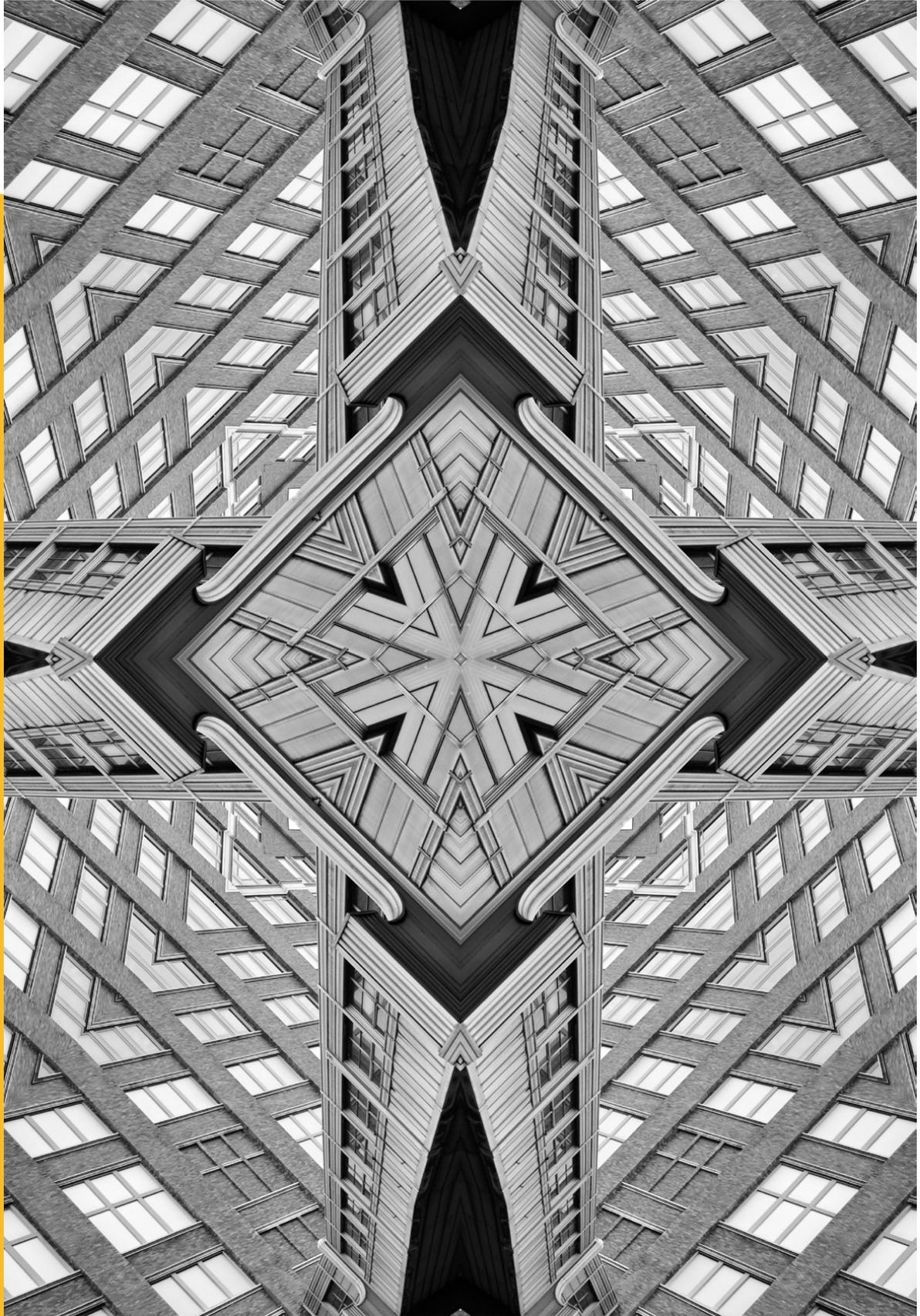


Occasional Paper



ISSUE NO. 364 SEPTEMBER 2022

© 2022 Observer Research Foundation. All rights reserved. No part of this publication may be reproduced, copied, archived, retained or transmitted through print, speech or electronic media without prior written approval from ORF.

Assessing the Efficacy of the West's Autonomous Cyber-Sanctions Regime and its Relevance for India

Sameer Patil

Abstract

Cyber-sanctions have emerged as a preferred tool for Western governments to deter cyberattacks emanating from their adversaries' territories. As they implement such sanctions, however, these states face various challenges one of which is the difficulty in attribution. Moreover, the sanctions have only partially curbed the malicious cyber activities. Yet, the regime continues to expand, and many allies of the United States are emulating its practice of cyber-sanctions. This paper makes an assessment of the practice of cyber-sanctions among western countries, and their effectiveness in containing cyber mischief. It also discusses the applicability of this coercive tool for India and the policy issues that are likely to emerge.

Geopolitical rivalries in the cyber domain have intensified in recent years due to continuing tensions between global powers. Certain states have executed cyberattacks against their adversaries targeting national and commercial computer networks, sabotaging critical infrastructure operations, and stealing sensitive data. In some cases, they have used proxy actors such as cybercriminal gangs and hacking syndicates to commit cybercrimes against their adversaries. Recent major cyberattacks include the breach of Indian power grids by Chinese hackers reported in April 2022, the breach of US government agencies by suspected Chinese hackers in March 2022, the disruption of Ukrainian government websites days before the Russian invasion in February 2022, and a ransomware attack against oil terminals in Belgium and Germany in February 2022.¹ This targeting of national, commercial, and critical infrastructure computer networks demonstrates that malicious cyber activities imperil national and economic security.

Indeed, as competition and conflict in cyberspace have thrived, efforts for the creation of common cyber norms are stalled by the polarisation between the western camp (i.e. the United States, its allies, and European countries) and the eastern camp (led by China and Russia). Individual states have had to explore tools to tackle emerging cyber threats. Since 2015, the United States (US) and the European Union (EU) have utilised the tool of cyber-sanctions against their adversaries, primarily targeting Russian, Chinese, and North Korean intelligence operatives and their proxies like the North Korea-backed Lazarus hacking group.

