. New York: Simon & Schuster, 2017.

[6] Ibid

[7] Nakashima, Ellen. "Russian Spies Hacked the Olympics and Tried to Make It Look like North Korea Did It, U.S. Officials Say." *Washington Post*. Accessed July 2, 2021. https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html.

[8] Tabbaa, Bishr. "Zer0 Days: How Stuxnet Disrupted the Iran Nuclear Program and Transformed Computer Security." Medium, July 17, 2020. https://medium.com/dataseries/zer0-days-how-stuxnet-disrupted-the-iran-nuclear-program-and-transformed-computer-security-9b9587199f06.

[9] "NotPetya: How a Russian Malware Created the World's Worst Cyberattack Ever | Business Standard News." Accessed July 13, 2021. https://www.business-standard.com/article/technology/notpetya-how-a-russian-malware-created-the-world-s-worst-cyberattack-ever-118082700261_1.html.

[10] Fischerkeller, M. P., and Harknett R. J. "Deterrence Is Not a Credible Strategy for Cyberspace (and What Is),". https://www.ida.org/-/media/feature/publications/w/we/welch-awards-2018-research-notes-fall-2019/welch-awards-2018-research-notes-fall-2019-article-1.ashx?la=en&hash=C725B2340ABA96463DBAF3D298E7671A

[11] Fischerkeller, M. P., Harknett, R. J. "Deterrence is Not a Credible Strategy for Cyberspace." Orbis 2017, 61 (3), 381-393.

[12] Nanda, Prashant K. "Cyber attacks Surged 3-Fold to 1.16 Mn Last Year in India." mint, March 23, 2021. https://www.livemint.com/news/india/as-tech-adoption-grew-india-faced-11-58-lakh-cyber attacks-in-2020-11616492755651.html.

[13] National Cyber Security Policy -2013. https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf

[14] IISS. "Cyber Capabilities and National Power: A Net Assessment." Accessed July 4, 2021. https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

[15] "BSNL's 44% Mobile Network Equipment from ZTE, 9% from Huawei - Times of India." Accessed July 4, 2021. https://timesofindia.indiatimes.com/business/india-business/bsnls-44-mobile-network-equipment-from-zte-9-from-huawei/articleshow/78175289.cms.

[16] www.indianarmy.nic.in. "The Official Home Page of the Indian Army." Accessed July 4, 2021. https://indianarmy.nic.in.

[17] The Financial Express. "Public Projects: Tech Transfers with Chinese Firms on Hold," July 3, 2021. https://www.financialexpress.com/industry/public-projects-tech-transfers-with-chinese-firms-on-hold/2283097/.

[18] IISS. "Cyber Capabilities and National Power: A Net Assessment."

[19] Cimpanu, Catalin. "In a First, Israel Responds to Hamas Hackers with an Air Strike." ZDNet. Accessed July 5, 2021. https://www.zdnet.com/article/in-a-first-israel-responds-to-hamas-hackers-with-an-air-strike/.

[20] Nakashima, Ellen. "Trump Approved Cyber-Strikes against Iranian Computer Database Used to Plan Attacks on Oil Tankers." *Washington Post*. Accessed July 5, 2021. https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html.

[21] Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Daniel Cassidy, and Anina Schwarzenbach. "National Cyber Power Index 2020". https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

[22] IISS. "Cyber Capabilities and National Power: A Net Assessment."

[23] Mihindukulasuriya, Regina. "China-Backed Hackers RedFoxtrot Targeted Defence Research, Telecom in India, US Firm Finds." *ThePrint* (blog), June 17, 2021. https://theprint.in/india/china-backed-hackers-redfoxtrot-targeted-defence-research-telecom-in-india-us-firm-finds/679807/.

[24] Rampal, Nikhil. "India Is No Superpower in Cyberspace, Claims Harvard Report." India Today. Accessed July 6, 2021. https://www.indiatoday.in/diu/story/india-is-no-superpower-in-cyberspace-claims-harvard-report-1724327-2020-09-22.

[25]" India to Have Defence Cyber Agency in May; Rear Admiral Mohit to Be Its First Chief." India Today. Accessed July 7, 2021. https://www.indiatoday.in/india/story/india-defence-cyber-agency-may-rear-admiral-mohit-1513381-2019-04-30.

[26]" Mission and Vision." Accessed July 7, 2021. https://www.cybercom.mil/About/Mission-and-Vision/.

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

www.delhipolicygroup.org