Cyber-sanctions can be defined as autonomous or unilateral economic sanctions and trade restrictions imposed by individual states to deter and punish their adversaries for malicious cyber activities and ensure accountability.^{a,2}

The frequent use of the cyber-sanctions instrument by Western countries^b raises the question of why they rely heavily on this coercive tool. Other questions relate to whether such sanctions have shaped the bad actors' ability to engage in malicious cyber activities, and what significant challenges are encountered by states in imposing these sanctions.

a These sanctions are enforced through enabling domestic legislation and broadly fall in the categories of sectoral and targeted sanctions. These sanctions include travel bans, asset freezes, restrictions on financial and commercial transactions, and curbs on the operations of technology companies.

b This brief defines the Western world to mean North America and Europe.

Introduction

This paper seeks to answer these questions by examining the concept of cyber-sanctions and their efficacy in deterring cyber sabotage. The aim is to highlight the evolution of cyber-sanctions and key trends in their implementation. It concludes with an exploration of whether this policy tool is relevant for India and what factors it should consider in using sanctions to tackle cyber maleficence, in particular from China and Pakistan.

“Efforts to create common cyber norms are stalled by the polarisation between the western and eastern camps, and states have had to explore their own tools to tackle cyber threats.”

The Western Autonomous Cyber-Sanctions Regime: An Overview

States that suffer cyber sabotage have mostly responded by launching retaliatory cyberattacks and hacking into their adversaries' systems. The spate of retaliatory attacks, for instance, between the US and Russia, the US and North Korea, or Iran and Israel, illustrates this tendency for punitive action.^{3,4} However, as the consequences of cyberattacks worsened in the last few years, national security establishments began debating the need to adopt a more coercive and proactive posture to counter malicious cyber activities. This has become particularly critical as many cyberattacks have caused significant disruptions, short of what is considered the equivalent of an 'armed attack' that causes casualties and damage or destruction of property.

In some cases, such acts of sabotage lowered the states' threshold for military retaliation—at least towards the non-state actors.⁵ For instance, in August 2015, the US military targeted an operative of the Daesh terrorist group in an airstrike in Syria, who had exposed the personal data of about 1,300 American military and government employees.⁶ In May 2019, the Israeli military bombed the Hamas terrorist group's technology division based in the Gaza Strip to preempt a cyberattack.⁷ While these examples are exceptions, states with requisite military capabilities will utilise this option when they see a suitable opportunity to prevent cyberattacks that could cause more harm.

Necessary as they were, however, these military actions did not deter the malicious cyber activities and only highlighted the blunted edge of existing policy instruments. Realising the risk posed by these cyberattacks to their national security and economic prosperity, Western countries looked for other instruments other than military action, to signal that malevolent cyber acts would not go unchecked.

In this context, cyber-sanctions emerged as a preferred tool for these Western governments, as defined in this paper. Since they had already become prolific in using coercive economic sanctions and trade restrictions against their adversaries—the same antagonists from where the cyber threats are emanating—the US and its allies found it convenient to activate cyber-sanctions as an extension of economic sanctions, to retaliate against the chronic cyberattacks and threat actors.

The Western Autonomous Cyber-Sanctions Regime: An Overview

In February 2012, as a counterterrorism measure, the administration of then US President Barak Obama designated the Iranian Ministry of Intelligence and Security for collaborating with the Hezbollah terrorist group in hacking activities.⁸ Yet, it was in January 2015 when sanctions as a tool in response to a specific cyberattack were first used, when the North Korea-sponsored threat actor Lazarus group targeted Sony Pictures Entertainment, allegedly in retaliation for the satirical movie ‘The Interview’ based on the North Korean ruler, Kim Jong-un.⁹ The hackers stole sensitive data in that breach, including confidential emails, business plans, and employee details. That hacking reportedly cost Sony some US\$ 100 million in the short term, and far more subsequently in cybersecurity measures and employee lawsuits.¹⁰

Responding to the Sony hack, the US Treasury Department sanctioned three North Korean entities and 10 individuals, including a government intelligence agency and a North Korean arms dealer.¹¹ As a follow-up, in April 2015, the US issued Executive Order 13694 creating a new sanctions regime aimed at threat actors engaged in malicious cyber activities.¹² These included targeting critical infrastructure, Distributed Denial of Service-type disruptive attacks, and activities causing a misappropriation of funds or economic resources, loss of trade secrets, and financial and personal information.¹³ Later, in December 2016, the US government added actions causing election interference to the list of malicious cyber activities after its intelligence community found evidence of actors linked to the Russian government interfering in the presidential elections.¹⁴

According to the Center for a New American Security tracker, the US Treasury Department announced 311 cyber-related sanctions from 2012 to 2021.¹⁵ Most of these sanctions focused on the US’s known adversaries: Russia (141); Iran (112); and North Korea (18). The exception was when the US sanctioned in June 2020 six Nigerian nationals who, in their private capacity, had defrauded US nationals through cybercrimes.¹⁶ Table 1 lists select significant US sanctions. Recent US sanctions have also targeted cybercriminal elements like Chatex and SUEX OTC, the virtual currency exchanges which facilitated ransomware payments.^{17,18}

The Western Autonomous Cyber-Sanctions Regime: An Overview

Table 1
Significant US Cyber-sanctions (2015-2021)

Date	Targets	Details
2 January 2015	Three North Korean agencies and ten individuals	For the first time, the US government imposed sanctions in response to a specific cyberattack. They were imposed on North Korea, and while doing so, President Obama accused Pyongyang of “destructive, coercive cyber-related actions.” ^{19,20}
29 December 2016	Nine Russian intelligence officials and entities	President Obama sanctioned nine entities and individuals that provided material support to the GRU’s (the Main Directorate of the General Staff of the Russian Armed Forces) cyber operations for interference in the 2016 hacking of the Democratic National Committee servers.
29 December 2016	Two Russian individuals	The Department of the Treasury designated two Russian individuals for using cyber-enabled means to cause misappropriation of funds and personal identifying information. One of the designated individuals was responsible for stealing over US\$ 100 million from American financial institutions, Fortune 500 firms, universities, and government agencies.
2 March 2020	Two Chinese nationals	The US sanctioned two Chinese nationals involved in laundering stolen cryptocurrency from a 2018 cyber intrusion against a cryptocurrency exchange. This cyber intrusion was linked to Lazarus Group, a North Korea-sponsored threat actor.

The Western Autonomous Cyber-Sanctions Regime: An Overview

16 June 2020	Six Nigerian nationals	The US took action against six Nigerian nationals for conducting an elaborate scheme to steal over US\$ 6 million from victims across the United States. The designated individuals targeted US businesses and individuals through deceptive global threats known as ‘business email compromise’ and ‘romance fraud’.
15 April 2021	Six Russian technology companies and 32 other entities and individuals	<p>US Treasury designated six Russian technology companies that supported the Russian intelligence services’ cyber programme, ranging from providing expertise to developing tools and infrastructure to facilitating malicious cyber activities.</p> <p>32 other entities and individuals were sanctioned for carrying out Russian government-directed attempts to influence the 2020 US presidential election and other acts of disinformation and interference.</p>

Source: Author’s own, using various open sources

Sanctions can also serve as a protective tool for the states to increase their resilience to repeated cyber sabotage by curtailing the adversaries’ access to the required technologies.²¹ This view rests on the belief that critical technologies augment the adversaries’ capability to execute cyber sabotage. Therefore, states can use sanctions to deny the adversary those very technologies. In April 2021, the US added the Russian technology sector to its cyber-sanctions regime, precisely seeking this.²²

Despite the steps mentioned above, the US government agencies have faced challenges in implementing the cyber-sanctions regime, particularly in attributing the cyberattacks to specific threat actors and establishing their linkages with foreign government agencies.

Logistical challenges notwithstanding, the US has steadfastly expanded the scope of activities included under cyber-sanctions. Following the Obama administration’s lead, the US under then President Donald Trump escalated the use of sanctions in August 2017, when it enacted the Countering America’s

The Western Autonomous Cyber-Sanctions Regime: An Overview

Adversaries Through Sanctions Act (CAATSA). This act called for, among others, the implementation of sanctions on Russia for undermining US cybersecurity.²³ Washington would later bring a new sanctions executive order, in April 2021, providing additional powers to US government agencies to target harmful cyber activities by the Russian government and its interference in elections. It also extended restrictions on US banks' dealings with Russian sovereign debt and authorised the US government to impose sanctions on Russian tech companies working with the Russian government.

Many allies have since emulated the US practice of cyber-sanctions. Across the Atlantic Ocean, the frequency of cyberattacks and hacking had forced a rethinking amongst the European countries to step up the EU's response. In June 2017, the EU ministers of foreign affairs endorsed the development of a framework for a joint EU diplomatic response to malicious cyber activities, termed the "Cyber Diplomacy Toolbox."²⁴ Its objective was to develop "signalling and reactive capacities" by the EU and its member states to influence the behaviour of potential aggressors.²⁵

Two years later, in May 2019, the EU Council adopted the "Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities," allowing the organisation to impose targeted restrictive measures to deter and respond to cyberattacks.²⁶ The Council implemented this measure for the first time in July 2020 when it imposed restrictive measures against six individuals and three entities responsible for or involved in various cyberattacks, including the WannaCry, NotPetya, and Operation Cloud Hopper attacks and the attack against the Organization for the Prohibition of Chemical Weapons.²⁷

The United Kingdom, too, after its exit from the EU in January 2020 put in place a mechanism called "The Cyber (Sanctions) (EU Exit) Regulations 2020"²⁸ that focuses on financial sanctions. As of May 2021, the UK has designated 16 individuals and six entities from North Korea, China, and Russia as targets of assets freeze.²⁹ Meanwhile, Australia inaugurated its cyber regime in December 2021, calling it a "thematic autonomous sanctions regime in relation to significant cyber incidents."³⁰ The Australian regime covers both financial sanctions and travel bans. However, its Consolidated List of all persons and entities subject to targeted financial sanctions under Australian sanctions law does not mention any Chinese national or entity for malicious cyber activities.³¹

Among the US allies, the exception is Canada. Ottawa has a comprehensive autonomous sanctions regime, except it does not cover malicious cyber activities.³² However, it has supported other like-minded partners' measures like the EU's

The Western Autonomous Cyber-Sanctions Regime: An Overview

cyber-sanctions listings.³³ Canada has also attributed specific cyberattacks to their perpetrators. For instance, in 2018, along with the US and Europe, it highlighted the role of the Chinese Ministry of State Security in the breach of several Managed Service Providers and third-party vendors.³⁴

It is relevant to note that while Russia and China have retaliated against the general sanctions imposed by the West by imposing counter-sanctions, they have not followed a similar practice in retaliation to the West's cyber-sanctions. Their response has instead been to insulate themselves from the West's coercive actions.³⁵

“Canada is the exception among US allies: it has an autonomous sanctions regime, but it does not cover malicious cyber activities.”

There are two dimensions in examining the efficacy of cyber-sanctions: their impact on the ability of bad actors to engage in malicious behaviour, and the challenges encountered in implementing these sanctions.

Empirical evidence suggests that current forms of cyber-sanctions have had little deterrent effect on the malicious behaviour of their target countries. For instance, the US sanctions on Russian intelligence officials and hacker groups have only generated additional cyberattacks on US computer networks. Likewise, repeated cyber-sanctions against North Korea have only emboldened its government to expand its targets over the years to include cryptocurrency exchanges and investment firms.³⁶

The inability of cyber-sanctions to modify the behaviour of the targeted states reflects the trend observed in the case of general sanctions. It also points to the motivations of the malicious actors who will persist in offensive cyber actions if those actions align with their national interests and geopolitical objectives. For example, North Korea has repeatedly committed cyber heists by targeting banks and other financial institutions to refill its treasury and compensate for the assets freeze implemented as part of the United Nations (UN) sanctions.³⁷ This is even more true in the case of non-state actors, who are well aware of the consequences of their actions and, therefore, would have eschewed those services and activities targeted by the sanctions. Thus, they persist in executing malicious cyber activities.

To be sure, cyber-sanctions have affected targeted countries like Russia in one crucial respect: They have adversely affected the ability of the Russian digital and technology sector to conduct business as many of their clients and business partners have been sanctioned.³⁸ This impact, coupled with the specific technology-related sanctions imposed by the West after Russia's Ukraine invasion, implies that the Russian tech companies have been losing out on commercial connections and contracts.³⁹ Businesses that are dependent on exports or foreign suppliers have particularly suffered.⁴⁰ The West's cyber-sanctions have demonstrated 'weaponised interdependence' by leveraging its lead in technology supply chains and global financial architecture for strategic advantage.⁴¹

Moreover, for the West, sanctions have also highlighted the malicious activities of bad actors, thereby casting aspersions on their credibility. Again, while this may not impact the malicious behaviour itself, sanctions have served as a valuable instrument for Western policymakers to continually highlight the cyber

The Question of Efficacy

threat stemming from its adversaries and the linkages between proxy actors like hacking groups, and state actors. In this context, sanctions have effectively exposed the Lazarus hacking group's intimate connections with the North Korean state.⁴²

Finally, to be successful, cyber-sanctions require a whole ecosystem approach, i.e., collaboration with other stakeholders such as financial institutions and other private sector elements. This is primarily for monitoring compliance and information sharing on potential sanctions regime violations. Western companies have generally adhered to both primary and secondary sanctions, despite multiple challenges like lack of clarity on sanctions rules, difficulties in payment mechanisms, and counter-sanctions from Russia and China.⁴³ However, since the Ukraine conflict began in February 2022, this has become a far more significant challenge for the companies given the severity of the latest Western sanctions, which seek to deny high-technology items and everyday industrial products to Russia.⁴⁴ On this count, therefore, both the US and EU will have to do more to on-board their businesses to ensure the latter's compliance.⁴⁵

“Cyber-sanctions have had little deterrent effect, though they do highlight the cyber threat stemming from a state's adversaries and their linkages to proxy actors.”

Effective implementation of cyber-sanctions crucially depends on the question of attribution—whether there is evidence to attribute a particular malicious cyber activity to a specific threat actor. Attribution is difficult because the malicious traffic is usually routed through multiple servers in different countries, making it difficult to determine the actual location of a computer. Moreover, identifying the location is not the same as finding out who the real perpetrator is—the computer could have been operated remotely.⁴⁶ Often, threat actors also use “The Onion Router” technology to anonymise their internet traffic.

It takes a combination of technical evidence, legal scrutiny, and political will to attribute a cyberattack to a specific perpetrator. Moreover, the evidence drawn for ascertaining attribution often relies upon classified technical capabilities. Those capabilities can become useless for future use or vulnerable to exposure once the evidence is brought into the public domain.⁴⁷ These dynamics weigh heavily when states ponder the question of attribution.⁴⁸ Leveraging these complexities, threat actors can conceal the origin of their actions. This has impacted the sanctioning country’s ability to punish the perpetrators and respond to cyberattacks.

However, the United States for instance, has developed significantly advanced technical forensic capabilities that can attribute an attack. Some experts therefore argue that the question is more of how long it will take to attribute a cyberattack, rather than if it can be done at all.⁴⁹

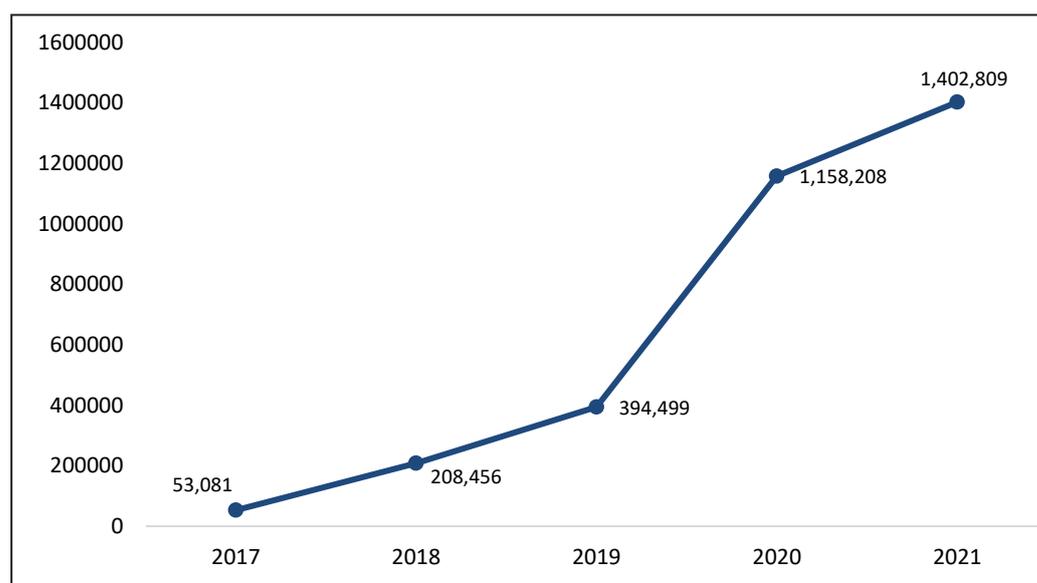
To be sure, the question of attribution still remains nettlesome for the EU, where differences in member states’ technical and intelligence capabilities have hampered the effective implementation of its cyber-sanctions regime.⁵⁰ The EU also has persistent difficulties in evolving a classified information-sharing mechanism on cybersecurity issues among the member states, given the differences in legal practices, varied threat perceptions, and other operational reasons.⁵¹ As pointed out by European cybersecurity expert Stefan Soesanto, classified intelligence sharing among the EU on malicious cyber activities occurs either by accident or by a proactive approach of an individual intelligence agency to seek relevant information.⁵²

The issue of attribution is particularly complicated when it involves allies. For example, whistle-blower Edward Snowden in 2013 revealed that the US National Security Agency (NSA) regularly spies on its European allies and their commercial entities.⁵³ In one case, NSA was found to have monitored the mobile phone of then German Chancellor Angela Merkel. In another case, it urged its German counterpart to spy on technology company Siemens for suspected contacts with the Russian secret service.⁵⁴ These examples show that even allies choose to conduct offensive cyber operations against one other, in line with their respective national security considerations. The victim state may not want to attribute the attack to an ally, particularly if that ally happens to be the United States of America.

Over the years, India's cyber-threat canvas has become complicated with the growing maleficence from China and Pakistan. Their attacks have become far more penetrating and advanced, as evident from the Chinese state-sponsored hackers' repeated breaches of the Indian power sector and Pakistan-origin malware 'ReverseRat 2.0' that targeted Indian government officials in 2021 to extract sensitive data.^{55,56} According to the Indian Computer Emergency Response Team (CERT-In), it handled 1,402,809 security incidents in 2021, as against 1,158,208 incidents in 2020 (see Figure 1).⁵⁷ Similarly, there was a 51-percent increase in ransomware incidents between 2021 and the first half of 2022.⁵⁸ This heightened cyber risk landscape threatens India's core security interests and undoes whatever achievements the country has scored in the digital domain, including the greater use of digital payments and various technological innovations.

While India has reinforced its cyber defences, the persistence of malicious cyber activities calls for greater proactiveness to build a cyber-deterrence posture.

Figure 1
Cybersecurity Incidents Handled by CERT-In



Source: Author's own, using data from CERT-In's annual reports

According to American political scientist Joseph Nye Jr., cyber-deterrence and dissuasion can be achieved through four means: the threat of punishment (retaliatory offensive actions); denial by defence (hardening cyber defences); entanglement (leveraging interdependence to avoid harms); and normative taboos (codes for responsible behaviour in cyberspace).⁵⁹ The West's cyber-sanctions typically become part of the 'threat of punishment,' whereby it has sought to punish its adversaries for malicious cyber activities and ensure accountability. In this context, given their extensive use, the question is whether the tool of cyber-sanctions holds relevance for India.

India has repeatedly called upon the UN to develop norms for responsible state behaviour in cyberspace or evolve a common understanding among the member states, including on concepts such as cyber sovereignty, deterrence, and attacks.⁶⁰ Speaking at the UN Security Council's open debate in June 2021, then Foreign Secretary Harsh Shringla, without naming Pakistan and China, highlighted that "some States are leveraging their expertise in cyberspace to achieve their political and security-related objectives and indulge in contemporary forms of cross-border terrorism."⁶¹

New Delhi has also flagged attribution and legality of cyberattacks as critical dimensions in stabilising cyberspace.⁶² Indian diplomats contend that while international law applies to cyberspace, it is inadequate to tackle the pressing issues of attribution, violation of sovereignty, and the threshold for invoking the right to self-defence.⁶³ Specifically, New Delhi has supported the 'right to self-defence' against state-sponsored cyberattacks.⁶⁴

This assertion of the 'right to self-defence' is significant as it demonstrates the Indian government's resolute approach to cybersecurity. As per the existing international legal principles, a state is only permitted to execute defensive actions in the case of an "armed attack," which means the use of force must reach a certain threshold (deaths and/or damage or destruction of property).⁶⁵ However, as has been seen repeatedly in multiple instances of cyberattacks on India, such a threshold has not been crossed yet by the cyber adversaries, i.e., these cyberattacks have so far not assumed the form of kinetic and crippling cyberattacks.⁶⁶ In such a scenario, it is unlikely that India will resort to military measures. Sanctions can therefore be explored as a potential tool under the 'right to self-defence' against cyberattacks from its adversaries.

India has never supported the West's autonomous/unilateral sanctions imposed outside the UN system, and it has been entangled in the West's sanctions regime and the impact of secondary sanctions through CAATSA. However, India has recently begun exploring its version of sanctions—restrictive trade, commercial and technological measures in the interest of national security—in the aftermath of the February 2019 Lethpora terrorist attack and border stand-off with China and the June 2020 Galwan Valley clash.

Following these incidents, India withdrew the 'Most Favoured Nation' status from Pakistan, banned Chinese apps, and instituted restrictive measures against Chinese investment in India.^{67,68,69} Additionally, New Delhi excluded Chinese telecom companies from participating in the 5G network trials in the country.⁷⁰ Cyber-sanctions can therefore be considered as a more formal variation of this coercive strategy.

“India has repeatedly called upon the UN to develop norms for responsible state behaviour in cyberspace.”

In considering cyber-sanctions as a relevant tool to tackle adversaries, New Delhi must deliberate upon certain crucial aspects (see Table 2).

Table 2
Merits and Disadvantages of Cyber-sanctions as an Official Strategy

Merits	Disadvantages
1. Deter the perpetrator of cyberattack	1. Require sophisticated technical capability to attribute cyberattacks
2. Signal a resolute approach to defending cyberspace	2. May not change adversary's behaviour
3. Name and shame the adversary/perpetrator	3. May violate international law
4. Create a favourable domestic perception about retaliatory action	4. Potential cyber, military or non-military retaliation from the adversary
5. Increase the opportunity costs for the adversary/perpetrator	5. Higher cost of compliance for concerned businesses
6. Provide an opportunity to collaborate with like-minded nations	6. Can lose effectiveness if used excessively and arbitrarily
	7. Can be difficult to roll-back

Source: Author's own

First, Indian policymakers will need to define the purpose for which they will consider using cyber-sanctions: coercion (to deter the adversary and change its behaviour); denial (to impose costs on them by curtailing their access to the Indian market or tech sector); and/or as a symbolic measure (signalling the intent, name and shame the perpetrators of cyberattacks by designating them and exposing linkages between the state and proxy actors). Defining these aims is important for the efficient use of the sanctions instrument.⁷¹ India will also need to be cognisant of the possible retaliatory measures like counter-sanctions from those sanctioned and more aggressive malicious cyber activities, and consider that autonomous cyber-sanctions may violate international law.⁷²

Policy Considerations for Utilising Cyber-Sanctions

Second, before India considers cyber-sanctions, it will need to put in place enabling domestic mechanisms like the Office of Foreign Assets Control in the US, a body within the Department of the Treasury that enforces economic and trade sanctions against the designated individuals and entities.⁷³ Creating such a body within the Indian setup will require setting a clear policy or law on sanctions and other restrictive measures and on what grounds they can be invoked.⁷⁴ Perhaps the National Cyber Security Coordinator's office located within the National Security Council Secretariat can initiate an inter-agency consultation to debate the pros and cons of formalising a sanctions policy. The much-delayed National Cyber Security Strategy can be used to discuss the larger issue of cyber-deterrence and dissuasion.⁷⁵

Third, as discussed briefly earlier, attribution is at the heart of cyber-sanctions. An examination of India's track record on this count reveals that India is averse to attributing cyberattacks to its adversaries, particularly China, save for two occasions. First, in 2010, then National Security Advisor, MK Narayanan, admitted Chinese attempts to hack into the computer network in the Prime Minister's Office.⁷⁶ Then, a decade later, in October 2020, Maharashtra's Energy Minister hinted at the possible role of Chinese malware in disrupting Mumbai's electricity supply.⁷⁷ However, enough technical, and anecdotal evidence suggests Chinese and Pakistani involvement in cyberattacks against India. Therefore, a key element of the potential cyber-sanctions strategy will require India to start outlining technical evidence to attribute cyberattacks to their perpetrators (state-sponsored or otherwise).⁷⁸ This will require working with the private sector cybersecurity community, which has begun to present such technical evidence. More importantly, India will need to consider the costs of such attribution, as it has live border disputes with China and Pakistan.

To mitigate such costs, it may be expedient to work with like-minded countries that can be partners in bringing accountability. These need not just include Quad members (Australia, Japan and the United States) and the European partners but also other countries that have fallen victim to China's cyber maleficence such as Vietnam, Singapore, and Taiwan. India can coordinate positions with them on attribution and other related aspects.

Finally, as seen in the experience of other countries, cyber-sanctions cannot work independently and rather must be part of a broader strategy to tackle and counter malicious cyber activities. India is now hardening its cyber defences and undertaking offensive cyber operations.⁷⁹ While there are capacity and technical challenges in executing these measures, they must be combined to shape a cyber-deterrence strategy for India, learning from the experience of other cyber powers while remaining anchored in the country's understanding of tackling cyber threats.⁸⁰ More importantly, as seen in the case of the West, relying too heavily on sanctions can diminish their efficacy. Therefore, the use of cyber-sanctions must be deliberate and selective.

Conclusion

The recent sanctions on Russia for its invasion of Ukraine indicate that the United States and its allies intend to ensure that its adversaries pay a cost for committing adversarial actions against them. Sanctions will play a critical role in tackling malicious cyber activities and will increasingly form part of a bouquet of coercive measures like technology export control regimes and trade restrictions.

The polarisation among the great powers and the lack of progress on global cyber cooperation connotes that affected states will resort to punitive measures such as cyber-sanctions to protect their cyberspace and national security. India will need to pay attention to these emerging trends to design its own cyber posture. 

Sameer Patil is a Senior Fellow at ORF's Strategic Studies Programme and has previously served in the National Security Council Secretariat.

The author thanks Trisha Ray, Ambika Khanna, Kartik Bommakanti, Arindrajit Basu, and Virpratap Vikram Singh for their comments on an earlier draft of this paper.

- 1 Center for Strategic & International Studies, “Significant Cyber Incidents,” <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>.
- 2 María Vásquez Callo-Müller and Iryna Bogdanova, “What Is the Role of Unilateral Cyber Sanctions in the Context of the Global Cybersecurity Law-Making?,” *Völkerrechtsblog*, May 10, 2022, <https://voelkerrechtsblog.org/what-is-the-role-of-unilateral-cyber-sanctions-in-the-context-of-the-global-cybersecurity-law-making/>.
- 3 Lesley Wroughton and Megha Rajagopalan, “Internet outage seen in North Korea amid U.S. hacking dispute,” *Reuters*, December 23, 2014, <https://www.reuters.com/article/us-sony-cybersecurity-northkorea-idUSKBN0K01WA20141222>.
- 4 TOI Staff, “Israel behind cyberattack that caused ‘total disarray’ at Iran port – report,” *The Times of Israel*, May 19, 2020, <https://www.timesofisrael.com/israel-said-behind-cyberattack-that-caused-total-disarray-at-iran-port-report/>.
- 5 Sameer Patil, *Securing India in the Cyber Era* (London and New York: Routledge, 2021), pp. 8.
- 6 Terri Moon Cronk, “Iraq Progresses in ISIL Fight, Key Extremist Confirmed Dead,” *DoD News*, August 28, 2015, <https://www.defense.gov/Explore/News/Article/Article/615305/iraq-progresses-in-isil-fight-key-extremist-confirmed-dead/>.
- 7 Israel Defense Forces (@IDF), “CLEARED FOR RELEASE: 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. HamasCyberHQ.exe has been removed,” Twitter Tweet, May 5, 2019, <https://twitter.com/IDF/status/1125066395010699264>.
- 8 US Department of the Treasury, “Treasury Designates Iranian Ministry of Intelligence and Security for Human Rights Abuses and Support for Terrorism,” February 16, 2012, <https://home.treasury.gov/news/press-releases/tg1424>.
- 9 Andrea Peterson, “The Sony Pictures hack, explained,” *The Washington Post*, December 18, 2014, <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/>.
- 10 Lisa Richwine, “Cyber attack could cost Sony studio as much as \$100 million,” *Reuters*, December 10, 2014, <https://www.reuters.com/article/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209>.
- 11 US Department of the Treasury, “Treasury Imposes Sanctions Against the Government of The Democratic People’s Republic Of Korea,” January 2, 2015, <https://home.treasury.gov/news/press-releases/jl9733>.
- 12 US Department of the State, “Cyber Sanctions,” <https://www.state.gov/cyber-sanctions/>.

- 13 The White House, “Executive Order – “Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities”,” April 1, 2015, <https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m>.
- 14 The White House, “FACT SHEET: Actions in Response to Russian Malicious Cyber Activity and Harassment,” December 29, 2016, <https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and>.
- 15 Jason Bartlett and Megan Ophel, “Sanctions by the Numbers: Spotlight on Cyber Sanctions”, *Center for a New American Security*, May 4, 2021, <https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber>.
- 16 US Department of the Treasury, “Treasury Sanctions Nigerian Cyber Actors for Targeting U.S. Businesses and Individuals”, June 16, 2020, <https://home.treasury.gov/news/press-releases/sm1034>.
- 17 US Department of the Treasury, “Publication of Updated Ransomware Advisory; Cyber-related Designation”, September 21, 2021, <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210921>.
- 18 US Department of the Treasury, “Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange”, November 8, 2021, <https://home.treasury.gov/news/press-releases/jy0471>.
- 19 Scott Neuman, “Obama Authorizes New Sanctions On North Korea Over Sony Hack,” *NPR*, January 2, 2015, <https://www.npr.org/sections/thetwo-way/2015/01/02/374598365/obama-authorizes-sanctions-on-n-korea-over-sony-hack>.
- 20 The White House, “Executive Order – “Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities”.
- 21 Arindrajit Basu, Google Meet interview, May 16, 2020.
- 22 US Department of State, “Holding Russia To Account,” April 15, 2021, <https://www.state.gov/holding-russia-to-account/>.
- 23 US Department of the Treasury, “Countering America’s Adversaries Through Sanctions Act,” January 3, 2017, https://home.treasury.gov/system/files/126/hr3364_pl1115-44.pdf.
- 24 Council of the European Union, “Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (“Cyber Diplomacy Toolbox”)- Adoption,” June 7, 2017, <https://ccdcoe.org/uploads/2018/11/EU-170607-CyberDiplomacyToolbox-1.pdf>.

- 25 Erica Moret and Patryk Pawlak, “The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?,” *European Union Institute for Security Studies*, 2017, <https://www.jstor.org/stable/pdf/resrep06815.pdf>.
- 26 Council of the European Union, “Cyber-attacks: Council is now able to impose sanctions,” May 17, 2019, <https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/>.
- 27 Council of the European Union, “Amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,” July 30, 2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN>.
- 28 “The Cyber (Sanctions) (EU Exit) Regulations 2020,” *Legislation.gov.uk*, June 17, 2020, <https://www.legislation.gov.uk/uksi/2020/597>.
- 29 Office of Financial Sanctions Implementation, HM Treasury, “Consolidated List of Financial Sanctions Targets in the UK,” May 27, 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1079301/Cyber.pdf.
- 30 Department of Foreign Affairs and Trade, Australian Government, “Significant cyber incidents sanctions regime,” <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/significant-cyber-incident-sanctions-regime>.
- 31 Department of Foreign Affairs and Trade, Australian Government, “Consolidated List,” https://www.dfat.gov.au/sites/default/files/regulation8_consolidated.xls.
- 32 Government of Canada, “Current sanctions imposed by Canada,” March 19, 2021, https://www.international.gc.ca/world-monde/international_relations_relations_internationales/sanctions/current-actuelles.aspx?lang=eng.
- 33 Global Affairs Canada, “Canada welcomes European Union’s announcement of new cyber sanctions listings,” July 30, 2020, <https://www.canada.ca/en/global-affairs/news/2020/07/canada-welcomes-european-unions-announcement-of-new-cyber-sanctions-listings.html>.
- 34 Communications Security Establishment, “Canada and Allies Identify China as Responsible for Cyber-Compromise,” December 12, 2018, <https://cse-cst.gc.ca/en/information-and-resources/announcements/canada-and-allies-identify-china-responsible-cyber>.
- 35 Caitríona Heintz “Debating the Tech Sanctions on Russia: Is ‘Splinternet’ Upon Us?,” *Observer Research Foundation*, April 26, 2022, <https://www.orfonline.org/expert-speak/debating-the-tech-sanctions-on-russia/>.
- 36 United Nations Security Council, “Letter dated 25 February 2022 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council,” March 1, 2022, <https://>

- www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/N2225209.pdf.
- 37 Bruce Klingner, “North Korean Cyberattacks: A Dangerous and Evolving Threat,” *The Heritage Foundation*, September 2, 2021, <https://www.heritage.org/asia/report/north-korean-cyberattacks-dangerous-and-evolving-threat>.
- 38 Ivan Timofeev, Zoom interview, May 20, 2022.
- 39 Arjun Gargeyas, “The effect of tech sanctions on the Russian economy,” *Hindustan Times*, March 16, 2022, <https://www.hindustantimes.com/opinion/the-effect-of-tech-sanctions-on-the-russian-economy-101647423272681.html>.
- 40 Ivan Timofeev, “Sanctions Against Russia: A Look into 2021,” *Russian International Affairs Council*, Report 65/2021, March 11, 2021, <https://russiancouncil.ru/papers/Sanctions2021-Report65-En.pdf>.
- 41 Farrell and Newman, “Weaponized Interdependence: How Global Economic Networks Shape State Coercion”, *International Security* 44, No. 1 (2019), https://doi.org/10.1162/isec_a_00351.
- 42 US Department of the Treasury, “Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups,” September 3, 2019, <https://home.treasury.gov/news/press-releases/sm774>.
- 43 Bruce Love, “Companies caught in EU-US sanctions crossfire”, *Financial Times*, January 30, 2020, <https://www.ft.com/content/97a75318-16a8-11ea-b869-0971bffa109>.
- 44 Ivan Timofeev, Zoom interview, May 20, 2022.
- 45 Christopher Burgess, “Internet sanctions against Russia pose risks, challenges for businesses,” *CSO*, March 22, 2022, <https://www.csoonline.com/article/3654157/internet-sanctions-against-russia-pose-risks-challenges-for-businesses.html>.
- 46 P. W. Singer, and Allan Friedman, *Cybersecurity and Cyberwar: What everyone needs to know* (New York: Oxford University Press, 2014), pp. 72.
- 47 Joseph S. Nye Jr, “Deterrence and Dissuasion in Cyberspace,” *International Security* 41 (2016/17) no. 3: 51.
- 48 Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks”, *The Journal of Strategic Studies* 38 (2014), no. 1-2: 4–37.
- 49 Manuel Fischer, “The Concept of Deterrence and Its Applicability in the Cyber Domain,” *Connections* 18 (2019), no. 1/2: 69-92.
- 50 Annegret Bendiek and Matthias Schulze, “Attribution: A Major Challenge for EU Cyber Sanctions,” *Stiftung Wissenschaft und Politik* Paper 11, December 2021,

- <https://www.swp-berlin.org/en/publication/attribution-a-major-challenge-for-eu-cyber-sanctions>.
- 51 Stefan Soesanto, “After a Year of Silence, Are EU Cyber Sanctions Dead?,” *Lawfare*, October 26, 2021, <https://www.lawfareblog.com/after-year-silence-are-eu-cyber-sanctions-dead>.
- 52 Soesanto, “After a Year of Silence, Are EU Cyber Sanctions Dead?”
- 53 Spiegel Staff, “Intelligence Scandal Puts Merkel in Tight Place,” *Spiegel International*, May 4, 2015, <https://www.spiegel.de/international/germany/bnd-intelligence-scandal-puts-merkel-in-tight-place-a-1031944.html>.
- 54 Spiegel Staff, “Intelligence Scandal Puts Merkel in Tight Place,” *Spiegel International*, May 4, 2015, <https://www.spiegel.de/international/germany/bnd-intelligence-scandal-puts-merkel-in-tight-place-a-1031944.html>.
- 55 Insikt Group, “Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group,” Recorded Future Blog, posted April 6, 2022, <https://www.recordedfuture.com/continued-targeting-of-indian-power-grid-assets/>.
- 56 Black Lotus Labs, “ReverseRat Reemerges With A (Night)Fury New Campaign And New Developments, Same Familiar Side-Actor,” Lumen Blog, posted August 11, 2021, <https://blog.lumen.com/reverserat-reemerges-with-a-nightfury-new-campaign-and-new-developments-same-familiar-side-actor/>.
- 57 CERT-In Annual Reports of 2021 and 2022, <https://www.cert-in.org.in/>.
- 58 CERT-In, “India Ransomware Report for H1-2022,” <https://www.cert-in.org.in/>.
- 59 Nye Jr., “Deterrence and Dissuasion in Cyberspace,”: 54—62.
- 60 Ministry of External Affairs, Government of India, “Statement at the Organisational Session of the Open-Ended Working Group (OEW) on Developments in the Field of Information and Telecommunications in the Context of International Security,” June 3, 2019, <http://meaindia.nic.in/cdgeneva/?8251?000>.
- 61 Ministry of External Affairs, Government of India, “Foreign Secretary’s Statement at the UN Security Council Open Debate on “Maintenance of International Peace and Security: Cyber Security,” June 29, 2021, https://www.mea.gov.in/Speeches-Statements.htm?dtl/33963/Foreign_Secretarys_Statement_at_the_UN_Security_Council_Open_Debate_on_Maintenance_of_International_Peace_and_Security_Cyber_Security_June_29_2021.
- 62 Patil, *Securing India in the Cyber Era*, pp. 68.
- 63 Patil, *Securing India in the Cyber Era*, pp. 68.

- 64 Hannes Ebert, “Hacked IT superpower: how India secures its cyberspace as a rising digital democracy,” *India Review* 19, no. 4 (2020): 376-413.
- 65 Manuel Fischer, “The Concept of Deterrence and Its Applicability in the Cyber Domain,”: 85.
- 66 Kartik Bommakanti, “India and cyberspace: Balance between offence and defence,” *Observer Research Foundation*, June 18, 2021, <https://www.orfonline.org/expert-speak/india-and-cyberspace-balance-between-offence-and-defence/>.
- 67 Press Information Bureau, Government of India, “Suspension of LoC Trade between J&K and PoJK,” April 18, 2019, <https://pib.gov.in/PressReleaseDetail.aspx?PRID=1570898>.
- 68 Press Information Bureau, Government of India, “Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order,” June 29, 2020, <https://pib.gov.in/PressReleaseDetailm.aspx?PRID=1635206>.
- 69 Press Information Bureau, Government of India, “Investment from Land Border Sharing Countries,” March 23, 2022, <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1808806>.
- 70 Anushree Fadnavis, “India doesn’t name Huawei among participants in 5G trials,” *Reuters*, May 4, 2021, <https://www.reuters.com/technology/india-doesnt-name-huawei-among-participants-5g-trials-2021-05-04/>.
- 71 Moret and Pawlak, “The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?”
- 72 <http://opiniojuris.org/2022/01/24/unilateral-cyber-sanctions-and-global-cybersecurity-law-making/>
- 73 US Department of the Treasury, “Office of Foreign Assets Control - Sanctions Programs and Information,” <https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information>.
- 74 Ambika Khanna, Google Meet interview, May 11, 2022.
- 75 PTI, “Government to unveil national cyber security strategy soon: National Cyber Security Coordinator,” *The Hindu*, July 3, 2021, <https://www.thehindu.com/business/government-to-unveil-national-cyber-security-strategy-soon-national-cyber-security-coordinator/article35119538.ece>.
- 76 Express News Service, “Chinese hacked PMO computers, says Narayanan,” *The Indian Express*, January 19, 2010, <https://indianexpress.com/article/news-archive/web/chinese-hacked-pmo-computers-says-narayanan/>.

- 77 “Sabotage suspected in Mumbai power outage: Nitin Raut, Energy minister”, *The Economic Times*, October 14, 2020, <https://economictimes.indiatimes.com/news/politics-and-nation/sabotage-suspected-in-mumbai-power-outage-nitin-raut-energy-minister/articleshow/78656392.cms>.
- 78 Sameer Patil and Kishika Mahajan, “Expanding Chinese cyber-espionage threat against India,” *Observer Research Foundation*, April 18, 2022, <https://www.orfonline.org/expert-speak/expanding-chinese-cyber-espionage-threat-against-india/>.
- 79 Gunjan Chawla, “Does India have offensive cyber capabilities?,” *The CCG Blog*, July 10, 2020, <https://ccgnludelhi.wordpress.com/2020/07/10/does-india-have-offensive-cyber-capabilities/>.
- 80 Deependra Singh Hooda, “Towards a Cyber Deterrence Strategy for India,” *Delhi Policy Group*, Policy Brief VI, no. 19 (July 2021), <https://www.delhipolicygroup.org/publication/policy-briefs/towards-a-cyber-deterrence-strategy-for-india.html>.

Images used in this paper are from Getty Images/Busà Photography.



Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. Fax : +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org